

Verwenden und Verwalten von VMware NSX Intelligence

Aktualisiert am 17. Mai 2022
VMware NSX Intelligence 3.2



Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

<https://docs.vmware.com/de/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2021–2022 VMware, Inc. Alle Rechte vorbehalten. Urheberrechts- und Markenhinweise.

Inhalt

Verwenden und Verwalten von VMware NSX Intelligence	6
1 Erste Schritte mit NSX Intelligence	7
Tour der NSX Intelligence-Startseite	8
Kennenlernen von NSX Intelligence-Grafikelementen	11
2 Grundlegendes zu NSX Intelligence-Ansichten und -Flows	14
Arbeiten mit der Ansicht „Gruppen“	15
Arbeiten mit der Ansicht „Berechnungen“	21
Arbeiten mit Datenverkehrsflows	27
3 Arbeiten mit NSX Intelligence-Empfehlungen	31
Verstehen von NSX Intelligence-Empfehlungen	31
Grundlegendes zur Generierung von NSX Intelligence-Empfehlungen	32
Generieren einer neuen NSX Intelligence-Empfehlung	34
NSX Intelligence-Empfehlungen erneut ausführen	40
Erstellte NSX Intelligence-Empfehlungen überprüfen und veröffentlichen	42
NSX Intelligence-Empfehlung als JSON-Datei exportieren	47
4 Erkennen von verdächtigem Netzwerksdatenverkehr in NSX-T Data Center	49
Erste Schritte beim Erkennen von verdächtigem Netzwerksdatenverkehr in NSX-T Data Center	49
Voraussetzungen zur Verwendung der NSX Suspicious Traffic-Funktion	49
Systemanforderungen für die NSX Suspicious Traffic-Funktion	50
Übersicht über die Funktion NSX Suspicious Traffic	51
Mit der NSX Suspicious Traffic-Funktion verwendete Terminologie	53
NSX Suspicious Traffic-Detektoren aktivieren	54
Analysieren der NSX Suspicious Traffic-Erkennungsereignisse	56
Verwalten der NSX Suspicious Traffic Detector-Definitionen	59
5 Arbeiten mit der NSX Network Detection and Response-Anwendung	62
Voraussetzungen zur Verwendung der NSX Network Detection and Response-Anwendung	62
Mit der NSX Network Detection and Response-Funktion verwendete Terminologie	63
Kennenlernen der NSX Network Detection and Response-Benutzeroberfläche	64
Erkunden der Dashboard-Seite	68
Aktive Aktivitäten in meinem Netzwerk	68
Netzwerk- und Sicherheitsübersicht	68
Erkannte Bedrohungen	69

Globale Ereigniszuordnung	71
Neue eindeutige Erkennungen	71
Liste heruntergeladener Dateien	72
Verwalten der Seite „Aktivitäten“	73
Arbeiten mit Aktionskarten	74
Informationen zum Widget „Untersuchen“	76
Grundlegendes zur Seite „Aktivitätsdetails“	76
Details zur Aktivität: Registerkarte „Übersicht“	77
Details zur Aktivität: Registerkarte „Hosts“	84
Details zur Aktivität: Registerkarte „Zeitachse“	84
Details zur Aktivität: Registerkarte „Verlauf“	85
Details zur Aktivität: Registerkarte „Nachweis“	86
Eigenschaften der Aktivität	87
Arbeiten mit der Seite „Hosts“	96
Filtern von Verknüpfungen	97
Verwenden von Filtern auf der Seite „Host“	97
Hostliste	99
Seite „Hostprofil“	101
Hostprofil: Registerkarte „Übersicht“	101
Hostprofil: Registerkarte „Bedrohungen“	102
Hostprofil: Registerkarte „Ereignisse“	108
Hostprofil: Registerkarte „Dateidownloads“	109
Arbeiten mit der Seite „Ereignisse“	110
Globale Ereigniszuordnung	110
Erkannte Bedrohungen auf der Seite „Ereignisse“	111
Verwenden von Filtern auf der Seite „Ereignisse“	112
Erkennungsereignisse	114
Seitenleiste „Ereignisübersicht“	115
WHOIS-Popup-Fenster	117
Popup-Fenster der Detektor-Dokumentation	118
Seite „Ereignisprofil“	119
Verwalten der Seite „Vorfälle“	122
Infektionen im Zeitverlauf	124
Erkannte Bedrohungen	124
Verwenden von Filtern auf der Seite „Vorfälle“	126
Vorfallsliste	128
Arbeiten mit der Seite „Heruntergeladene Dateien“	132
Registerkarte „Eindeutig“	133
Heruntergeladene Dateien im zeitlichen Verlauf	133
Verwenden von Filtern auf der Seite „Heruntergeladene Dateien“	134
Eindeutige Liste heruntergeladener Dateien	135

Details zu heruntergeladenen Dateien	136
Registerkarte „Alle“	141
Verwenden der Seite „Warnungsmanagement“	143
Arbeiten mit der Sidebar „Warnung verwalten“	145
Syntax für Warnungsregeln	148
Verwenden des Analyseberichts	153
Analysebericht: Registerkarte „Übersicht“	153
Analysebericht: Registerkarte „Bericht“	157
Widget „Analysebeziehungen“	158
Analysedateibericht	159
Analysedateiaktivitäten	159
Analysedateiartefakte	160
Analyse-URL-Bericht	161
6 NSX Intelligence-Vorgänge und -Verwaltung	164
Rollenbasierte Zugriffssteuerung in NSX Intelligence	164
Erfassen von NSX Intelligence-Support-Paketen	166
Suche nach NSX Intelligence-Einheiten	168
Suchen von NSX Intelligence-Einheiten	169
Verwalten der NSX Intelligence-Einstellungen	171
Verwalten der privaten IP-Bereiche für NSX Intelligence	172
7 Beheben von Problemen bei der Verwendung von NSX Intelligence	174
Überprüfen des Status der NSX Intelligence-Funktion	174
Vorhandensein herabgestufter Dienste nach einer erfolgreichen Aktivierung von NSX Intelligence	175
Inkonsistenzen bei der inkrementellen Topologieberichterstellung	176
Informationen zum FTP-Flow werden nach dem Anhalten der FTP-Sitzung weiterhin angezeigt.	
177	
Ansicht "Gruppen" wird nicht mit Datenverkehrsflow-Daten aktualisiert	178

Verwenden und Verwalten von VMware NSX Intelligence

Das *Verwenden und Verwalten von VMware NSX Intelligence*-Dokument enthält Informationen zur Verwendung und Verwaltung der VMware NSX® Intelligence™-Funktion.

Zielgruppe

Diese Informationen sind für alle Benutzer bestimmt, die über die Berechtigung zur Verwendung und Verwaltung der NSX Intelligence-Funktion verfügen. Die Informationen sind für erfahrene Systemadministratoren vorgesehen, die mit der Virtualisierungstechnologie und den Vorgängen zur Netzwerksicherheit vertraut sind.

Verwandte Dokumentation

- VMware NSX-T Data Center™-Dokumentation für Version 3.2 oder höher unter <https://docs.vmware.com/de/VMware-NSX-T-Data-Center/index.html>.
Sie verwenden die NSX Manager-Benutzeroberfläche, um die VMware NSX® Intelligence™-Funktion zu aktivieren und darauf zuzugreifen.
- *Bereitstellung und Verwaltung von VMware NSX Application Platform*-Dokumentation, enthalten in der Dokumentation für NSX-T Data Center Version 3.2 oder höher unter <https://docs.vmware.com/de/VMware-NSX-T-Data-Center/index.html>.
Sie müssen zuerst die VMware NSX® Application Platform bereitstellen, bevor Sie die NSX Intelligence-Funktion aktivieren können.
- *Aktivieren und Aktualisieren von VMware NSX Intelligence*-Dokument für Version 3.2 oder höher für Informationen zum Aktivieren und Aktualisieren der NSX Intelligence-Funktion.
Dieses Dokument wird mit der unter <https://docs.vmware.com/de/VMware-NSX-Intelligence/index.html> festgelegten NSX Intelligence-Dokumentation bereitgestellt.
- *Handbuch zur Aktivierung und Verwaltung von VMware NSX Network Detection and Response* mit Informationen zum Aktivieren und Verwalten der VMware NSX® Network Detection and Response™-Funktion.
Dieses Dokument wird mit der unter <https://docs.vmware.com/de/VMware-NSX-Intelligence/index.html> festgelegten NSX Intelligence-Dokumentation bereitgestellt.

Erste Schritte mit NSX Intelligence

1

Um mit der Verwendung der VMware NSX® Intelligence™-Funktion zu beginnen, müssen Sie sie aktivieren und sich dann mit der NSX Intelligence-Benutzeroberfläche vertraut machen.

Übersicht

Ab Version 3.2 ist NSX Intelligence nicht mehr nur eine VM-basierte Appliance, sondern eine moderne Anwendung, die auf der VMware NSX® Application Platform gehostet wird, einer Plattform, die auf einer Mikrodienste-Architektur basiert.

Die NSX Intelligence-Funktion bietet eine Visualisierung der Sicherheitsposition Ihrer lokalen VMware NSX-T Data Center™-Umgebung. Die Visualisierung verwendet die Netzwerdatenverkehrsflows, die innerhalb des von Ihnen angegebenen Zeitraums aggregiert werden.

Die NSX Intelligence-Funktion unterstützt Sie auch bei der Planung der Mikrosegmentierung, indem sie Empfehlungen für Firewallregeln ausspricht, die die Analyse des Netzwerdatenverkehrs und die Durchsetzung von Sicherheitsrichtlinien nutzen.

Darüber hinaus stehen Ihnen die NSX Suspicious Traffic-Funktion und die VMware NSX® Network Detection and Response™-Funktion ab Version NSX Intelligence 3.2 zur Verfügung. Diese beiden Funktionen verwenden Netzwerdatenverkehrsanalysen, um verdächtige Netzwerdatenverkehrsaktivitäten zu erkennen, die in Ihrer Umgebung mit NSX-T Data Center 3.2 oder höher auftreten. Sie müssen über eine gültige Lizenz verfügen, die NSX Firewall mit Advanced Threat Prevention Edition entspricht, um diese Funktionen nutzen zu können.

Voraussetzungen

Bevor Sie die verfügbaren NSX Intelligence-Funktionen verwenden können, müssen Sie die NSX Intelligence-Funktion auf dem NSX Application Platform aktivieren. Sie müssen auch konfigurieren, von welchen Hosts oder Hostclustern die NSX Intelligence-Funktion die Netzwerdatenverkehrsdaten erfassen soll. Standardmäßig erfasst die NSX Intelligence-Funktion Netzwerdatenverkehrsdaten von allen bekannten Hosts und Hostclustern in Ihrer NSX-T Data Center-Umgebung. Weitere Informationen hierzu finden Sie unter *Aktivieren und Aktualisieren von VMware NSX Intelligence*.

Starten der Verwendung der NSX Intelligence-Funktion

Nach dem Aktivieren und Konfigurieren der NSX Intelligence-Funktion sind die Visualisierungs-, Empfehlungs- und verdächtigen Datenverkehrsfunktionen auf der Benutzeroberfläche NSX Manager verfügbar.

- Um die visualisierten NSX-T-Einheiten und -Datenverkehrsflows anzuzeigen, die zwischen ihnen aufgetreten sind, klicken Sie auf **Planen und Fehler beheben > Entdecken und Ergreifen von Aktionen**. Siehe [Kapitel 2 Grundlegendes zu NSX Intelligence-Ansichten und -Flows](#).
- Verwenden Sie **Planen und Fehler beheben > Empfehlungen**, um Empfehlungen für Regeln für verteilte Firewalls für die Planung der Mikrosegmentierung zu erhalten. Siehe [Kapitel 3 Arbeiten mit NSX Intelligence-Empfehlungen](#).
- Um die NSX Suspicious Traffic-Funktion zum Erkennen verdächtiger Datenverkehrsereignisse zu verwenden, klicken Sie auf **Sicherheit > Verdächtiger Datenverkehr**. Wenn die NSX Network Detection and Response-Funktion aktiviert ist, werden erkannte verdächtige Ereignisse markiert und an den VMware NSX® Advanced Threat Prevention-Cloud-Dienst gesendet. Wenn festgestellt wird, dass Erkennungsereignisse verwandt sind, werden sie in einer Aktivität korreliert, die Sie mithilfe der NSX Network Detection and Response-Benutzeroberfläche weiter untersuchen können. Einzelheiten dazu finden Sie unter [Kapitel 4 Erkennen von verdächtigem Netzwerksverkehr in NSX-T Data Center](#).

Dieses Kapitel enthält die folgenden Themen:

- [Tour der NSX Intelligence-Startseite](#)
- [Kennenlernen von NSX Intelligence-Grafikelementen](#)

Tour der NSX Intelligence-Startseite

Sie greifen auf die NSX Intelligence-Startseite zu, indem Sie auf der NSX Manager-Benutzeroberfläche auf **Planen und Fehler beheben > Entdecken und Ergreifen von Aktionen** klicken.

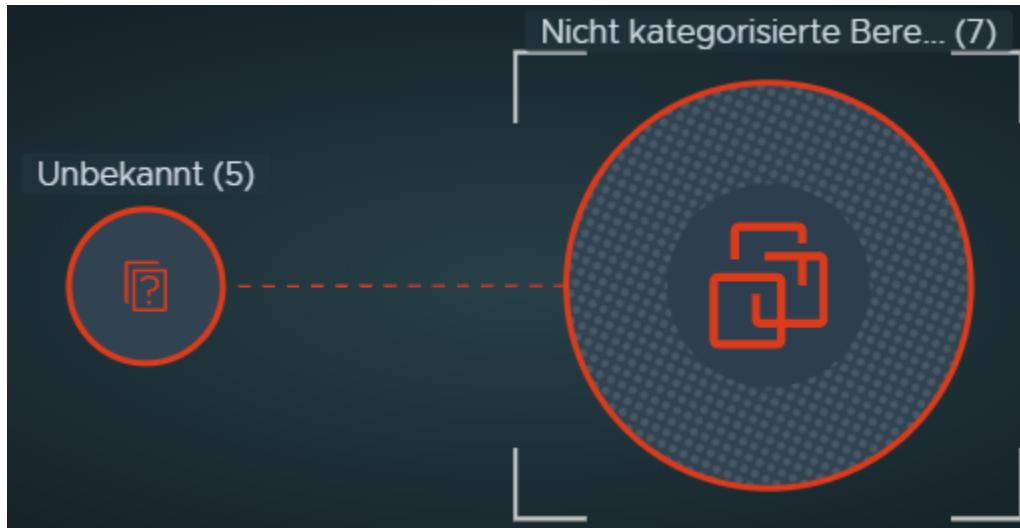
Wenn Sie nach der erstmaligen Aktivierung und Konfiguration der NSX Intelligence-Funktion auf **Planen und Fehler beheben > Entdecken und Ergreifen von Aktionen** klicken, beginnt NSX Intelligence mit dem Rendern einiger Visualisierungen, nachdem einige Daten zum Netzwerksverkehr von den Transportknoten und die Bestandsinformationen von NSX Manager empfangen wurden.

Standardmäßig wird die Visualisierung der Sicherheitsposition aller in Ihrem lokalen NSX-T Data Center-Bestand definierten Gruppen angezeigt, wenn Sie auf **Entdecken und Ergreifen von Aktionen** klicken.

- Wenn noch keine Gruppen definiert sind, werden keine Gruppen angezeigt.
- Für Gruppen gab es in der letzten Stunde möglicherweise zulässige, blockierte und ungeschützte Datenverkehrsflows zwischen den zugehörigen Computing-Mitgliedseinheiten.

- Wenn VMs oder physische Server vorhanden sind, die jedoch keiner Gruppe angehören, wird das Symbol für die Gruppe „Nicht kategorisierte Berechnungen“ angezeigt.
- Wenn IP-Adressen vorhanden sind, die zu keiner Gruppe gehören, wird das Symbol „Unbekannt“ angezeigt.

Die beiden Symbole für die Gruppen „Unbekannt“ und „Nicht kategorisierte Berechnungen“ werden im folgenden Bild dargestellt.



Wenn Sie bereits Gruppen definiert und Daten zum Netzwerksdatenverkehr erfasst haben, kann eine Visualisierung ähnlich dem folgenden Screenshot angezeigt werden. In der folgenden Tabelle sind die nummerierten Abschnitte im Screenshot beschrieben.

Abschnitt	Beschreibung
1	<p>Der Auswahlbereich für die Sicherheitsansicht ist der Ort, an dem Sie den Typ der anzuzeigenden Sicherheitsvisualisierung auswählen. Es stehen zwei Typen von Sicherheitsansichten zur Verfügung: Gruppen und Berechnungen. Wenn Sie auf Entdecken und Ergreifen von Aktionen klicken, wird für die Standard-Sicherheitsansicht die Ansicht „Gruppen“ aller Gruppenobjekten in Ihrer NSX-T Data Center-Umgebung angezeigt.</p> <ul style="list-style-type: none"> ■ Wenn Sie bestimmte Gruppen in der Ansicht „Gruppen“ auswählen möchten, klicken Sie auf den Pfeil nach unten neben ALLE, treffen Sie im Dropdown-Menü der verfügbaren Gruppen eine Auswahl und klicken Sie auf Anwenden. ■ Um die Ansicht „Berechnungen“ auszuwählen, klicken Sie neben Gruppen auf den Pfeil nach unten und wählen Sie Berechnungen aus und klicken Sie auf Anwenden. Alle VMs, IP-Adressen und physischen Server, die in ihrer NSX-T Data Center-Umgebung vorhanden sind, werden visualisiert. ■ Um bestimmte VMs, IP-Adressen oder physische Server auszuwählen, die in die Ansicht „Berechnungen“ aufgenommen werden sollen, klicken Sie neben ALLE auf den Pfeil nach unten, klicken Sie auf Alle Typen anzeigen und wählen Sie einen Berechnungstyp (VMs, IPs oder Physische Server) aus dem Dropdown-Menü aus. Alternativ können Sie im Dropdown-Menü bestimmte Berechnungselemente auswählen oder deaktivieren und auf Anwenden klicken. ■ Wenn Sie Ihre gewählten Einstellungen in den Ansichtstypen löschen möchten, klicken Sie oben rechts auf der Visualisierungsseite auf LÖSCHEN und bestätigen Sie den Vorgang, indem Sie im Dialogfeld „Alle Filter löschen“ auf LÖSCHEN klicken. Wenn Sie in der Ansicht „Berechnungen“ auf LÖSCHEN klicken, werden die Auswahlfilter gelöscht und die Ansicht „Gruppen“ wird angezeigt. <p>Weitere Informationen zum Arbeiten mit den beiden Ansichtstypen finden Sie unter Arbeiten mit der Ansicht „Gruppen“ und Arbeiten mit der Ansicht „Berechnungen“.</p>
2	Im Bereich Filter anwenden können Sie die für die aktuelle Visualisierung zu verwendenden Kriterien präzisieren. Klicken Sie auf Filter anwenden , wählen Sie ein Filterkriterium aus und klicken Sie auf Anwenden . Sie können mehrere Filter angeben, indem Sie erneut auf Filter anwenden klicken.
3	<p>Im Abschnitt Flows können Sie den Typ des Datenverkehrsflows auswählen, der im ausgewählten Zeitraum in die Visualisierung einbezogen werden soll. Die Farben, die in der Visualisierung für die Flow-Typen verwendet werden, werden in diesem Abschnitt ebenfalls gezeigt.</p> <ul style="list-style-type: none"> ■ Rot gefärbte gestrichelte Linie für ungeschützte Flows ■ Blau gefärbte durchgehende Linie für blockierte Flows ■ Grün gefärbte durchgehende Linie für die zulässigen Flows <p>Standardmäßig werden alle Datenverkehrsflow-Typen für die aktuelle NSX Intelligence-Visualisierung ausgewählt. Weitere Informationen hierzu finden Sie unter Arbeiten mit Datenverkehrsflows.</p>
4	Der Bereich Aktualisierungsstatus enthält Informationen zu dem Zeitpunkt, zu dem das Visualisierungsdiagramm zuletzt aktualisiert wurde. Wenn Sie eine Aktualisierung der aktuellen Ansicht durchführen möchten, klicken Sie auf das Aktualisierungssymbol.
5	<p>Wenn Sie auf das Zahnradsymbol klicken, werden Links zu den folgenden Einstellungsseiten im Dialogfeld Einstellungen für NSX Intelligence bereitgestellt.</p> <ul style="list-style-type: none"> ■ Einstellungen speziell für die NSX Intelligence-Funktion in den Systemeinstellungen > NSX Intelligence. Weitere Informationen hierzu finden Sie unter Verwalten der NSX Intelligence-Einstellungen. ■ Datenschutzeinstellungen in der Allgemeine Sicherheitseinstellungen > Datenschutz. ■ Private IP-Bereiche im Allgemeine Sicherheitseinstellungen > Private IP-Bereiche. Weitere Informationen finden Sie unter Verwalten der privaten IP-Bereiche für NSX Intelligence.

Abschnitt	Beschreibung
6	<p>In diesem Abschnitt wählen Sie den Zeitraum aus, um zu bestimmen, welche Datenverkehrsflows zum Generieren der gewünschten Visualisierung und Empfehlung verwendet werden. Ihre Auswahl bestimmt die Verlaufsdaten, die in der Ansicht „Gruppen“ oder „Berechnungen“ verwendet werden. Der Zeitraum ist relativ zum aktuellen Zeitpunkt und umfasst einen bestimmten Zeitraum in der Vergangenheit.</p> <p>Jetzt ist der standardmäßig verwendete Zeitraum. Diese Option zeigt die neuesten Datenverkehrsflow-Daten an, die das System erfasst hat, bis zu der letzten Million verarbeitete Datenverkehrsflows.</p> <p>Um den ausgewählten Zeitraum zu ändern, klicken Sie auf den aktuell ausgewählten Zeitraum und wählen im Dropdown-Menü einen anderen aus. Sie können Jetzt, Letzte 1 Std., Letzte 12 Std., Letzte 24 Std., Letzte 1 Woche, Letzte 2 Wochen oder Letzter 1 Monat auswählen.</p>
7	<p>Im Arbeitsflächenabschnitt wird das Visualisierungsdiagramm der Sicherheitspositionen der Gruppen oder Berechnungseinheiten in Ihrer lokalen NSX-T Data Center-Umgebung angezeigt. Er enthält auch die Visualisierung der Datenverkehrsflows, die während des ausgewählten Zeitraums aufgetreten sind. In diesem Abschnitt können Sie auf einen spezifischen Knoten oder einen Flow-Pfeil zeigen, um Details zu dieser spezifischen Entität zu erhalten.</p> <p>Weitere Informationen hierzu finden Sie unter Kennelnern von NSX Intelligence-Grafikelementen und Kapitel 2 Grundlegendes zu NSX Intelligence-Ansichten und -Flows.</p>
8	<p>Diese Minikarte bietet eine Übersicht über das gesamte Visualisierungsdiagramm. Wenn Sie bestimmte Einheiten vergrößern, die im Diagramm angezeigt werden, wird die Minikarte aktualisiert. Daraufhin können Sie nachvollziehen, wo sich Ihre aktuelle Ansicht in Bezug auf das Gesamtdiagramm befindet. Wenn Sie in das Fenster mit der Minikarte klicken und die opake rechteckige Überlagerung ziehen, wird die aktuelle Ansicht des Visualisierungsdiagramms ebenfalls aktualisiert.</p>
9	<p>Verwenden Sie diese Ansichtssteuerschaltflächen zum Vergrößern, Verkleinern, Anwenden des 1:1-Seitenverhältnisses, zur Größenanpassung der Ansicht und zum Wechseln zum bzw. Beenden des Vollbildmodus. Sie können auch Tastenkombinationen verwenden, um Ihre Ansichtssteuereinstellungen zu verwalten. Um das Fenster Hilfe für die Tastenkombinationen anzuzeigen, drücken Sie Umschalt+.. Um zu einer zuvor angezeigten Visualisierung zu navigieren, verwenden Sie die Schaltfläche „Zurück“ Ihres Webbrowsers. Wenn Sie sich im Vollbildmodus befinden, drücken Sie die ESC-Taste, um den Vollbildmodus zu beenden, und verwenden Sie die Schaltfläche „Zurück“ Ihres Webbrowsers.</p>

Kennenlernen von NSX Intelligence-Grafikelementen

Die Benutzeroberfläche von NSX Intelligence bietet mehrere grafische Elemente, die bei der Visualisierung der NSX-T Data Center-Entitäten, der Datenverkehrsflows und bestimmter Aktivitäten in Ihrer NSX-T Data Center-Umgebung helfen.

Die folgende Tabelle enthält ein Glossar der NSX-T Data Center-Grafikelemente, die möglicherweise in einem NSX Intelligence-Visualisierungsdiagramm angezeigt werden.

Grafikelement	Beschreibung
	Dieses Symbol repräsentiert eine Gruppe, auf die Sicherheitsrichtlinien, einschließlich der Regeln für die horizontale Firewall, angewendet werden können. Eine Gruppe kann eine Sammlung von VMs, physischen Servern oder Sätzen von IP-Adressen sein. Siehe Arbeiten mit der Ansicht „Gruppen“ .
	Dies ist das verwendete Symbol für eine virtuelle Maschine (VM), die Teil von NSX-T Data Center ist. Eine VM kann mehr als einer Gruppe angehören. Siehe Arbeiten mit der Ansicht „Berechnungen“ .
	Dieses Symbol repräsentiert einen physischen Server, der Teil Ihrer NSX-T Data Center-Umgebung ist. Ein physischer Server kann mehreren Gruppen angehören. Siehe Arbeiten mit der Ansicht „Berechnungen“ .
	Dies ist das Symbol für die öffentlichen IP-Adressen im Internet. Wenn mindestens eine Berechnungseinheit in Ihrer NSX-T Data Center-Umgebung während des ausgewählten Zeitraums mit einer öffentlichen IP-Adresse kommuniziert hat, ist dieser Datenverkehrsflow in der aktuellen Visualisierung enthalten.
	Dieses Symbol stellt eine IP-Adresse dar, z. B. eine Unicast-, Broadcast- oder Multicast-IP-Adresse, die während des ausgewählten Zeitraums am Netzwerkdatenverkehr innerhalb Ihrer NSX-T Data Center-Umgebung beteiligt war.
	Dieses Knotensymbol wird für die Gruppe von Berechnungseinheiten (VMs, physische Server oder IP-Adressssätze) verwendet, die momentan keiner Gruppe angehören.
	Dieser Pfeil stellt einen Netzwerk-Datenverkehrsflow dar, der während eines ausgewählten Zeitraums zwischen zwei Gruppen oder Berechnungseinheiten aufgetreten ist. Es gibt drei verschiedene Arten von Pfeilen. <ul style="list-style-type: none"> ■ einen gestrichelten rötlichen Pfeil für einen ungeschützten Flow ■ einen durchgezogenen bläulichen Pfeil für einen blockierten Flow ■ einen durchgezogenen grünen Pfeil für einen zulässigen Flow Weitere Informationen hierzu finden Sie unter Arbeiten mit Datenverkehrsflows .
	Ein Knoten, der als aktueller Knoten im Fokus ausgewählt wurde, ist von einem gestrichelten Kreis umgeben. Es handelt sich um den angehefteten Knoten während des Auswahlmodus und die aktuell angezeigte Ansicht.
	Dieses Symbol wird auf dem Rand eines Gruppenknotens angezeigt, wenn die Gruppe während des ausgewählten Zeitraums der NSX-T Data Center-Bestandsliste hinzugefügt wurde. Wenn NSX-T Data Center während des ausgewählten Zeitraums eine neue Berechnungseinheit erkennt, z. B. eine VM oder einen physischen Server, wird das Symbol auf dem Rand des Knotens der Berechnungseinheit angezeigt.

Grafikelement	Beschreibung
	<p>Dieses Symbol wird auf dem Rand des Gruppenknotens angezeigt, wenn die Gruppe während des ausgewählten Zeitraums aus dem Bestand entfernt wurde. Möglicherweise wurden die zugehörigen Einheitsmitglieder gelöscht oder nicht gelöscht.</p> <p>Auf dem Rand eines Berechnungseinheitsknotens gibt dieses Symbol an, dass die Berechnungseinheit während des ausgewählten Zeitraums aus dem Bestand entfernt wurde.</p> <p>Auch wenn eine Berechnungseinheit oder Gruppe aus dem Bestand entfernt wurde, wird sie weiterhin im aktuellen Visualisierungsdiagramm angezeigt, um eine Verlaufsansicht mit dem Hinweis zu erhalten, dass die Einheit während des ausgewählten Zeitraums entfernt wurde.</p>
	<p>Dieses Symbol wird angezeigt, wenn eine Gruppe und Berechnungseinheiten zusammen angezeigt werden. Dies ist beispielsweise in einer Deep-Dive-Gruppenansicht oder bei verbundenen Berechnungseinheiten einer Gruppe der Fall.</p> <p>Das Symbol wird auf dem Rand eines Berechnungseinheitsknotens angezeigt, nachdem die Berechnungseinheit aus der aktuell angezeigten Gruppe verschoben wurde. Es wird in den folgenden Fällen auf dem Rand des Knotens für die Berechnungseinheit angezeigt.</p> <ul style="list-style-type: none"> ■ wenn die Berechnungseinheit während des ausgewählten Zeitraums aus der aktuell angezeigten Gruppe verschoben wurde ■ wenn die Berechnungseinheit irgendwann während des ausgewählten Zeitraums Teil der aktuell angezeigten Gruppe war, jetzt jedoch kein Mitglied dieser Gruppe mehr ist
	<p>Dieses Symbol wird am Rand eines Berechnungseinheitsknotens angezeigt, wenn die NSX Suspicious Traffic-Funktion festgestellt hat, dass die Berechnungseinheit während des angegebenen Zeitraums Teil einer verdächtigen Netzwerkdatenverkehrsaktivität war. Einzelheiten dazu finden Sie unter Kapitel 4 Erkennen von verdächtigem Netzwerkdatenverkehr in NSX-T Data Center.</p>

Grundlegendes zu NSX Intelligence-Ansichten und -Flows

2

Die NSX Intelligence-Visualisierung besteht aus den Gruppen oder Berechnungseinheiten und den Netzwerk-Datenverkehrsflows, die während des ausgewählten Zeitraums bei diesen Gruppen oder Berechnungseinheiten aufgetreten sind.

Die Funktion von NSX Intelligence 3.2 oder höher, die mit NSX-T Data Center 3.2 oder höher aktiviert wird, unterstützt Gruppen mit Mitgliedstypen, bei denen es sich entweder um eine VM, einen physischen Server, eine IP-Adresse oder eine Kombination dieser Berechnungseinheiten handelt.

Wichtig Die Visualisierung, die für einen bestimmten Zeitraum angezeigt wird, stellt alle Netzwerkdatenverkehrs-Flows und Arbeitslastaktivitäten dar, die während dieses Zeitraums in Ihrem NSX-T Data Center aufgetreten sind. Zu diesen Aktivitäten gehören das Hinzufügen, Entfernen oder Verschieben von Berechnungseinheiten (VMs, physische Server, IP-Adresssätze) und Gruppen. Es ist möglich, dass eine VM in der Visualisierung mehr als einmal angezeigt wird. Wenn eine VM beispielsweise mit einem ESXi-Host verbunden wird, der ursprünglich nicht verwaltet wurde, und der Host während des ausgewählten Zeitraums von einem VMware vCenter Server™ verwaltet wird, dann wird die VM in der Ansicht „Berechnungen“ zweimal angezeigt. Wenn ein ESXi-Host von vCenter Server getrennt und während desselben ausgewählten Zeitraums wieder hinzugefügt wurde, werden die mit dem Host verbundenen VMs während des ausgewählten Zeitraums ebenso als gelöscht und neu angezeigt. Wenn in der Ansicht „Gruppen“ eine VM in der Gruppe „Nicht kategorisiert“ enthalten war und während desselben ausgewählten Zeitraums einer Gruppe hinzugefügt wurde, wird die VM sowohl in der Gruppe „Nicht kategorisiert“ als auch in der neuen Gruppe angezeigt.

Die NSX Intelligence-Funktion unterstützt nur Gruppen mit VMs, physischen Servern oder IP-Adressen. Wenn Gruppen weitere Mitgliedstypen enthalten, werden in der Ansicht „Gruppen“ anstelle der tatsächlichen Gruppen in der Sicherheitsregel möglicherweise nur die korrelierten Datenverkehrsflows zwischen den Gruppen mit unterstützten Mitgliedstypen angezeigt.

Das angezeigte Visualisierungsdiagramm wird aktualisiert, wenn sich die Sicherheitsposition in Ihrem NSX-T Data Center ändert. Beispielweise wird beim Hinzufügen einer neuen Gruppe ein neuer Gruppenknoten auf der Visualisierungsarbeitsfläche angezeigt, ohne dass Sie Ihren Webbrowser aktualisieren müssen. Im Abschnitt „Aktualisierungsstatus“ im oberen rechten Bereich der Virtualisierungsarbeitsfläche wird angezeigt, wann die Ansicht zuletzt aktualisiert wurde.

Verwenden Sie die Informationen in diesem Abschnitt, um mehr über das Arbeiten mit den Ansichten „Gruppen“ und „Berechnungen“ und den verschiedenen Arten von Datenverkehrsflows zu erfahren.

Dieses Kapitel enthält die folgenden Themen:

- [Arbeiten mit der Ansicht „Gruppen“](#)
- [Arbeiten mit der Ansicht „Berechnungen“](#)
- [Arbeiten mit Datenverkehrsflows](#)

Arbeiten mit der Ansicht „Gruppen“

Die Standardansicht, die auf der NSX Intelligence-Startseite angezeigt wird, ist die Ansicht „Gruppen“. In der Ansicht „Gruppen“ werden alle Gruppen und die Datenverkehrsflows angezeigt, die in der letzten Stunde stattfanden.

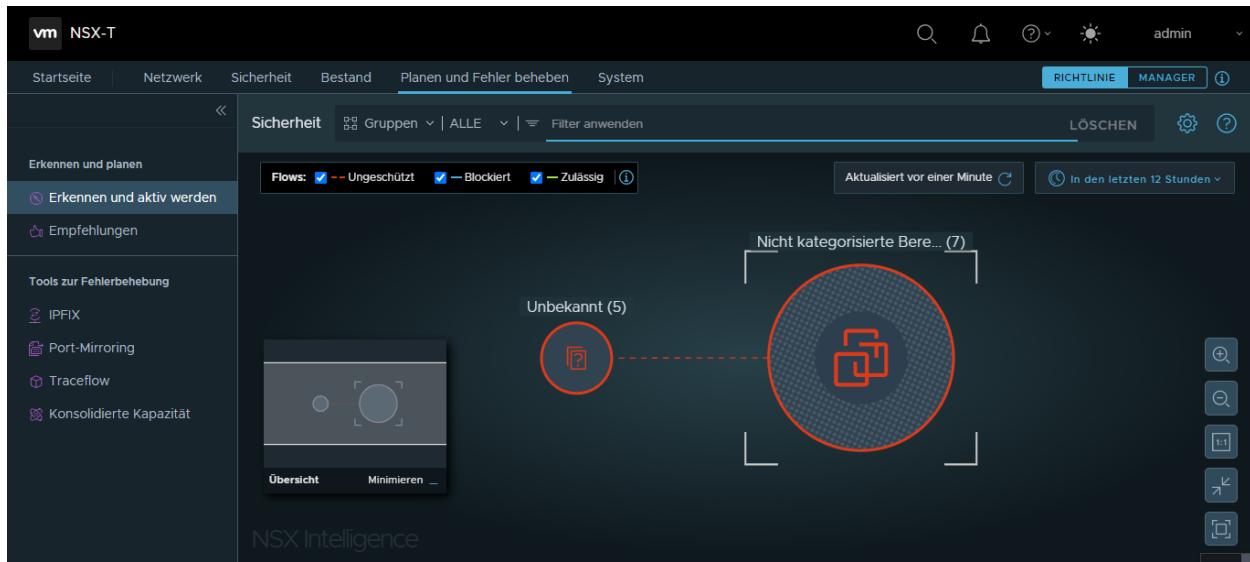
Auswahl anzeigen

Wenn die Ansicht „Gruppen“ nicht angezeigt wird, klicken Sie im Auswahlbereich für die Sicherheitsansicht neben **Berechnungen** auf den Pfeil nach unten und wählen Sie **Gruppen** aus. Im angezeigten Dropdown-Menü können Sie **Alle Gruppen** oder bestimmte Gruppen aus der Liste auswählen und dann auf **Anwenden** klicken.

Verwenden Sie das Textfeld **Suchen**, um die Liste der verfügbaren Gruppen zu filtern. Wenn Sie auf eine andere Stelle klicken, ohne eine Auswahl im Dropdown-Menü vorzunehmen, oder wenn Sie **Alle Gruppen** im Dropdown-Menü auswählen, wird das Menüelement **Alle Gruppen** auf die Ansicht „Gruppen“ angewendet.

Knoten in einer Gruppenansicht

Ein Knoten in der Ansicht „Gruppen“ stellt NSX-Objekteinheiten wie VMs, physische Server und IP-Adressen oder eine Gruppe von nicht kategorisierten VMs in Ihrem NSX-T Data Center-Bestand dar. Die Ansicht „Gruppen“ enthält auch Knoten, die Einheiten repräsentieren, die zwar mit Mitgliedern der Gruppen kommunizieren, jedoch nicht Teil Ihres NSX-T Data Center-Bestands sind. Der folgende Screenshot zeigt ein Beispiel der Ansicht „Gruppen“.



In der folgenden Tabelle sind die Typen der Gruppenknoten aufgeführt, die in der Ansicht „Gruppen“ angezeigt werden.

Gruppenknotentyp	Symbol	Beschreibung
Reguläre Gruppe		Ein Knoten „Reguläre Gruppe“ im NSX Intelligence-Visualisierungsdiagramm stellt eine beliebige Sammlung von Recheneinheiten dar, die in Ihrer NSX-T Data Center-Umgebung verwaltet werden. Das NSX Intelligence-Diagramm unterstützt regelmäßige Gruppen mit Berechnungseinheiten, die VMs, physische Server, IP-Adressen oder eine Kombination dieser Einheiten umfassen. Eine NSX Einheit kann mehr als einer Gruppe angehören und in mehr als einem regulären Gruppenknoten angezeigt werden.
Gruppe „Nicht kategorisiert“		Ein nicht kategorisierter Gruppenknoten repräsentiert eine Erfassung von NSX-Einheiten, die zu keiner Gruppe gehören, aber nicht im NSX-T Data Center-Bestand.
Gruppe „Unbekannt“		Ein unbekannter Gruppenknoten stellt eine Reihe von verschiedenen Berechnungseinheiten dar, die nicht zum NSX-T Data Center-Bestand gehören, sich jedoch innerhalb des Datencenters befinden und mit einer oder mehreren NSX Einheiten in NSX-T Data Center kommunizieren.
Gruppe „Öffentliche IPs“		Ein Knoten der Gruppe „Öffentliche IPs“ stellt eine Sammlung von öffentlichen IP-Adressen (IPv4 oder IPv6) dar, die mit NSX-Objekten in Ihrem NSX-T Data Center kommunizieren. IP-Adressen, die zu keiner der in den Einstellungen für den privaten IP-Bereich für NSX Intelligence aufgeführten CIDR-Notationen gehören, werden als öffentliche IP-Adresse klassifiziert.

Knotengröße und -farbe

Die Größe eines Knotens in der Ansicht „Gruppen“ basiert auf der Anzahl Mitglieder, die zu dieser Gruppe gehören. Je größer die Knotengröße der Gruppe ist, desto mehr Berechnungseinheiten gehören zu dieser Gruppe. Der Gruppenname und die Gesamtzahl der Mitglieder werden oberhalb des Knotens angezeigt.

Die Randfarbe des Knotens gibt die Typen der Datenverkehrsflows an, die bei den Berechnungseinheiten dieser Gruppe aufgetreten sind.

Gruppenknotentyp	Beschreibung
	Ein Gruppenknoten mit einem rötlichen Rand gibt an, dass mindestens ein ungeschützter Datenverkehrsflow erkannt wurde. Die Anzahl blockierter oder zulässiger Flows, die während des ausgewählten Zeitraums erkannt wurden, ist dabei unerheblich.
	Ein Knoten mit einem blauen Rand bedeutet, dass zwar keine ungeschützten Datenverkehrsflows erkannt wurden, aber mindestens ein blockierter Flow vorhanden ist, unabhängig davon, wie viele zulässige Flows während des ausgewählten Zeitraums erfasst wurden.
	Ein Knoten mit einem grünen Rand zeigt, dass während des ausgewählten Zeitraums keine ungeschützten oder blockierten Flows erkannt wurden und mindestens ein zulässiger Flow festgestellt wurde.
	Ein Knoten mit einem grauen Rand bedeutet, dass während des ausgewählten Zeitraums keine Datenverkehrsflows für die Berechnungseinheiten erkannt wurden, die zu dieser Gruppe gehören.

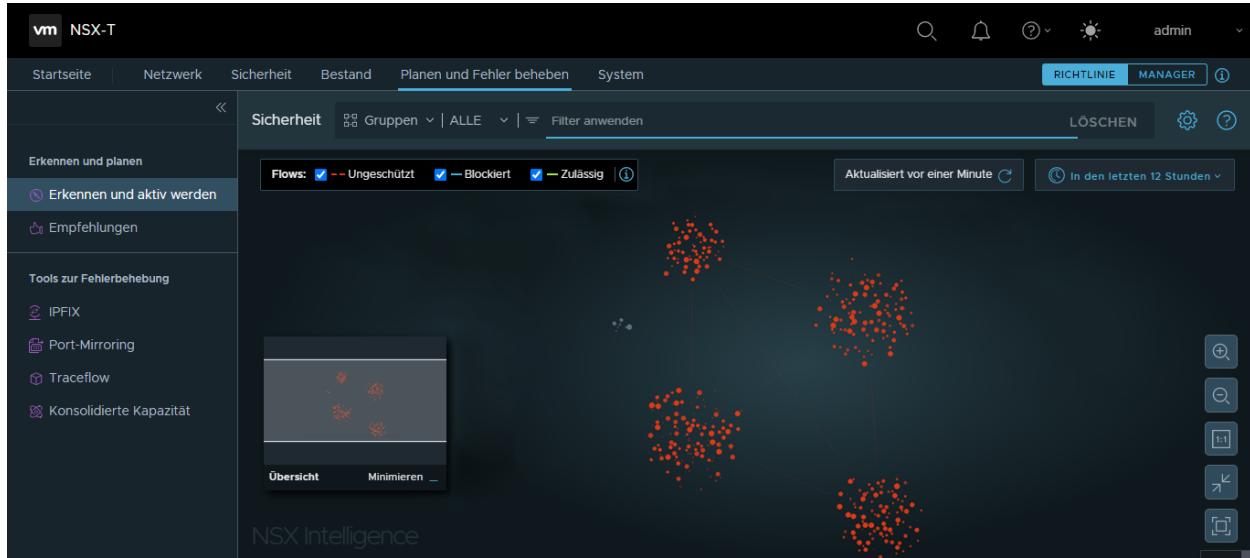
Pfeile in einer Gruppenansicht

Die Pfeile zwischen den Gruppenknoten stellen die Datenverkehrsflows dar, die während des ausgewählten Zeitraums zwischen den Berechnungseinheiten in diesen verbundenen Gruppenknoten aufgetreten sind. Ein selbstreferenzierender Pfeil auf einem Gruppenknoten gibt an, dass mindestens eine Berechnungseinheit mit einer anderen Berechnungseinheit innerhalb dieser Gruppe kommuniziert hat. Weitere Informationen hierzu finden Sie unter [Arbeiten mit Datenverkehrsflows](#).

Cluster von Gruppenknoten

Wenn 100 oder mehr Gruppenknoten und 1.000 oder mehr Datenverkehrsflows angezeigt werden müssen, zeigt das NSX Intelligence-Diagramm die Gruppenknoten in Clustern an. Diese Gruppen-Cluster basieren auf der Konnektivität zwischen den Berechnungseinheiten in diesen Gruppen während des ausgewählten Zeitraums. Durch das Gruppen-Clustering erhalten Sie eine Übersicht der Aktivitäten in Ihrer NSX-T Data Center-Umgebung während dieses ausgewählten Zeitraums.

Der folgende Screenshot ist ein Beispiel für eine Visualisierung dieser Gruppencluster. Die Farben der Knoten entsprechen den Typen der Datenverkehrs-Flows, die während des ausgewählten Zeitraums bei diesen Gruppen stattfanden. Gruppen, bei denen während des ausgewählten Zeitraums keine Mitglieder mit Mitgliedern anderer Gruppen kommunizierten, werden in einem eigenen Gruppen-Cluster zusammengefasst.



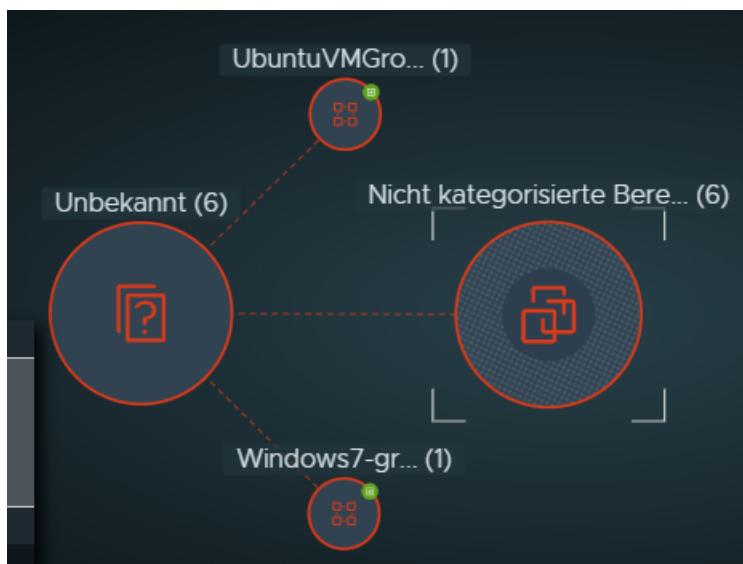
Wenn Sie auf einen bestimmten Gruppencluster verweisen, wird eine Zahl oberhalb des Clusterbereichs angezeigt. Diese Zahl gibt an, wie viele Gruppen sich in dieser bestimmten Clustervisualisierung befinden. Um weitere Details zu einem bestimmten Cluster und den Gruppen anzuzeigen, die Teil dieses Clusters sind, vergrößern Sie das Diagramm. Wenn Sie näher an die Knoten und die Pfeile heranzoomen, werden die Details der Gruppe und des Datenverkehrsflows besser erkennbar und auswählbar. Sie können auch Filter anwenden, um die Gruppen einzuzgrenzen, die im Visualisierungsdiagramm angezeigt werden.

Knotenauswahl in Ansicht „Gruppen“

Wenn Sie auf den Knoten einer Gruppe zeigen, werden Informationen zu dieser Gruppe angezeigt, wie im folgenden Beispiel für die Gruppe „UbuntuVMGroup“ dargestellt. Wenn die Gruppe während des ausgewählten Zeitraums hinzugefügt wurde, werden das grüne Badge-Symbol „Neu“ und die Details zum Zeitpunkt der Erstellung der Gruppe angezeigt. Die Gesamtzahl Flows und die Anzahl und Typen der während des ausgewählten Zeitraums erkannten Flows werden aufgeführt. Falls vorhanden, wird auch die Anzahl der für die Gruppe verfügbaren Empfehlungen angezeigt.



Wenn Sie auf den Knoten einer Gruppe klicken, wird die Auswahl durch einen gestrichelten Kreis als angehefteter Gruppenknoten markiert. Die anderen Gruppen, die mit dem ausgewählten Gruppenknoten verbunden sind, werden in der Ansicht auch stärker hervorgehoben. Alle anderen Knoten werden abgeblendet. Beispielsweise wird im folgenden Screenshot der Knoten „UbuntuVMGroup“ ausgewählt und zum angehefteten Gruppenknoten. Die Gruppe „Nicht kategorisierte Berechnungen“ hat während des ausgewählten Zeitraums mindestens einen Datenverkehrsflow mit mindestens einem UbuntuVMGroup-Mitglied geteilt und wird daher ebenfalls hervorgehoben. Alle anderen Gruppen, die nicht mit UbuntuVMGroup kommuniziert haben, werden in der Ansicht abgeblendet.



Um die angeheftete Auswahl zu löschen, klicken Sie auf einen leeren Bereich der Visualisierungsarbeitsfläche.

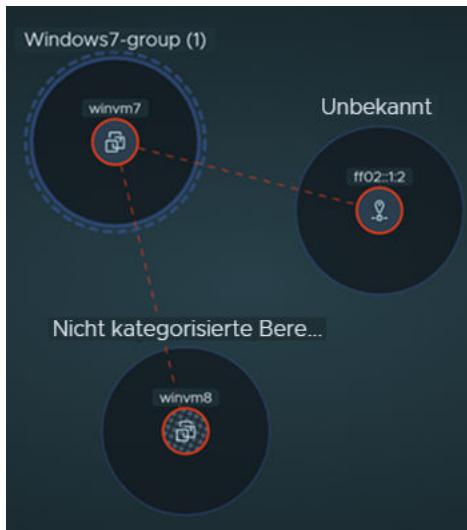
Wenn Sie die Ansicht „Gruppen“ verkleinern und die Details zu den Knoten nicht mehr sichtbar sind, zeigen Sie auf einen beliebigen sichtbaren Teil eines Knotens, um die Details anzuzeigen.

Verfügbare Aktionen in der Ansicht „Gruppen“

Wenn Sie mit der rechten Maustaste auf den Knoten einer Gruppe klicken, wird ein Kontextmenü mit verfügbaren Aktionen oder Informationen angezeigt, wie in der folgenden Abbildung dargestellt.



- Durch Auswahl von **Deep Dive: Gruppenname** wird der Knoten der ausgewählten Gruppe mit einem gestrichelten Kreis umrandet, um ihn als angehefteten Gruppenknoten oder als aktuelle Gruppe im Fokus zu markieren. Die Berechnungseinheiten, die zur Gruppe gehören, werden innerhalb des Knotens der Gruppe angezeigt. Alle Gruppen, die während des ausgewählten Zeitraums einen Datenverkehrsflow mit den Mitgliedern der angehefteten Gruppe gemeinsam genutzt haben, werden ebenfalls in der Ansicht „Gruppen“ platziert. Im folgenden Beispiel ist der Knoten „Windows7-group“ die angeheftete Gruppe. Die anderen Gruppen werden in der Ansicht angezeigt, weil für ihre Mitglieder während des ausgewählten Zeitraums Netzwerk-Datenverkehrsflows mit der einzelnen VM in der Gruppe „Windows7-group“ vorlagen.



- Wenn Sie **Filtern nach** auswählen, wird die aktuelle Gruppe dem Visualisierungsfilter hinzugefügt, der für die aktuelle Ansicht „Gruppen“ verwendet wird.

- Wenn Sie **Empfehlungen** auswählen, wird die Tabelle mit den verfügbaren Empfehlungen für die aktuelle Gruppe angezeigt. In der Tabelle **Empfehlungen** können Sie die Empfehlungsdetails anzeigen und die verfügbaren Aktionen ausführen. Weitere Informationen hierzu finden Sie unter [Kapitel 3 Arbeiten mit NSX Intelligence-Empfehlungen](#).
- Wenn Sie **Mitglieder** auswählen, wird eine Tabelle mit allen Berechnungseinheiten angezeigt, die während des ausgewählten Zeitraums zu der aktuellen angehefteten Gruppe gehörten. In der Tabelle **Mitglieder** sehen Sie die Details zu den VMs, IP-Adressen und physischen Servern, die zur ausgewählten Gruppe gehören, und zu den anderen Gruppen, zu denen die einzelnen Berechnungseinheiten ebenfalls gehören. Um dem aktuellen Visualisierungsfilter eine bestimmte VM, IP-Adresse oder einen bestimmten physischen Server hinzuzufügen, klicken Sie auf das Filtersymbol  auf der rechten Seite.
- Wenn Sie **Flow-Details** auswählen, wird im Dialogfeld **Flow-Details einer Gruppe** eine Tabelle für die aktuell ausgewählte Gruppe angezeigt. Die Tabelle zeigt die Details zu den abgeschlossenen Flows und zu den Flows, die während des ausgewählten Zeitraums aktiv waren. Weitere Informationen hierzu finden Sie unter [Arbeiten mit Datenverkehrsflows](#).
- Wenn Sie **Empfehlung starten** auswählen, wird der Assistent **Neue Empfehlung starten** angezeigt, der Sie beim Generieren einer neuen Empfehlung für eine Mikrosegmentierungsregel unterstützt. Einzelheiten dazu finden Sie unter [Generieren einer neuen NSX Intelligence-Empfehlung](#).

Arbeiten mit der Ansicht „Berechnungen“

Ein Knoten in der Ansicht „Berechnungen“ stellt eine Berechnungseinheit in Ihrer lokalen NSX-T Data Center-Umgebung dar. Bei einer Berechnungseinheit handelt es sich entweder um eine virtuelle Maschine (VM), einen physischen Server oder eine IP-Adresse.

Auswahl anzeigen

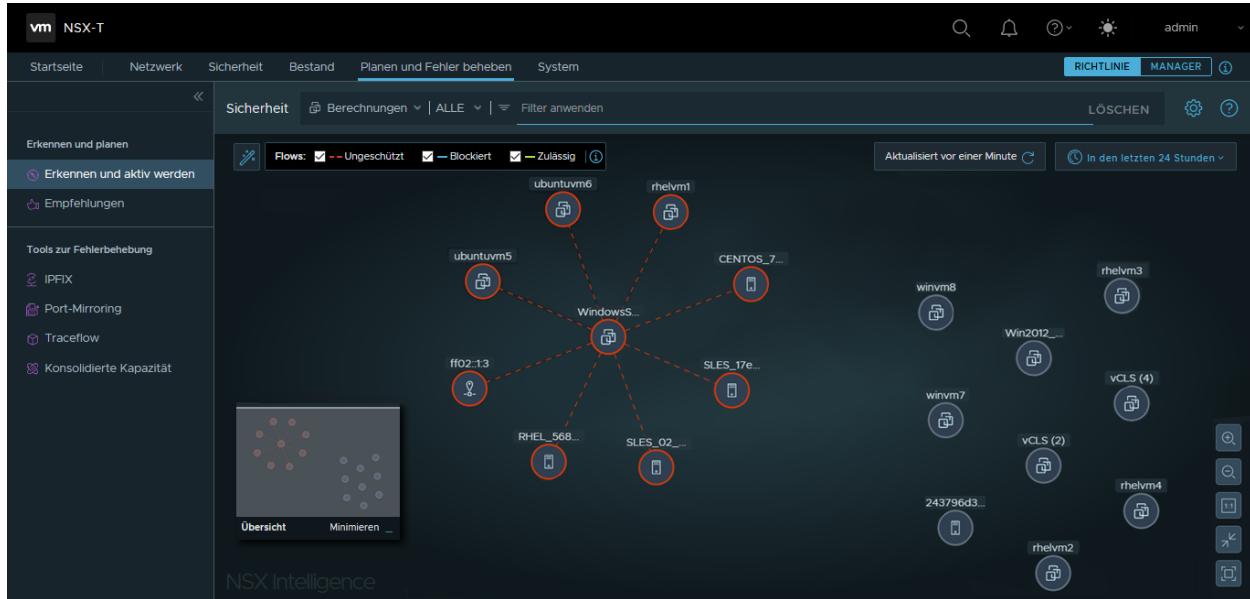
Wenn die Ansicht „Berechnungen“ nicht angezeigt wird, klicken Sie im Auswahlbereich der Sicherheitsansicht neben **Gruppen** auf den Pfeil nach unten und wählen Sie **Berechnungen** aus. Im Dropdown-Menü können Sie **Alle Berechnungen auswählen** auswählen, um alle Berechnungseinheiten während des ausgewählten Zeitraums anzuzeigen. Wenn Sie nur VMs, IP-Adressen oder physische Server anzeigen möchten, klicken Sie auf **Alle Typen anzeigen** und wählen Sie im Dropdown-Menü **VMs, IPs** oder **Physische Server** aus.

In der Liste **Verfügbare Elemente** können Sie auch bestimmte Berechnungseinheiten auswählen. Verwenden Sie das Textfeld **Suchen**, um die Auswahlliste zu filtern. Klicken Sie auf **Anwenden**, nachdem Sie Ihre Auswahl getroffen haben.

Wenn Sie auf eine Stelle außerhalb des Dropdown-Menüs klicken, ohne darin eine Auswahl vorzunehmen oder wenn Sie im Dropdown-Menü **Alle Berechnungen auswählen** auswählen, wird die Option **Alle Berechnungen auswählen** auf die Ansicht „Berechnungen“ angewendet.

Knoten in Ansicht „Berechnungen“

Wenn Sie sich in der Ansicht „Berechnungen“ befinden, werden die Gruppengrenzen nicht angezeigt. Jeder Knoten, der mit einer der Berechnungseinheiten in Ihrer NSX-T Data Center-Umgebung kommuniziert, aber nicht als Teil des NSX-T Data Center-Bestands identifiziert wurde, wird auch in der Ansicht „Berechnungen“ dargestellt. Im Folgenden wird eine einfache Ansicht „Berechnungen“ dargestellt.



In der folgenden Tabelle sind die Typen der VM-Knoten aufgeführt, die unter „Ansichten“ angezeigt werden.

Knotentyp der Berechnungseinheit	Symbol	Beschreibung
Reguläre VM		Ein regulärer VM-Knoten stellt eine virtuelle Maschine (VM) dar, die Teil Ihrer NSX-T Data Center-Umgebung ist. Eine VM kann mehr als einer Gruppe angehören.
Öffentliche IP-Adresse		Ein öffentlicher IP-Knoten stellt eine öffentliche IP-Adresse (entweder IPv4 oder IPv6) dar, die mit oder von ihrer NSX-T Data Center-Umgebung aus kommuniziert. Wenn Sie mit der rechten Maustaste auf dieses Symbol klicken, werden alle öffentlichen IP-Adressen aufgelistet, für die während des ausgewählten Zeitraums Netzwerkdatenverkehraktivität aufgetreten ist. Wenn Sie auf einen mit diesem Knoten verbundenen Datenverkehrsflow-Pfeil zeigen, wird die tatsächliche IP-Adresse angezeigt, die an diesem Datenverkehrsflow-Austausch beteiligt war.

Knotentyp der Berechnungseinheit	Symbol	Beschreibung
IP		Ein IP-Knoten stellt eine IP-Adresse dar, die während des ausgewählten Zeitraums am Netzwerkdatenverkehr beteiligt war. Eine IP-Adresse kann eine Unicast-, Broadcast- oder Multicast-IP-Adresse sein.
Physischer Server		<p>Dieser Knoten repräsentiert einen physischen Server, der Teil Ihrer NSX-T Data Center-Umgebung ist. Ein physischer Server kann mehreren Gruppen angehören.</p> <p>Die aktuell unterstützten physischen Server lauten wie folgt.</p> <ul style="list-style-type: none"> ■ RHEL Server-Version 7.9, 8.2, 8.4 ■ Ubuntu 16.04., 18.04 ■ CentOS 7.9, 8.4 ■ SUSE 12 SP4 ■ Windows Server 2016, 2019

Knotenfarbe

Die Farbe des Randes eines Berechnungseinheitsknotens gibt den Typ der Datenverkehrsflows an, die während des ausgewählten Zeitraums für die Berechnungseinheit aufgetreten sind.

- Ein Knoten mit einem rötlichen Rand gibt an, dass mindestens ein ungeschützter Datenverkehrsflow erkannt wurde. Die Anzahl blockierter oder zulässiger Flows, die während des ausgewählten Zeitraums erkannt wurden, ist dabei unerheblich.
- Ein Knoten mit einem blauen Rand bedeutet, dass zwar keine ungeschützten Datenverkehrsflows erkannt wurden, aber mindestens ein blockierter Flow vorhanden ist, unabhängig davon, wie viele zulässige Flows während des ausgewählten Zeitraums erfasst wurden.
- Ein Knoten mit einem grünen Rand zeigt, dass während des ausgewählten Zeitraums keine ungeschützten oder blockierten Flows erkannt wurden und mindestens ein zulässiger Flow festgestellt wurde.
- Ein Knoten mit einem grauen Rand bedeutet, dass während des ausgewählten Zeitraums keine Datenverkehrsflows für die jeweilige Berechnungseinheit erkannt wurden.

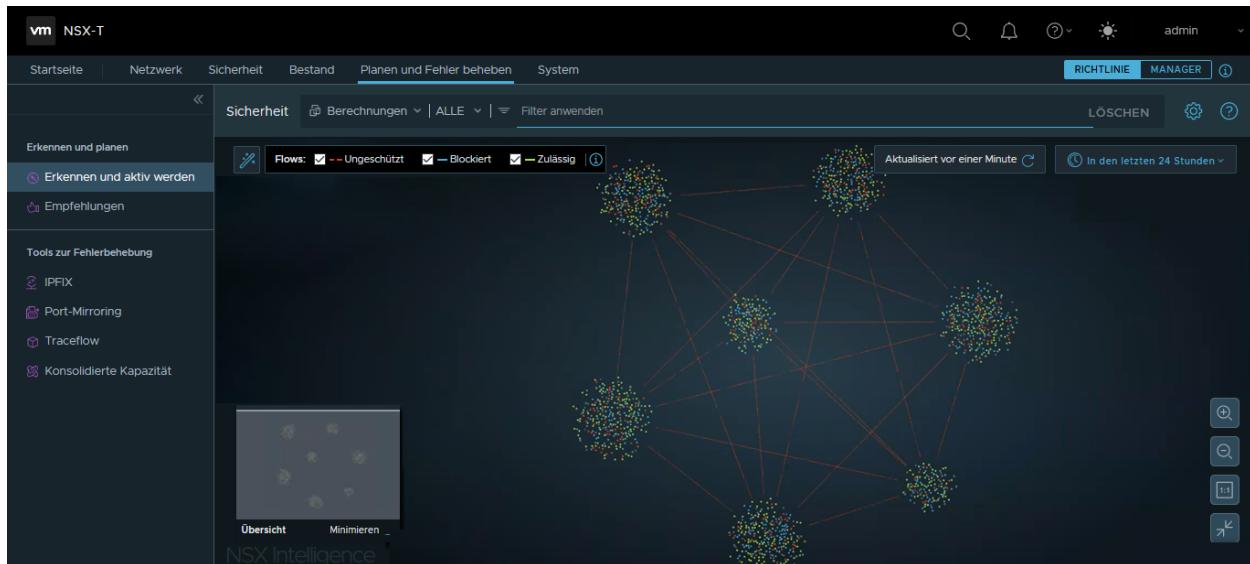
Pfeile in Ansicht „Berechnungen“

Die Pfeile zwischen den Knoten der Berechnungseinheit stellen die Datenverkehrsflows dar, die während des ausgewählten Zeitraums zwischen den Berechnungseinheiten aufgetreten sind. Weitere Informationen hierzu finden Sie unter [Arbeiten mit Datenverkehrsflows](#).

Cluster mit Berechnungseinheitsknoten

Wenn 100 oder mehr Berechnungseinheitsknoten und 1.000 oder mehr Datenverkehrsflows angezeigt werden müssen, zeigt das NSX Intelligence-Diagramm die Berechnungseinheitsknoten in Clustern an. Diese Cluster mit Berechnungseinheiten basieren auf der Konnektivität zwischen den Berechnungseinheiten während des ausgewählten Zeitraums. Durch das Clustering der Berechnungseinheiten erhalten Sie eine Übersicht der Netzwerk-Datenverkehrsaktivitäten in Ihrer gesamten NSX-T Data Center-Umgebung während des ausgewählten Zeitraums.

Der folgende Screenshot liefert ein Beispiel für diese Berechnungs-Clustervisualisierung. Die verschiedenen Farben der Knoten und Pfeile entsprechen den Typen der Datenverkehrsflows, die während des ausgewählten Zeitraums bei den Berechnungseinheiten auftraten. Berechnungseinheiten, die während des ausgewählten Zeitraums nicht mit anderen Berechnungseinheiten kommuniziert haben, werden in einem separaten Cluster zusammengefasst.



Wenn Sie auf einen bestimmten Cluster zeigen, wird eine Zahl oberhalb des Clusterbereichs angezeigt. Diese Zahl gibt an, wie viele Berechnungseinheiten sich in dieser bestimmten Clustervisualisierung befinden. Um weitere Details zu einem bestimmten Cluster und den Berechnungseinheiten anzuzeigen, die Teil dieses Clusters sind, vergrößern Sie das Diagramm. Wenn Sie näher an den Knoten und die Pfeile heranzoomen, werden die Details zu den Berechnungseinheiten und den Datenverkehrsflows besser sichtbar und sind einfacher auszuwählen. Sie können auch Filter anwenden, um die Berechnungseinheiten einzuschränken, die im Visualisierungsdiagramm angezeigt werden.

Knotenauswahl in der Ansicht „Berechnungen“

Wenn Sie auf den Knoten einer Berechnungseinheit zeigen, werden Informationen zum Knoten angezeigt, wie im folgenden Beispiel dargestellt. Zudem werden die Anzahl und die Typen der während des ausgewählten Zeitraums erkannten Flows für die Berechnungseinheit aufgeführt. Wenn die Berechnungseinheit während des ausgewählten Zeitraums hinzugefügt wurde, werden das Badge-Symbol „Neu“ und die Details zum Zeitpunkt, an dem die Berechnungseinheit hinzugefügt wurde, ebenfalls angezeigt.

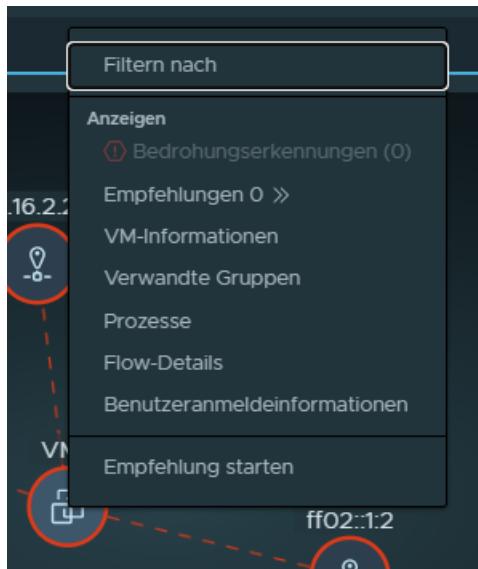


Wenn Sie auf den Knoten einer Berechnungseinheit klicken, wird die Auswahl durch einen gestrichelten Kreis als angehefteter Knoten der Berechnungseinheit markiert. Weitere Berechnungseinheitsknoten, die Datenverkehrflows mit diesem angehefteten Knoten gemeinsam genutzt haben, werden in der Ansicht „Berechnungen“ ebenfalls stärker hervorgehoben. Alle anderen Knoten werden abgeblendet, um sie weniger sichtbar zu machen. Wenn Sie die angeheftete Auswahl löschen möchten, klicken Sie in der Ansicht „Berechnungen“ auf einen leeren Bereich.

Wenn Sie die Ansicht „Berechnungen“ verkleinern und die Details in den Berechnungseinheitsknoten nicht mehr sichtbar sind, können Sie auf einen beliebigen sichtbaren Teil des Knotens zeigen. Die Details für die Berechnungseinheit werden angezeigt.

Verfügbare Aktionen in der Ansicht „Berechnungen“

Wenn Sie mit der rechten Maustaste auf den Knoten einer Berechnungseinheit klicken, wird ein Kontextmenü mit verfügbaren Aktionen angezeigt, wie in der folgenden Abbildung dargestellt.



Auswahl	Beschreibung
Filtern nach	Die Berechnungseinheit wird dem Visualisierungsfilter hinzugefügt, der für die aktuelle Ansicht „Berechnungen“ verwendet wird.
Verdächtige Netzwerkaktivitäten < n >	Wenn eine verdächtige Netzaktivität festgestellt wird, die diese Berechnungseinheit betrifft, ist dieses Element auswählbar. Das (n) gibt die Anzahl der entdeckten verdächtigen Aktivitäten an. Weitere Informationen hierzu finden Sie unter Kapitel 4 Erkennen von verdächtigem Netzwerksdatenverkehr in NSX-T Data Center .
Empfehlungen (< n >)	Die Empfehlungstabelle für die aktuelle Berechnungseinheit wird angezeigt. Das (n) gibt die Anzahl verfügbarer Empfehlungen an. In der Empfehlungstabelle können Sie die Empfehlungsdetails anzeigen und die verfügbaren Aktionen ausführen. Weitere Informationen hierzu finden Sie unter Kapitel 3 Arbeiten mit NSX Intelligence-Empfehlungen .
< Berechnungseinheitstyp >-Informationen	Die Details werden für die aktuell ausgewählte Berechnungseinheit während des ausgewählten Zeitraums angezeigt. Die Details hängen vom Typ ab und können den Namen, die IP-Adresse, die ID, die Betriebssysteminformationen und vieles mehr enthalten. Hinweis Wenn eine VM als Standardprofil für die IP Discovery an das Segmentprofil angehängt ist und Trust On First Use (TOFU) aktiviert ist, erhält die VM zunächst eine IP-Adresse von DHCP. Wenn die DHCP-IP-Adresse freigegeben und die IP-Adresse der VM in eine statische IP-Adresse geändert wird, werden sowohl die DHCP- als auch die statische IP-Adresse unter den VM-Informationen angezeigt. Wenn TOFU im Standardprofil für IP Discovery deaktiviert wurde, wird beim Freigeben der anfänglich zugewiesenen DHCP-IP-Adresse und beim Ändern der IP-Adresse der VM in eine statische Adresse nur die statische IP-Adresse unter den VM-Informationen angezeigt.
Verwandte Gruppen	Zeigt die Tabelle „Gruppen“ mit Informationen zu Gruppen an, zu denen die Berechnungseinheit während des ausgewählten Zeitraums gehörte.
Prozesse	(Nur für VM-Knoten) Zeigt die Tabelle „Prozesse“ mit Details zu den Prozessen an, die die Datenverkehrsflows beinhalten, bei denen Daten entweder an die VM gesendet oder empfangen wurden oder beides.

Auswahl	Beschreibung
Flow-Details	<p>Zeigt die Details zu den abgeschlossenen Flows und den Flows an, die für die Berechnungseinheit während des ausgewählten Zeitraums momentan aktiv sind.</p> <p>Hinweis Die aktiven Flows während des ausgewählten Zeitraums sind zum Anzeigezeitpunkt der Details älter als 2,5 Minuten.</p> <p>Mögliche Details:</p> <ul style="list-style-type: none"> ■ Flowtyp: abgeschlossen oder aktiv ■ Quell- und Zielgruppen des Flows ■ verwendete Dienste ■ L7-Informationen: Anwendungs-ID und FQDN ■ Typ des letzten Flows: nicht geschützt, blockiert, zulässig ■ Endzeit des Flows <p>Sie können auf einige der Details klicken, um weitere Informationen zu erhalten. Weitere Informationen hierzu finden Sie unter Arbeiten mit Datenverkehrsflows.</p>
Benutzeranmeldeinformationen	(Nur für-VM-Knoten) Zeigt Benutzeranmeldeinformationen für die ausgewählte VM an.
Empfehlung starten	Zeigt den Assistenten Neue Empfehlungen starten an. Weitere Informationen finden Sie unter Kapitel 3 Arbeiten mit NSX Intelligence-Empfehlungen .

Arbeiten mit Datenverkehrsflows

Die Pfeile zwischen den Knoten der Gruppe oder Berechnungseinheit stellen die Netzwerk-Datenverkehrsflows dar, die während des ausgewählten Zeitraums zwischen den Berechnungseinheiten aufgetreten sind.

Der Netzwerkdatenverkehr basiert auf den vorhandenen L3-Regeln der verteilten Firewall (DFW) und den Datenverkehrsflows, die während des ausgewählten Zeitraums aufgetreten sind. Alle Datenverkehrsflows, die mit einer statusbehafteten L3-DFW-Regel unter Verwendung von IPv4 oder IPv6 und mit TCP-, UDP-, GRE-, ESP- und SCTP-Protokollen übereinstimmen, sind in den Visualisierungs- und Flow-Details enthalten. TCP- und UDP-Flows verfügen über Details auf IP- und Port-Ebene, für andere Flows sind nur Details auf IP-Ebene vorhanden.

Die Datenverkehrsflows werden in die folgenden Typen kategorisiert.

Flow-Typ	Grafik	Beschreibung
Ungeschützt		Ein gestrichelter rötlicher Pfeil weist darauf hin, dass das System erkannt hat, dass der Datenverkehrsflow eine Regel erreicht hat (Quelle: Beliebig Ziel: Beliebig Aktion: Zulassen oder Ablehnen oder Verwerfen) und dass präzisere Sicherheitsrichtlinien erforderlich sind. Diese Regel kann Ihre Standardregel sein oder sie kann sich an beliebiger Stelle der verteilten Firewall für den Ost-West-Datenverkehr befinden.
Blockiert		Ein durchgezogener blauer Pfeil zeigt, dass das System erkannt hat, dass der Datenverkehrsflow eine „Ablehnen“- oder „Verwerfen“-Regel erreicht hat, die präziser ist als die in der Flow-Definition „Ungeschützt“ angegebene Regel.
Zulässig		Ein durchgezogener grüner Pfeil zeigt, dass das System erkannt hat, dass der Datenverkehrsflow eine „Zulässig“-Regel erreicht hat, die präziser ist als die in der Flow-Definition „Ungeschützt“ angegebene Regel.

Sie können die Details zu den Datenverkehrsflows anzeigen, an denen eine bestimmte Gruppe oder eine bestimmte Berechnungseinheit teilgenommen hat, indem Sie mit der rechten Maustaste auf den zugehörigen Knoten im Visualisierungsdiagramm klicken und **Flow-Details** auswählen. Im Dialogfeld **Flow-Details** wird eine Tabelle angezeigt, wie in der folgenden Abbildung für einen Gruppenknoten dargestellt.

The screenshot shows the 'Flow-Details' dialog box with the following details:

- Time filter: Letzte Woche
- Section: Abgeschlossene Flows
- Count: 5 Flow(s)
- Table Headers (from left to right):
 - Quelle
 - Ziel
 - Dienste
 - App-ID
 - FODN
 - Neuester Flow (Gegen die aktuelle Richtlinie)
 - Endzeit
- Table Data (5 rows):

Berechnen	Gruppe	Benutzer	Prozess	Berechnen	Gruppe	Dienste	App-ID	FODN	Neuester Flow (Gegen die aktuelle Richtlinie)	Endzeit
> VM1	UbuntuV...	NV	NV	[redacted]	Unbekannt	... und 1 weitere			Ungeschützt	28.11.20, 23:52
> VM1	UbuntuV...	NV	NV	ff02:1:2	Unbekannt	DHCPv6 Servi			Ungeschützt	28.11.20, 23:51
> VM1	UbuntuV...	NV	NV	[redacted]	Unbekannt	... und 4 weitere			Ungeschützt	28.11.20, 23:22
> VM1	UbuntuV...	NV	NV	[redacted]	Unbekannt	... und 1 weitere			Ungeschützt	28.11.20, 23:22
> VM1	UbuntuV...	NV	NV	ff02:1:3	Unbekannt	... und 1 weitere			Ungeschützt	28.11.20, 23:22
- Buttons at the bottom: Aktualisieren, SCHLIESSEN

In der Tabelle werden die Registerkarte **Abgeschlossene Flows** und die Registerkarte **Aktive Flows** angezeigt, die Details zu den entsprechenden Flows anzeigen, die während des ausgewählten Zeitraums abgeschlossen wurden oder aktiv waren. Zu den Details gehören die Quell- und Zielerinformationen des Flows, die Gruppen, zu der sie gehören, sofern bekannt; verwendete Dienste und der Typ des letzten Flows.

Wenn Sie eine Zeile erweitern, werden zusätzliche Informationen angezeigt, wie z. B. Informationen zur Anwendungs-ID und zum FQDN der Schicht 7 (L7); wenn der Flow beendet wurde; die Gesamtanzahl der empfangenen/übertragenen Pakete von der Quelle und dem Ziel; und die Quell- und Ziel-IP-Adressen. Sie können auf der in der Tabelle aufgelisteten Detail-Links klicken, um weitere Informationen zu erhalten. Wenn z. B. öffentliche IPs an einem Flow beteiligt waren, können Sie auf den Link **Öffentliche IPs klicken** um die tatsächlichen IP-Adressen dieser öffentlichen IPs anzuzeigen.

Um sich nur auf Berechnungseinheiten mit bestimmten Datenverkehrsflow-Typen zu konzentrieren, wählen Sie im Auswahlbereich für die **Sicherheitsansicht** den Ansichtstyp aus und verwenden Sie das Filterattribut **Flow > Typ**, um die Auswahl einzuschränken.

Wenn Sie die Auswahl eines Flow-Typs im Bereich **Flows** aufheben, werden die Flow-Linien für diesen Flow-Typ aus dem angezeigten Visualisierungsdiagramm ausgeblendet. Sofern keine Filter angewendet werden, die bestimmte Objekte ausschließen, werden alle Gruppen- oder Berechnungseinheiten unabhängig von den Datenverkehrsflow-Typen, die mit diesen Einheiten während des ausgewählten Zeitraums aufgetreten sind, weiterhin angezeigt. Wenn Sie beispielsweise die Auswahl des Flow-Typs „Zulässig“ aufheben, werden alle Linien für zulässige Flows im Diagramm ausgeblendet. Allerdings werden immer noch alle NSX-Objekte angezeigt, selbst die NSX-Objekte, für die während des ausgewählten Zeitraums nur „zulässige“ Datenverkehrsflows vorhanden waren.

Die Richtung eines Flow-Pfeils gibt die Quelle und das Ziel des erkannten Datenverkehrsstroms an. In der Ansicht „Gruppen“ gibt ein selbstreferenzierender Pfeil auf einem Gruppenknoten an, dass mindestens eine Berechnungseinheit mit einer anderen Berechnungseinheit innerhalb dieser Gruppe kommuniziert hat. In einer Ansicht vom Typ „Berechnungen“ gibt ein selbstreferenzierender Pfeil an, dass ein NSX-Objekt in der Berechnungseinheit mit einem anderen NSX-Objekt in derselben Berechnungseinheit kommuniziert hat.

Wenn Sie auf einen Flow-Pfeil zeigen, werden Informationen zu den Flows, die die Gruppe oder die Berechnungseinheit betreffen, angezeigt, wie im folgenden Beispiel für den Knoten „Windows7-group“ dargestellt.



Wenn Sie auf einen Flow-Pfeil klicken, wird das Dialogfeld „Flow-Details“ angezeigt. Es zeigt die Details zu den abgeschlossenen und aktiven Flows an, die während des ausgewählten Zeitraums aufgetreten sind. Um detailliertere Informationen über die Quelle, das Ziel, den Diensttyp und den Typ des Flows zu erhalten, klicken Sie auf die Links in der Tabelle.

Wenn Sie die Ansicht „Berechnungen“ vergrößern, werden in den Flow-Zeilen Informationen zu L4-Ports und -Protokollen angezeigt. Wenn mehr als ein L4-Detail vorhanden ist, wird ein Link mit der Anzahl der zusätzlichen Details auch in der Flow-Zeile angezeigt. Klicken Sie auf die Zahl, wie im folgenden Bild dargestellt, und die Anzahl der L4-Ports und -Protokolle wird angezeigt.



Arbeiten mit NSX Intelligence-Empfehlungen

3

Die NSX Intelligence-Funktion kann Mikrosegmentierungs-Empfehlungen bereitstellen, die auf den Mustern der Netzwerkdatenverkehrsflows basieren, die zwischen den VMs, physischen Servern oder IP-Adressen in Ihrer NSX-T Data Center-Umgebung während eines ausgewählten Zeitraums aufgetreten sind.

Dieses Kapitel enthält die folgenden Themen:

- Verstehen von NSX Intelligence-Empfehlungen
- Generieren einer neuen NSX Intelligence-Empfehlung
- NSX Intelligence-Empfehlungen erneut ausführen
- Erstellte NSX Intelligence-Empfehlungen überprüfen und veröffentlichen
- NSX Intelligence-Empfehlung als JSON-Datei exportieren

Verstehen von NSX Intelligence-Empfehlungen

Zu den von der NSX Intelligence-Funktion generierten Mikro-Segmentierungsempfehlungen zählen Sicherheitsrichtlinien, Richtlinien-Sicherheitsgruppen und Dienste für Anwendungen.

Funktionsübersicht

Die NSX Intelligence-Empfehlungen basieren auf den Datenverkehrs-Flow-Mustern des Netzwerks, die zwischen den Computing-Mitgliedern einer ausgewählten Richtliniengruppe, VMs oder physischen Servern aufgetreten sind. Die Empfehlungen können Sie beim Durchsetzen einer dynamischeren Sicherheitsrichtlinie unterstützen, indem sie die Datenverkehrsmuster der Kommunikation korrelieren, die in Ihrer NSX-T Data Center-Umgebung aufgetreten sind.

- Die Sicherheitsrichtlinien-Empfehlungen entsprechen in ihrer Kategorie Ost-West-Sicherheitsrichtlinien für Anwendungen bei verteilten Firewalls (DFWs).
- Die Sicherheitsgruppen-Empfehlungen bestehen aus den VMs oder physischen Servern, deren Datenverkehrs-Flows für den Zeitraum und die angegebene Begrenzung analysiert wurden.
- Die Dienstempfehlungen sind Dienstobjekte, die von Anwendungen in den von Ihnen angegebenen VMs oder physischen Servern verwendet wurden, aber die Dienste sind noch nicht in der NSX-T Data Center-Bestandsliste definiert.

Übersicht über den Empfehlungsworkflow

Es gibt mehrere Möglichkeiten, die NSX Intelligence-Empfehlungen anzufordern, aber am einfachsten ist es, zur Registerkarte **Planen und Fehler beheben > Empfehlungen** zu navigieren und auf **Neue Empfehlung starten** zu klicken.

Sie geben Folgendes als Eingabe an, wenn Sie eine zu generierende NSX Intelligence-Empfehlung anfordern.

- Alle Berechnungseinheiten (Gruppen, VMs oder physische Server) oder der vorhandene verteilte Firewall-Abschnitt (Distributed Firewall, DFW) in Ihrer NSX-T-Umgebung.
- Zeitbereich, in dem die Netzwerksdatenverkehrsflows für die bereitgestellten Berechnungseinheiten oder bestehenden Sicherheitsregeln analysiert werden sollen.

Für die vorhandenen Regeln kann das System Aktualisierungen empfehlen, die an den Regeln in diesem Abschnitt vorgenommen werden können, um alle Lecks zu schließen, die für eingehende, ausgehende oder anwendungsinterne Flows zwischen den Workloads entdeckt wurden. Weitere Informationen hierzu finden Sie unter [Generieren einer neuen NSX Intelligence-Empfehlung](#).

Nachdem die Empfehlungsanalyse abgeschlossen ist, können Sie die Details der Empfehlung anzeigen und bei Bedarf die Empfehlung ändern, bevor sie veröffentlicht wird. Einzelheiten dazu finden Sie unter [Erstellte NSX Intelligence-Empfehlungen überprüfen und veröffentlichen](#).

Sie können eine generierte NSX Intelligence-Empfehlung auch in eine JSON-formatierte Datei exportieren. Ändern Sie diese JSON-Datei bei Bedarf mit einem externen REST API-Tool, bevor Sie sie zur Verarbeitung an NSX Policy Manager senden. Weitere Informationen hierzu finden Sie unter [NSX Intelligence-Empfehlung als JSON-Datei exportieren](#).

Grundlegendes zur Generierung von NSX Intelligence-Empfehlungen

Basierend auf dem Datenverkehrsumfang, den Sie zum Zeitpunkt des Starts der Generierung einer Empfehlung ausgewählt haben, wählt die Dienstaufgabe „Empfehlung“ nicht segmentierte Ingress- (eingehend), Egress- (ausgehend) oder anwendungsinterne Datenverkehrsflows von und zwischen den Entitäten des ausgewählten Empfehlungsgrenzwerts aus.

Die Flows werden dann durch den Dienst (Port oder Protokoll) aggregiert, mit dem diese Flows kommunizieren. Die Quellen und Ziele für jeden der Flows für einen bestimmten Dienst werden dann gruppiert. Während der Gruppierung wird versucht, vorhandene Gruppen, die bereits in der Bestandsliste vorhanden sind, basierend auf dem vom Benutzer angegebenen Schwellenwert für das übereinstimmende Verhältnis wiederzuverwenden.

Wenn keine vorhandene Gruppe gefunden wird, die den festgelegten Gruppierungsschwellenwert erfüllen kann, wird eine neue Gruppe erstellt.

Basierend auf dem Wert, den Sie für die Option **Regeln erstellen für** festlegen, werden bei der Erstellung einer Empfehlungsregel nur die Datenverkehrsflows in einer bestimmten Richtung berücksichtigt. Wenn der Geltungsbereich des Datenverkehrsflows der gesamte Datenverkehr war, eingehend und ausgehend, oder eingehend und innerhalb der Anwendung, dann werden die Datenverkehrsflows in diesen Richtungen aggregiert, um die auf dem Dienst basierende Regel zu bilden.

Nehmen Sie diese Flows, z. B.

- Begrenzung wird mithilfe von VM1 und VM2 festgelegt
- Gruppen: CG mit VM1 und VM2 als Mitglieder
- Gruppen: G3 mit VM3 und VM4 als Mitglieder
- Angenommener Übereinstimmungsschwellenwert: 50%

Die nicht segmentierten Datenverkehrsflows lauten wie folgt.

- VM3 zu VM1 über SSH
- VM1 zu VM2 über SSH

Im Folgenden ist die resultierende Mikrosegmentierungsempfehlung aufgeführt, bei der es sich um eine einzelne Regel für SSH handelt.

Neue Quellgruppe	Zielgruppe	Dienst	Angewendet-auf Gruppe
Gruppe mit VM1 und VM3 als Mitglieder	CG mit VM1, VM2 als Mitglieder	SSH	Gruppen-CG mit VM1 und VM2 als Mitglieder

Wenn die Datenverkehrsflows von außerhalb der konfigurierten Maske privater IP-Adressen stammen, werden die Flows von und zu solchen IP-Adressen, die nicht in der privaten IP-Präfixliste enthalten sind, als „ANY“ markiert.

Beachten Sie die folgenden nicht segmentierten Flows.

- ANY-Flows zu VM1 über SSH
- Flows von VM1 zu VM3 über SSH
- Begrenzung wird mithilfe von VM1 und VM2 festgelegt
- Die definierte Gruppe ist CG mit VM1 und VM2 als Mitglieder

In diesem Fall werden die eingehenden und ausgehenden Flows bei der Aggregation zu ANY-Flows von VM1 zu VM1 und VM3 über SSH.

Dies führt wiederum zu der folgenden Mikrosegmentierungsregel.

Quelle	Ziel	Dienst	Angewendet auf
ANY	[VM1] in CG, [VM3] in G3	SSH	CG [VM1, VM2]

Hinweis Alle Regeln werden immer nur auf die Mitglieder der Empfehlungsgrenze angewendet, die Sie vor dem Generieren der Empfehlung angegeben haben. Die Grundzusammenfassung dient dazu, die Anzahl der Regeln zu reduzieren, die basierend auf dem Dienst entstehen würden.

Generieren einer neuen NSX Intelligence-Empfehlung

Die Funktion für NSX Intelligence-Empfehlungen bietet Empfehlungen zur Unterstützung der Mikro-Segmentierung Ihrer Anwendungen.

Das Generieren einer NSX Intelligence-Empfehlung beinhaltet Empfehlungen für Sicherheitsrichtlinien, Richtlinien-Sicherheitsgruppen und Dienste für die Anwendung. Die Empfehlungen werden basierend auf dem Datenverkehrsmuster bei der Kommunikation zwischen virtuellen Maschinen (VMs) und physischen Servern in Ihrem NSX-T Data Center erstellt.

Sie können eine Empfehlung generieren, indem Sie die Eingabeentitäten von Gruppen oder 100 VMs und physischen Servern oder eine Kombination aus Gruppen, VMs und physischen Servern oder vorhandenen Sicherheitsrichtlinien auswählen. Die Gesamtanzahl der VMs und physischen Server, die Sie als Eingabe auswählen können, darf 100 dieser Entitäten nicht überschreiten. Die Gesamtanzahl der effektiven VMs und physischen Server, die Sie in einer Eingabe verwenden können, die Gruppen, VMs oder physische Server enthält, darf 250 Eingabeentitäten nicht überschreiten.

Wenn Sie z. B. 50 VMs und 50 physische Server als Teil Ihrer Empfehlungseingabeentitäten auswählen, können Sie nur Gruppen in Kombination mit nicht mehr als 150 Computing-Mitgliedern auswählen.

Wichtig Sie können nur eine neue Empfehlung für Sicherheitsgruppen generieren, die im Richtlinienmodus erstellt wurden. Die Sicherheitsgruppen müssen mindestens einen der unterstützten Mitgliedstypen aufweisen, damit die Funktion NSX Intelligence eine Empfehlungsanalyse für diese Sicherheitsgruppen starten kann. Zu den unterstützten Mitgliedstypen gehören virtuelle Maschinen, physische Server, virtuelle Netzwerkschnittstellen (VIFs), logische Ports und logische Switches. Wenn mindestens ein unterstützter Mitgliedstyp in der Sicherheitsgruppe enthalten ist, kann die Empfehlungsanalyse fortgesetzt werden, aber nicht unterstützte Mitgliedstypen werden während der Empfehlungsanalyse nicht berücksichtigt.

Es gibt mehrere Möglichkeiten, eine Empfehlung mithilfe der NSX Intelligence-Benutzeroberfläche zu generieren. In der folgenden Vorgehensweise werden die verfügbaren Methoden beschrieben.

Voraussetzungen

- Aktivieren Sie die Funktion NSX Intelligence 3.2 oder höher auf der NSX Application Platform. Weitere Informationen finden Sie im *Aktivieren und Aktualisieren von VMware NSX Intelligence 3.2*-Dokument.

- Stellen Sie sicher, dass Sie über die erforderlichen Rechte zum Generieren von Empfehlungen verfügen. Weitere Informationen hierzu finden Sie unter [Rollenbasierte Zugriffssteuerung in NSX Intelligence](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://<nsx-manager-ip-address>` mit den entsprechenden Rechten bei einem NSX Manager an.
- 2 Initiiieren Sie die Generierung einer neuen Empfehlung mithilfe einer der folgenden Methoden.

Startpunkt	Nächster Schritt
Wählen Sie Planen und Fehler beheben > Empfehlungen aus.	Klicken Sie auf Neue Empfehlungen starten .
Wählen Sie als Empfehlungen für eine Gruppe Planen und Fehler beheben > Entdecken und Ergreifen von Aktionen aus.	<ol style="list-style-type: none"> 1 Stellen Sie sicher, dass die Ansicht Gruppen im Ansichtsauswahlbereich Sicherheit ausgewählt ist. 2 Klicken Sie mit der rechten Maustaste auf den Knoten für die Gruppe, für die Sie eine Empfehlung generieren möchten. 3 Wählen Sie Empfehlungen starten im Dropdown-Menü aus.
Für Empfehlungen für VMs oder physische Server wählen Sie Planen und Fehler beheben > Entdecken und Ergreifen von Aktionen .	<p>Wählen Sie mindestens eine VM oder einen physischen Server oder eine Kombination aus beidem aus.</p> <ol style="list-style-type: none"> 1 Klicken Sie im Ansichtsauswahlbereich Sicherheit auf den Pfeil nach unten neben Gruppen und wählen Sie Berechnungen. 2 Klicken Sie auf Alle Typen anzeigen und wählen Sie VMs oder Physische Server. Alternativ können Sie in der Liste „Verfügbare Elemente“ bestimmte VMs oder physische Server auswählen. 3 Klicken Sie auf Übernehmen. 4 Klicken Sie auf das Stabsymbol für Empfehlungen  links im Flows-Balken. 5 Wählen Sie Empfehlungen für die gefilterten Berechnungen starten.

- 3 Ändern Sie im Assistenten **Neue Empfehlung starten** den Standardwert für das Textfeld **Empfehlungsname**.

Benennen Sie die Anwendung, für die die Segmentierung durchgeführt wird. Der Name wird als Präfix für die Namen aller empfohlenen Gruppen und Regeln verwendet, die während der Empfehlungsanalyse erstellt werden.

- 4 Ändern Sie den Standardwert für das Textfeld **Beschreibung**, um die Informationen über die Empfehlung leichter wieder aufzurufen.

- 5 Definieren oder ändern Sie die VMs oder physischen Server, die als Begrenzung für die Sicherheitsrichtlinien-Empfehlung verwendet werden sollen.
 - a Klicken Sie in **Ausgewählte Elemente im Geltungsbereich** auf **Entitäten auswählen**. Wenn Sie die Gruppen, die VMs oder die physischen Server bereits ausgewählt haben, klicken Sie auf den Link zur Anzahl der ausgewählten Entitäten, um Ihre aktuelle Auswahl zu bearbeiten.
 - b Klicken Sie im Dialogfeld **Entitäten auswählen** auf **Gruppen**, um eine oder mehrere Gruppen auszuwählen. Um die VMs oder physischen Server auszuwählen, die Sie als Begrenzung für die Analyse verwenden möchten, klicken Sie auf die Registerkarte **VMs** oder auf die Registerkarte **Physische Server** und treffen Sie Ihre Auswahl.
Sie können Gruppen und bis zu 100 VMs oder physische Server auswählen, aber nicht mehr als 250 effektive Berechnungseinheiten, die für den Empfehlungsgrenzwert verwendet werden sollen. Deaktivieren Sie diejenigen, die Sie nicht einschließen möchten. Sie können auch auf **Filter** klicken und die Attribute auswählen, die zum Filtern der Gruppen, der VMs oder der physischen Server verwendet werden, die ausgewählt werden sollen.
 - c Klicken Sie auf **Speichern**.
 - d (Optional) Wenn das System festgestellt hat, dass mit den Gruppen, die Sie im vorherigen Schritt ausgewählt haben, ein vorhandener Abschnitt für verteilte Firewall (DFW) verknüpft ist, wählen Sie im Dialogfeld **Abschnitt „Verteilte FW“ auswählen** aus, ob Sie den vorhandenen Abschnitt für verteilte Firewall (DFW) verwenden oder einen neuen erstellen möchten. Klicken Sie auf **Speichern**.

Im Assistenten **Neue Empfehlung starten** gibt der Zahlenlink im Textfeld **Ausgewählte Elemente im Geltungsbereich** die Anzahl der ausgewählten Entitäten an.

Wenn Sie während der Empfehlungsanalyse die Verwendung eines vorhandenen Abschnitts für verteilte Firewall (DFW) ausgewählt haben, gibt das System den Abschnitt an, der unter dem Textfeld **Ausgewählte Elemente im Geltungsbereich** angezeigt wird.

- 6 Ändern Sie im Textfeld **Zeitbereich** optional den Standardwert, der zum Generieren der Empfehlung verwendet werden soll.

Der Standardwert für den Zeitbereich ist **Letzten 1 Monat**. Netzwerksdatenverkehrs-Flows, die zwischen den ausgewählten VMs oder physischen Servern oder einer Gruppe von VMs oder physischen Servern im Zeitbereich aufgetreten sind, werden während der Empfehlungsanalyse verwendet. Weitere Werte zur Auswahl sind **Letzte 1 Stunde**, **Letzte 12 Stunden**, **Letzte 24 Stunden**, **Letzte 1 Woche**, **Letzte 2 Wochen** oder **Letzter 1 Monat**.

- 7 Erweitern Sie den Abschnitt **Erweiterte Optionen** und ändern Sie bei Bedarf die zugewiesenen Standardwerte.

Wenn Sie keinen vorhandenen DFW-Abschnitt verwenden, können Sie die standardmäßig zugewiesenen Werte ändern. Wenn Sie einen vorhandenen DFW-Abschnitt verwenden möchten, werden die in diesem Abschnitt angezeigten Werte aus diesem vorhandenen DFW-Abschnitt bezogen.

- Wählen Sie im Dropdown-Menü **Regeln erstellen für** den Typ der Datenverkehrsflows aus, der in der Empfehlungsanalyse berücksichtigt werden soll. Die Standardeinstellung ist **All Traffic**.
 - **Eingehender und ausgehender Datenverkehr** – Alle Datenverkehrsflow-Typen, die von innerhalb der Anwendungsgrenze nach außerhalb der Grenze und von außerhalb der Anwendungsgrenze nach innerhalb der Grenze fließen.
 - **Eingehender Datenverkehr** – Nur Datenverkehrsflows, die außerhalb ihrer Anwendungsbegrenzung liegen, werden berücksichtigt.
 - **Gesamter Datenverkehr** – Alle ausgehenden, eingehenden und interne Anwendungsdatenverkehrs-Flow-Typen werden berücksichtigt.
 - **Eingehender und in der Anwendung abgewickelter Datenverkehr** – Alle Datenverkehrsflow-Typen, die von inner- und außerhalb Ihrer Anwendungsbegrenzung stammen, werden berücksichtigt.
- Wählen Sie im Dropdown-Menü **Standardregel** die Konnektivitätsstrategie aus, die verwendet werden soll, um die Standardregel für die Sicherheitsrichtlinie zu erstellen. Eine geeignete Aktion wird basierend auf dem Wert der Konnektivitätsstrategie auf der Regel festgelegt. Der Standardwert lautet **Keine**.
 - **Negativliste** – Erstellt eine standardmäßige Genehmigungsregel.
 - **Positivliste** – Erstellt eine standardmäßige Ablageregel.
 - **Keine** – Es wird keine Standardregel erstellt.
- Ändern Sie bei Bedarf den Standardwert für die **Empfehlungsausgabe**.

Computergestützt ist der verwendete Standardausgabemodus. Dieser Modus bedeutet, dass die von der Empfehlungs-Engine generierte DFW-Richtlinienempfehlung Gruppen enthält, deren Mitglieder VMs, physische Server oder beides sind. Wenn der **IP-basierte**-Empfehlungsausgabemodus ausgewählt ist, enthält die generierte DFW-Richtlinienempfehlung Gruppen, deren Mitglieder IPSet-Objekte mit einer statischen Liste von IP-Adressen sind. Eine IP-basierte Empfehlung ist nicht fest an eine VM gebunden. Wenn eine VM gelöscht und ihre IP-Adresse einer neuen VM zugewiesen wird, wird die neue VM derselben Gruppe zugewiesen. Die DFW-Richtlinien für die Gruppe werden auch auf die neue VM angewendet.

- d Ändern Sie bei Bedarf den Wert für **Empfehlungsdiensttyp**.
Der Standardtyp ist **L4-Dienste**, der sich aus dem entsprechenden Layer 4-Port und -Protokoll zusammensetzt. Alternativ können Sie **L7-Kontextprofile** für Layer-7-Kontextprofile auswählen.
 - e Ändern Sie den Standardwert für den **Schwellenwert für Gruppenwiederverwendung** so, wie Sie es für die Erstellung der Regelempfehlung für angemessen halten.
Sie können den prozentualen Schwellenwert zwischen 10 und 100 festlegen. Der Wert gibt an, wie streng das System Gruppen wiederverwendet, um die erkannten Flows abzudecken, die nicht mikrosegmentiert sind. Verwenden Sie diesen Wert, um zu steuern, ob vorhandene Gruppen wiederverwendet oder neue Gruppen erstellt werden sollen. Die Gruppenwiederverwendungsfunktion ist für jeden Empfehlungsauftrag mit vorhandener Sicherheitsrichtlinie oder neuer Sicherheitsrichtlinie anwendbar.
Wenn dieser Wert auf 100 gesetzt wird, können nur Gruppen als zusätzliche Regelquellen oder -ziele ausgewählt werden, die genau dieselben Mitglieder haben wie die Berechnungsentitäten, die das System gruppieren möchte. Die Verwendung eines sehr hohen Werts kann jedoch dazu führen, dass mehr neue Gruppen erstellt werden, da vorhandene Gruppen weniger wahrscheinlich in geänderten Regeln wiederverwendet werden.
Wenn Sie diesen Wert auf niedrigere Werte wie 10 oder 20 festlegen, können auch Gruppen mit anderen Mitgliedern als den Berechnungsentitäten, die das System gruppieren möchten, als zusätzliche Regelquellen oder -ziele ausgewählt werden. Die Verwendung eines niedrigeren Werts kann zu einer Wiederverwendung aggressiver Gruppen führen, weshalb weniger neue Gruppen empfohlen werden.
 - f Ändern Sie bei Bedarf die im Textfeld **Flows ausschließen** ausgewählten Standardwerte, um die Flow-Typen des Datenverkehrs anzugeben, die Sie bei der Empfehlungsanalyse ausschließen möchten.
Diese Funktion ist ab NSX Intelligence 3.2.1 verfügbar. Die Standardwerte lauten **Broadcast-Flows** und **Multicast-Flows**. Diese Flow-Typen sind nicht relevant für Regeln für Anwendungskategorien. Durch den Ausschluss von Broadcast-Flows, Multicast-Flows oder beider Flow-Typen kann die Analyse der DFW-Regelempfehlung optimiert werden.
- 8** Um mit der Empfehlungsanalyse zu beginnen, klicken Sie auf **Ermittlung starten**.
- Die Empfehlungen werden seriell verarbeitet. Im Durchschnitt kann es zwischen 3 und 4 Minuten dauern, bis die Verarbeitung einer Empfehlung abgeschlossen ist, je nachdem, ob noch weitere Empfehlungen verarbeitet werden müssen. Wenn die Anzahl der zu analysierenden Datenverkehr-Flows zwischen den VMs und physischen Servern umfangreich ist, kann das Generieren einer Empfehlung zwischen 10 und 15 Minuten dauern.
- In der Tabelle **Empfehlungen** werden die Empfehlungen angezeigt, die Sie initiiert haben (siehe folgende Abbildung).

Name	Status	Eingabeelemente	Empfohlene Entitäten	Überwachung
REC 201201 08:23:57	Warten	1 Gruppe(n), 7 VM(s)	N/A	<input checked="" type="checkbox"/> Ein
REC 201201 07:03:44	Bereit zum Veröffentlichen	1 Gruppe(n)	4 Regel(n), 4 Gruppe(n), 1Dienst(e)	<input checked="" type="checkbox"/> Ein
REC 201201 06:59:10	Veröffentlicht	1 Gruppe(n)	3 Regel(n), 6 Gruppe(n), 1Dienst(e)	<input type="checkbox"/> Aus
REC 201201 06:54:14	Bereit zum Veröffentlichen	1 Gruppe(n)	4 Regel(n), 4 Gruppe(n), 2Dienst(e)	<input checked="" type="checkbox"/> Ein

- Sie können die Status der Empfehlungsanalyse in der Spalte **Status** der Tabelle **Empfehlungen** verfolgen. Es gibt folgende Status-Phasen: Warten, Ermittlung wird ausgeführt, Bereit zum Veröffentlichen und Veröffentlicht. Wenn das System keine Empfehlung generiert, wird der Wert **Status** auf Keine Empfehlungen verfügbar festgelegt. Wenn die Empfehlungsanalyse aus irgendeinem Grund fehlgeschlagen ist, wird der Status Fehlgeschlagen angezeigt.
- In der Spalte **Eingabeentitäten** werden die Elemente aufgelistet, die zum Generieren der Empfehlung verwendet wurden. Wenn Sie auf den verknüpften Text in dieser Spalte klicken, wird das Dialogfeld **Ausgewählte Entitäten** im schreibgeschützten Modus angezeigt.
- In der Spalte **Überwachung** wird angegeben, ob Änderungen für die ursprünglichen Eingabeentitäten überwacht werden, die zum Generieren der Empfehlung verwendet werden. Diese Funktion steht für Empfehlungen mit dem Status Bereit zum Veröffentlichen, Keine Empfehlungen verfügbar oder Fehlgeschlagen zur Verfügung. Sie können die Option **Überwachung** ein- oder ausschalten. Wenn der Umschalter aktiviert ist, werden Änderungen im Geltungsbereich der Eingabeentitäten oder an der Konnektivitätsstrategie ständig überprüft.
- Wenn bei einer der verwendeten Eingabeentitäten Änderungen vorgenommen wurden, wird das Symbol für eine erkannte Änderung neben dem Status Bereit zum Veröffentlichen, Keine Empfehlungen verfügbar oder Fehlgeschlagen angezeigt. Sie können die Änderungen überprüfen und die Empfehlung erneut ausführen. Weitere Informationen hierzu finden Sie unter [NSX Intelligence-Empfehlungen erneut ausführen](#).

- Wenn Sie auf das Arbeitsflächensymbol  auf der rechten Seite der Empfehlungszeile klicken, wird die Visualisierung der ausgewählten Entitäten auf der grafischen Arbeitsfläche unter der Benutzeroberfläche **Planen und Fehler beheben > Entdecken und Ergreifen von Aktionen** angezeigt. Wenn der angezeigte Empfehlungsstatus **Veröffentlicht** lautet, werden empfohlene Gruppen auf der grafischen Arbeitsfläche **Entdecken und Ergreifen von Aktionen** angezeigt, wenn Sie auf das Arbeitsflächensymbol klicken.
- 9 Wenn der Wert für **Status** **Bereit zum Veröffentlichen** ist, überprüfen Sie die generierte Empfehlung und entscheiden Sie, ob Sie sie veröffentlichen möchten. Siehe [Erstellte NSX Intelligence-Empfehlungen überprüfen und veröffentlichen](#).

NSX Intelligence-Empfehlungen erneut ausführen

Wenn das Symbol für eine erkannte Änderung neben einem Status **Bereit zum Veröffentlichen**, **Keine Empfehlungen verfügbar oder Fehlgeschlagen** erscheint, überprüfen Sie die Änderungen im ursprünglichen Geltungsbereich der Eingabeeinheiten der NSX Intelligence-Empfehlung. Führen Sie bei Bedarf die Empfehlungsanalyse erneut aus.

Das Symbol für eine erkannte Änderung  zeigt an, dass einige Änderungen an den Eingabeelementen vorgenommen wurden, die zum Generieren der vorherigen NSX Intelligence-Empfehlung verwendet wurden. Wenn mindestens eine der folgenden Bedingungen auftritt, wird das Symbol für erkannte Änderungen in der Tabelle Empfehlungen neben der betroffenen Empfehlung angezeigt.

- Zu den ursprünglich ausgewählten Entitäten, die zur Erstellung der NSX Intelligence-Empfehlung verwendet wurden, wurden neue effektive Mitglieder hinzugefügt oder daraus entfernt.
- Wenn sich der „Anwendungsbereich“ der Sicherheitsrichtlinie gegenüber dem Wert, der zu Beginn des NSX Intelligence-Empfehlungsprozesses verwendet wurde, geändert hat.

Voraussetzungen

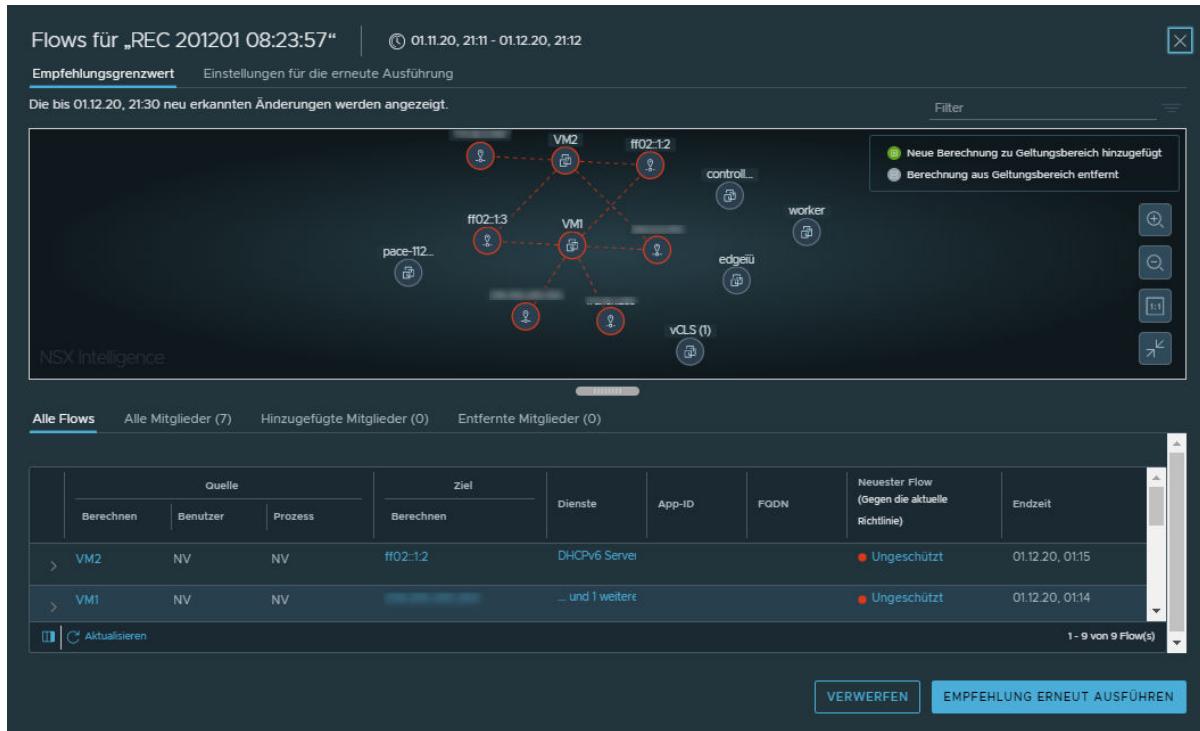
- Sie müssen zuvor eine NSX Intelligence-Empfehlung generiert haben. Siehe [Generieren einer neuen NSX Intelligence-Empfehlung](#).
- Stellen Sie sicher, dass Sie über die erforderlichen Rechte zum erneuten Ausführen von NSX Intelligence-Empfehlungen verfügen. Weitere Informationen hierzu finden Sie unter [Rollenbasierte Zugriffssteuerung in NSX Intelligence](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://<nsx-manager-ip-address>` mit den entsprechenden Rechten bei einem NSX Manager an.
- 2 Wählen Sie **Planen und Fehler beheben > Empfehlungen** aus.

- 3 Um die NSX Intelligence-Empfehlung zu überprüfen und erneut zu erstellen, wählen Sie eine der folgenden Methoden aus.
 - Klicken Sie auf das Symbol für eine erkannte Änderung  rechts neben dem Status und wählen Sie **Empfehlung erneut ausführen** aus.
 - Klicken Sie auf der linken Seite der Zeile der Empfehlung auf das Dreipunkt-Menü  und wählen Sie **Überprüfen und erneut ausführen** aus.
- 4 Überprüfen Sie die Änderungen im Dialogfeld **Überprüfen und erneut ausführen**.

Ein Dialogfeld ähnlich dem folgenden wird angezeigt.



The screenshot shows the 'Flows' dialog for a specific recording period from 01.11.20, 21:11 to 01.12.20, 21:12. The title bar includes the recording name 'REC 201201 08:23:57'. Below the title, there's a section for 'Empfehlungsgrenzwert' (Recommendation threshold) with a note: 'Die bis 01.12.20, 21:30 neu erkannten Änderungen werden angezeigt.' (Changes detected since 01.12.20, 21:30 are displayed). A 'Filter' button is also present.

The main area displays a network visualization with nodes labeled VM2, ff02-12, ff02-13, VM1, control..., worker, edgeui, and vCLS(1). Nodes VM2, ff02-12, ff02-13, VM1, and vCLS(1) have red outlines, while others have grey outlines. A legend indicates: 'Neue Berechnung zu Geltungsbereich hinzugefügt' (New calculation added to validity range) and 'Berechnung aus Geltungsbereich entfernt' (Calculation removed from validity range).

Below the visualization, there are tabs for 'Alle Flows' (selected), 'Alle Mitglieder (7)', 'Hinzugefügte Mitglieder (0)', and 'Entfernte Mitglieder (0)'. A table lists the flows:

Quelle			Ziel	Dienste	App-ID	FQDN	Neuester Flow (Gegen die aktuelle Richtlinie)	Endzeit
	Berechnen	Benutzer						
> VM2	NV	NV	ff02:12	DHCPv6 Server			● Ungeschützt	01.12.20, 01:15
> VM1	NV	NV	[redacted]	... und 1 weitere			● Ungeschützt	01.12.20, 01:14

At the bottom right of the dialog are buttons for 'VERWERFEN' and 'EMPFEHLUNG ERNEUT AUSFÜHREN'.

Das Visualisierungsdiagramm in der oberen Hälfte des Dialogfelds zeigt die Berechnungsentitäten, die seit dem Generieren der vorherigen Empfehlung hinzugefügt oder entfernt wurden. Ein grau umrandeter Berechnungsentitätsknoten zeigt an, dass er aus dem Geltungsbereich der Empfehlungsbegrenzung entfernt wurde. Ein Knoten mit dem grünen Rand zeigt an, dass die neue Berechnungsentität dem Geltungsbereich der Empfehlungsbegrenzung hinzugefügt wurde.

- a Klicken Sie auf die Registerkarten **Alle Flows** und **Alle Mitglieder**, um die Flows und Berechnungsentitäten zu überprüfen, die für die Generierung der Empfehlung in Betracht gezogen werden.
- b Um Änderungen an der Berechnungsentität, die als Eingabeeinheit verwendet wird, zu überprüfen, klicken Sie auf die Registerkarte **Hinzugefügte Mitglieder** oder **Entfernte Mitglieder**.

- 5 (Optional) Wenn Sie zu den ursprünglichen Berechnungsentitäten wechseln möchten, die als Grenzwert für die vorherige Empfehlungsanalyse verwendet werden, klicken Sie auf die Registerkarte **Einstellungen für die erneute Ausführung** und ändern Sie die Einstellungen nach Bedarf.
- 6 Um das Dialogfeld zu verlassen, ohne eine weitere Empfehlungsanalyse zu generieren, klicken Sie auf **Verwerfen**.
- 7 Klicken Sie zum Generieren einer weiteren Empfehlungsanalyse auf **Empfehlung erneut ausführen**.

Ergebnisse

Nachdem Sie **Empfehlung erneut ausführen** ausgewählt haben, wird die zuvor generierte Empfehlung gelöscht und kann nicht wiederhergestellt werden. Die NSX Intelligence-Funktion generiert die Empfehlung mithilfe der geänderten Eingabeelementen als Empfehlungsbegrenzung neu. Neu erkannte Flows und Berechnungsentitäten für den ausgewählten Zeitraum sind auch in der Empfehlungsanalyse enthalten. Datenverkehrsströme für Berechnungsentitäten, die aus den ursprünglichen Eingabeeinheiten gelöscht wurden, werden in der Analyse nicht berücksichtigt.

Nächste Schritte

Nachdem die neue Empfehlung den Status **Bereit** zum Veröffentlichen hat, überprüfen Sie die Empfehlung mithilfe der Informationen in [Erstellte NSX Intelligence-Empfehlungen überprüfen und veröffentlichen](#).

Erstellte NSX Intelligence-Empfehlungen überprüfen und veröffentlichen

Wenn die generierte NSX Intelligence-Empfehlung den Status **Bereit** zum Veröffentlichen erreicht, können Sie die Empfehlung überprüfen, sie bei Bedarf ändern und entscheiden, ob sie veröffentlicht werden soll.

Voraussetzungen

- Generieren Sie eine neue Empfehlung. Siehe [Generieren einer neuen NSX Intelligence-Empfehlung](#).
- Vergewissern Sie sich, dass Sie über die erforderlichen Berechtigungen verfügen, bevor Sie die Empfehlungen veröffentlichen. Weitere Informationen hierzu finden Sie unter [Rollenbasierte Zugriffssteuerung in NSX Intelligence](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://<nsx-manager-ip-address>` mit den entsprechenden Rechten bei einem NSX Manager an.
- 2 Klicken Sie auf **Planen und Fehler beheben > Empfehlungen**.

- 3 (Optional) Um die Liste der anzuzeigenden Empfehlungen einzuschränken, klicken Sie in der oberen rechten Ecke der Benutzeroberfläche auf **Filtern**. Klicken Sie auf **Filter anwenden** und wählen Sie mindestens einen Filter aus dem Dropdown-Menü aus.

Wählen Sie nach dem Klicken auf **Filter anwenden** beispielsweise **Grundlegende Details > Überwachung > Ein** aus, um nur die Empfehlungen anzuzeigen, für die der Überwachungsparameter auf „Ein“ festgelegt ist.

- 4 (Optional) Wenn Sie die generierte Empfehlung nicht verwenden möchten, klicken Sie auf das und wählen Sie **Löschen** aus.
- 5 Um mit der Überprüfung und Verwaltung der Details einer Empfehlung mit dem Status **Bereit** zum Veröffentlichen zu beginnen, klicken Sie auf den Link des Empfehlungsnamens oder klicken Sie auf das und wählen Sie **Überprüfen und veröffentlichen** aus.

Der Assistent **Empfehlungen** wird ähnlich der folgenden Abbildung angezeigt. Im Bereich **Empfehlungen überprüfen** werden die Details zu den Empfehlungen in einer geteilten Ansicht angezeigt. In der oberen Hälfte des Bereichs wird eine Visualisierung der Empfehlungen im grafischen Format angezeigt. In der unteren Hälfte des Bereichs werden die Empfehlungen im tabellarischen Format aufgelistet.

Quelle	Ziel	Dienste	App-ID	FQDN	Neuester Flow (Gegen die aktuelle Richtlinie)	Endzeit
Berechnen	Berechnen					
> VM1 NV NV	... und 1 weiter...				● Ungeschützt	01.12.20, 01:14
> VM1 NV NV	ff02:12	DHCPv6 Server			● Ungeschützt	01.12.20, 01:11

- 6 Verwenden Sie die obere Hälfte des Bereichs, um die grafische Visualisierung der Empfehlungen zu untersuchen.

Sie können auf bestimmte Knoten und Flow-Pfeile klicken, um die Details für die Empfehlungen anzuzeigen. Sie können auf den Flow-Pfeil zwischen zwei Gruppenknoten verweisen, um zu sehen, welche Richtlinienregeln zwischen Gruppen angewendet oder welche Dienste erstellt wurden. Klicken Sie mit der rechten Maustaste auf den Flow-Pfeil, um die Empfehlung nach den entsprechenden Richtlinienregeln zu filtern.

Knoten mit dem Empfehlungszeichen  am Rand weisen darauf hin, dass der Knoten eine empfohlene Gruppe darstellt. Sie können mit der rechten Maustaste auf den Knoten einer Gruppenempfehlung klicken, die Gruppe umbenennen oder die dieser Gruppe angehörenden Berechnungsentitätsmitglieder bearbeiten. Sie können auch mit der rechten Maustaste auf einen Gruppenknoten klicken, um ihn umzubenennen, anzuzeigen oder seine Mitglieder zu bearbeiten, und **Filtern nach** auswählen, um die aktuelle Gruppe als Filter zu verwenden, mit dem Details zur generierten Empfehlung angezeigt werden.

Änderungen, die mithilfe der grafischen Ansicht der Empfehlungen vorgenommen wurden, werden in der Tabelle in der unteren Hälfte des Fensterspeichers angezeigt. Ebenso werden Änderungen an den Empfehlungsinformationen der Tabelle in der grafischen Visualisierung widergespiegelt.

- 7 In der unteren Hälfte des Bereichs **Empfehlungen überprüfen** können Sie die tabellarische Ansicht der Empfehlungen verwenden, um die Details zu den Regeln, Gruppen und Diensten zu sehen, die in der Empfehlung enthalten sind. Verwenden Sie die Registerkarte **Für Empfehlungen verwendete Flows**, um ungeschützten Datenverkehrsflows anzuzeigen, die zum Generieren der Empfehlungen verwendet wurden.

Sie können alle Empfehlungsdetails prüfen und ändern, indem Sie auf die Registerkarte **Regeln, Gruppen oder Dienste** klicken.

Im Abschnitt **Empfohlene Richtlinien** werden Zahlen auf den Registerkarten **Regeln, Gruppen** und **Dienste** angezeigt. Diese Zahlen geben die Anzahl der empfohlenen Regeln, Gruppen und Dienste an. Sie waren nicht in der NSX-T-Bestandsliste vorhanden, als die Empfehlungen generiert wurden. Beispielsweise werden im Screenshot oben auf der Registerkarte **Dienste** null empfohlene Dienste angezeigt. Die Dienste, die von den Gruppen verwendet werden, waren zum Zeitpunkt der Empfehlungsgenerierung in der NSX-T-Bestandsliste vorhanden. Aus diesem Grund werden keine neuen Dienste empfohlen.

Alle Änderungen, die an den Regeln auf der Registerkarte **Regeln** vorgenommen werden (z. B. das Hinzufügen, Löschen oder Bearbeiten einer Regel oder eines Abschnitts), werden sofort in der Regeltablette und im grafischen Visualisierungsbereich angezeigt. In der Tabelle „Regeln“ zeigen Regeln, die links von ihrem Namen das Badge **Neu** aufweisen, dass es sich um eine neu erstellte Regel handelt und nicht um eine bereits vorhandene DFW-Regel,

die ausgewählten Entitäten zugeordnet ist. Wenn eine bestehende Regel verwendet wird, die nicht geändert wurde, wird die Zeile für die Regel abgeblendet dargestellt. Wenn die Empfehlungs-Engine eine vorhandene Regel geändert hat, wird die Zeile für diese Regel nicht abgeblendet angezeigt und weist nicht das Badge „Neu“ daneben auf.

- a Um die Details in den Spalten **Quellen**, **Ziele** oder **Angewendet auf** zu bearbeiten, zeigen Sie auf die entsprechende Spalte und klicken Sie auf das Bearbeitungssymbol (Bleistift). Überprüfen Sie im resultierenden Dialogfeld (z. B. **Quellgruppen festlegen**) die neu empfohlene Regel oder vorhandene Gruppen, die die Empfehlungs-Engine ausgewählt hat. Wenn Sie Änderungen vornehmen, klicken Sie auf **Speichern**.
- b Um zu definieren, wie die Pakete beim Zutreffen der DFW-Regel verarbeitet werden sollen, wählen Sie **Zulassen**, **Verwerfen** oder **Ablehnen** in der Spalte **Aktion** aus.
- c Um die DFW-Regel zu aktivieren oder zu deaktivieren, schalten Sie die Schaltschaltfläche auf der rechten Seite der Spalte **Aktion** entsprechend ein oder aus. Standardmäßig ist die generierte Regel zum Veröffentlichungszeitpunkt der Empfehlung auf **Activated** festgelegt.
- d Um die Details zu den Gruppen in der Empfehlung zu überprüfen, klicken Sie auf die Registerkarte **Gruppen**.
Bevor Sie eine Gruppe löschen, stellen Sie sicher, dass die Gruppe von keinen Regeln verwendet wird.
- e Klicken Sie auf den Link in der Spalte **Mitglieder**, um die Details zu den VMs, IPs und physischen Servern zu überprüfen, die für die Gruppenempfehlung festgelegt wurden.
- f Klicken Sie auf das  neben dem Namen der Gruppe und wählen Sie **Bearbeiten** aus, um Änderungen an der Gruppenempfehlung vorzunehmen.
- g Klicken Sie auf die Registerkarte **Dienste** und überprüfen Sie die Details.
h Klicken Sie auf das  neben dem Namen des Dienstes und wählen Sie **Bearbeiten** aus, um Änderungen am Namen oder an der Beschreibung vorzunehmen.
Bevor Sie einen Dienst löschen, stellen Sie sicher, dass der Dienst von keinen Regeln verwendet wird.
- 8 Um mit der Veröffentlichung der Empfehlung fortzufahren, klicken Sie auf **Fortfahren**. Alternativ können Sie auf **Später fortfahren** klicken, um alle von Ihnen vorgenommenen Änderungen zu speichern und die Sitzung der Empfehlungsbewertung zu beenden.

- 9 Definieren Sie im Bereich **Sequenzieren und Veröffentlichen** die Reihenfolge, in der die neu empfohlenen Sicherheitsrichtlinien in Bezug auf die bestehenden Regeln der DFW angewendet werden sollen.
 - a Wählen Sie die Zeile für die neue Sicherheitsrichtlinienempfehlung aus.
 - b Klicken Sie bei einer der aufgelisteten Sicherheitsrichtlinien auf das  auf der linken Seite der Zeile.
 - c Um die ausgewählte Zeile für die neu empfohlene Sicherheitsrichtlinie über oder unter die Zeile der vorhandenen Sicherheitsrichtlinie zu verschieben, wählen Sie **Ausgewählte Richtlinien über diese Richtlinie verschieben** oder **Ausgewählte Richtlinien unter diese Richtlinie verschieben** aus dem angezeigten Menü.
Alternativ können Sie die Zeile für die aktuell ausgewählte neue Richtlinienempfehlung nach oben oder unten in die gewünschte Reihenfolge ziehen.

10 Klicken Sie auf **Veröffentlichen**.

- Um die Überprüfung der Empfehlung abzubrechen, klicken Sie auf **Abbrechen**.
- 11 Klicken Sie im Dialogfeld **Empfehlungen veröffentlichen** auf **Ja**.
- 12 Klicken Sie im Dialogfeld **Veröffentlichte Richtlinien** auf **Abbrechen**, um das Dialogfeld zu schließen, oder auf **In Tabelle „Verteilte Firewall“ anzeigen**, um die Sicherheitsrichtlinien anzuzeigen, die gerade auf der Registerkarte **Sicherheit > Verteilte Firewall > Alle Regeln** veröffentlicht wurden.
- Im Bereich **Planen und Fehler beheben > Empfehlungen** wurde die Spalte **Status** der gerade von Ihnen veröffentlichten Empfehlung nun in **Veröffentlicht** in der Tabelle **Empfehlungen** geändert.

Ergebnisse

Nachdem die Empfehlungen für die Sicherheitsrichtlinie erfolgreich veröffentlicht wurden, befinden Sie sich im schreibgeschützten Modus auf der Registerkarte **Planen und Fehler beheben > Empfehlungen**. Um die veröffentlichten Regel-Empfehlungen anzuzeigen und zu verwalten, wechseln Sie zu **Sicherheit > Verteilte Firewall**.

Wichtig Nachdem Sie die Regel-Empfehlungen veröffentlicht haben, zeigt die Visualisierung weiterhin die betroffenen Flows zwischen den Berechnungsentitäten als orangefarbene Pfeile (ungeschützte Flows) an, bis neue Flows zwischen den betroffenen Berechnungsentitäten generiert werden. Die Visualisierung meldet nur Datenverkehr-Flows basierend auf der Zeit, in der sie auf dem Host aufgetreten sind, und spiegelt nicht den Regelsatz wider, der nach dem Auftreten der Datenverkehr-Flows veröffentlicht wurde. Nachdem der Regelsatz veröffentlicht und neue Datenverkehr-Flows generiert wurden, werden die neuen Flows als grüne Pfeile (zulässige Flows) angezeigt.

NSX Intelligence-Empfehlung als JSON-Datei exportieren

Wenn eine generierte NSX Intelligence-Empfehlung den Status Bereit zum Veröffentlichen erreicht, haben Sie die Möglichkeit, sie in eine JSON-Datei zu exportieren. Sie können Änderungen an dieser Datei vornehmen, bevor Sie sie als REST API-Anfrage zur Verarbeitung an NSX Policy Manager senden.

Voraussetzungen

- Generieren Sie eine neue Empfehlung. Siehe [Generieren einer neuen NSX Intelligence-Empfehlung](#).
- Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen, bevor Sie die Empfehlung exportieren. Weitere Informationen hierzu finden Sie unter [Rollenbasierte Zugriffssteuerung in NSX Intelligence](#).

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://<nsx-manager-ip-address>` mit den entsprechenden Rechten bei einem NSX Manager an.
- 2 Klicken Sie auf **Planen und Fehler beheben > Empfehlungen**.
- 3 (Optional) Listen Sie nur die NSX Intelligence-Empfehlungen mit dem Status Bereit zum Veröffentlichen auf.
 - a Klicken Sie im oberen rechten Bereich auf **Filter**.
 - b Wählen Sie im Dropdown-Menü **Filter anwenden** die Filter **Status** und **Bereit zum Veröffentlichen** aus.
 - c Klicken Sie auf **Übernehmen**.
- 4 Klicken Sie in der Liste der Bereit zum Veröffentlichen-Empfehlungen auf das  links neben dem Namen der NSX Intelligence-Empfehlung, die Sie exportieren möchten. Wählen Sie **Als JSON exportieren** aus dem Dropdown-Menü.

Der folgende Codeausschnitt zeigt ein Beispiel für einen Teilinhalt einer exportierten JSON-Datei.

```
{
  "resource_type": "Infra",
  "id": "Infra",
  "children": [
    {
      "resource_type": "ChildDomain",
      "id": "default",
      "marked_for_delete": false,
      "Domain": {
        "resource_type": "Domain",
        "id": "default",
        "children": [
          {
            "resource_type": "SubDomain"
          }
        ]
      }
    }
  ]
}
```

```

    "resource_type": "ChildGroup",
    "marked_for_delete": false,
    "Group": {
        "resource_type": "Group",
        "id": "Group-384fe490-837e-11eb-9688-
dd7fccb572d0-904d61f0-0d71-4bc9-ac18-632b6b02efc9",
        "display_name": "Group-1 (REC 210312 01:59:18)",
        "description": "Created from REC 210312 01:59:18",
        "marked_for_delete": false,
        "expression": [
            {
                "resource_type": "ExternalIDExpression",
                "marked_for_delete": false,
            ...
            ...
        "marked_for_delete": false
    }
}

```

- 5** Nehmen Sie alle erforderlichen Änderungen an der exportierten JSON-Datei vor, bevor Sie sie als REST API-Anforderung senden, die von NSX Policy Manager verarbeitet werden kann.

Beachten Sie, dass Sie ab NSX-T Data Center 3.1.1 zuerst die Zeile mit der Eigenschaft "id" : "Infra" aus der exportierten JSON-Datei entfernen müssen, bevor Sie die JSON-Nutzlast als PATCH-Anfrage senden. Andernfalls erhalten Sie eine 400 Bad Request-Antwort von NSX Policy Manager zurück.

- 6** Übermitteln Sie mit einem externen REST API-Tool die JSON-Datei mit der NSX Intelligence-Empfehlung zur Verarbeitung an NSX Policy Manager.

Wenn Sie die NSX Intelligence-Empfehlung als JSON-Nutzlast über ein externes REST API-Tool, wie z. B. Postman, an Ihr NSX-T Data Center-Setup senden, weiß die NSX Intelligence-Anwendung nicht, dass die Empfehlung erfolgreich verarbeitet wurde. Diese NSX Intelligence-Empfehlung wird weiterhin mit dem Status Bereit zum Veröffentlichen in der Liste der Empfehlungen aufgeführt. Wenn Sie versuchen, die Empfehlung zu überprüfen, indem Sie auf ihren Namen klicken, erhalten Sie die folgende Meldung.

Es wurden keine unveröffentlichten empfohlenen Richtlinien gefunden.
Eine Version dieser empfohlenen Richtlinien wurde möglicherweise bereits mit einem externen Tool in Ihr NSX-T Data Center importiert und veröffentlicht, oder sie wurden gelöscht.

- 7** Nachdem Sie die exportierte Empfehlung erfolgreich als JSON-Nutzlast übermittelt haben, löschen Sie diese Empfehlung manuell aus der Liste der Bereit zum Veröffentlichen-Empfehlungen in der Tabelle **Planen und Fehler beheben > Empfehlungen**.

Erkennen von verdächtigem Netzwerkdatenverkehr in NSX-T Data Center

Sie können verdächtigen Datenverkehr, wie z. B. abnormale Aktivitäten und böswilliges Verhalten, in Ihrer NSX-T Data Center-Umgebung erkennen, indem Sie die ab Version 3.2 der NSX Intelligence-Funktion bereitgestellte NSX Suspicious Traffic-Funktion verwenden.

Verwenden Sie die Informationen in diesem Abschnitt, um mit der NSX Suspicious Traffic-Funktion zu beginnen, Erkennungsereignisse zu analysieren und die NSX Suspicious Traffic-Detektor-Definitionen zu verwalten.

Dieses Kapitel enthält die folgenden Themen:

- Erste Schritte beim Erkennen von verdächtigem Netzwerkdatenverkehr in NSX-T Data Center
- Analysieren der NSX Suspicious Traffic-Erkennungsereignisse
- Verwalten der NSX Suspicious Traffic Detector-Definitionen

Erste Schritte beim Erkennen von verdächtigem Netzwerkdatenverkehr in NSX-T Data Center

Machen Sie sich mit den Voraussetzungen vertraut, die erfüllt sein müssen, bevor Sie mit der Verwendung der NSX Suspicious Traffic-Funktion beginnen können. Erhalten Sie einen Überblick über die Funktionsweise, lernen Sie die mit der Funktion verwendeten Terminologien kennen und bereiten Sie die Detektoren vor, die Sie zum Überwachen des Netzwerkdatenverkehrsflows in Ihrer NSX-T Data Center-Umgebung verwenden möchten.

Voraussetzungen zur Verwendung der NSX Suspicious Traffic-Funktion

Ihre NSX-T Data Center-Umgebung muss die folgenden Voraussetzungen erfüllen, bevor Sie die NSX Suspicious Traffic-Funktion verwenden können.

- Stellen Sie sicher, dass alle Lizenz- und Softwareanforderungen erfüllt sind, einschließlich der Konfiguration der NSX Intelligence-Funktion.
Einzelheiten dazu finden Sie unter [Systemanforderungen für die NSX Suspicious Traffic-Funktion](#).
- Stellen Sie sicher, dass Sie über eine NSX-T-Rolle verfügen, die zur Verwendung der NSX Suspicious Traffic-Funktion autorisiert ist.

Um während einer NSX Manager-Sitzung auf alle NSX Suspicious Traffic-Funktionen zuzugreifen, muss dem NSX-T Benutzerkonto, das Sie verwenden, eine der folgenden NSX-T Data Center integrierten Rollen zugewiesen werden. Weitere Informationen hierzu finden Sie unter [Rollenbasierte Zugriffssteuerung in NSX Intelligence](#).

- Unternehmens-Admin
- Sicherheits-Admin

Systemanforderungen für die NSX Suspicious Traffic-Funktion

Bevor Sie mit der Verwendung der NSX Suspicious Traffic-Funktion beginnen können, müssen Ihre NSX-T Data Center-Umgebung und die NSX Intelligence-Funktion bestimmte Lizenz- und Softwareanforderungen erfüllen.

Lizenzanforderungen

Eine der folgenden Lizenzen muss während Ihrer NSX Manager-Sitzung in Kraft sein. Im Folgenden sind die verschiedenen NSX Data Center Lizenzen aufgeführt, die die NSX Suspicious Traffic-Funktion unterstützen.

- NSX Data Center Evaluation
- NSX-T Evaluation
- NSX Advanced Threat Prevention (Nur für Kunden, die die Lizenz zuvor erworben haben.)
- NSX Advanced Threat Prevention Add-On für die NSX Distributed Firewall mit Threat Prevention
- NSX Advanced Threat Prevention Add-On für NSX Distributed Firewall oder NSX Advanced oder NSX Enterprise Plus
- NSX Distributed Firewall mit Advanced Threat Prevention
- NSX Gateway Firewall mit Advanced Threat Prevention
- NSX Advanced Threat Prevention-Add-On für NSX Gateway-Firewall
- NSX-T Advanced mit NSX Advanced Threat Prevention Add-On for NSX Distributed Firewall oder NSX Advanced oder NSX Enterprise Plus
- NSX-T Enterprise Plus mit NSX Advanced Threat Prevention Add-On für NSX Distributed Firewall oder NSX Advanced oder NSX Enterprise Plus

Softwareanforderungen

Sie müssen die folgenden Softwareanforderungen erfüllen, bevor Sie mit der Verwendung der NSX Suspicious Traffic-Funktion beginnen können.

- Installieren Sie NSX-T Data Center 3.2 oder höher.
- Stellen Sie die VMware NSX® Application Platform mithilfe eines erweiterten Formfaktors bereit.

- Aktivieren Sie die Anwendung NSX Intelligence 3.2 oder höher auf der NSX Application Platform.
- Konfigurieren Sie die Funktion NSX Intelligence 3.2 oder höher so, dass nur Netzwerkdatenverkehrsdaten für bestimmte eigenständige Hosts oder Hostcluster erfasst werden, die überwacht werden sollen. Die NSX Suspicious Traffic-Funktion wird nur auf eigenständigen Hosts oder Hostclustern unterstützt, für die die Datenerfassung aktiviert ist. Informationen zum Konfigurieren der Einstellungen für die Funktion NSX Intelligence 3.2 oder höher finden Sie im Dokument *Aktivieren und Aktualisieren von VMware NSX Intelligence*.
- Aktivieren Sie die NSX Network Detection and Response-Funktion, wenn Sie mit Aktivitäten arbeiten, um eine tiefere Analyse der erkannten verdächtigen Datenverkehrsergebnisse mithilfe der VMware NSX® Advanced Threat Prevention-Cloud-Dienste zu erhalten. Weitere Informationen zur Funktionsaktivierung finden Sie im Dokument *Handbuch zur Aktivierung und Verwaltung von VMware NSX Network Detection and Response*, das mit der Funktion NSX Intelligence 3.2 oder höher unter <https://docs.vmware.com/de/VMware-NSX-Intelligence/index.html> bereitgestellt wird.

Hinweis Um die Funktionen für eine tiefere Analyse der erkannten böswilligen oder anomalen Ereignisse bereitzustellen, erfordert die NSX Network Detection and Response-Funktion, dass Ihre NSX-T Data Center 3.2-Umgebung oder höher mit dem Internet verbunden ist.

Übersicht über die Funktion NSX Suspicious Traffic

Ziel der NSX Suspicious Traffic-Funktion ist es, verdächtige oder anomale Verhaltensweisen des Netzwerkdatenverkehrs in Ihrer NSX-T Data Center-Umgebung zu erkennen.

Funktionsweise

Nachdem Sie die Voraussetzungen erfüllt haben, kann die Funktion NSX Suspicious Traffic mit der Erstellung von Netzwerkbedrohungsanalysen zu den Flow-Daten des Ost-West-Netzwerkverkehrs beginnen, die die NSX Intelligence-Anwendung von Ihren berechtigten NSX-T-Workloads (Hosts oder Cluster von Hosts) erfasst hat. Die NSX Intelligence-Anwendung speichert die erfassten Daten und persistiert diese Daten 30 Tage lang. Die NSX Suspicious Traffic-Funktion analysiert die Daten und kennzeichnet verdächtige Aktivitäten mithilfe der unterstützten Detektoren. Sie können die Informationen zu den erkannten Bedrohungsergebnissen auf der Registerkarte **Erkennungsergebnisse** auf der Seite der NSX Suspicious Traffic-Benutzeroberfläche anzeigen.

Wenn diese Option aktiviert ist, sendet die NSX Network Detection and Response-Funktion zur tieferen Analyse die verdächtigen Ereignisse an den VMware NSX® Advanced Threat Prevention-Cloud-Dienst. Wenn der NSX Advanced Threat Prevention-Dienst feststellt, dass bestimmte verdächtige Ereignisse miteinander in Zusammenhang stehen, ordnet er diese verdächtigen Ereignisse einer Aktivität zu. Der Dienst organisiert dann die Ereignisse in dieser Aktion in einer Zeitachse und visualisiert sie auf der NSX Network Detection and Response-Benutzeroberfläche. Alle Bedrohungsergebnisse werden über die NSX Network Detection and

Response-Benutzeroberfläche visualisiert. Die einzelnen Bedrohungsergebnisse und -aktivitäten können von Ihrem Netzwerksicherheitsteam weiter untersucht werden. Der NSX Advanced Threat Prevention-Cloud-Dienst ruft in regelmäßigen Abständen Updates zu den zuvor erkannten Bedrohungen ab und aktualisiert bei Bedarf die Bildschirme der Visualisierungsoberfläche.

Unterstützte Detektoren

Die folgende Tabelle listet die unterstützten Detektoren auf, die die NSX Suspicious Traffic-Funktion verwendet, um den erkannten verdächtigen Netzwerksdatenverkehr zu klassifizieren. Die von diesen Detektoren generierten Erkennungen sind möglicherweise mit bestimmten Techniken oder Taktiken im [MITRE ATT&CK® Framework](#) verknüpft.

Diese Detektoren sind standardmäßig ausgeschaltet, und Sie müssen jeden Detektor, den Sie in Ihrer NSX-T-Umgebung verwenden möchten, explizit einschalten. Unter [NSX Suspicious Traffic-Detektoren aktivieren](#) finden Sie weitere Informationen zu den Voraussetzungen und zum Einschalten der Detektoren.

Sie können die Ausschlusslisten und den Wahrscheinlichkeitswert für einige der Definitionen dieser unterstützten Detektoren mithilfe der Registerkarte **Detector-Definitionen** verwalten. Einzelheiten dazu finden Sie unter [Verwalten der NSX Suspicious Traffic Detector-Definitionen](#).

Tabelle 4-1. Zur Erkennung verdächtigen Datenverkehrs verwendete Detektor-Kategorien

Detektor-Name	Beschreibung
Daten-Upload/Download	Erkennen Sie ungewöhnlich große Datenübertragungen (Uploads/Downloads) für einen Host.
Ziel-IP-Profiler	Erkennen von Versuchen interner Geräte, ungewöhnliche Verbindungen zu anderen internen Hosts herzustellen.
DNS-Tunneling	Erkennen von Versuchen eines internen Geräts, verdeckt mit einem externen Server zu kommunizieren, indem es den DNS-Verkehr missbraucht.
Algorithmen zur Domänengenerierung (Domain Generation Algorithm, DGA)	Erkennen von Anomalien in den von einem internen Host durchgeföhrten DNS-Lookups, die durch DGA-Malware verursacht werden können.
Horizontale Portprüfung	Erkennen, wenn ein Eindringling versucht, einen oder mehrere Ports oder Dienste über mehrere Systeme hinweg zu scannen (Sweeping).
LLMNR/NBT-NS Poisoning and Relay	Erkennen, wenn eine VM ein ungewöhnliches Antwortmuster auf LLMNR/NBT-NS-Anforderungen zeigt.
NetFlow-Signalprüfung	Erkennen von Signalprüfungsverhalten eines internen Hosts.
Auslassung von Netzwerksdatenverkehr	Erkennen, wenn ungewöhnlich viel Datenverkehr durch eine verteilte Firewallregel unterbrochen wird.
Port-Profiler	Erkennen, wenn ein interner Clienthost auf einem ungewöhnlichen Port mit einem externen Host kommuniziert.
Port-Profiler des Servers	Erkennen, wenn ein interner Host mit einem anderen internen Host auf einem ungewöhnlichen Port verbunden ist.
Remotedienste	Erkennen verdächtiger Verhaltensweisen für Remoteverbindungen wie Telnet, SSH und VNC.

Tabelle 4-1. Zur Erkennung verdächtigen Datenverkehrs verwendete Detektor-Kategorien (Fortsetzung)

Detektor-Name	Beschreibung
Ungewöhnlicher Port verwendet	Erkennen von L7-Anwendungs-ID-Datenverkehr, der nicht mit dem standardmäßig zugewiesenen Port/Protokoll übereinstimmt. Beispielsweise wird SSH-Datenverkehr über einen nicht standardmäßigen Port anstelle des Standard-Ports 22 ausgeführt.
Ungewöhnliches Muster des Netzwerkdatenverkehrs	Erkennen Sie Anomalien im Zeitreihenprofil eines Hosts.
Vertikale Portprüfung	Erkennen, wenn ein Eindringling versucht, mehrere offene Ports oder Dienste eines einzelnen Systems anzugreifen (Scanning).

Mit der NSX Suspicious Traffic-Funktion verwendete Terminologie

Machen Sie sich mit den Terminologien der NSX Suspicious Traffic-Funktion vertraut.

Terminologie	Definition
Anomalie-Ereignis	Die in der vorherigen NSX Intelligence-Version verwendete Terminologie, in der die Funktion NSX-Anomalieerkennung (jetzt NSX Suspicious Traffic) als Technologievorschaufunktion eingeführt wurde. Diese Terminologie wird jetzt durch Erkennungsergebnis ersetzt.
Aktivität	Eine korrelierte Gruppe von Vorfällen, die sich über einen bestimmten Zeitraum auf ein oder mehrere Geräte auswirken. Wenn die NSX Network Detection and Response-Funktion aktiviert ist, werden gegebenenfalls Links zu Aktivitäten auf der NSX Suspicious Traffic-Benutzeroberfläche angezeigt.
Konfidenzbewertung	Die Punktzahl, die berechnet wurde, um anzugeben, wie sicher das System ist, dass ein Ereignis basierend auf den proprietären Algorithmen, die die NSX Suspicious Traffic-Funktion verwendet, anomal ist.
Erkennungsergebnis	Eine Netzwerkdatenverkehrsaktivität, die von dem abweicht, was als Standard betrachtet oder erwartet wird. Die Daten werden von einem NSX Suspicious Traffic-Detektor generiert.
Detektor	Ein Sensor zur Erkennung von Ereignissen in Ihrem Netzwerk-Datenverkehrsflow. Ein Detektor ist einer einzelnen MITRE ATT&CK-Kategorie oder -Technik zugeordnet.
Auswirkungsbewertung	Eine Punktzahl, die von einem proprietären Algorithmus berechnet wird, der eine Kombination aus der Konfidenzbewertung für das Erkennungsergebnis und dessen Schweregrad verwendet, wenn es korrekt erkannt wurde.
Schweregrad	Gibt an, wie schwerwiegend eine Bedrohung ist. Die gültigen Werte sind Kritisch, Hoch, Mittel oder Niedrig.
Taktik	Stellt den Grund dar, warum ein Angreifer eine Aktion mit einer ATT&CK-Technik oder Untertechnik ausführt. Informationen zum MITRE ATT&CK-Framework finden Sie unter https://attack.mitre.org/ .
Technik	Gibt an, wie ein Angreifer versucht, sein taktisches Ziel durch eine Aktion zu erreichen. Informationen zum MITRE ATT&CK-Framework finden Sie unter https://attack.mitre.org/ .

NSX Suspicious Traffic-Detektoren aktivieren

Bevor Bedrohungen oder verdächtige Netzwerkdatenverkehrsdaten in Ihrer NSX-T Data Center-Umgebung erkannt werden können, müssen Sie die zu verwendenden NSX Suspicious Traffic-Detektoren manuell einschalten. Nur die aktivierte Detektoren werden für die Überwachung verdächtiger Netzwerkdatenverkehrsereignisse verwendet.

Voraussetzungen

- Überprüfen Sie, ob die unter [Systemanforderungen für die NSX Suspicious Traffic-Funktion](#) aufgeführten Lizenz- und Softwarevoraussetzungen erfüllt sind.
- Sie müssen bei NSX Manager mit einer der folgenden integrierten NSX-T Data Center-Rollen angemeldet sein. Weitere Informationen hierzu finden Sie unter [Rollenbasierte Zugriffssteuerung in NSX Intelligence](#).
 - Unternehmens-Admin
 - Sicherheits-Admin

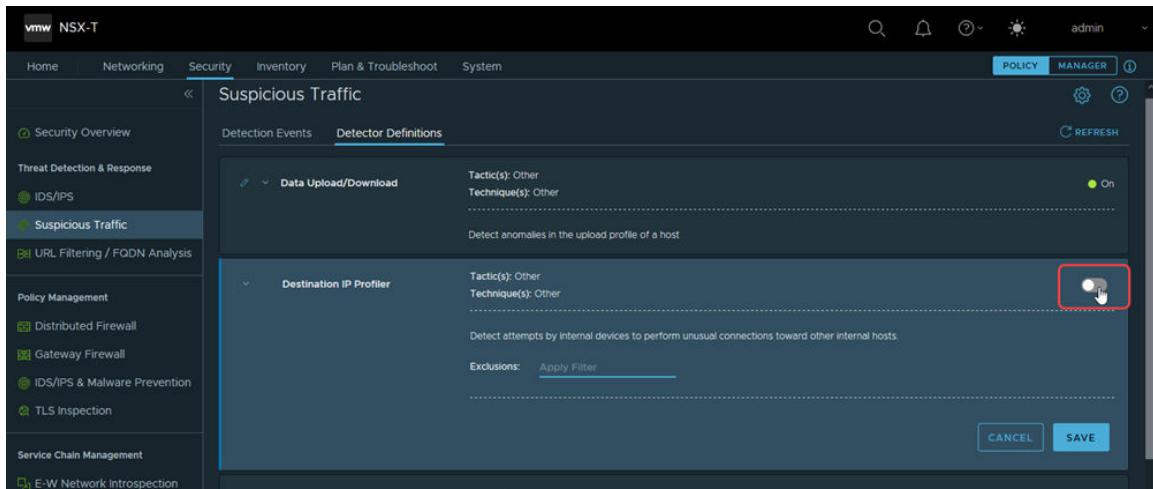
Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://<nsx-manager-ip-address>` mit den entsprechenden Rechten bei einer NSX Manager-Appliance an.
- 2 Verwenden Sie die folgenden Schritte, um einen unterstützten NSX Suspicious Traffic-Detektor einzuschalten, um eine Analyse des Netzwerkdatenverkehrs für die erfassten Datenverkehrsdaten durchzuführen.

Beachten Sie, dass die folgenden Schritte für alle verfügbaren Detektoren gelten, außer für die DNS-basierten Detektoren, die manuell konfiguriert werden müssen, bevor sie verwendet werden können. Informationen zur Konfiguration von DNS-basierten Detektoren finden Sie im nachfolgenden Schritt.

- a Navigieren zur Registerkarte **Sicherheit > Verdächtiger Datenverkehr > Detector-Definitionen**.
- b Suchen Sie nach dem Detektor, den Sie aktivieren möchten, und klicken Sie auf **Bearbeiten** (Stiftsymbol).

- c Suchen Sie den Umschalter ganz rechts in der erweiterten Reihe und klicken Sie auf den Umschalter, um den Detektor einzuschalten, wie in der folgenden Abbildung dargestellt.



- d Klicken Sie auf **Speichern**.
- 3 Um DNS-basierte Detektoren wie „Algorithmen zur Domänenengenerierung“ (Domain Generation Algorithm, DGA) und „DNS-Tunneling“ zu aktivieren, führen Sie die folgenden Schritte nur einmal aus.
- Erstellen Sie ein benutzerdefiniertes DNS-Kontextprofil oder verwenden Sie ein vom System bereitgestelltes Standardkontextprofil.
Weitere Informationen zum Hinzufügen eines Kontextprofils für Version 3.2 oder höher finden Sie im *Administratorhandbuch für NSX-T Data Center* unter <https://docs.vmware.com/de/VMware-NSX-T-Data-Center/index.html>.
 - Erstellen Sie eine Regel für die verteilte Firewall, indem Sie **ANY** in den Spalten **Quellen** und **Ziele** verwenden und das DNS-Kontextprofil nutzen, falls Sie eines erstellt haben.
Weitere Informationen zum Hinzufügen einer Regel für verteilte Firewalls für Version 3.2 oder höher finden Sie im *Administratorhandbuch für NSX-T Data Center* unter <https://docs.vmware.com/de/VMware-NSX-T-Data-Center/index.html>.
 - Navigieren zur Registerkarte **Sicherheit > Verdächtiger Datenverkehr > Detector-Definitionen**.
 - Suchen Sie den DNS-basierten Detektor, den Sie aktivieren möchten, und klicken Sie auf **Bearbeiten** (Bleistiftsymbol).
 - Suchen Sie ganz rechts in der erweiterten Zeile den Umschalter für diesen DNS-basierten Detektor. Um den Detektor einzuschalten, klicken Sie auf den Umschalter.
 - Klicken Sie auf **Speichern**.

Ergebnisse

Die Umschalter für die aktivierte Detektoren werden auf der Registerkarte **Detectordefinitionen** als **Ein** angezeigt.

Nächste Schritte

Verwalten Sie die erkannten verdächtigen Datenverkehrsereignisse. Einzelheiten dazu finden Sie unter [Analysieren der NSX Suspicious Traffic-Erkennungsereignisse](#).

Analysieren der NSX Suspicious Traffic-Erkennungsereignisse

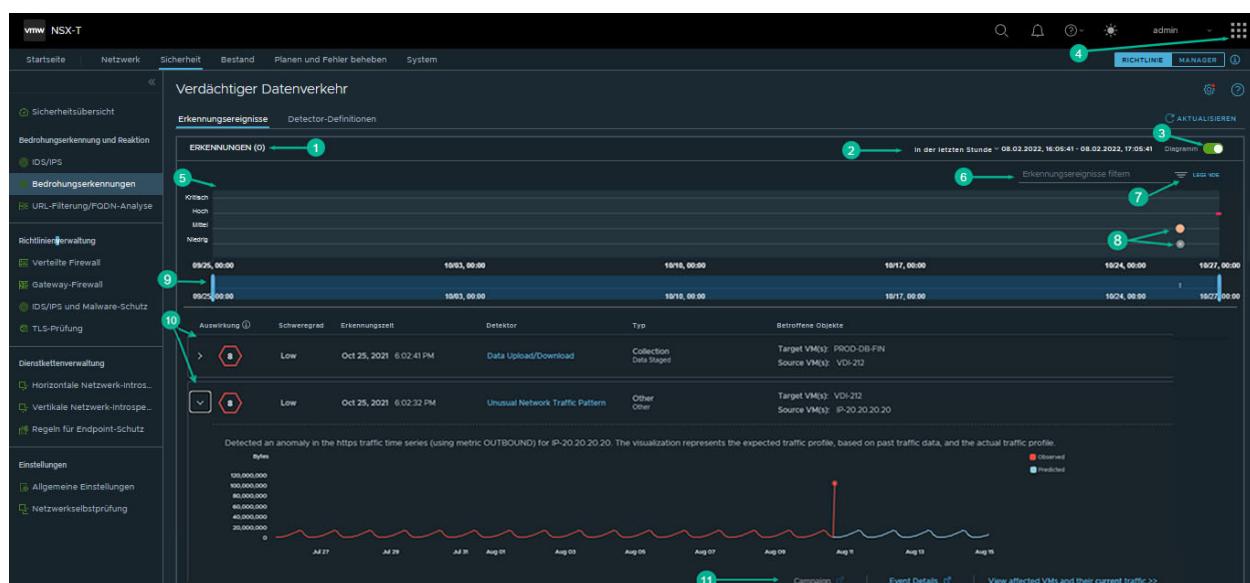
Die NSX Suspicious Traffic-Funktion generiert aus den erfassten Flow-Daten des Netzwerks Analysen zu Netzwerkbedrohungen und meldet die erkannten verdächtigen Ereignisse auf der Seite **Erkennungsereignisse**. Sie können die Erkennungsereignisse entweder in einem Blasendiagramm, in einem Raster oder in beidem anzeigen.

Voraussetzungen

- Die Anwendung NSX Intelligence 3.2 oder höher muss aktiviert sein, und die NSX Suspicious Traffic-Detektoren müssen eingeschaltet werden. Siehe [Erste Schritte beim Erkennen von verdächtigem Netzwerksverkehr in NSX-T Data Center](#).
- Sie müssen bei NSX Manager mithilfe einer der folgenden NSX-T-Rollen angemeldet sein.
 - Unternehmens-Admin
 - Sicherheits-Admin

Verwalten von Erkennungsereignissen

Wenn Sie zu **Sicherheit > Verdächtiger Datenverkehr > Erkennungsereignisse** navigieren, werden die Erkennungsereignisse standardmäßig sowohl in einem Blasendiagramm als auch in einem Raster angezeigt, wie in der folgenden Abbildung dargestellt. In der Tabelle, die dem Bild folgt, werden die nummerierten Abschnitte beschrieben, die im Bild hervorgehoben sind.



Abschnitt	Beschreibung
1	Gibt die Gesamtzahl der Erkennungen verdächtiger Ereignisse an, die das NSX Suspicious Traffic-Funktion während des ausgewählten Zeitraums gemeldet hat.
2	In diesem Abschnitt wählen Sie den Zeitraum aus, den das System verwendet, um zu bestimmen, welche historischen Daten zu den erkannten Ereignissen von NSX Suspicious Traffic auf dieser Seite der Benutzeroberfläche gemeldet werden. Der Zeitraum ist relativ zum aktuellen Zeitpunkt und umfasst einen bestimmten Zeitraum in der Vergangenheit. Der Standardzeitraum ist Letzte 1 Stunde . Um den ausgewählten Zeitraum zu ändern, klicken Sie auf den aktuell ausgewählten Zeitraum und wählen im Dropdown-Menü einen anderen aus. Die verfügbaren Optionen sind Letzte 1 Stunde , Letzte 12 Stunden , Letzte 24 Stunden , Letzte 1 Woche , Letzte 2 Wochen und Letzter 1 Monat .
3	Die Umschaltoption Diagramm bestimmt, ob das Blasendiagramm angezeigt wird. Wenn die Umschaltoption Diagramm deaktiviert ist, werden Informationen über die Erkennungereignisse nur im Raster angezeigt. Standardmäßig ist die Umschaltoption auf Ein gestellt.
4	Wenn die NSX Network Detection and Response-Funktion aktiviert ist, wird bei der Anzeige der NSX Suspicious Traffic-Benutzeroberfläche das Anwendungsstartsymbol  in der oberen rechten Ecke der Benutzeroberfläche angezeigt. Um weitere Details zu den erkannten anomalen Ereignissen über die NSX Network Detection and Response-Benutzeroberfläche anzuzeigen, klicken Sie auf das  und wählen Sie NSX Network Detection and Response aus. Klicken Sie in der NSX Network Detection and Response-Benutzeroberfläche erneut auf das Anwendungsstart-Symbol und wählen Sie NSX-T aus, um zur NSX Suspicious Traffic-Benutzeroberfläche zurückzukehren.
5	Dieses Blasendiagramm bietet eine visuelle Zeitleiste, die zeigt, wann die erkannten Ereignisse während des ausgewählten Zeitraums aufgetreten sind. Jedes Ereignis wird basierend auf dem Schweregrad des Erkennungereignisses dargestellt. Im Folgenden sind die Schweregradkategorien und die entsprechenden Schweregradwerte aufgeführt. <ul style="list-style-type: none"> ■ Kritisch: 75-100 ■ Hoch: 50-74 ■ Mittel: 25-49 ■ Niedrig: 0-24
6	Mit dem Filterbereich können Sie die Erkennungereignisse eingrenzen, die für den ausgewählten Zeitraum angezeigt werden. Klicken Sie auf Erkennungereignisse filtern und wählen Sie aus dem Dropdown-Menü die Filter aus, die Sie anwenden möchten, sowie bestimmte Elemente in dem zusätzlich angezeigten Dropdown-Menü. Zu den verfügbaren Filtern gehören die folgenden. <ul style="list-style-type: none"> ■ Konfidenzbewertung – Die Bewertung, die das System anhand der proprietären Algorithmen, die die NSX Suspicious Traffic-Funktion verwendet, zuweist, je nachdem, wie sicher es ist, dass ein Ereignis anomal ist. ■ Detektor – Ein Sensor zur Erkennung von anomalen Ereignissen im Datenverkehrsflow Ihres Netzwerks. Ein Detektor ist einer einzelnen MITRE ATT&CK-Kategorie oder -Technik zugeordnet. ■ Auswirkungspunktzahl – Eine Punktzahl, die von einem proprietären Algorithmus berechnet wird, der eine Kombination aus der Konfidenzbewertung für das Erkennungereignis und dessen Schweregrad verwendet, wenn es korrekt erkannt wurde. ■ Taktiken – Stellen den Grund dar, warum ein Angreifer eine Aktion unter Verwendung einer ATT&CK-Taktik ausführt. ■ Techniken – Darstellung der Art und Weise, wie ein Angreifer versucht, ein taktisches Ziel seines Angriffs mithilfe bestimmter Techniken/Subtechniken zu erreichen. ■ VMs – Die VMs, die an den erkannten Ereignissen im ausgewählten Zeitraum beteiligt waren.

Abschnitt	Beschreibung
7	<p>Klicken Sie auf Legende um die verschiedenen Arten von Blasen aufzulisten, die im Blasendiagramm angezeigt werden können. In der folgenden Liste werden die einzelnen Blasen und die Art des Erkennungsereignisses, das sie darstellen, beschrieben.</p> <ul style="list-style-type: none"> ■ Persistenz – Der Angreifer versucht, seine Kontrolle über die Systeme in Ihrem Netzwerk aufrechtzuerhalten. ■ Zugang mit Anmeldedaten – Der Angreifer versucht, Kontonamen und Kennwörter zu stehlen. ■ Erkennung – Der Angreifer versucht, mehr über Ihre Netzwerkumgebung zu erfahren. ■ Befehl und Steuerung – Der Angreifer versucht, mit den gefährdeten Systemen zu kommunizieren und die Kontrolle über sie zu erlangen. ■ Lateral Movement – Ein Angreifer versucht, sich in Ihrer Netzwerkumgebung zu bewegen. ■ Erfassung – Ein Angreifer versucht, Informationen zu sammeln, die ihm bei der Verwirklichung seines Ziels behilflich sein könnten. ■ Exfiltration – Der Angreifer versucht, Daten aus Ihrem Netzwerk zu entwenden. ■ Andere – Der Detektor kann keiner spezifischen Taktik zugeordnet werden, wie sie im MITRE ATT&CK Framework definiert ist. ■ Mehrere Ereignisse – Mehr als ein Erkennungsereignis trat im selben Zeitsegment auf. Wenn Sie den Schieberegler für das Zeitfenster nach rechts bewegen, ändert sich der Umfang der angezeigten Blasen. So lässt sich eine Blase „Mehrere Ereignisse“ in mehrere und andere Arten von Blasen aufteilen.
8	Jede Blase im Diagramm stellt ein Erkennungsereignis oder mehrere Ereignisse dar, die während des ausgewählten Zeitraums aufgetreten sind. Die Farbe oder Art der Blase repräsentiert die Taktik, die der Angreifer während des entdeckten Angriffs verwendet hat. Weitere Informationen finden Sie in den Beschreibungen in der Legende .
9	Mit dem Schieberegler für das Zeitfenster können Sie Erkennungsereignisse anzeigen, die innerhalb einer Teilmenge des ausgewählten Zeitraums aufgetreten sind. Der blau hervorgehobene Bereich entspricht der Darstellung im Blasendiagramm. Je weiter Sie den Schieberegler nach rechts oder links bewegen, desto aktueller wird das Blasendiagramm mit den Erkennungsereignissen, die in dem durch den Schieberegler hervorgehobenen Zeitraum aufgetreten sind. Wenn es Erkennungsereignisse gibt, die etwa zur gleichen Zeit aufgetreten sind, werden diese durch eine Blase Mehrere Ereignisse dargestellt. Wenn Sie den Schieberegler nach rechts bewegen, werden Sie feststellen, dass sich die Blase Mehrere Ereignisse in mehrere Blasen erweitert, die die verschiedenen Erkennungsereignisse darstellen, die in diesem Zeitraum aufgetreten sind.

Abschnitt	Beschreibung
10	<p>Das Raster zeigt Informationen zu jedem Erkennungsereignis an, das die NSX Suspicious Traffic-Funktion während des ausgewählten Zeitraums identifiziert hat. Wenn sie nicht erweitert ist, werden in einer Zeile die folgenden wichtigen Ereignisdaten angezeigt.</p> <ul style="list-style-type: none"> ■ Auswirkung – Die Auswirkungspunktzahl, die die NSX Suspicious Traffic-Funktion für das Erkennungsereignis berechnet hat ■ Schweregrad – Gibt an, wie schwerwiegend das Ereignis ist. Mögliche Werte sind „Niedrig“, „Mittel“, „Hoch“ und „Kritisch“. Diese Werte entsprechen den im Blasendiagramm verwendeten Werten. ■ Erkennungszeit – Das Datum und die Uhrzeit, zu dem/der das Ereignis erkannt wurde. ■ Detektor – Der Name des Detektors, den die NSX Suspicious Traffic-Funktion zur Erkennung des Ereignisses verwendet hat. Wenn Sie auf den Namen des Detektors klicken, werden in einem Dialogfeld zusätzliche Informationen zu diesem Detektor angezeigt, z. B. sein Ziel, die ATT&CK-Kategorie und eine Zusammenfassung des Detektors. Der Abschnitt ATT&CK-Kategorie enthält einen Link zur MITRE ATT&CK-Website, auf der Sie weitere Details zu der im Erkennungsereignis verwendeten ATT&CK-Kategorie finden. ■ Typ – Listet die im Erkennungsereignis verwendete Taktik und Technik auf. ■ Betroffene Objekte – Listet die von dem Erkennungsereignis betroffenen Quell-VMs und Ziel-VMs auf. Der Beispiel-Screenshot zeigt auch eine erweiterte Zeile. Wenn eine Zeile erweitert wird, werden zusätzliche Ereignisinformationen angezeigt. Die Details umfassen eine Zusammenfassung des erkannten Ereignisses und eine Erläuterung für die Visualisierung oder zusätzliche Ereignisdaten, die in der erweiterten Zeile angezeigt werden. Im obigen Screenshot wird in der erweiterten Zeile beispielsweise eine Zusammenfassung des erkannten Ereignisses und eine Erläuterung der Visualisierung angezeigt. Nicht alle erkannten Ereignisse werden visuell dargestellt. Für andere werden nur zusätzliche detaillierte Daten angezeigt.
11	<p>In einer erweiterten Zeile können auch ein oder mehrere Links in der unteren rechten Ecke angezeigt werden. Wenn Sie auf einen Link klicken, gelangen Sie zu einer anderen Seite der Benutzeroberfläche, auf der weitere Informationen über das erkannte Ereignis bereitgestellt werden. Im Folgenden sind die verfügbaren Links aufgeführt, sofern sie für das Erkennungsereignis zutreffen.</p> <p>Der folgende Link kann aktiviert sein, auch wenn die NSX Network Detection and Response-Funktion nicht aktiviert ist.</p> <ul style="list-style-type: none"> ■ Betroffene VMs und ihren aktuellen Datenverkehr anzeigen - Wenn Sie auf diesen Link klicken, zeigt das System die Visualisierungsfläche auf der Registerkarte Planen und Fehler beheben an. Es zeigt die Recheneinheiten an, die an dem Erkennungsereignis beteiligt waren. Weitere Informationen hierzu finden Sie unter Arbeiten mit der Ansicht „Berechnungen“. ■ Aktivität – Wenn der NSX Advanced Threat Prevention-Cloud-Dienst dieses Erkennungsereignis als Teil einer Aktivität identifiziert hat, ist dieser Link aktiviert. Wenn Sie auf den Link klicken, werden auf der Seite Aktivitäten der NSX Network Detection and Response-Benutzeroberfläche Details zur Aktivität angezeigt. Weitere Informationen hierzu finden Sie unter Verwalten der Seite „Aktivitäten“. ■ Ereignisdetails – Wenn Sie auf diesen Link klicken, wird eine neue Browserregisterkarte geöffnet und weitere Details zum Erkennungsereignis werden auf der Seite Ereignisprofil der NSX Network Detection and Response-Benutzeroberfläche angezeigt. Weitere Informationen hierzu finden Sie unter Arbeiten mit der Seite „Ereignisse“.

Verwalten der NSX Suspicious Traffic Detector-Definitionen

Auf der Registerkarte **Detector-Definitionen** auf der Seite **Verdächtiger Datenverkehr** werden alle Detectors angezeigt, die derzeit von der NSX Suspicious Traffic-Funktion unterstützt werden.

Ein Detector ist standardmäßig deaktiviert. Sie müssen jeden Detector manuell aktivieren, bevor er mit der Überwachung der Netzwerkdatenverkehrsflows in Ihrer NSX-T-Umgebung beginnen kann. Einzelheiten dazu finden Sie unter [NSX Suspicious Traffic-Detektoren aktivieren](#).

Jeder NSX Suspicious Traffic-Detector, der auf der Registerkarte **Detector-Definitionen** aufgeführt ist, enthält in der Regel Folgendes.

- Detector-Name und -Beschreibung
- Umschaltfläche zum Aktivieren/Deaktivieren
- Schieberegler „Wahrscheinlichkeit (Empfindlichkeit)“

Mit dem Schieberegler können Sie die Wahrscheinlichkeit festlegen, mit der ein Detector eine Warnung generiert. Für eine Erkennung, die unter den Schwellenwert der Wahrscheinlichkeit fällt, verwirft das System das Erkennungsergebnis. Dieser Schieberegler ist nicht für alle Detectors enthalten.

- Ausschlüsse.

Ein VM-Ausschluss ist eine statische Liste von VMs, die die NSX Suspicious Traffic-Funktion von der Überwachung durch den Detector ausschließt. Ob ein Mitglied vom Detector ausgeschlossen wird, hängt bei einem Gruppenausschluss davon ab, wann das System den Detector ausführt. Wenn die Gruppe zum Zeitpunkt der Ausführung des Detectors nicht vorhanden ist, generiert das System möglicherweise eine Warnung in den Systemprotokollen. Wenn die VM zum Zeitpunkt der Ausführung des Detectors nicht vorhanden ist, ignoriert der Detector im Hintergrund die Ausschlusseinstellung. Gruppenausschluss wird nicht von allen NSX Suspicious Traffic-Detectors unterstützt.

Ändern einiger Eigenschaftswerte einer Detector-Definition

Um einige der Standard-Eigenschaftswerte für ausgewählte NSX Suspicious Traffic-Detector-Definitionen zu ändern, verwenden Sie die Registerkarte **Detector-Definitionen**.

Die folgende Abbildung zeigt ein Beispiel für eine Detector-Definition, die sich im Bearbeitungsmodus befindet.



Voraussetzungen

- Die Anwendung NSX Intelligence 3.2 oder höher muss aktiviert sein.
- Sie müssen bei NSX Manager mithilfe einer der folgenden NSX-T-Rollen angemeldet sein.
 - Unternehmens-Admin
 - Sicherheits-Admin

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://<nsx-manager-ip-address>` mit den entsprechenden Rechten bei einer NSX Manager-Appliance an.
- 2 Navigieren zur Registerkarte **Sicherheit > Verdächtiger Datenverkehr > Detector-Definitionen**.
- 3 Suchen Sie nach dem Detector, dessen Definition Sie ändern möchten, und klicken Sie auf **Bearbeiten** (Bleistiftsymbol).
- 4 Um den Detector ein- oder auszuschalten, klicken Sie auf die Umschaltfläche.
- 5 Wenn ein Schieberegler in der Definition enthalten ist, bewegen Sie den Schieberegler auf den gewünschten Wert, den der Detector zum Generieren eines Erkennungsereignisses verwendet.

Wenn Sie den Schieberegler auf einen kleineren Wert setzen, ist es wahrscheinlicher, dass dieser Detector ein Erkennungsereignis generiert.
- 6 Definieren Sie die Ausschlussliste.
 - a Klicken Sie auf „Filter anwenden“ und wählen Sie im Dropdown-Menü **Gruppen** oder **VMs** für die Quelle aus.
 - b Treffen Sie Ihre Auswahl aus der Liste der verfügbaren Gruppen oder VMs.
 - c Klicken Sie auf **Übernehmen**.
- 7 Klicken Sie auf **Speichern**.

Arbeiten mit der NSX Network Detection and Response-Anwendung



Die VMware NSX® Network Detection and Response™-Anwendung bietet eine Reihe von eng integrierten Netzwerkerkennungs- und Reaktionsfunktionen für vertikale und horizontale Sicherheit in Ihrer NSX-T Data Center-Umgebung. Diese Funktion ist ab NSX Intelligence Version 3.2 und NSX-T Data Center Version 3.2 verfügbar.

Dieses Kapitel enthält die folgenden Themen:

- Voraussetzungen zur Verwendung der NSX Network Detection and Response-Anwendung
- Mit der NSX Network Detection and Response-Funktion verwendete Terminologie
- Kennenlernen der NSX Network Detection and Response-Benutzeroberfläche
- Erkunden der Dashboard-Seite
- Verwalten der Seite „Aktivitäten“
- Arbeiten mit der Seite „Hosts“
- Arbeiten mit der Seite „Ereignisse“
- Verwalten der Seite „Vorfälle“
- Arbeiten mit der Seite „Heruntergeladene Dateien“
- Verwenden der Seite „Warnungsmanagement“
- Verwenden des Analyseberichts

Voraussetzungen zur Verwendung der NSX Network Detection and Response-Anwendung

Sie müssen die folgenden Voraussetzungen erfüllen, bevor Sie mit der Verwendung der vollständigen Funktionen der NSX Network Detection and Response-Anwendung beginnen können.

- Machen Sie sich mit dem Hauptziel der NSX Network Detection and Response-Anwendung und ihrem Aktivierungs- und Nutzungsablauf vertraut.

Informationen zu den ersten Schritten finden Sie im *Handbuch zur Aktivierung und Verwaltung von VMware NSX Network Detection and Response*, das mit der Dokumentation zu NSX Intelligence für Version 3.2 oder höher unter <https://docs.vmware.com/de/VMware-NSX-Intelligence/index.html> bereitgestellt wird.

- Aktivieren Sie die Anwendung NSX Network Detection and Response auf der NSX Application Platform.

Informationen zu den Systemanforderungen und zur Anwendungsaktivierung finden Sie im Dokument *Handbuch zur Aktivierung und Verwaltung von VMware NSX Network Detection and Response*, das mit der Dokumentation zu NSX Intelligence für Version 3.2 oder höher geliefert wird, unter <https://docs.vmware.com/de/VMware-NSX-Intelligence/index.html>.

- Stellen Sie sicher, dass Sie über eine NSX-T-Rolle verfügen, die zur Verwendung der NSX Network Detection and Response-Anwendung autorisiert ist.

Um auf alle NSX Network Detection and Response-Funktionen zuzugreifen, muss dem Benutzerkonto, das Sie während Ihrer NSX Manager-Sitzung verwenden, eine der folgenden NSX-T integrierten Rollen zugewiesen werden. Weitere Informationen hierzu finden Sie unter [Rollenbasierte Zugriffssteuerung in NSX Intelligence](#).

- Unternehmens-Admin
- Sicherheits-Admin
- Sicherheitsbeauftragter
- Auditor (schreibgeschützter Zugriff)

Mit der NSX Network Detection and Response-Funktion verwendete Terminologie

Machen Sie sich mit der folgenden Schlüsselterminologie vertraut, die im Zusammenhang mit der NSX Network Detection and Response-Funktion verwendet wird.

Terminologie	Definition
Aktivität	Ein korrelierter Satz von Vorfällen, die sich über einen bestimmten Zeitraum auf eine oder mehrere Arbeitslasten auswirken.
Ereignis	Stellt eine sicherheitsrelevante Aktivität dar, die im überwachten Netzwerk aufgetreten ist. Ein Ereignis kann mehrere Datenflows umfassen (z. B. TCP-Verbindungen), aber es stellt eine einzige Art von Aktivität dar, die zwischen einem bestimmten IP-Adressenpaar innerhalb eines kurzen Zeitraums stattfindet. Mehrere Ereignisse werden automatisch zu Vorfällen zusammengefasst.
Vorfall	Stellt eine sicherheitsrelevante Aktivität dar, die im überwachten Netzwerk aufgetreten ist. Ein Vorfall kann aus einem einzelnen Ereignis oder mehreren Ereignissen bestehen, die automatisch zu einem Vorfall zusammengefasst wurden.
Infektion	Ein Vorfall, der als kritisch eingestuft wurde. Infektionen sollten ohne Verzögerung behandelt werden.

Terminologie	Definition
Störung	Ein Vorfall mit geringem Risiko. In der Regel handelt es sich dabei um potenziell unerwünschte/riskante Aktivitäten, die nicht unbedingt auf eine Gefährdung oder Infektion des überwachten Netzwerks hindeuten. Störungen werden verfolgt, da sie dazu beitragen, ein umfassenderes Lagebild des Netzes zu erstellen.
Bewertung der Auswirkungen eines Ereignisses	Die Gesamt-Auswirkungsbewertung, die für ein von der NSX Network Detection and Response-Funktion erkanntes Ereignis berechnet wurde. Die Punktzahl reicht von 0-100, wobei 100 die gefährlichste Erkennung darstellt. Die folgenden Stufen der Ereignisauswirkungen werden verwendet. <ul style="list-style-type: none"> ■ Niedrig: Auswirkung 1-29 ■ Mittel: Auswirkung 30-69 ■ Hoch: Auswirkung 70-100
Watchlist	Ein Vorfall, der als mittleres Risiko eingestuft wurde. Solche Vorfälle weisen zwar auf ein potenzielles Risiko hin, erfordern aber keine sofortige Aufmerksamkeit. Sie werden genau beobachtet, falls neue Erkenntnisse auftauchen, die ihren Status ändern. So wird beispielsweise ein Vorfall, bei dem eine nicht funktionsfähige Befehls- und Steuerungsinfrastruktur betroffen ist, als beobachtet eingestuft.

Kennenlernen der NSX Network Detection and Response-Benutzeroberfläche

Die NSX Network Detection and Response-Benutzeroberfläche bietet eine zentrale Steuerung für die Verwaltung der in Ihrer NSX-T-Umgebung erkannten Bedrohungsereignisse und korrelierten Aktivitäten sowie für die Anzeige der generierten Berichte über diese Bedrohungen.

Wichtig Um auf die NSX Network Detection and Response-Benutzeroberfläche zuzugreifen, müssen Sie zuerst die NSX Network Detection and Response-Anwendung auf der NSX Application Platform aktivieren. Sie müssen auch eine oder mehrere NSX-Funktionen aktivieren, deren Erkennungsereignisse die NSX Network Detection and Response-Anwendung nutzt. Im *Handbuch zur Aktivierung und Verwaltung von VMware NSX Network Detection and Response* finden Sie eine Anwendungsübersicht und die Details zur Aktivierung.

Bestimmte Elemente der NSX Network Detection and Response-Benutzeroberfläche sind nur sichtbar, wenn Sie die entsprechende Funktion oder Anwendung des Elements aktivieren, die die von der NSX Network Detection and Response-Anwendung genutzten Ereignisse bereitstellt.

Zugreifen auf die Benutzeroberfläche

Wenn Ereignisberichte oder generierte Aktivitäten vorhanden sind, können Sie mithilfe einer der folgenden Methoden auf die NSX Network Detection and Response-Benutzeroberfläche (UI) zugreifen.

- Klicken Sie auf das Symbol für den Anwendungsstart  in der oberen rechten Ecke der Benutzeroberfläche NSX Manager und wählen Sie **NSX Network Detection and Response**.

- Navigieren Sie auf der NSX Manager-Benutzeroberfläche zu **Sicherheit > Sicherheitsübersicht** und klicken Sie auf der Registerkarte **Bedrohungserkennung und Reaktion > Aktivitäten** auf **Zu „Aktivitäten“**.
- Wenn Sie die NSX Intelligence aktiviert haben, navigieren Sie auf der NSX Manager-Benutzeroberfläche zu **Sicherheit > Verdächtiger Datenverkehr**. Erweitern Sie die Zeile für ein erkanntes verdächtiges Ereignis, klicken Sie auf **Aktivitäten** oder **Ereignisdetails**, falls verfügbar. Diese Links werden nur angezeigt, wenn Aktivitäten oder Ereignisberichte für die erkannten verdächtigen Aktionen verfügbar sind.
- Wenn Sie die VMware NSX® Malware-Schutz-Anwendung aktiviert haben, navigieren Sie auf der NSX Manager-Benutzeroberfläche zu **Sicherheit > Malware-Schutz**, erweitern Sie die Zeile für eine gemeldete Malware und klicken Sie entweder auf die **Aktivitäten** oder auf **Ereignisdetails**, falls verfügbar. Diese Links werden nur angezeigt, wenn Aktivitäten oder Ereignisberichte für die erkannte Malware verfügbar sind.

In den folgenden Abschnitten werden die allgemeinen Bereiche beschrieben, die Sie sehen, wenn Sie auf der NSX Network Detection and Response-Benutzeroberfläche navigieren. Auf der linken Seite der Schnittstelle befindet sich das Hauptnavigationsmenü. Oben auf fast jeder Seite befinden sich die Widgets der Anzeigeeinstellungen. Daten, die auf den Seiten der Benutzeroberfläche angezeigt werden, werden mithilfe der von Ihnen ausgewählten Anzeigeeinstellungen angezeigt.

Navigieren auf der Benutzeroberfläche

Sie können das Hauptnavigationsmenü auf der linken Seite der Browserseite verwenden, um auf die entsprechenden Seiten der obersten Ebene der NSX Network Detection and Response-Benutzeroberfläche zuzugreifen. Sie können dieses Navigationsmenü vorübergehend reduzieren, indem Sie in der oberen rechten Ecke des Menübereichs auf das  klicken. Wenn Sie zum ersten Mal die NSX Network Detection and Response-Benutzeroberfläche sehen, ist die Seite **Dashboard** standardmäßig ausgewählt. Die Seite **Dashboard** besteht aus Widgets, die einen Überblick über mehrere überwachte Elemente bieten. Diese Widgets werden in [Erkunden der Dashboard-Seite](#) ausführlicher beschrieben.

Um auf eine andere NSX Network Detection and Response-Benutzeroberflächenseite zuzugreifen, klicken Sie auf die entsprechende Registerkarte im Hauptnavigationsmenü auf der linken Seite. Jede Registerkartenseite besteht aus mehreren Widgets, die weitere Informationen zu den überwachten Bereichen bereitstellen. Die Themen, die weiter unten in diesem Handbuch verfügbar sind, enthalten Details zu jeder dieser NSX Network Detection and Response-Benutzeroberflächenseiten.

Festlegen des Anzeigedesigns

Sie legen das Anzeigedesign, das in Ihrer aktuellen NSX Network Detection and Response-Sitzung verwendet wird, mithilfe des Symbols für den Anzeigedesignmodus im oberen rechten Bereich der Benutzeroberfläche fest. Das angezeigte Symbol hängt vom Anzeigedesign ab, das aktuell aktiv ist. Um in einen hellen Modus zu wechseln, klicken Sie auf das ☀️. Um in einen dunklen Modus zu wechseln, klicken Sie auf das 🌙.

Unterstützung

Um auf die verfügbaren NSX Network Detection and Response-Themen in der *Verwenden und Verwalten von VMware NSX Intelligence*-Dokumentation zuzugreifen, klicken Sie auf das ⓘ und dann auf **Hilfe**.

Um den Status Ihrer Verbindung zum NSX Network Detection and Response Cloud Connector anzuzeigen, klicken Sie auf **Konnektivitätsstatus überprüfen**. Der Cloud Connector bietet einen sicheren Tunnel der Kommunikation zwischen Ihrer NSX Manager-Sitzung und den NSX Advanced Threat Prevention-Cloud-Diensten.

Wenn ein Konnektivitätsproblem auftritt, das Sie mithilfe der Informationen im Abschnitt „Fehlerbehebung“ dieser Dokumentation nicht beheben können, klicken Sie auf **Support-Ticket** und melden Sie das Problem.

Zugreifen auf die Haupt-NSX-T-Benutzeroberfläche

Um zur Haupt-NSX Manager-Benutzeroberfläche zurückzukehren, klicken Sie in der oberen rechten Ecke auf das 🖥 und wählen Sie **NSX-T** aus.

Festlegen des Zeitraums

Um die Anzahl der Tage festzulegen, die Daten in den NSX Network Detection and Response-Widgets angezeigt werden sollen, verwenden Sie die Schaltfläche **Zeitbereich**

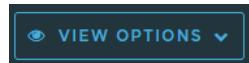
 Um bei der Datumsauswahl vorwärts und rückwärts zu navigieren, während der ausgewählte Datumsbereich konstant bleibt, klicken Sie auf das Symbol ⏪ oder ⏩, das sich auf beiden Seiten der Schaltfläche **ZEITBEREICH: LETZTE 7 TAGE** befindet. Angenommen, der Standardzeitraum beträgt 7 Tage. Wenn Sie auf die Pfeilschaltfläche nach links klicken, wird ein Bereich mit dem Enddatum vor 7 Tagen ausgewählt.

Sie können einen detaillierteren Zeitraum mithilfe des Popup-Fensters **Zeitbereich** definieren. Klicken Sie auf die Schaltfläche **ZEITBEREICH: LETZTE 7 TAGE** und wählen Sie im Dropdown-Menü **Relativ** (Standard) oder **Absolut** aus. Im relativen Modus wählen Sie die Anzahl der Tage seit dem aktuellen Datum aus, für das Daten angezeigt werden sollen. Der Standardwert beträgt 7 Tage, der Mindestwert 1 Tag und der Maximalwert 31 Tage. Im Modus „Absolut“ geben Sie die Daten in **Von** und **Bis** ein, indem Sie die Datumsangaben im Popup-Fenster des Kalenders auswählen. Um Ihre Auswahl zu speichern, klicken Sie auf **Anwenden**.

Verwenden der Schaltfläche „Optionen anzeigen“

Alle Datums- und Uhrzeitdaten, die auf der NSX Network Detection and Response-Benutzeroberfläche angezeigt werden, verwenden die UTC-Standardzeitzone so lange, bis Sie sie ändern.

Um die für die angezeigten Daten verwendete Zeitzone zu ändern, klicken Sie auf die

 , die sich oben rechts auf der Benutzeroberfläche befindet, und wählen Sie die aktuell ausgewählte Zeitzone aus. Klicken Sie im Popup-Fenster **Zeitzone** auf das Dropdown-Menü und wählen Sie eine andere Zeitzone aus. Um die Menüauswahl einzuschränken, beginnen Sie mit der Eingabe des Namens einer Zeitzone im Suchfeld. Nachdem Sie die gewünschte Zeitzone ausgewählt haben, klicken Sie auf **Anwenden**.

Verwalten der Widgets

Jede der NSX Network Detection and Response-Benutzeroberflächenseiten besteht aus mehreren Widgets, auf denen Details zu den erkannten Bedrohungen und Berichten angezeigt werden, die aus der Analyse dieser Bedrohungen generiert wurden.

Sie können die Widgets mithilfe der folgenden Informationen verwalten.

- Um die in einem Widget angezeigten Daten neu zu laden, klicken Sie oben rechts im Widget auf das .
- Sie können ein Widget minimieren bzw. maximieren, indem Sie neben dem Widget-Titel auf das  bzw. auf das  klicken.
- Um den Fokus weiter auf die in einigen Widgets angezeigten Daten zu legen, klicken Sie auf das .
- Um die Daten im XML/JSON-Format anzuzeigen, die in einigen Widgets verfügbar sind, klicken Sie auf das .
- Einige Widgets verfügen über kontextbezogene Hilfe, die in einem Popup-Fenster angezeigt wird. Um auf die Hilfeinformationen zuzugreifen, klicken Sie auf das . In einigen Kontexthilfe-Popup-Fenstern können Sie auf den Link **hier** klicken, um weitere Informationen zu den im Widget angezeigten Daten abzurufen.

Erkunden der Dashboard-Seite

Die Seite **Dashboard** wird angezeigt, wenn Sie die NSX Network Detection and Response-Benutzeroberfläche aufrufen.

Die Seite bietet eine allgemeine Übersicht über die aktiven Aktivitäten in Ihrem Netzwerk, erkannte Vorfälle und Bedrohungen sowie die neuesten beobachteten Bedrohungereignisse in Ihrer NSX-T Data Center-Umgebung.

Die Seite besteht aus mehreren Widgets, die mithilfe der Informationen in [Kennenzulernen der NSX Network Detection and Response-Benutzeroberfläche](#) verwaltet werden können.

Sie können einen Drilldown zu den Details einzelner Aspekte der Benutzeroberfläche durchführen und detaillierte Informationen anzeigen. Einige dieser detaillierten Informationen werden direkt im Widget angezeigt. Andere Informationen werden auf verknüpften Seiten an anderer Stelle auf der NSX Network Detection and Response-Benutzeroberfläche angezeigt.

Aktive Aktivitäten in meinem Netzwerk

Das Widget **Aktive Aktivitäten in meinem Netzwerk** bietet einen Überblick über die Aktivitäten, die von der NSX Network Detection and Response-Anwendung identifiziert wurden und derzeit in Ihrem Netzwerk aktiv sind. Es zeigt die kritischsten Aktivitäten an, auf die Sie sofort reagieren müssen.

Das Widget zeigt Statistiken für alle aktiven Aktivitäten, offene Aktivitäten mit großer Wirkung, in Bearbeitung befindliche Aktivitäten mit großer Wirkung und betroffene Hosts an.

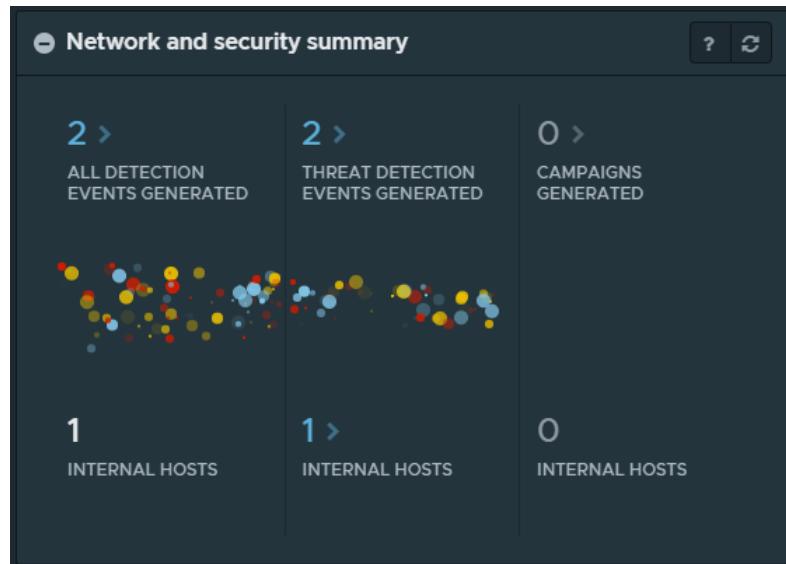
Wenn Sie weitere Details zu diesen Aktivitäten anzeigen möchten, klicken Sie auf **Zu Aktivitätenübersicht** in der unteren linken Ecke des Widgets, um die Seite **Aktivitäten** aufzurufen. Einzelheiten dazu finden Sie unter [Verwalten der Seite „Aktivitäten“](#).

Netzwerk- und Sicherheitsübersicht

Das Widget **Netzwerk- und Sicherheitsübersicht** zeigt, wie die NSX Network Detection and Response Daten zu Netzwerksdatenverkehrsflows verarbeitet und analysiert.

Das Widget zeigt die Verarbeitungs-Pipeline an, die für die Analyse aller Ereignisse (einschließlich informationsbezogener Ereignisse), das Erkennen von Bedrohungereignissen (nur wichtige Ereignisse) und das Generieren von Aktivitäten verwendet wird.

Das Widget verfügt über Segmente, die die verschiedenen Verarbeitungsphasen angeben, die das System bei eingehenden Daten durchführt. Wie in der folgenden Abbildung dargestellt, beginnt die Verarbeitung mit „Alle generierten Erkennungsereignisse“ und wird fortgesetzt, bis die generierten Aktivitäten erreicht sind.

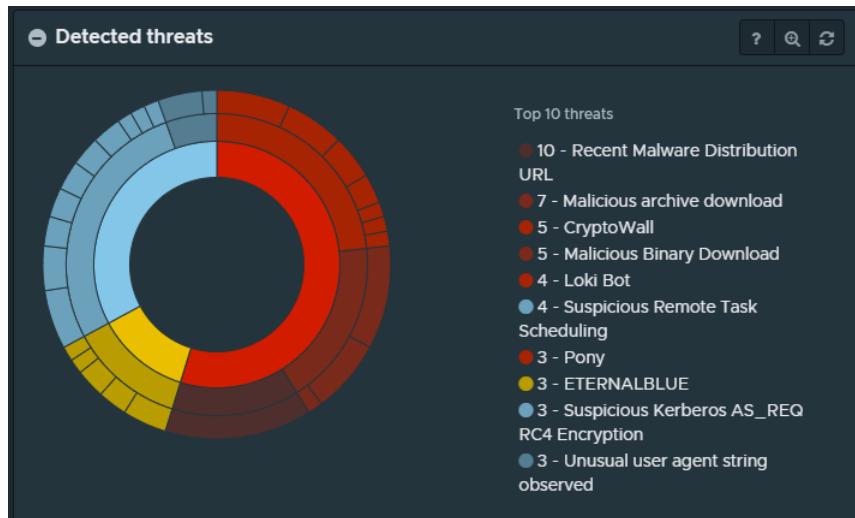


- Wenn Sie auf den Link „Anzahl“ für das Segment „Alle generierten Erkennungssereignisse“ klicken, gelangen Sie zur Seite **Ereignisse**, die gefiltert wird, um alle Erkennungssereignisse anzuzeigen, einschließlich unwichtiger Info-Erkennungssereignisse. Weitere Informationen finden Sie unter [Arbeiten mit der Seite „Ereignisse“](#).
- Wenn Sie auf den Link „Anzahl“ für das Segment „Generierte Bedrohungserkennungssereignisse“ klicken, gelangen Sie zur Seite **Ereignisse**, die gefiltert wurde, um nur die Liste der Bedrohungserkennungssereignisse anzuzeigen. Wenn Sie auf den Link „Anzahl“ unterhalb des Segments „Generierte Bedrohungserkennungssereignisse“ klicken, gelangen Sie zur Seite **Hosts**. Siehe [Arbeiten mit der Seite „Hosts“](#).
- Wenn Sie auf den Link „Anzahl“ für das Segment „Generierte Aktivitäten“ klicken, gelangen Sie zur Seite **Aktivitäten**, auf der die Karten für die erkannten Aktivitäten angezeigt werden. Einzelheiten dazu finden Sie unter [Verwalten der Seite „Aktivitäten“](#).

Erkannte Bedrohungen

Das Widget **Erkannte Bedrohungen** bietet eine grafische Übersicht über die verschiedenen Arten von Bedrohungen, die die NSX Network Detection and Response-Anwendung im Netzwerk erkannt hat.

Die Bedrohungsinformationen werden in einem mehrschichtigen Kreis angezeigt, ähnlich wie in der folgenden Abbildung.



Die Unterteilungen der Kreise stellen die Anzahl der Hosts dar, die von den angezeigten Vorfalltypen betroffen sind. Die Bewegung zu den äußeren Kreisen bietet eine präzisere Granularität und spezifischere Informationen.

- Der innere Ring zeigt die drei verschiedenen Arten von Vorfällen an.

Vorfalltyp	Beschreibung
Infektionen	Dies sind Vorfälle, die die NSX Network Detection and Response-Anwendung als kritisch festgestellt hat. Diesen Vorfällen wurde eine Auswirkungsbewertung von 70 oder höher zugewiesen, und sie werden in Rot angezeigt.
Watchlist	Hierbei handelt es sich um Vorfälle, bei denen die NSX Network Detection and Response-Anwendung ein mittleres Risiko festgestellt hat. Solche Vorfälle weisen zwar auf ein potenzielles Risiko hin, erfordern aber möglicherweise keine sofortige Aufmerksamkeit. Sie werden genau überwacht, falls neue Nachweise ihren Status ändern. Diesen Vorfällen wird eine Auswirkungsbewertung von 30 bis 69 zugewiesen, und sie werden gelb angezeigt.
Belästigungen	Dies sind Vorfälle, die als gering oder ohne Risiko betrachtet werden. In der Regel handelt es sich dabei um potenziell unerwünschte/riskante Aktivitäten, die nicht unbedingt auf eine Gefährdung oder Infektion des überwachten Netzwerks hindeuten. Diesen Vorfällen wurde eine Auswirkungsbewertung von weniger als 30 zugewiesen, und sie werden blau angezeigt.

- Im mittleren Ring wird die Bedrohungsklasse zusammen mit der Anzahl der relevanten Vorfälle für jeden Typ von Mandanten angezeigt. Bedrohungsklassen umfassen Befehls- und Steuerungsserver, Downloads bösartiger Dateien, Crypto-Miner und vieles mehr.
- Der äußere Ring stellt die einzelnen Bedrohungsfamilien dar, die im Netzwerk erkannt werden. Bedrohungsfamilien umfassen Ransomware, bösartige Binärdateien usw.

Wenn Sie auf das Diagramm zeigen, zeigt das Widget den Bedrohungsnamen und eine Anzahl der Hosts an, auf denen die NSX Network Detection and Response-Anwendung die Bedrohung beobachtet hat.

Wenn Sie auf ein Element im Diagramm klicken, wird die Ansicht vergrößert und zeigt weitere Details zum ausgewählten Informationstyp an. Durch erneutes Klicken auf das Element wird die Ansicht wieder vergrößert.

Wenn Sie im inneren Ring auf einen Vorfalltyp klicken, vergrößert sich die Diagrammansicht und zeigt die entsprechenden Vorfälle im mittleren und äußeren Ring an. Wenn Sie im mittleren Ring auf eine Bedrohungsklasse klicken, wird die Diagrammansicht vergrößert und zeigt die entsprechenden Bedrohungsfamilien an. Wenn Sie auf den äußeren Ring klicken, wird die Diagrammansicht vergrößert und zeigt Details zur ausgewählten Bedrohung an.

Die Legende auf der rechten Seite des Widgets liefert eine Anzahl der Vorkommen der am häufigsten erkannten Bedrohungen. Wenn Sie auf ein Element in der Legende zeigen, enthält ein Popup-Fenster weitere Informationen zur Bedrohungsklasse, zur Anzahl der Vorfälle und zur Anzahl der betroffenen Hosts. Wenn Sie auf das Element klicken, wird die Diagrammansicht für den ausgewählten Bedrohungstyp vergrößert und bietet weitere kontextbezogene Informationen.

Globale Ereigniszuzuordnung

Das Widget **Globale Ereigniszuzuordnung** bietet einen visuellen Überblick über die Geolocations der aggregierten Ereignisse.

Es markiert den ungefähren Speicherort der anderen Hosts, die an dem von der NSX Network Detection and Response-Anwendung erkannten Ereignis beteiligt sind. Die Markierungsfarbe stellt die Ereigniswirkung dar. Die Markierungsgröße stellt die Anzahl der betroffenen Hosts dar.

Ereignisse ohne bestimmten Speicherort sind von dieser Zuordnung ausgeschlossen.

Um mehr über die Bedrohungen und Hosts zu erfahren, die an diesem bestimmten Standort dargestellt werden, klicken Sie auf eine Markierung auf der Zuordnung.

Im angezeigten Popup-Fenster **Standortdetails** können Sie den ungefähren Standort, die Bedrohungen und die Zielhosts für das ausgewählte Ereignis anzeigen. Klicken Sie neben jedem Eintrag auf das Symbol um Filter auf die Liste anzuwenden, die auf der Seite **Ereignisse** angezeigt wird.

Neue eindeutige Erkennungen

Das Widget **Neue eindeutige Erkennungen** zeigt eine Liste der Ereignisse an, die die NSX Network Detection and Response-Anwendung zum ersten Mal in Ihrem Netzwerk identifiziert hat.

Das folgende Bild zeigt ein Beispiel für die angezeigte Liste.

New unique detections					
TIME	SCORE	DETECTION	THREAT	TYPE	REFERENCE
2021-08-12	56	tw:4101719	CVE-2017-0143 EXP...	Lastline network signature	
2021-08-12	56	et:2025650	ETERNALBLUE	Lastline network signature	
2021-08-12	10	llrules:1494798612289	POTENTIAL SMB PRO...	Lastline network signature	

Die Liste enthält den Zeitpunkt des Ereignisses, seine Auswirkungsbewertung, die Erkennungssignatur (die eine URL mit einer bösartigen Reputation oder eine bestimmte Regel sein kann), die Bedrohung, den Ereignistyp und einen permanenten Linkverweis auf das zugehörige Ereignis.

Wenn Sie auf eine der Zeilen in der Liste zeigen, werden weitere Details zum Erkennungsergebnis angezeigt. Wenn Sie auf den Namen der Bedrohung klicken, wird ein Popup-Fenster mit Informationen über den Bedrohungstyp, den Schweregrad und Details zur erkannten Bedrohung angezeigt.

Wichtig Untersuchen Sie diese Ereignisse, da die NSX Network Detection and Response-Anwendung diese Bedrohungen in Ihrer NSX-T Data Center-Umgebung zum ersten Mal erkannt hat.

Liste heruntergeladener Dateien

Das Widget **Liste heruntergeladener Dateien** zeigt eine Liste eindeutiger Dateien an, die die NSX Network Detection and Response-Anwendung als von Hosts in Ihr Netzwerk heruntergeladen erkannt hat. Dieses Widget kann nur Daten anzeigen, wenn die NSX Malware-Schutz-Anwendung aktiviert ist.

Die folgende Abbildung zeigt ein Beispiel für das Widget **Liste heruntergeladener Dateien** an.

MD5	TYPE	SIZE	DOWNLOADS	AV CLASS	MALWARE	SCORE	☰
+895006de3c22c2e907...	Executable	740.500 KB	3 ↗	PWD-STEALER ...	LOKI BOT ⚡ PONY ⚡	100	
+936e73lb8be167a396e...	Executable	480.133 KB	2 ↗	TROJAN	EMOTET ⚡	100	
+2e61ed247b60ef7fa77c...	Java	470.109 KB	1 ↗	PWD-STEALER TROJAN	ORAT	100	
+c3138c2c7dd16daa812c...	Archive	108.811 KB	2 ↗	TROJAN	EMOTET ⚡	100	
+2773e3dc59472296cb...	Executable	283.500 KB	2 ↗	RANSOMWARE ⚡	JIGSAW	100	
+72d2bb1a2574411c968...	Executable	12.354 KB	3 ↗	No tags	No tags	0	
+69dcca2c07d75aa7ba8...	Executable	19.386 KB	3 ↗	No tags	No tags	0	

Das Textfeld für die **Schnellsuche** in der oberen linken Ecke der Liste bietet eine schnelle Suchfunktion, die direkt nach der Eingabe ausgeführt wird. Es filtert die Zeilen in der Liste und zeigt nur die Zeilen mit Text in einer Spalte an, die mit der Abfragezeichenfolge übereinstimmt, die Sie im Suchtextfeld eingegeben haben.

Um die in der Liste angezeigten Spalten anzupassen, klicken Sie auf das in der oberen rechten Ecke der Liste.

Sie können die Anzahl der Zeilen, die angezeigt werden sollen, anpassen. Die Standardeinstellung ist 20 Einträge. Verwenden Sie das Symbol mit dem und das Symbol mit dem , um durch mehrere Seiten zu navigieren.

Jede Zeile ist eine Zusammenfassung einer heruntergeladenen Datei. Klicken Sie auf das oder an einer beliebigen Stelle in einer Eingabezeile, um auf eine detaillierte Ansicht der heruntergeladenen Datei zuzugreifen.

Die Liste ist nach Punktzahl sortiert und enthält die folgenden Spalten.

Spaltenname	Beschreibung
MD5	Der MD5-Hash der heruntergeladenen Datei.
Typ	<p>Der allgemeine Dateityp der heruntergeladenen Datei. Unterstützte Typen sind derzeit:</p> <ul style="list-style-type: none"> ■ Archiv – Archivformate wie ZIP oder RAR ■ Dokument – Enthält andere Arten von Office-Dokumenten ■ Ausführbare Datei – Binäre Anwendungsformate, wie z. B. Windows Portable Executable ■ Java – Java-Anwendung oder -Applet ■ Medien – Flash-Datei von Macromedia (Adobe) ■ Andere – Anderes erkanntes Dateiformat ■ PDF – Dateien im Portable Document Format ■ Skript – Ein ausführbares Skript wie JavaScript, Python und andere ■ Unbekannt – Unbekannter Dateityp
Größe	Größe der heruntergeladenen Datei in Byte.
Downloads	<p>Anzahl der Downloads der Datei durch Hosts im Netz.</p> <p>Die angezeigte Nummer und das  sind ein Link zur detaillierten Download-Seite. Der Link übergibt einen Analyse-UUID-Filter, der die Ansicht auf Downloads dieser spezifischen Datei beschränkt.</p>
AV-Klasse	<p>Eine Bezeichnung, die die Antivirenklasse der heruntergeladenen Datei definiert. Wenn die Bezeichnung über ein  verfügt, können Sie in einem Popup-Fenster auf dieses Symbol klicken, um eine Beschreibung zu erhalten.</p>
Malware	<p>Eine Bezeichnung, die den Malware-Typ der heruntergeladenen Datei definiert. Wenn die Bezeichnung über ein  verfügt, können Sie in einem Popup-Fenster auf dieses Symbol klicken, um eine Beschreibung zu erhalten.</p>
Bewertung	<p>Die der heruntergeladenen Datei durch die Analyse zugewiesene Punktzahl gibt den kritischen Grad der erkannten Bedrohung an und reicht von 0-100:</p> <ul style="list-style-type: none"> ■ Bedrohungen ab 70 werden als kritisch betrachtet. ■ Bedrohungen zwischen 30 und 69 gelten als mittleres Risiko. ■ Bedrohungen zwischen 1 und 29 gelten als harmlose Bedrohungen. <p>Einzelheiten zum Kern der Bösartigkeit und zur Risikoeinschätzung finden Sie unter Analysebericht: Registerkarte „Übersicht“.</p> <p>Wenn das  angezeigt wird, bedeutet dies, dass das Artefakt blockiert wurde. Die Liste wird in absteigender Reihenfolge sortiert (die kritischsten Bedrohungen oben). Klicken Sie auf den , um die Liste in aufsteigender Reihenfolge zu sortieren (am wenigsten kritische Bedrohungen oben). Klicken Sie dann auf den , um zur Standardeinstellung zurückzukehren.</p>

Verwalten der Seite „Aktivitäten“

Die Seite **Aktivitäten** bietet eine Schnittstelle zum Überwachen der Aktivitäten, die die NSX Network Detection and Response-Anwendung in Ihrem Netzwerk erkannt hat.

Die Seite besteht aus mehreren Widgets, die mithilfe der Informationen in [Kennenzulernen der NSX Network Detection and Response-Benutzeroberfläche](#) verwaltet werden können.

Wenn keine Aktivitäten erkannt werden, wird die Nachricht Keine Aktivitäten angezeigt.

Wenn es erkannte Aktionen gibt, werden auf der Seite die entsprechenden Aktionskarten angezeigt. Die folgende Abbildung zeigt eine Beispielseite **Aktivitäten** mit einer Karte für die Während des ausgewählten Zeitraums erkannte Aktivität. Siehe [Arbeiten mit Aktionskarten](#).

The screenshot shows a dark-themed user interface for the 'Campaigns' section. At the top, there's a search bar labeled 'Quick search' and a dropdown menu 'Sort By' set to 'IMPACT'. To the right are buttons for 'TIME RANGE: AUG 7 - AUG 13' and 'VIEW OPTIONS'. Below this, a large card displays the following information:

- Campaign ID:** b6f9b5
- Dates:** 2021-08-12 – 2021-08-12
- Stage:** Stage 2 of 8 EXPLOITATION
- Hosts:** 1
- Threats:** 2
- Status:** OPEN

Below the card, a message says 'You might also want to investigate...'. It lists '3 Hosts' and '9 Network anomalies'.

Unten auf der Seite wird das Widget **Sie möchten möglicherweise auch untersuchen** angezeigt. Weitere Informationen finden Sie unter [Informationen zum Widget „Untersuchen“](#).

Arbeiten mit Aktionskarten

Auf der Seite **Aktivitäten** werden Aktivitätskarten für alle erkannten Aktivitäten angezeigt. Eine Aktivitätskarte zeigt den berechneten Bedrohungswert, den Aktivitätsnamen (Aktivitäts-ID), die letzte Angriffsstufe, die die NSX Network Detection and Response-Anwendung entdeckt hat, die Anzahl der betroffenen Hosts, die Anzahl der verschiedenen Bedrohungen und den Aktivitätsstatus.

Verwalten von Aktivitätskarten

Sie können die Aktivitätskarten sortieren, indem Sie auf das Dropdown-Menü **Sortieren nach** klicken und aus der Liste der Kriterien auswählen: **Auswirkung** (Standardeinstellung), **Stufe**, **Hosts**, **Bedrohungen**, **Neueste** oder **Letzte Aktionen**.

Wählen Sie die angezeigten Aktivitätskarten aus, indem Sie auf das Dropdown-Menü **Status** klicken und **Alle anzeigen** (Standardeinstellung), **Offen**, **In Bearbeitung**, **Abgeschlossen** oder **Aktualisiert** auswählen. Sie können mehr als eine Option auswählen. Löschen Sie eine Auswahl, indem Sie erneut auf die Option klicken.

Um alle verfügbaren Details zu einer Aktivität anzuzeigen, klicken Sie auf den Link **Aktivitäts-ID** und die Details zur Aktivität werden angezeigt. Siehe [Grundlegendes zur Seite „Aktivitätsdetails“](#).

Klicken Sie auf eine beliebige Stelle auf einer Aktivitätskarte und die Seitenleiste **Aktivitätsübersicht** wird auf der rechten Seite angezeigt.

Grundlegendes zur Seitenleiste „Aktivitätsübersicht“

Die Seitenleiste **Aktivitätsübersicht** wird auf der rechten Seite der Seite **Aktivitäten** angezeigt, wenn Sie auf eine beliebige Stelle auf einer Aktivitätskarte klicken.

Im Folgenden wird beschrieben, was auf der **Aktivitätsübersicht**-Seitenleiste angezeigt wird.

Oberster Abschnitt

Oben in der Seitenleiste finden Sie die folgenden Elemente:

- Die berechnete Bedrohungspunktzahl und der Name/die ID der Aktivität (im langen Hash-Format) werden oben angezeigt.
- Wenn Sie auf die Schaltfläche **Details anzeigen** klicken, erhalten Sie Zugriff auf die Seite **Aktivitätsdetails**. Weitere Informationen hierzu finden Sie unter [Grundlegendes zur Seite „Aktivitätsdetails“](#).
- Es wird die Anzahl der von der Aktivität betroffenen Hosts angezeigt.
- Die Anzahl der Bedrohungstypen, die an der Aktivität beteiligt sind, wird angezeigt.

Aktionen

Der nächste Abschnitt des Fensters enthält die folgenden Informationen.

- **Aktivitätsname/Aktivitäts-ID** – Sie können auf das Stiftsymbol klicken und optional den Namen/die ID der Aktivität bearbeiten.
- **Status** – Wählen Sie den Triage-Status der Aktivität aus dem Dropdown-Menü. Wählen Sie unter **Offen**, **In Bearbeitung**, **Aktualisiert** oder **Abgeschlossen** aus.
- „Erste Erkennung“ und „Letzte Erkennung“ – Zeigt ein lineares Diagramm mit dem Zeitstempel, wann der Nachweis zuerst und zuletzt gesehen wurde. Die Dauer wird nach dem Diagramm angezeigt.

Erkannte Angriffsphasen

Im Abschnitt **Erkannte Angriffsphasen** werden die Angriffsphasen angezeigt, wobei die aktuellen Angriffsphasen hervorgehoben werden. Zeigen Sie auf eine hervorgehobene Aktivität (z. B. **Exploitation**), um ein Popup-Fenster mit weiteren Informationen zur Phase anzuzeigen. Einzelheiten dazu finden Sie unter [Informationen zu Angriffsphasen](#).

Betroffener Host

Im Abschnitt **Betroffene Hosts** werden die Hosts angezeigt, die an der ausgewählten Aktivität beteiligt sind. Klicken Sie auf den Link IP-Adresse, um die Seite **Hostprofil** anzuzeigen. Siehe Seite „[Hostprofil](#)“.

Um Details zu den Hosts auf der Registerkarte **Hosts** anzuzeigen, klicken Sie auf **Hosts anzeigen**. Weitere Informationen hierzu finden Sie unter [Details zur Aktivität: Registerkarte „Hosts“](#).

Bedrohungen

Im Abschnitt **Bedrohungen** werden die aktuellen Bedrohungen angezeigt, die in der ausgewählten Aktivität erkannt wurden. Der Farbcode zeigt den Schweregrad der Bedrohung an: rot für hohen Schweregrad, gelb für mittleren und blau für niedrigen.

Um detaillierte Informationen zur Aktivität auf der Registerkarte **Aktivitätszeitleiste** anzuzeigen, klicken Sie auf **Bedrohungen anzeigen**. Weitere Informationen hierzu finden Sie unter [Details zur Aktivität: Registerkarte „Zeitachse“](#).

Informationen zum Widget „Untersuchen“

Das Widget **Untersuchen** zeigt die Meldung Sie möchten möglicherweise auch untersuchen... und eine Liste von benutzerdefinierten Fakten und Zielen, die von der NSX Network Detection and Response-Anwendung basierend auf der Aktivität in Ihrem Netzwerk erstellt wurden.

Um interessante Sicherheitsinformationen zu erhalten, folgen Sie den in der Liste aufgeführten Links. Das Widget zeigt eine der folgenden Informationen an, je nachdem, was die NSX Network Detection and Response-Anwendung erkannt hat.

Detailname	Beschreibung
Hosts	Meldet verdächtige Aktivitäten auf den Hosts in Ihrem Netzwerk. Klicken Sie auf den Link, um zur Seite Hosts zu wechseln.
Verdächtige Dateidownloads	Meldet verdächtige Dateidownloads. Klicken Sie auf den Link, um zur Registerkarte Alle auf der Seite Heruntergeladene Dateien zu wechseln.
Netzwerkanomalien	Meldet INFO -Ereignisse, die möglicherweise untersucht werden müssen. Klicken Sie auf den Link, um zur Seite Ereignisse zu wechseln.

Grundlegendes zur Seite „Aktivitätsdetails“

Auf der Seite **Aktivitätsdetails** auf der NSX Network Detection and Response-Benutzeroberfläche werden alle verfügbaren Details für die Aktivität angezeigt, die Sie aktuell auf der Seite **Aktivitäten** ausgewählt haben.

Sie greifen auf diese Seite zu, indem Sie auf der Seite **Aktivitäten** auf die ID einer Aktivität klicken.

Diese Seite ist in mehrere Registerkarten unterteilt, wie in der folgenden Abbildung dargestellt.

- **Übersicht** – Bietet eine Übersicht und einen grafischen Blueprint der Aktivität, die die NSX Network Detection and Response-Anwendung generiert hat.
- **Hosts** – Enthält eine Liste der Hosts, die von der Aktivität betroffen sind.
- **Zeitachse** – Zeigt die in der Aktivität enthaltenen Ereignisse in chronologischer Reihenfolge an.
- **Verlauf** – Bietet einen Textverlauf der Aktivität.
- **Nachweis** – Zeigt eine Liste der für die aktuell ausgewählte Aktivität erkannten Nachweise an.

Oben auf der Seite „Aktivitätsdetails“ befinden sich die Daten von der ausgewählten Aktivitätskarte. Sie zeigt die berechnete Bedrohungspunktzahl, den Aktivitätsnamen (Aktivitäts-ID), die letzte Angriffsphase, die Anzahl der betroffenen Hosts, die Anzahl der verschiedenen Bedrohungen und den Aktivitätsstatus an.

Um zur Seite **Aktivitäten** zurückzukehren, klicken Sie auf das Symbol mit dem Symbol mit dem ⏪ in der oberen linken Ecke der Seite neben der Bedrohungspunktzahl für die Aktivität und der Aktivitäts-ID.

Details zur Aktivität: Registerkarte „Übersicht“

Auf der Registerkarte **Übersicht** auf der Seite **Details zur Aktivität** werden eine Zusammenfassung der Aktivität und ein interaktiver grafischer Blueprint angezeigt.

Die folgenden Informationen beschreiben die drei Abschnitte auf dieser Registerkarte.

Bedrohungen und Hosts der Aktivität

Im Abschnitt **Bedrohungen und Hosts** werden die Widgets **Bedrohungen** und **Hosts** angezeigt.

Das Widget **Bedrohungen** zeigt die aktuellen Bedrohungen an, die die NSX Network Detection and Response-Anwendung in der ausgewählten Aktivität erkannt hat. Der Schweregrad der Bedrohung wird durch den Farbcode angezeigt: rot für hoch, gelb für mittel und blau für niedrig. Zeigen Sie auf den Namen der aufgelisteten Bedrohungen; in einem Popup-Fenster werden die IP-Adressen der betroffenen Hosts angezeigt. Klicken Sie auf **Bedrohungsdetails anzeigen**; auf der Registerkarte **Zeitachse** werden detaillierte Informationen zur Aktivität angezeigt.

Das Widget **Hosts** zeigt die Hosts an, die von der ausgewählten Aktivität betroffen sind. Der Schweregrad der Bedrohung wird durch den Farbcode angezeigt: rot für hoch, gelb für mittel und blau für niedrig.

Zeigen Sie auf die IP-Adresse eines betroffenen Hosts. In einem daraufhin angezeigten Popup-Fenster werden die Namen der Bedrohungen angezeigt, die sich auf den Host auswirken. Klicken Sie auf **Details zu Hosts anzeigen**; auf der Registerkarte **Hosts** werden detaillierte Informationen zu den Hosts angezeigt.

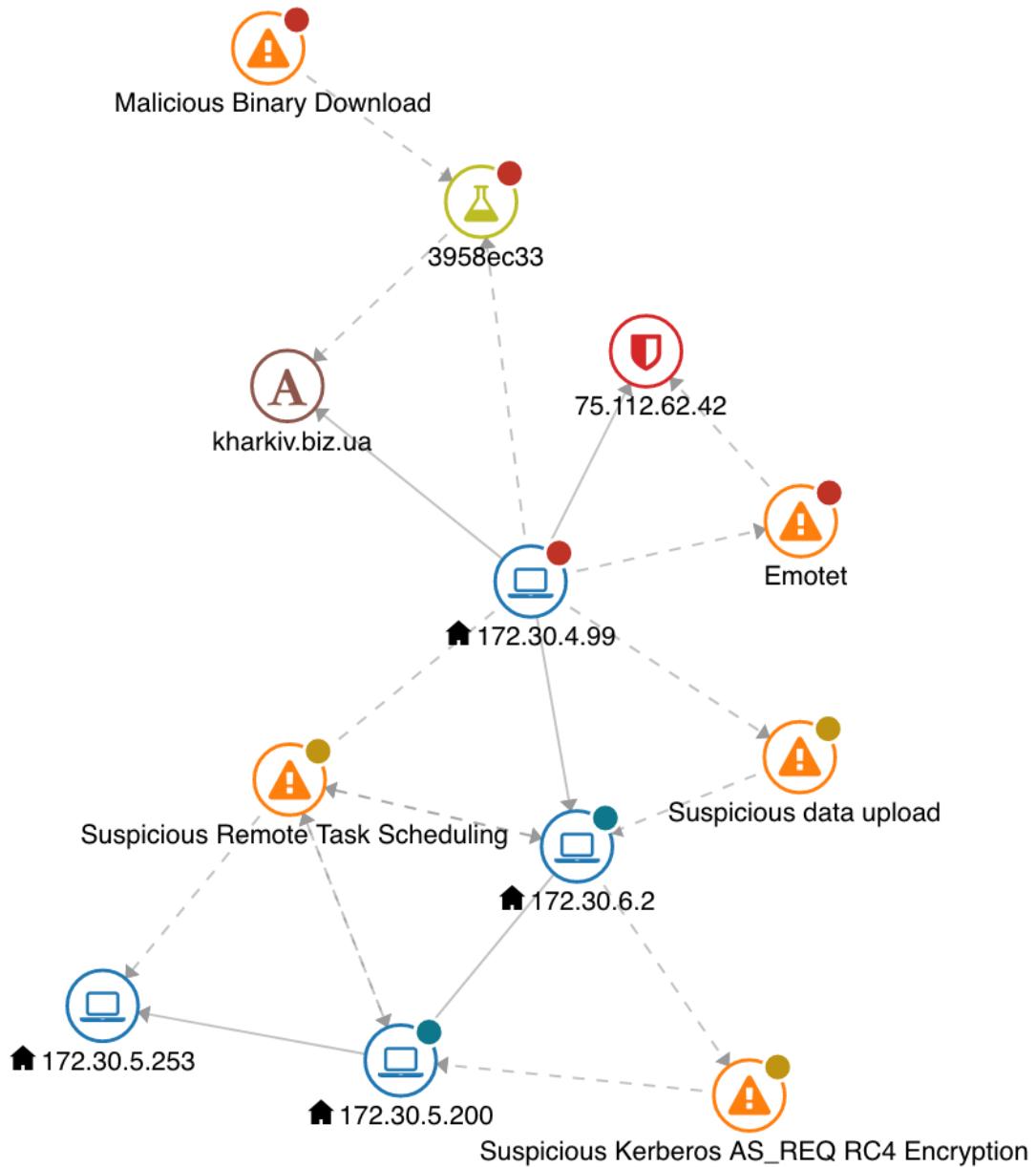
Angriffsphasen der Aktivität

Das Widget **Angriffsphasen** zeigt die Angriffsphasen an und hebt die aktuellen Phasen für Angriffsangriffe der Aktivität hervor. Zeigen Sie auf eine markierte Aktivität. In einem daraufhin angezeigten Popup-Fenster werden weitere Informationen über die Angriffsphase angezeigt. Unter [Eigenschaften der Aktivität](#) finden Sie Details zu Angriffsphasen.

Aktivitäts-Blueprint

Das Widget **Aktivitäts-Blueprint** bietet eine interaktive grafische Darstellung der Aktivität. Es zeigt die an der Aktivität beteiligten Hosts (sowohl intern als auch extern für Ihr Netzwerk), die Bedrohungen, die sie betroffen haben, sowie zusätzliche Informationen an, die die Beschreibung der Aktivität abschließen.

Es folgt ein Beispiel für ein Blueprint-Diagramm.



Dieses Blueprint-Diagramm zeigt die folgenden Aktivitäten an.

- Eine bösartige Binärdatei wird auf den Hostknoten mit der Bezeichnung 172.30.4.99 heruntergeladen. Diese Aktivität steht im Einklang mit dem Öffnen einer E-Mail durch einen Benutzer auf diesem Host (z. B. Aufrufen einer URL oder Öffnen eines in der E-Mail enthaltenen Anhangs).
- Der Hostknoten mit der Bezeichnung 172.30.4.99 ist mit dem Hostnamenknoten mit der Bezeichnung kharkiv.biz.ua verbunden. Der Analysebericht 3958ec33 zeigt, dass ein Download über die URL <http://kharkiv.biz.ua/hPpD/> vorgenommen wurde. Der Analysebericht zeigt auch, dass es sich bei dem heruntergeladenen Programm um eine ausführbare PE-Anwendung, 32-Bit, Intel i386-Datei handelt.

- Der Hostknoten mit der Bezeichnung 172.30.4.99 ist mit einem Emotet command and control verbunden. Der Server ist der blockierte Eintrag 75.112.62.42.
- Der Hostknoten mit der Bezeichnung 172.30.4.99 ist mit einem verdächtigen Daten-Upload mit dem Hostknoten mit der Bezeichnung 172.30.6.2 und mit einer verdächtigen Remote-Aufgabenplanung mit den Hostknoten mit den Bezeichnungen 172.30.5.200 und 172.30.5.200 verbunden; alle Aktivitäten stehen in Zusammenhang mit einer seitlichen Bewegung.
- Der Hostknoten mit der Bezeichnung 172.30.6.2 ist mit dem Hostknoten mit der Bezeichnung 172.30.5.200 mit einer verdächtigen Kerberos-Verschlüsselung verbunden; einer Aktivität, die mit exfiltration-Daten konsistent ist.

Knotenschlüssel

Die folgenden Knotentypen können im Blueprint-Diagramm angezeigt werden.

Sy mb ol	Knotentyp	Beschreibung
	Analysebericht	<p>Dieser Knotentyp stellt die Ergebnisse der Detonierung eines Beispiels (Datei oder URL) in der NSX Network Detection and Response-Sandbox dar.</p> <ul style="list-style-type: none"> ■ Analyseberichtsknoten sind mit einer verkürzten Version der entsprechenden Analyseaufgabe-UUID gekennzeichnet. ■ Der Punktzahlbereich der Analyseausführung wird mithilfe des farbcodierten Badges oben rechts im Knoten ausgedrückt.
	Heruntergeladene Datei	<p>Dieser Knotentyp stellt eine Datei dar, die in das Netzwerk heruntergeladen wurde.</p> <ul style="list-style-type: none"> ■ Heruntergeladene Dateiknoten sind mit einer verkürzten Version des SHA1-Hashs der entsprechenden Datei gekennzeichnet.
	Host	<p>Dieser Knotentyp stellt ein Netzwerkgerät dar.</p> <ul style="list-style-type: none"> ■ Hostknoten sind mit der IP-Adresse des entsprechenden Hosts gekennzeichnet. ■ Der Hostknoten gibt an, ob ein Host intern oder extern ist. Interne Hosts zeigen ein neben ihrer IP-Adresse an. Die Bestimmung, ob ein Host intern ist, basiert auf der Konfiguration der privaten IP-Bereiche. ■ Die maximale Auswirkung von Vorfällen, die den entsprechenden Host betreffen, wird mithilfe des farbcodierten Badges oben rechts im Knoten ausgedrückt.
	Info	<p>Dieser Knotentyp stellt die Erkennung einer Aktivität auf Infoebene dar. Dieser Knoten wird nur im Blueprint-Diagramm Netzwerkanalyse angezeigt.</p> <ul style="list-style-type: none"> ■ Ein Info-Ereignis wird bei Aktivitäten oder Verhaltensweisen erstellt, die nicht unbedingt böswillig sind, aber zusätzliche nützliche Informationen bereitstellen. ■ Die maximale Auswirkung von Ereignissen, die für die entsprechende Bedrohung erkannt werden, wird mithilfe des farbcodierten Badges oben rechts im Knoten ausgedrückt.
	Bedrohung	<p>Dieser Knotentyp stellt eine Erkennung dar.</p> <ul style="list-style-type: none"> ■ Bedrohungsknoten sind mit dem Bedrohungsnamen gekennzeichnet, der mit dem erkannten Ereignis verknüpft ist. ■ Die maximale Auswirkung von Ereignissen, die für die entsprechende Bedrohung erkannt werden, wird mithilfe des farbcodierten Badges oben rechts im Knoten ausgedrückt.

Informationen zu Edges

Die Linien, die die Knoten verbinden, werden als Edges bezeichnet.

Ein Hostknoten ist mit Bedrohungs- oder Analyseberichtsknoten mit einer gepunkteten Linie verbunden, um anzugeben, dass der dem Hostknoten entsprechende Host der Bedrohung ausgesetzt war, die durch den Bedrohungs- oder Analyseberichtsknoten repräsentiert wurde.

Andere Verbindungen werden mit einer durchgezogenen Linie dargestellt, um auszudrücken, dass eine Aktivität (z. B. eine Netzwerkverbindung, ein DNS-Suchlauf oder eine Webanforderung) die Entitäten, die zwei Knoten entsprechen, in Beziehung setzt.

Blueprint-Interaktion

Das Blueprint-Diagramm ist interaktiv: Unterstützung der Elementauswahl, Verschieben von Knoten und Vergrößern und Verkleinern.

Knoten und Edges können ausgewählt werden, indem Sie darauf klicken: Weitere Informationen zum ausgewählten Element finden Sie in der Seitenleiste.

Wenn Sie den Mauszeiger über einen Knoten bewegen, werden die verbindenden Edges mit der Markierung der Interaktion dieses Knotens dargestellt.

Einzelne Knoten können an neue Positionen im Diagramm gezogen werden. Das gesamte Diagramm kann geschwenkt werden, wodurch sich der Blickwinkel effektiv ändert.

Das Diagramm kann durch Scrollen des Mausrads vergrößert und verkleinert werden. In höheren Zoomstufen werden mehr Details angezeigt. Insbesondere ist das Badge, das mit mehreren Knotentypen verwendet wird, um Auswirkungsinformationen zu übermitteln, mit der tatsächlichen Auswirkungsbewertung angereichert.

Seitenleiste „Aktivität“

Die Seitenleiste **Aktivität** wird verwendet, um Informationen anzuzeigen, die relativ zu einem oder mehreren Elementen des Blueprint-Diagramms sind. Standardmäßig ist sie minimiert.

- Klicken Sie auf das , um Knoten- oder Edge-Informationen anzuzeigen.
- Klicken Sie auf das , um Tools von Drittanbietern anzuzeigen.

Um die Seitenleiste zu minimieren, klicken Sie auf den .

Knoten- oder Edge-Informationen

Die Registerkarte „Knoten-/Edge-Informationen“ enthält zusätzliche Informationen zu einem ausgewählten Knoten oder Edge im Blueprint-Diagramm. Um einen Knoten auszuwählen, klicken Sie auf das jeweilige Symbol im Diagramm.

Knotentyp	Informationen
Analysebericht	<p>Zusätzliche Informationen zu einem Analysebericht.</p> <p>Berichtdetails:</p> <ul style="list-style-type: none"> ■ Analyseberichte – Zeigt die Aufgaben-UUID und die Punktzahl an. Klicken Sie auf das  um den Analysebericht in einer neuen Browserregisterkarte anzuzeigen. ■ MD5 – Datei-Hashwert. ■ SHA1 – Datei-Hashwert. ■ Größe – Dateigröße in Byte. ■ Kategorie – Die Kategorie, zu der die analysierte Datei gehört. ■ Typ – Detailliertere Informationen zur Datei. <p>Details der analysierten Stichprobe werden angezeigt:</p> <ul style="list-style-type: none"> ■ Anzahl der Downloads – Wie oft die analysierte Datei beim Herunterladen beobachtet wurde. ■ Hosts – IP-Adresse der Hosts, die die analysierte Datei heruntergeladen haben. ■ URLs – Die vollständige URL der heruntergeladenen Datei.
Heruntergeladene Datei	<p>Zusätzliche Informationen zu einer heruntergeladenen Datei</p> <p>Dateidetails:</p> <ul style="list-style-type: none"> ■ MD5 – Datei-Hashwert. ■ SHA1 – Datei-Hashwert. ■ Größe – Dateigröße in Byte. ■ Kategorie – Die Kategorie, zu der die analysierte Datei gehört. ■ Typ – Detailliertere Informationen zur Datei. <p>Details zu den Sichtungen:</p> <ul style="list-style-type: none"> ■ Anzahl der Downloads – Wie oft die analysierte Datei beim Herunterladen beobachtet wurde. ■ Herunterladende Hosts – IP-Adresse der Hosts, die die analysierte Datei heruntergeladen haben. ■ URLs – Die vollständige URL der heruntergeladenen Datei. ■ Berichte – Zeigt den Berichtsstatus, die Aufgaben-UUID und die Punktzahl an. Klicken Sie auf das  um den Analysebericht in einer neuen Browserregisterkarte anzuzeigen.
Host	<p>Zusätzliche Informationen zu einem Host.</p> <p>Details auf Hostebene:</p> <ul style="list-style-type: none"> ■ IP-Adresse – Symbol für Geostandort-Zuordnung oder lokales Netzwerk. ■ Hostnamen – Domänenname für den Host. ■ Dienste – Alle Dienste, die auf dem Host erkannt werden. <p>Vorfälle im Zusammenhang mit dem Host:</p> <ul style="list-style-type: none"> ■ Anzahl der Vorfälle – Anzahl aller Vorfälle. ■ Max. Auswirkung – Zeigt die maximale Auswirkung aller Vorfälle an. ■ Bedrohungen – Eine Liste der erkannten Ereignisse. <p>Ein Hinweis gibt an, ob der Host gegenüber dem überwachten Netzwerk intern oder extern ist.</p>

Knotentyp	Informationen
HTTP-Anforderung	<p>Zusätzliche Informationen zu einer HTTP-Anforderung.</p> <p>URL-Details:</p> <ul style="list-style-type: none"> ■ Download-URLs – Die beobachtete(n) URL(s) in der HTTP-Anforderung. ■ IPs herunterladen – Die IP-Adresse(n) wurde(n) für die HTTP-Anforderung aufgelöst. Klicken Sie auf das , um die IP-Adresse der Anforderung in der Netzwerkanalyse anzuzeigen. <p>Anforderungsdetails</p> <ul style="list-style-type: none"> ■ Anzahl der Anforderungen – Wie oft die HTTP-Anforderung beobachtet wurde. ■ Hosts – IP-Adresse der Hosts, die die HTTP-Anforderung ausgeben. ■ Referenz – Die in der HTTP-Anforderung beobachteten „Referenz“-Header-Werte. ■ Benutzer-Agents – In der HTTP-Anforderung beobachtete Benutzer-Agent-Werte.
Bedrohung	<p>Zusätzliche Informationen zu einer Bedrohung</p> <p>Bedrohungsdetails:</p> <ul style="list-style-type: none"> ■ Bedrohungsklasse – Der Name der erkannten Bedrohungsklasse. Beispiel: command&control. ■ Bedrohung – Der Name der erkannten Bedrohung. Beispiel: Loki Bot. ■ Schweregrad – Die berechnete Bedrohungspunktzahl. ■ Informationen – Eine Beschreibung der erkannten Bedrohung

Wenn Sie auf einen Edge klicken, werden die folgenden Informationen zur Verbindung angezeigt:

- Quellknoten – Die Quelle der Verbindung. Hierbei kann es sich um einen Knotennamen, eine IP-Adresse, einen Domänennamen usw. handeln.
- Zielknoten – Das Ziel der Verbindung. Hierbei kann es sich um einen Knotennamen, eine IP-Adresse, einen Domänennamen usw. handeln.

Unter dem Knoten Quelle und Zielknoten befindet sich die tatsächliche Quelle oder das Ziel der Verbindung. Klicken Sie auf das , um die Quelle oder das Ziel zu erweitern.

Drittanbiertools

Die Registerkarte „Drittanbiertools“ verweist auf externe Tools, die zusätzliche Informationen zu einem im Diagramm ausgewählten Element bereitstellen können. Derzeit werden die Tools [DomainTools](#) und [VirusTotal](#) unterstützt.

Die folgenden Suchvorgänge werden unterstützt:

- Wenn Sie einen Hostknoten auswählen, können Sie in DomainTools und VirusTotal nach der entsprechenden IP-Adresse suchen.
- Wenn Sie einen Hostnamenknoten auswählen, können Sie in DomainTools und VirusTotal nach dem entsprechenden Domänennamen suchen.
- Wenn Sie einen heruntergeladenen Dateiknoten auswählen, können Sie in VirusTotal nach dem entsprechenden Hash suchen.
- Wenn Sie einen HTTP-Anforderungsknoten auswählen, können Sie in DomainTools und VirusTotal nach dem Hostnamen der Anforderung suchen.

Details zur Aktivität: Registerkarte „Hosts“

Auf der Registerkarte **Hosts** der Seite **Details zur Aktivität** wird eine Liste der Hosts angezeigt, die von der Aktivität betroffen sind.

Die Spalten enthalten die folgenden Informationen.

Spaltenname	Beschreibung
Hosts	Die IP-Adresse des Hosts, der von der Aktivität betroffen ist. Klicken Sie auf den Link der IP-Adresse. Daraufhin wird die Seitenleiste Hostübersicht wird auf der rechten Seite angezeigt.
Bedrohungen	Eine Liste aller Bedrohungen, die NSX Network Detection and Response auf dem Host erkannt hat.
Angriffsphasen	Die während der Bedrohungsaktivität beobachteten Angriffsphasen, die sich auf den jeweiligen Host auswirken.
Letzte Aktivität	Der Zeitstempel, wann zuletzt eine Aktivität für den Host erkannt wurde.

Details zur Aktivität: Registerkarte „Zeitachse“

Auf der Registerkarte **Zeitachse** der Seite **Details zur Aktivität** werden die von NSX Network Detection and Response erkannten Bedrohungen durch Bedrohungskarten dargestellt.

Eine Bedrohungskarte zeigt den mit dieser Bedrohung verbundenen Host, die berechnete Bedrohungspunktzahl, den Bedrohungsnamen und die Klasse, das Erkennungsergebnis (sofern verfügbar), den Bedrohungsstatus und andere Aktionen an. Um die zugehörigen Nachweise anzuzeigen, erweitern Sie die Karte, indem Sie auf den **>** klicken, wie in der folgenden Abbildung dargestellt. Klicken Sie auf das **▼**, um den Abschnitt „Nachweis“ zu reduzieren.

The screenshot shows the Threat Timeline section of the VMware NSX Intelligence interface. At the top, it displays campaign details: Campaign ID: b6f9b5, Date: 2021-08-12 – 2021-08-12, Latest stage: Exploitation, Affected hosts: 1, Threats: 2, and State: Open. Below this, there are tabs for Overview, Hosts, Timeline (which is selected), History, and Evidence. The Timeline shows two threat events:

- Aug 12, 12:48:57 - Aug 12, 12:48:57:** This card is expanded. It shows a host icon with IP 192.168.0.04, a threat level of 56 (ETERNALBLUE), and an evidence summary: 1 type: Signature. It indicates the latest stage is Exploitation and provides links to OPEN and NEXT STEPS. Below this, under Evidence, it lists a signature event from 12:48:57 on Aug 12 with a confidence of 75. It also shows network interactions and supporting data with 1 detection event.
- Aug 12, 12:48:50 - Aug 12, 12:48:50:** This card is collapsed, showing a host icon with IP 192.168.0.04, a threat level of 56 (CVE-2017-0143 EXPLOIT), and an evidence summary: 1 type: Signature. It indicates the latest stage is Exploitation and provides links to OPEN and NEXT STEPS.

Sortieren Sie die Bedrohungskarten mit dem Dropdown-Menü **Sortieren nach**. Treffen Sie eine Auswahl aus **Aktuellste** (Standardeinstellung), **Früheste**, **Höchste Auswirkung** und **Geringste Auswirkung**.

Das Textfeld **Bedrohungen suchen** oberhalb der Liste ermöglicht eine schnelle Suche direkt nach der Eingabe. Es filtert die Zeilen in der Liste und zeigt nur die Zeilen an, die in einem beliebigen Feld Text enthalten, der mit der Abfragezeichenfolge übereinstimmt. Ihre Abfrage wird mit Werten in den folgenden Kategorien abgeglichen: Auswirkung, IP-Adresse, Bedrohung/Malware, letzte Aktivitätsphase, erste Erkennung, Nachweise und andere Hosts sowie Nachrichteninformationen für E-Mail-Nachrichten.

Um die angezeigten Bedrohungskarten nach Bedrohungsstatus zu filtern, schalten Sie die Schaltfläche **Geschlossene Bedrohungen anzeigen** um. Standardmäßig werden alle Bedrohungen angezeigt.

Bedrohungskarten

Die Bedrohungskarten zeigen alle Bedrohungen im Zusammenhang mit der ausgewählten Aktivität und ihre entsprechenden Bedrohungsstufen an.

Jede Karte zeigt die berechnete Bedrohungsauswirkung, den Bedrohnamen, die Bedrohungsklasse und, falls verfügbar, das Erkennungsergebnis an. Außerdem wird der Bedrohungsstatus angezeigt: **OPEN** oder **CLOSED**.

Sie können auf **Weitere Schritte** klicken und eine Aktion aus dem Dropdown-Menü auswählen. Wählen Sie **Schließen** aus, um die Bedrohung zu schließen, **Öffnen**, um eine geschlossene Bedrohung erneut zu öffnen, oder **Warnung verwalten**, um eine Warnungsverwaltungsregel für die Bedrohung zu erstellen.

Der Abschnitt **Nachweisübersicht** enthält eine Übersicht über die Nachweise und andere Daten, die für die Bedrohung erkannt wurden. Klicken Sie auf das **▼** (oder fast überall auf der Karte), um den Abschnitt „Nachweisdetails“ zu erweitern.

Nachweisdetails

In der Spalte **Nachweise** werden die Dateidownloads, Signaturen und andere Kategorien zusammen mit einem Zeitstempel angezeigt, zu dem der Nachweis angezeigt wurde.

In der Spalte **Netzwerkinteraktionen und Netzwerk-IOCs** wird die IP-Adresse oder der Domänenname externer Hosts angezeigt. Klicken Sie auf den Link der IP-Adresse, um die Seitenleiste **Netzwerkinteraktion** zu erweitern.

Die Spalte **Unterstützende Daten** enthält einen Link zu den erkannten Ereignissen, einen Link zu den erfassten Daten und einen Link zu den Bedrohungsdetails.

Details zur Aktivität: Registerkarte „Verlauf“

Auf der Registerkarte **Verlauf** der Seite **Details zur Aktivität** der NSX Network Detection and Response-Benutzeroberfläche wird ein beschreibender Textverlauf zur Form der Aktivität angezeigt.

Jeder Eintrag enthält einen Hinweis und eine Beschreibung der aufgezeichneten Aktivitätsphasen sowie den Hinweiszeitstempel.

Details zur Aktivität: Registerkarte „Nachweis“

Auf der Registerkarte **Nachweise** der Seite **Details zur Aktivität** der NSX Network Detection and Response-Benutzeroberfläche wird eine Liste der für die aktuell ausgewählte Aktivität erkannten Nachweise angezeigt.

Jede Zeile ist eine Zusammenfassung der Nachweise für die Aktivität. Klicken Sie auf das  (oder an einer beliebigen Stelle in einer Eingabezeile), um die Zeile zu erweitern und die Informationen zu den Signurnachweisen anzuzeigen.

Die Nachweisliste enthält die folgenden Spalten.

Nachweisspalten	Beschreibung
IP-Adresse	Die IP-Adresse des Hosts, der die Quelle der Bedrohung ist.
Erste Erkennung	Zeitstempel, der die Startzeit der Aktivität anzeigt.
Letzte Erkennung	Zeitstempel, der die letzte aktive Aktion der Aktivität anzeigt.
Bedrohung	Name des erkannten Sicherheitsrisikos.
Bedrohungsklasse	Name der erkannten Sicherheitsrisikoklasse.
Auswirkung	<p>Der Auswirkungswert gibt die kritische Stufe der erkannten Bedrohung an und liegt zwischen 1 und 100:</p> <ul style="list-style-type: none"> ■ Bedrohungen ab 70 werden als kritisch betrachtet. ■ Bedrohungen zwischen 30 und 69 gelten als mittleres Risiko. ■ Bedrohungen zwischen 1 und 29 gelten als harmlose Bedrohungen. <p>Wenn das  [Blockieren-Symbol] angezeigt wird, weist dies darauf hin, dass das Artefakt blockiert wurde.</p>
Nachweise	Der abgeleitete Wert der Nachweise für die Aktivität. Einzelheiten dazu finden Sie unter Informationen zu Nachweisen .
Subjekt	Zusätzliche Informationen aus der Aktivität. Dies kann eine IP-Adresse, ein HTTP-Antwortcode oder einige andere Daten sein.
Verweis	Klicken Sie auf den Link, um auf die Seite Netzwerkereignisdetails zuzugreifen. Der Link wird auf einer neuen Browserregisterkarte geöffnet. Einzelheiten dazu finden Sie unter Seite „Ereignisprofil“ .
Vorfall-ID	Ein Permalink zu einem korrelierten Vorfall. Der Link wird auf einer neuen Browserregisterkarte geöffnet. Siehe Verwalten der Seite „Vorfälle“ .

Klicken Sie auf das , um die anzuzeigenden Spalten zu ändern. Standardmäßig werden alle verfügbaren Spalten angezeigt.

Wenn Sie auf das  klicken (oder an einer beliebigen Stelle in einer Nachweiszeile), werden die folgenden Informationen angezeigt.

Informationsname	Beschreibung
Bedrohung	Name des erkannten Sicherheitsrisikos.
Bedrohungsklasse	Name der erkannten Sicherheitsrisikoklasse.
Auswirkung	Die Auswirkungsbewertung der Aktivität.

Informationsname	Beschreibung
Detektor	Falls vorhanden, wird das NSX Network Detection and Response-Modul angezeigt, das die Bedrohung identifiziert hat. Klicken Sie auf den Link, um das Popup-Fenster Detektor anzuzeigen.
Netzwerkerkennung anzeigen	Falls vorhanden, wird das NSX Network Detection and Response-Modul angezeigt, das die Bedrohung identifiziert hat. Klicken Sie auf den Link, um das Popup-Fenster „Detektor“ anzuzeigen.
Vorfall anzeigen	Klicken Sie auf den Link, um auf die Seite „Netzwerkereignisdetails“ zuzugreifen. Der Link wird auf einer neuen Browserregisterkarte geöffnet. Siehe Seite „Ereignisprofil“.
Erste Erkennung	Zeitstempel, der die Startzeit der Aktivität anzeigt.
Letzte Erkennung	Zeitstempel, der die letzte aktive Aktion der Aktivität anzeigt.
Schweregrad	Eine Schätzung, wie kritisch die erkannte Bedrohung ist. Beispielsweise wird eine Verbindung zu einem Befehl und einem Steuerungsserver in der Regel als hoher Schweregrad betrachtet, da die Verbindung potenziell schädlich ist.
Konfidenz	Gibt die Wahrscheinlichkeit an, dass die erkannte individuelle Bedrohung böswillig ist. Da das System fortschrittliche Heuristiken verwendet, um unbekannte Bedrohungen zu erkennen, kann die erkannte Bedrohung in einigen Fällen einen niedrigeren Konfidenzwert haben, wenn die Menge der für diese spezifische Bedrohung verfügbaren Informationen begrenzt ist.

Eigenschaften der Aktivität

Eine von der NSX Network Detection and Response-Anwendung erkannte Aktivität ist durch mehrere Eigenschaften gekennzeichnet.

Im Folgenden sind die Eigenschaften der Aktivität und ihre Definitionen aufgeführt.

Eigenschaftsname	Beschreibung
Name	Eine Aktivitäts-ID, die die Aktivität eindeutig identifiziert.
Hosts	Die Hosts, die von der Aktivität betroffen sind.
Bedrohung	Die Bedrohungen, die für die Aktivität erkannt wurden.
Angriffsphasen	Die Phasen im Lebenszyklus des Angreifers, die den erkannten Aktivitäten entsprechen. Einzelheiten dazu finden Sie unter Informationen zu Angriffsphasen .
Dauer	Das Zeitintervall, in dem die Aktionen im Zusammenhang mit einer Aktivität beobachtet wurden.

Informationen zu Angriffsphasen

Angriffsphasen sind die Phasen im Lebenszyklus eines Angriffs, die den von der NSX Network Detection and Response-Anwendung erkannten Aktivitäten entsprechen.

Ein Angreifermodell beschreibt die Aktionen, die ein Angreifer ausführen kann, um in ein Unternehmensnetzwerk einzudringen und darin zu agieren. Die NSX Network Detection and Response-Anwendung verwendet das [ATT&CK™-Modell \(Adversarial Tactics, Techniques, and Common Knowledge\)](#) von MITRE zur Beschreibung des Angreiververhaltens. In diesem Modell werden die Techniken, die ein Angreifer einsetzen könnte, in eine Reihe von Taktikkategorien eingeteilt, die verschiedenen Phasen im Lebenszyklus eines Angriffs entsprechen.

Im System kann die Aktivität, die mit jedem erkannten Ereignis verbunden ist, einer bestimmten Angriffsphase zugeordnet werden und einen Hinweis auf den Fortschritt der Angriffsaktivität während ihres Lebenszyklus liefern. (Aktivitäten, die in verschiedenen Angriffsphasen auftreten, werden möglicherweise nicht einer bestimmten Angriffsphase zugeordnet.) Derzeit werden die folgenden Angriffsphasen verwendet.

Name der Angriffsphase	Beschreibung
Einsatz	Die Phase, in der Angreifer die Nutzlast an das Ziel senden. Zu den üblichen Verbreitungsmechanismen gehören Remote-Exploits, Drive-by-Download-Websites und bösartige USB- oder andere Wechselmedien.
Ausnutzung	Die Phase, in der die Nutzlast des Angreifers im Zielnetzwerk bereitgestellt wird. Dies ermöglicht es dem Angreifer, ein oder mehrere Geräte im Zielnetz zu kompromittieren und deren Steuerung zu übernehmen.
Befehl und Steuerung	Die Phase, in der die Angreifer mit den von ihnen kontrollierten Systemen im Zielnetz kommunizieren und effektiv einen („Hands-On-Keyboard“) Remotezugriff auf diese Systeme erlangen.
Zugang mit Anmeldedaten	Die Phase, in der Angreifer Zugriff auf oder Kontrolle über System-, Domänen- oder Dienstanmeldedaten erlangen, die in der Zielumgebung verwendet werden. In der Regel versuchen Angreifer, legitime Anmeldedaten von Benutzer- und Administratorkonten abzurufen, um sich als diese Benutzer auszugeben oder um neue Konten zu erstellen.
Ermittlung	Die Phase, in der Angreifer versuchen, weitere Informationen über die Zielumgebung zu finden. Angreifer versuchen oft, zusätzliche Geräte im Netzwerk zu identifizieren, die sie zur Erreichung ihrer Ziele nutzen können.
Lateral Movement	Die Phase, in der sich Angreifer durch das Zielnetz bewegen, indem sie Zugriff und Kontrolle über entfernte Systeme erlangen.
Sammlung	Die Phase, in der Angreifer Informationen aus einem Zielnetzwerk identifizieren und sammeln, um sie anschließend zu exfiltrieren.
Exfiltration	Die Phase, in der Angreifer Dateien und Informationen aus einem Zielnetzwerk entfernen.

Informationen zu Korrelationsregeln

Im Allgemeinen werden Vorfälle zu einer Aktivität zusammengefasst, wenn es Anhaltspunkte dafür gibt, dass die betreffenden böswilligen Aktionen oder Angriffe miteinander in Zusammenhang stehen.

Da diese Korrelationsregeln im NSX Advanced Threat Prevention Cloud Service ausgeführt werden, können sie unabhängig von den NSX-T-Versionszyklen verbessert oder erweitert werden. Darüber hinaus kann sich die Liste der Korrelationsregeln oder das spezifische Verhalten einer Regel im Laufe der Zeit ändern.

Im Folgenden finden Sie die aktuell unterstützten Korrelationsregeln.

Anomalie-Ereignis

Diese Regel korreliert die Erkennungsergebnisse der NSX Suspicious Traffic-Funktion mit Ereignissen vom Typ „Infektion“, die eine größere Auswirkung haben. So fällt beispielsweise ein anormales Ereignis der NSX Suspicious Traffic-Funktion mit einem Netzwerkereignis mit großer Auswirkung für dieselben Hosts zusammen.

Exfiltration

Diese Regel korreliert Exfiltrationsereignisse, denen Ereignisse vom Typ „Infektion“ vorausgehen. Zum Beispiel folgt auf ein Befehls- und Steuerungs-Netzwerkereignis ein Netzwerkereignis, von dem wir wissen, dass es Daten exfiltriert.

Dateiübermittlung (hashbasiert)

Diese Regel korreliert schädliche Dateiübermittlungen. Wenn beispielsweise dieselbe bösartige Datei auf mehrere Hosts im Netzwerk heruntergeladen wird, ordnet die Regel alle diese Übertragungen einem Eindringling zu. Die Ähnlichkeit schädlicher Dateiübertragungen wird auf der Grundlage des SHA-1-Hash der übertragenen Datei bestimmt.

Dateiübermittlung (Analyse-Tag-basiert)

Diese Regel korreliert schädliche Dateiübermittlungen. Wenn beispielsweise dieselbe bösartige Datei auf mehrere Hosts im Netzwerk heruntergeladen wird, ordnet die Regel alle diese Übertragungen einem Eindringling zu. Die Ähnlichkeit schädlicher Dateiübermittlungen wird auf der Grundlage der Tags bestimmt, die den Analyseaufgaben der Dateien zugeordnet sind.

Schwachstellenprüfung

Diese Regel korreliert verschiedene Arten von Netzwerkereignissen, die alle potenziell auf einen Schwachstellenprüfung hindeuten. Beispielsweise werden mehrere ausgehende Infektions- oder NTA-Ereignisse von einem einzelnen Host zu einem oder mehreren internen Zielhosts beobachtet.

Welle

Diese Regelgruppe identifiziert „Angriffswellen“, bei denen derselbe Angriff (d. h. Vorfälle für dieselbe Bedrohung) auf mehreren Hosts im gesamten Netzwerk innerhalb eines bestimmten Zeitfensters beobachtet wird.

Diese Gruppe von Regeln ist nützlich, um Hosts im Netzwerk zu identifizieren, die in dieselbe Befehls- und Steuerungsinfrastruktur eingebunden sind oder demselben Angriffsvektor ausgesetzt waren (z. B. Drive-by-Angriff oder Malwareverteilung). Daher sind diese Regeln auf Bedrohungen der Klassen Befehl und Steuerung, Drive-by, Malwareverteilung, Sinkhole, Fake-AV und Crypto Mining beschränkt.

Die Regeln in dieser Gruppe werden in den folgenden Fällen ausgelöst.

- Es liegen Netzwerksignaturereignisse vor, bei denen die Bedrohungsklasse „Befehl und Steuerung“ lautet und die sich auf mehrere Hosts auswirken.
- Es liegen Netzwerksignaturereignisse vor, bei denen die Bedrohungsklasse „Malwareverteilung“ lautet und die sich auf mehrere Hosts auswirken.

- Für den gleichen Eintrag (IP-Adresse oder Hostname) liegen Netzwerksignaturereignisse vor, bei denen die Bedrohungsklasse „Drive-by“ lautet und mehrere Hosts betroffen sind.
- Für den gleichen Eintrag (IP-Adresse oder Hostname) liegen Reputationsereignisse vor, wobei die Bedrohungsklasse „Befehl und Steuerung“ lautet und mehrere Hosts betroffen sind.
- Für den gleichen Eintrag (IP-Adresse oder Hostname) liegen Reputationsereignisse vor, wobei die Bedrohungsklasse „Malwareverteilung“ lautet und mehrere Hosts betroffen sind.

In diesem Fall ist das Korrelationsfenster auf drei Tage festgelegt. Daher werden zwei Vorfälle für dieselbe Bedrohung, die verschiedene Hosts betreffen, als zusammenhängend betrachtet, wenn sie innerhalb dieses begrenzten Zeitbereichs auftreten.

Hinweis Diese Regeln können Aktivitäten erstellen, die nur aus einem Host und einem Vorfall bestehen.

Bestätigter Drive-by-Angriff

Diese Regelgruppe identifiziert Aktionen, bei denen ein interner Host einem erfolgreichen Drive-by-Angriff ausgesetzt ist. Ein Drive-by-Angriff auf einen Host gilt als erfolgreich, wenn darauf ein Befehls- und Steuerungsdatenverkehr (C&C), ein Malware-Download, ein Sinkhole oder eine gefälschte AV-Aktivität folgt. Die Regeln in dieser Gruppe werden in den folgenden Fällen ausgelöst.

- Drive-by-Angriff dicht gefolgt von Malware-Download-Aktivität: In diesem Fall beträgt das Korrelationsfenster 10 Minuten, da wir davon ausgehen, dass der Download unmittelbar durch einen erfolgreichen Browser-Exploit ausgelöst wurde.
- Drive-by-Angriff dicht gefolgt von einer gefälschten AV-Aktivität: In diesem Fall beträgt das Korrelationsfenster 10 Minuten, da wir erwarten, dass die gefälschte AV-Aktivität unmittelbar auf einen Drive-by-Exploit folgt.
- Drive-by-Angriff mit anschließender Befehls- und Steuerungsaktivität: In diesem Fall beträgt das Korrelationsfenster vier Stunden, da die Einrichtung des Befehls- und Steuerungskanals einige Zeit dauern kann.
- Drive-by-Angriff mit anschließender Sinkhole-Aktivität: In diesem Fall beträgt das Korrelationsfenster vier Stunden, da die Aktivität in Richtung eines bösartigen Sinkhole-Servers über einen Befehl- und Steuerungskanal einige Zeit in Anspruch nehmen kann.

Hinweis Diese Regeln können Aktivitäten erstellen, die nur einen Host betreffen.

Bestätigter Dateidownload

Diese Gruppe von Regeln identifiziert Aktivitäten, bei denen eine bösartige Datei heruntergeladen und erfolgreich auf einem Host ausgeführt wird. Eine heruntergeladene Datei gilt als erfolgreich auf einem Host ausgeführt, wenn kurz nach dem Download Netzwerkereignisse für Aktivitäten auftreten, die mit den bei der Dateianalyse beobachteten Aktivitäten übereinstimmen.

Insbesondere kann die Dateianalyse zwei weitere Informationen zur Charakterisierung der während der Analyse beobachteten Aktivität liefern.

Malware-Informationen

Wenn das Dateiverhalten mit dem Verhalten einer bekannten Bedrohung übereinstimmt, wird der Malware-Name verfügbar.

Informationen zum Netzwerk-IoC

Wenn die Probe während der Analyse Netzwerksignaturen oder Threat Intelligence übereinstimmt, werden Indikatoren für diesen Datenverkehr zur Verfügung gestellt. Das heißt, es werden Informationen über bösartige Reputationen und Netzwerksignaturübereinstimmungen bereitgestellt.

Die Regeln in dieser Gruppe werden in den folgenden beiden Fällen ausgelöst, je nach Art der aus der Dateianalyse abgeleiteten Informationen.

- Malware-basierter Fall
 - Eine Datei wird auf einen Host heruntergeladen.
 - Die Dateianalyse weist der Datei eine bestimmte Bedrohung zu (z. B. Emotet-Malware).
 - Zu einem späteren Zeitpunkt wird für den Host, der die Datei heruntergeladen hat, ein Netzwerkereignis für dieselbe Bedrohung (d. h. Emotet) erkannt.
- Netzwerk IoC-basierter Fall
 - Eine Datei wird auf einen Host heruntergeladen.
 - Die Dateianalyse identifiziert das Netzwerk-IoC für die Datei.
 - Zu einem späteren Zeitpunkt versucht der Host, der die Datei heruntergeladen hat, eine IP-Adresse oder einen Hostnamen zu kontaktieren, der in der für die Datei extrahierten Reputations-IoC enthalten ist. Dieser Datenverkehr stimmt mit einer Netzwerksignatur überein.

Die NSX Network Detection and Response-Anwendung legt das Korrelationsfenster in diesem Fall auf drei Tage fest.

Hinweis Mit dieser Regel können Aktivitäten erstellt werden, die nur aus einem Host bestehen.

Lateral Movement

Diese Regelgruppe identifiziert Aktivitäten, bei denen die Angreifer einen „Brückenkopf“ im Netz geschaffen haben, indem sie nach dem Eindringen in einige Hosts versuchen, sich seitlich im Netz zu bewegen, um weitere Hosts zu kompromittieren.

Diese Gruppe umfasst zwei Regeln, von denen jede einen separaten Schritt des Lateral Movement-Angriffs erfasst.

Ausgehende laterale Bewegung

Diese Regel korreliert ausgehende Lateral Movement-Aktivitäten von einem Host im Home-Netzwerk mit Infektionen auf diesem Host, die vor den Lateral Movement-Erkennungen (aber innerhalb des Korrelationsfensters) stattfanden.

Eingehende laterale Bewegung

Diese Regel korreliert eingehende Lateral Movement-Aktivitäten in Richtung eines Hosts im konfigurierten Home-Netzwerk mit Aktivitäten, die üblicherweise nach einer anfänglichen Kompromittierung beobachtet werden (Befehl und Kontrolle, Sondierung und Auslesen von Anmelddaten) und die auf demselben Host nach den Lateral Movement-Erkennungen auftreten.

Diese Regeln werden nur für Hosts innerhalb des Home-Netzwerks ausgelöst, d. h. die Aktivität wird nur erstellt, wenn sowohl Quell- als auch Zielhosts, auf denen die Lateral Movement-Aktionen stattfinden, dem Home-Netzwerk angehören. Wenn das Home-Netzwerk nicht konfiguriert ist, verwendet das System standardmäßig [RFC1918-Bereiche](#).

Heraufstufung der INFO-Ereignisse

Die NSX Network Detection and Response-Anwendung erkennt mehrere Aktivitäten in einem geschützten Netzwerk, die für einen Analysten von Interesse sein könnten, aber wahrscheinlich nicht böswillig sind. Diese Erkennungen erzeugen INFO-Ereignisse, die durch Einstellen eines geeigneten Werts für den Filter „Ereignisergebnis“ angezeigt werden können.

Die NSX Network Detection and Response-Anwendung berücksichtigt INFO-Ereignisse nicht für Korrelationszwecke.

Eine Herausforderung bei diesen Erkennungen besteht darin, dass ein und dieselbe INFO-Ereignisaktivität normal oder höchst verdächtig sein kann, je nachdem, in welchem Netzwerk die NSX Network Detection and Response-Anwendung sie entdeckt hat. So kann beispielsweise die Verwendung des Remote-Desktop-Protokolls (RDP) in einer Umgebung, in der dieses Tool für legitime Verwaltungszwecke verwendet wird, normal sein. Ansonsten ist dies jedoch ein höchst verdächtiger Hinweis darauf, dass ein Angreifer versucht, einen Opfer-Host remote zu steuern.

Die Anomalieerkennungslogik kann ermitteln, wann bestimmte Arten von INFO-Erkennungen für das überwachte Netzwerk und für die jeweiligen betroffenen Quellhosts und Zielhosts ungewöhnlich sind. Wenn das System feststellt, dass eine INFO-Erkennung ungewöhnlich ist, wird das Ereignis zum Modus „Erkennung“ heraufgestuft und infolgedessen unter den regulären Ereignissen angezeigt. Dieses Szenario ist im Kontext von Korrelationsregeln für laterale Bewegungen relevant, da die Erkennung von Lateral Movement-Aktivitäten häufig zur Erstellung von INFO-Ereignissen führt.

Home-Netzwerk

Die Konfiguration des Home-Netzwerks hat folgende Auswirkungen auf die Aktivitätenkorrelationsregeln.

- Alle Aktivitätenkorrelationsregeln ignorieren Ereignisse, die auf Hosts außerhalb des Home-Netzwerks aufgetreten sind.

- Wenn kein Home-Netzwerk konfiguriert ist, verwendet das System standardmäßig die [RFC1918-Bereiche](#).

Das Home-Netzwerk wird unter **Sicherheit > Allgemeine Einstellungen > Private IP-Bereiche** konfiguriert.

Stilllegung von Hosts (Host Silencing)

Die Konfiguration von Host Silencing hat die folgenden Auswirkungen auf die Aktivitätenkorrelationsregeln.

- Wenn Host Silencing konfiguriert ist, ignorieren alle Aktivitätenkorrelationsregeln Ereignisse, die auf stillgelegten Hosts stattgefunden haben.
- Wenn kein Host Silencing konfiguriert ist, werden alle Quellhosts, die in einem Ereignis erkannt werden, als gültig für die Korrelation betrachtet.

Um sicherzustellen, dass Host Silencing nicht fälschlicherweise Hosts einschließt, deren Aktionen in Aktivitäten berücksichtigt werden sollten, müssen Sie Ihre Host Silencing-Konfiguration überprüfen.

Informationen zu Nachweisen

Die NSX Network Detection and Response-Anwendung liefert Berichte über die Aktionen, die bei der Analyse eines Ereignisses, Vorfalls oder einer Aktivität beobachtet wurden.

Der Nachweis enthält die folgenden Informationen.

Basiserkennungsnachweis: Netzwerk

Nachweistyp: REPUTATION

Gibt an, dass Netzwerkdatenverkehr zu einer IP oder Domäne erkannt wurde, die mit einer bekannten Bedrohung verknüpft ist.

Ein SUBJEKT-Feld und eine IP-Adresse oder Domäne werden angezeigt. Beispiel: Reputation: evil.com (Referenzereignis), 6.6.6.6 (Referenzereignis) oder bad.org (Referenzereignis).

Diese fehlerhaften Domänen und IP-Adressen werden in der Regel blockiert. Wenn verfügbar, werden zusätzliche Reputationsinformationen angezeigt.

IP-Adressen können mit einer Ortsangabe (Landesflagge) versehen werden.

Nachweistyp: SIGNATUR

Gibt an, dass Netzwerkdatenverkehr erkannt wurde, der einer Netzwerksignatur für eine bekannte Bedrohung entspricht.

Es wird ein Detector-Feld angezeigt, das den Namen bzw. den eindeutigen Bezeichner der übereinstimmenden Signatur enthält. Beispiel: Detector: et:2014612 oder Detector: llrules:1490720342088.

Nachweistyp: ANOMALIE

Ähnlich wie bei SIGNATUR, mit dem Unterschied, dass die Erkennung auf einer Heuristik basiert, die eine Anomalie entdeckt hat. Beispiel: `Anomaly: anomaly:download_smb`.

Nachweistyp: DATEIDOWNLOAD

Eine bösartige oder verdächtige Datei wurde heruntergeladen.

Eine `task_uuid`, der Bezeichner einer Analyse (Detonation in der Sandbox), und der `severity`, die Bewertung dieser Analyse, werden angezeigt. Beispiel: `File download: a7ed621`.

Im Folgenden sind zusätzliche optionale Informationen aus dem Referenzereignis aufgeführt.

- Die URL, von der die Datei heruntergeladen wurde
- Der Dateityp (in der Regel ausführbare Datei)
- Der Dateiname

Nachweistyp: UNUSUAL_PORT

Gibt an, dass ein TCP- oder UDP-Port verwendet wird, der ein ungewöhnlicher Port ist und dem entspricht, was von dieser spezifischen Bedrohung erwartet wird.

Die IP-Adresse oder Domäne, die an dem Datenverkehr beteiligt ist, der den ungewöhnlichen Port verwendet hat, wird im SUBJEKT-Feld angezeigt.

Nachweistyp URL_PATH_MATCH

Ähnlich wie „Unusual Port“, mit dem Unterschied, dass die Erkennung auf einem URL-Pfad basiert. Zum Beispiel `http://evil.com/evil/path?evil=threat`, die Erkennung wird durch den `/evil/path`-Teil der URL ausgelöst.

Nachweistyp DGA

DGA steht für „Algorithmus zur Domänengenerierung“, ein Ansatz, der von einigen Malware-Programmen verwendet wird. Anstatt eine kleine Anzahl von Domänen für den Command-and-Control-Angriff zu verwenden, enthält die Malware einen Algorithmus, der jeden Tag Tausende von neuen, zufällig aussehenden Domänen erzeugt. Anschließend versucht sie, jede von ihnen zu erreichen. Um die Malware zu steuern, registriert der Hacker einfach eine oder einige dieser Domänen. Der Einsatz von DGA ist im Netz aufgrund der Auflösungsversuche vieler solcher Domänen deutlich zu erkennen.

Die DGA-Nachweise werden zurzeit zusätzlich zu regulären Reputationsnachweisen verwendet, wenn mehrere ungültige Domänen von einem DGA-Algorithmus erkannt werden, der aufgelöst wird.

Nachweis aus Korrelation mehrerer Ereignisse

Nachweis aus Korrelation mehrerer Ereignisse

Die folgenden Nachweistypen werden erstellt, wenn die Kombination mehrerer Netzwerkereignisse auf einem Host das Vertrauen erhöht, dass eine Bedrohung korrekt erkannt wurde. Bei den Nachweistypen kann es sich z. B. um denselben Reputationseintrag handeln, der kontaktiert wurde, oder um dieselbe Netzwerksignatur, die ausgelöst wurde.

Für jeden dieser Fälle kann die Bedrohung wie folgt gekennzeichnet werden.

- **Repeated:** Die konkrete Bedrohung wurde drei oder mehr Mal beobachtet.
- **Periodic:** Die konkrete Bedrohung trat auch in regelmäßigen Abständen auf.

Die entsprechenden Reputations-/Signurnachweise werden mit einer Kennzeichnung versehen.

Im Beispiel des REPUTATION-Nachweises wird ein REPEATED- oder PERIODIC-Tag angezeigt, wenn wiederholte und periodische Nachweise für bad.org erkannt werden.

Nachweistyp: CONFIRMED_EXECUTION

Dies steht im Zusammenhang mit Bedrohungen, wie z. B. SCHÄDLICHER DATEIDOWNLOAD. Das bedeutet, dass von dem Host, der die Datei heruntergeladen hat, ein Netzwerkverhalten erkannt wurde, das bestätigt, dass die heruntergeladene Datei tatsächlich ausgeführt wurde.

Das bedeutet:

- Eine bösartige Datei wurde auf den Host 1.2.3.4 heruntergeladen.
- Wenn sie in einer Sandbox ausgeführt wurde, kontaktierte diese Datei den bösartigen Host evil.com.
- Kurz danach wird der Befehls- und Steuerungsdatenverkehr vom Host 1.2.3.4 zu evil.com beobachtet, der bestätigt, dass die schädliche Datei ausgeführt wurde.

Das verknüpfte Referenzereignis ist der Ort, an dem die Datei heruntergeladen wurde.

Zusätzliche Nachweise können die Bedrohung bestätigen, z. B. die folgenden Informationen über die Datei.

- Aufgaben-UUID
- Bewertung
- Dateiname
- URL, von der sie heruntergeladen wurde

Nachweistyp: CONFIRMED_C&C

Ähnlich wie der Nachweis CONFIRMED_EXECUTION wird dieser Nachweis zur Erkennung von Befehls- und Steuerungsdatenverkehr für die angegebene Bedrohung hinzugefügt, da der Host zuvor eine Datei für diese Bedrohung heruntergeladen hat.

Nachweistyp: CONFIRMED_DRIVE_BY

Dies wird hinzugefügt, wenn ein Drive-By-Angriff erkannt wurde, gefolgt von einem Hinweis, dass der Angriff erfolgreich war. Beispiel:

- Host 1.2.3.4 scheint Opfer eines Drive-by-Angriffs zu sein.
- Kurze Zeit später wird Host 1.2.3.4 ebenfalls zum Opfer:
 - Eine schädliche Datei wurde heruntergeladen.
 - Befehls- und Steuerungsdatenverkehr wurde ausgeführt

Dieser Nachweis wird dem Referenzereignis des anfänglichen Drive-by-Ereignisses hinzugefügt.

Nachweistyp: DRIVEBY_CONFIRMATION

Ähnlich wie der Nachweis CONFIRMED_DRIVEBY wird dieser Nachweis als Referenzereignis zu den Erkennungen des Herunterladens einer schädlichen Datei oder der Ausführung der Befehls- und Steuerungsdatenverkehrs hinzugefügt, die kurz nach einem Drive-by-Angriff erfolgten.

Arbeiten mit der Seite „Hosts“

Auf der Seite **Hosts** wird eine Liste der überwachten Hosts in Ihrem NSX-T Data Center-Netzwerk angezeigt.

Die Seite besteht aus mehreren Widgets, die mithilfe der Informationen in [Kennenzlernen der NSX Network Detection and Response-Benutzeroberfläche](#) verwaltet werden können.

Sie können die Auswahl von Hosts mithilfe der Filterverknüpfungen schnell anpassen. Sie können auch Ihre eigenen Filter auswählen. Verwenden Sie diese Filter, um die Hostliste anzupassen, die auf der Seite **Hosts** angezeigt wird.

Das folgende Bild zeigt ein Beispiel für eine **Hosts**-Seite.

The screenshot shows the 'Hosts' page interface. At the top, there's a header bar with 'Hosts', 'TIME RANGE: LAST 7 DAYS', and 'VIEW OPTIONS'. Below it is a toolbar with 'Filter shortcuts' (Hosts with Threats, Open High Impact Threats, Non-Campaign Threats), a search bar ('Search IP address or range'), and a 'GO' button. A 'Filters' section includes a 'Quick search' input and a 'SELECT' dropdown. The main area displays a table of host information with columns: IMPACT, HOST IP, THREATS, THREAT ACTIVITY, and CAMPAIGNS. There are 5 hosts listed:

IMPACT	HOST IP	THREATS	THREAT ACTIVITY	CAMPAIGNS
92	35.199.17.54	Testcrypt	2021-08-24 14:36:56 - 2021-08-26 09:...	-
60	15.199.04	ETERNALBLUE, CVE-2017-0143 Expl...	2021-08-24 14:36:55 - 2021-08-26 15:...	1
60	1.2.238.177	ETERNALBLUE	2021-08-24 14:36:31 - 2021-08-26 15:4...	-
60	1.2.19.3	CVE-2017-0143 Exploit	2021-08-24 14:36:25 - 2021-08-26 15:...	-
1	52.4.181.42	Lastline sensor rule test	2021-08-24 14:38:22 - 2021-08-25 11:4...	-

Filtern von Verknüpfungen

Verwenden Sie die Filterverknüpfungen, um die Daten in der Hostliste auf der Seite **Hosts** der NSX Network Detection and Response-Benutzeroberfläche zu begrenzen.

Um eine der folgenden Filterverknüpfungen auszuwählen, klicken Sie auf die entsprechende Schaltfläche, die auf der Benutzeroberfläche angezeigt wird.

Verknüpfungsname	Beschreibung
Hosts mit Bedrohungen	Listet alle Hosts im Startnetzwerk mit erkannten Bedrohungen auf.
Offene Bedrohungen mit hoher Auswirkung	Listet alle Hosts im Startnetzwerk mit offenen Bedrohungen mit hoher Auswirkung auf.
Bedrohungen ohne Aktivität	Listet alle Hosts im Startnetzwerk mit Bedrohungen auf, die nicht Teil einer Aktivität sind.

Alternativ können Sie auch die angezeigten Daten einschränken, indem Sie eine gültige IPv4-IP-Adresse, einen gültigen IP-Adressbereich oder einen CIDR-Block in das Suchtextfeld rechts neben dem Widget **Filterverknüpfungen** eingeben und auf **Gehe zu** klicken.

Verwenden von Filtern auf der Seite „Host“

NSX Network Detection and Response-Anwendung bietet einen Filtermechanismus, mit dem Sie sich auf bestimmte Host-Informationen konzentrieren können, die für Sie von Interesse sind. Die Verwendung von Filtern ist optional.

Verfahren

- 1 Klicken Sie auf der Seite **Hosts** auf das anzuzeigen und das Widget **Filter** zu erweitern.
- 2 Klicken Sie auf eine beliebige Stelle im Textfeld **Filter auf** und wählen Sie ein Element im Dropdown-Menü aus.

Sie können aus den folgenden verfügbaren Filtern auswählen. Um den Fokus der angezeigten Informationen weiter einzuschränken, können Sie mehrere Filter kombinieren.

Filtername	Beschreibung
Aktivitäten-UUID	Schränken Sie die angezeigten Einträge durch die Aktivitäten-UUID ein. Dies ist eine 32-stellige hexadezimale Zeichenfolge, z. B. 7dabc0fc9b3f478a850e1089a923df3a. Alternativ können Sie die Zeichenfolge <code>null</code> eingeben, um Datensätze auszuwählen, die zu keiner Aktivität gehören.
Home-Netzwerk	Schränken Sie die angezeigten Einträge durch die Einstellung Home-Netzwerk ein. Wählen Sie im Dropdown-Menü Nur Home-Netzwerk oder Nicht identifizierte Netzwerke aus.
Host-IP	Beschränken Sie die angezeigten Einträge auf eine bestimmte Quell-IP-Adresse, einen bestimmten IP-Adressbereich oder einen CIDR-Block. Geben Sie den Wert in das Textfeld ein.
Hosts mit Bedrohungen	Schränken Sie die angezeigten Einträge auf die Hosts mit Bedrohungssatus ein. Wählen Sie im Dropdown-Menü Hosts mit Bedrohungen oder Alle Hosts aus.

Filtername	Beschreibung
Priorität	Schränken Sie die angezeigten Einträge nach dem Prioritätsstatus ein. Wählen Sie im Dropdown-Menü Infektionen , Überwachungsliste oder Belästigungen aus.
Gelesen	Schränken Sie die angezeigten Einträge nach ihrem Gelesenstatus ein. Wählen Sie im Dropdown-Menü Gelesen oder Ungelesen aus.
Status	Schränken Sie die angezeigten Einträge nach ihrem Status ein. Wählen Sie Geschlossen oder Offen im Dropdown-Menü aus.
Bedrohung	Schränken Sie die angezeigten Einträge auf eine bestimmte Bedrohung ein. Wählen Sie eine Bedrohung aus dem Dropdown-Menü aus. Das Menü wird mit einer Liste katalogisierter Bedrohungen vorausgefüllt. Verwenden Sie die Suchfunktion oben im Menü, um schnell einen Bedrohungsnamen zu finden.
Bedrohungsklasse	Schränken Sie die angezeigten Einträge auf eine bestimmte Bedrohungsklasse ein. Wählen Sie die Bedrohungsklasse aus dem Dropdown-Menü. Das Menü ist mit einem Katalog von Klassen vorausgefüllt, von denen einige unten aufgeführt sind. Verwenden Sie die Suchfunktion oben im Menü, um schnell einen Klassennamen zu finden. <ul style="list-style-type: none"> ■ Adware: Malware, die auf einem infizierten Computer Werbung anzeigt oder herunterlädt. ■ Klickbetrug: Klickbetrug zielt auf Pay-per-Click-Online-Werbung ab. ■ Befehl und Steuerung: Ein infizierter Computer gehört zu einem Botnet und kann von einem Angreifer aus der Ferne gesteuert werden. ■ Drive-by: Ein Angreifer versucht, eine Sicherheitslücke auf dem Computer auszunutzen, um zusätzliche Malware auf dem Zielsystem zu installieren. ■ Exploit-Toolkit: Erkennung eines Exploit-Toolkits, das einen Drive-by-Download-Angriff versucht hat ■ Fake-AV: Gefälschte Antiviren-Software oder andere Arten betrügerischer Sicherheitssoftware, die darauf abzielt, Ihre Benutzer zu täuschen oder in die Irre zu führen. ■ Inaktives C&C: Der Befehls- und Steuerungsserver für dieses spezifische Botnet ist inaktiv. ■ Download bösartiger Dateien, Malwareverteilung und Malware-Download: Die IP-Adresse oder Domäne hostet bösartige ausführbare Dateien. ■ Sinkhole: Ein Sinkhole wird von einer legitimen Organisation betrieben, stellt also keine Bedrohung dar. Allerdings können Hosts, die versuchen, einen solchen Host zu kontaktieren, infiziert werden. ■ Spyware: Malware, die versucht, vertrauliche Informationen zu entwendern. ■ suspicious-dns: Verdächtige DNS-Domänen sind Domänen, die von Malware kontaktiert werden, die auf infizierten Computern ausgeführt wird. Unsere proprietären Techniken konnten diese Domänen proaktiv als böswillig identifizieren. ■ Unbekannt: Ein unbekanntes Sicherheitsrisiko wurde erkannt.

- 3 Um die ausgewählten Filter anzuwenden, klicken Sie auf **Anwenden**.
- 4 (Optional) Um einen einzelnen Filter zu löschen, klicken Sie neben dem Eintrag auf die Schaltfläche – **Entfernen**. Um alle ausgewählten Filter zu löschen, klicken Sie auf das Symbol **X** rechts neben dem Widget **Filter**.

Das Widget **Filter** wird ausgeblendet, wenn Sie alle ausgewählten Filter löschen.

Hostliste

Im unteren Teil der Seite **Hosts** der NSX Network Detection and Response-Benutzeroberfläche wird eine Liste der Hosts angezeigt, die die Kriterien der ausgewählten Filter erfüllen. Wenn keine Filter ausgewählt wurden, werden alle Hosts in Ihrem Netzwerk angezeigt.

Suchen

Das Textfeld **Schnellsuche** im oberen linken Abschnitt des Listen-Widgets bietet eine Schnelleingabefunktion für die Suche. Das System filtert die Zeilen in der Liste und zeigt nur die Zeilen an, deren Text in jeder Spalte mit der Abfragezeichenfolge übereinstimmt.

Hinweis Wenn die Liste lang ist, scannt die **Schnellsuche** nur die ersten 1.000 Einträge und kann unvollständige Ergebnisse zurückgeben. Die Gesamtanzahl der zurückgegebenen Suchergebnisse wird in der oberen rechten Ecke des Listen-Widgets angezeigt.

Auswahl

Verwenden Sie das Dropdown-Menü **AUSWÄHLEN** für eine detaillierte Auswahl. Die verfügbaren Auswahloptionen sind **Alle sichtbar**, **Alle Seiten** oder **Auswahl löschen**. Um alle sichtbaren Hosts auszuwählen, können Sie in der Zeile für Spaltennamen auch auf das klicken.

Hostliste

Sie können die Anzahl der Zeilen anpassen, die in der Hostliste angezeigt werden. Die Standardeinstellung ist 20 Einträge. Verwenden Sie die Symbole mit dem  und dem , um durch mehrere Seiten zu navigieren.

Jede Zeile enthält eine Informationsübersicht für einen Host. Um eine Hostzeile auszuwählen, klicken Sie auf das . Um auf weitere Informationen zu einem Host zuzugreifen, klicken Sie auf eine beliebige Stelle in einer Eingabezeile und das Seitenleistenbereich **Host-Übersicht** wird angezeigt. Einzelheiten dazu finden Sie unter [Seitenleiste „Hostübersicht“](#).

Die Liste enthält die folgenden Spalten.

Spaltenname	Beschreibung
AUSWIRKUNG	<p>Aktive Bedrohungen auf dem Host werden mit dem Symbol für  angezeigt.</p> <p>Der Auswirkungswert gibt die kritische Stufe der erkannten Bedrohung an und liegt zwischen 1 und 100:</p> <ul style="list-style-type: none"> ■ Ein Bedrohungswert von 70 oder höher gilt als kritisch. Die Zahl wird rot angezeigt. ■ Ein Bedrohungswert zwischen 30 und 69 gilt als mittleres Risiko. Die Zahl wird gelb angezeigt. ■ Ein Bedrohungswert zwischen 1 und 29 wird als ungefährlich eingestuft. Die Zahl wird blau angezeigt.
HOST-IP	Die IP-Adresse des Hosts. Klicken Sie auf den Link IP-Adresse, um die Seite Hostprofil für den Host anzuzeigen.
BEDROHUNGEN	Zeigt den Namen des am häufigsten erkannten Sicherheitsrisikos und die Anzahl der auf dem Host erkannten Bedrohungen an. Wenn der Name mit einem  versehen ist, klicken Sie darauf und ein Popup-Fenster zeigt die Beschreibung der Bedrohung an.

Spaltenname	Beschreibung
BEDROHUNGSAKTIVITÄT	Zeitstempel des ersten und des letzten Ereignisses, das zu diesem Vorfall gehört.
AKTIVITÄTEN	Das Symbol  gibt die Anzahl der Aktivitäten an, zu denen der Host gehört.

Seitenleiste „Hostübersicht“

Klicken Sie auf eine beliebige Stelle in einer Eintragszeile für einen Host in der Hostliste und die Seitenleiste **Hostübersicht** wird auf der rechten Seite der Seite **Hosts** angezeigt.

Im Folgenden wird beschrieben, was in der Seitenleiste „Hostübersicht“ angezeigt wird.

Oberster Abschnitt

Die folgenden Elemente werden im oberen Fensterbereich angezeigt.

- Um die Seitenleiste zu schließen, klicken Sie auf das Symbol zum .
- Der Auswirkungswert und die IP-Adresse des ausgewählten Hosts werden angezeigt.
- Zeigen Sie auf den Auswirkungswert und der Bedrohungsstatus wird angezeigt.
- Um zur Seite **Hostprofil** zu wechseln, klicken Sie auf **Profil anzeigen**.
- Die Anzahl der Aktionen, Bedrohungen, Anwendungen und Dienste wird angezeigt.

Abschnitt „Details“

Die folgenden Details zum Host werden angezeigt:

- Im Abschnitt „Hostname“ werden alle bekannten Hostnamen für den Host aufgelistet.
- Im Abschnitt „Hostbezeichnung“ werden alle Bezeichnungen aufgelistet, die dem Host zugewiesen sind. Sie können die Bezeichnung bearbeiten.

Aktive Aktivitäten

Der Abschnitt „Aktive Aktivitäten“ listet ggf. die Aktivitäten auf, die mit diesem Host während des aktuellen Zeitraums verknüpft sind. Jeder Eintrag ist eine Zusammenfassung einer Aktivität und enthält die folgenden Informationen.

- Auswirkungen der Aktivität.
- Die Aktivitäts-ID, die ein Link zur Seite **Aktivitätsdetails** ist. Siehe [Grundlegendes zur Seite „Aktivitätsdetails“](#).
- Die Anzahl der Hosts, die Teil der Aktivität sind.

Bedrohungen

Im Abschnitt „Bedrohungen“ werden die Bedrohungsvorfälle aufgelistet, die während des aktuellen Zeitraums mit dem ausgewählten Host verknüpft sind. Jeder Eintrag ist eine Zusammenfassung einer Bedrohung:

- Auswirkungswert der Bedrohung.

- Der Name der Bedrohung. Wenn Sie den Mauszeiger über den Namen bewegen, wird ein Popup-Fenster mit weiteren Informationen über die Bedrohung angezeigt.
- Der Zeitbereich der Bedrohungsaktivität.

Klicken Sie auf den Link **Bedrohungen anzeigen**, um die Details auf der Registerkarte **Hostprofil > Bedrohungen** anzuzeigen.

Seite „Hostprofil“

Die Seite **Hostprofil** bietet einen Überblick und Details zu dem Host, den Sie in der Hostliste auf der Seite NSX Network Detection and Response **Hosts** ausgewählt haben.

Die Seite **Hostprofil** besteht aus den folgenden Registerkarten.

Registerkarte	Beschreibung
Übersicht	Bietet eine Übersicht über den Host und ist die Standardansicht.
Bedrohungen	Zeigt die erkannten Vorfälle mit den zugehörigen Nachweisen, Netzwerkinteraktionen und IOCs an.
Ereignisse	Zeigt Informationen zu Erkennungs- und Infoereignissen an.
Dateidownload	Listet die heruntergeladenen Dateien auf.

Am oberen Rand der Seite **Hostprofil** befinden sich Steuerelemente und Schaltflächen, die allen Registerkarten gemeinsam sind.

- Klicken Sie auf das Symbol mit dem ↺, um zur Auflistung der Seite **Hosts** zurückzukehren.

Neben dem Navigationselement befindet sich der Bedrohungsstufenindikator für den Host, gefolgt von seiner IP-Adresse. Wenn sich der Host im Home-Netzwerk befindet, wird das Symbol 🏠 angezeigt.

- Um die Seitenleiste **Warnung verwalten** zu starten, klicken Sie oben rechts auf der Benutzeroberfläche auf **Hostaktionen** und wählen Sie im Dropdown-Menü **Warnung verwalten** aus. Die Seitenleiste **Warnung verwalten – Filter** wird auf der rechten Seite angezeigt.

Verwenden Sie die Seitenleiste **Warnung verwalten**, um Warnungen zu unterdrücken oder herabzustufen, die durch harmlose Ereignisse vom Host ausgelöst werden, wie z. B. die Systemtest- oder Blockierungsereignisse, oder um den Ereignissen benutzerdefinierte Auswirkungswerte zuzuweisen. Einzelheiten dazu finden Sie unter [Arbeiten mit der Sidebar „Warnung verwalten“](#).

Hostprofil: Registerkarte „Übersicht“

Die Registerkarte **Übersicht** auf der Seite **Hostprofil** in der NSX Network Detection and Response-Benutzeroberfläche bietet eine Übersicht über den ausgewählten Host.

Hostübersicht

Der Abschnitt **Hostübersicht** enthält das Widget **Bedrohungen**, das einen schnellen Überblick über die auf dem Host erkannten Bedrohungen bietet.

Zugehörige Aktivitäten

Im Abschnitt „Zugehörige Aktivitäten“ werden Aktivitäten aufgelistet, die den ausgewählten Host betreffen. Klicken Sie auf den Link für die Aktivitäts-ID, und in der Seitenleiste mit der Aktivitätsübersicht wird eine Übersicht über die Aktivitäten angezeigt.

Hostidentität

Der Abschnitt „Hostidentität“ enthält die folgenden Details.

- Host-IP: Die IP-Adresse des Hosts.
- Hostname: Der erkannte Name des Hosts.
- Hostbezeichnung: Die Bezeichnung für den Host. Um die Bezeichnung zu bearbeiten, klicken Sie auf das Symbol.

Hostkonfiguration

Der Abschnitt „Hostkonfiguration“ enthält die folgenden Eigenschaften.

- Im Home-Netzwerk: Um den Host hinzuzufügen, klicken Sie auf die Umschaltoption, um **JA** auszuwählen. Schalten Sie ansonsten auf **NEIN** um.
- Deaktiviert: Um den Host hinzuzufügen, klicken Sie auf die Umschaltoption, um **JA** auszuwählen. Schalten Sie ansonsten auf **NEIN** um.

Hosteigenschaften

Der Abschnitt „Hosteigenschaften“ enthält die folgenden Details.

- Erste Erkennung: Zeitstempel, der angibt, wann der Host zum ersten Mal angezeigt wurde.
- Letzte Erkennung: Zeitstempel, der angibt, wann der Host zuletzt angezeigt wurde.

Hostprofil: Registerkarte „Bedrohungen“

Von NSX Network Detection and Response erkannte Bedrohungen werden auf der Registerkarte **Bedrohungen** der Seite **Hostprofil** durch Bedrohungskarten dargestellt.

Eine Bedrohungskarte zeigt die berechnete Bedrohungspunktzahl, den Bedrohungsnamen und die Klasse, das Erkennungsergebnis (sofern verfügbar), den Bedrohungsstatus und andere Aktionen an. Wenn verfügbar, wird die Aktivität angezeigt, mit der diese Bedrohung verbunden ist. Erweitern Sie die Karte, um die zugehörigen Nachweise anzuzeigen.

Verwenden Sie das Dropdown-Menü **Sortieren nach**, um die Bedrohungskarten zu sortieren. Sie können zwischen **Jüngste**, **Früheste**, **Höchste Auswirkung** (Standardeinstellung) und **Geringste Auswirkung** wählen.

Das Textfeld **Bedrohungen suchen** ermöglicht eine schnelle Suche direkt nach der Eingabe. Dabei werden die Zeilen in der Liste gefiltert, sodass nur die Zeilen angezeigt werden, die in einem beliebigen Feld Text enthalten, der mit der von Ihnen angegebenen Abfragezeichenfolge übereinstimmt.

Schalten Sie die Schaltfläche **Geschlossene Bedrohungen anzeigen** ein, um die angezeigten Bedrohungskarten nach dem Bedrohungsstatus zu filtern. Standardmäßig werden alle Bedrohungen angezeigt.

Verwalten der Bedrohungskarten

Die Bedrohungskarten zeigen alle Bedrohungen im Zusammenhang mit dem ausgewählten Host und ihre entsprechenden Bedrohungsstufen an. Jede Karte zeigt die berechnete Bedrohungsauswirkung, den Bedrohnugnamen, die Bedrohungsklasse und, falls verfügbar, das Erkennungsergebnis an. Außerdem wird der Status der Bedrohung angezeigt: Offen oder Geschlossen.

Klicken Sie auf **Nächste Schritte** und wählen Sie eine Aktion aus dem Dropdown-Menü.

- Wählen Sie **Schließen**, um die Bedrohung zu schließen. Wählen Sie **Öffnen**, um eine geschlossene Bedrohung erneut zu öffnen.
- Wählen Sie **Warnung verwalten** aus, um eine Warnungsverwaltungsregel für die Bedrohung zu erstellen.

Der Abschnitt **Nachweisübersicht** enthält eine Übersicht über die Nachweise und andere Daten, die für die Bedrohung erkannt wurden. Klicken Sie auf das Symbol mit dem > oder fast überall sonst auf der Karte, um die Nachweisdetails zu erweitern.

Wenn Aktivitätsdaten im Zusammenhang mit dieser Bedrohung verfügbar sind, wird die **Aktivität** mit einem Link zur Seitenleiste der **Aktivitätsübersicht** angezeigt.

Nachweisdetails

In der Spalte **Nachweis** werden die Dateidownloads, Signaturen und andere Kategorien des Nachwestyps sowie ein Zeitstempel für den Zeitpunkt des Auftretens des Nachweises angezeigt. Wenn Sie auf den Link „Nachwestyp“ klicken, wird die entsprechende Seitenleiste **Nachweiszusammenfassung** für diesen Typ rechts auf der Seite angezeigt. Die Seitenleiste **Nachweiszusammenfassung** ist für die folgenden Nachwestypen verfügbar.

- Anomalie
- Dateidownload
- Signatur

In der Spalte **Netzwerkinteraktionen und Netzwerk-IOCs** wird die IP-Adresse oder der Domänenname externer Hosts angezeigt. Wenn Sie auf den Link klicken, wird die Seitenleiste für **Netzwerkinteraktion** erweitert.

Die Spalte **Unterstützungsdaten** enthält einen Link zu den Erkennungseignissen sowie einen Link zu den Bedrohungsdetails.

Erkennungsergebnisse

Die Ergebnisse von Bedrohungserkennungsereignissen weisen die folgenden möglichen Werte auf, die in der Reihenfolge ihres Schweregrads aufgeführt sind.

Erkennungsergebnis	Beschreibung
Erfolg	Es wurde festgestellt, dass die Bedrohung ihr Ziel erreicht hat. Dies könnte bedeuten, dass sein Anmeldeversuch beim C&C-Server abgeschlossen wurde und Daten vom böswilligen Endpoint empfangen wurden.
Fehlgeschlagen	Die Bedrohung konnte ihr Ziel nicht erreichen. Dies kann darauf zurückzuführen sein, dass der C&C-Server offline ist, der Angreifer Codierungsfehler gemacht hat usw.
Blockiert	Die Bedrohung wurde von der NSX Network Detection and Response-Anwendung oder von einer Drittanbieteranwendung blockiert.

Wenn das Ereignisergebnis unbekannt ist, wird dieses Feld nicht angezeigt.

Seitenleiste für Netzwerkinteraktion

Sie erweitern die **Netzwerkinteraktion**-Seitenleiste, indem Sie in der Spalte **Netzwerkinteraktionen und Netzwerk-IOCs** der Registerkarte **Bedrohungen** auf den Link IP-Adresse oder Domänenname für einen bestimmten Host klicken.

Die Auswirkungen und die IP-Adresse des ausgewählten Hosts werden oben in der Seitenleiste angezeigt.

WHOIS-Übersicht

Im Abschnitt **WHOIS-Übersicht** werden Schlüsselfelder aus dem WHOIS-Datensatz für die ausgewählte IP-Adresse oder den ausgewählten Domänennamen angezeigt. Klicken Sie auf das Symbol , um auf das Popup-Fenster **WHOIS** zuzugreifen, um weitere Details zur IP-Adresse oder Domäne zu erhalten. Einzelheiten dazu finden Sie unter [WHOIS-Popup-Fenster](#).

Öffnen in

Der **Öffnen in...** Abschnitt enthält Links zu Drittanbietern wie [DomainTools](#), [VirusTotal](#), [Google](#) usw. Wenn es mehr Anbieter gibt, als in die Ansicht passen, können Sie auf **Erweitern ▾** klicken, um sie anzuzeigen.

Übersicht der Anomalie-Nachweise in der Seitenleiste

Die Seitenleiste **Nachweisübersicht** für den Beweistyp „Anomalie“ wird angezeigt, wenn Sie in der Spalte „Nachweis“ der Registerkarte **Bedrohungen** auf den Link für einen Anomalie-Nachweis klicken.

Klicken Sie auf **Referenzereignis >**, um auf die Seite **Ereignisprofil** und die vollständigen Details des zugehörigen Ereignisses zuzugreifen.

Eine kurze Beschreibung der Nachweise wird bereitgestellt.

Bedrohungsdetails

Die folgenden Details zu der Gefährdung werden bereitgestellt.

- Bedrohung – Name des erkannten Sicherheitsrisikos.

- Bedrohungsklasse – Name der erkannten Sicherheitsrisikoklasse.
- Zuerst gesehen ↔ Zuletzt gesehen – Ein Diagramm mit dem Zeitstempel, wann der Nachweis zuerst und zuletzt gesehen wurde. Die Dauer wird unterhalb des Diagramms angezeigt.

Übersicht zum Detektor

Es wird eine Übersicht über den Detektor angezeigt. Klicken Sie für weitere Details auf den Link

Weitere Details ➤, um das Fenster **Detektor-Popup** anzuzeigen. Einzelheiten dazu finden Sie unter [Popup-Fenster der Detektor-Dokumentation](#).

- Detektorname – Der Name des Detektors.
- Ziel – Kurze Beschreibung des Ziels des Detektors.
- ATT&CK-Kategorisierung – Sofern zutreffend, wird ein Link zur MITRE ATT&CK-Technik bereitgestellt. Andernfalls wird **N/A** angezeigt.

Anomaliedetails

Details zur Anomalie werden bereitgestellt.

Detail	Beschreibung
Beschreibung	Eine kurze Beschreibung der Anomalie, die angibt, wie sie vom Baseline-Verhalten abweicht oder warum sie als verdächtig betrachtet werden sollte.
Zustandtyp	Der Typ der Anomalie. Zum Beispiel: Ausreißer.
Anomalie	Das anomale Element, das auf dem Host beobachtet wurde. Beispiel: Zugriff auf einen ungewöhnlichen Port.
Baselineelemente	Die Elemente, die typischerweise auf diesem Host beobachtet werden.
Profil erstellt um	Zeitstempel für die Erstellung der Baseline.
Profil aktualisiert um	Zeitstempel zum Zeitpunkt der Erkennung der Anomalie.
Ausreißerdiagramm	Das Diagramm veranschaulicht den normalen Daten-Upload/Download für den Host zum Vergleich mit der Datenübertragung, die als anomal gekennzeichnet wurde. Je nach Detektor können die folgenden Daten angezeigt werden <ul style="list-style-type: none"> ■ Die Upload-/Download-Größe, die zur Auslösung der Anomaliewarnung geführt hat. ■ Die maximale Upload-/Download-Größe, bevor die Anomaliewarnung ausgelöst wurde. ■ Die durchschnittliche Upload-/Download-Größe für den Host.

Seitenleiste „Nachweisübersicht“ für Dateidownload

Die Seitenleiste **Nachweisübersicht** für einen „Dateidownload“-Nachweistyp wird angezeigt, wenn Sie auf den Link für den Nachweis eines Dateidownloads in der Spalte „Nachweise“ der Registerkarte **Bedrohungen** klicken.

Klicken Sie auf **Referenzereignis ➤**, um auf die Seite **Ereignisprofil** und die vollständigen Details des zugehörigen Ereignisses zuzugreifen.

Eine kurze Beschreibung der Nachweise wird bereitgestellt.

Dateidetails

Die folgenden Details zur Datei werden bereitgestellt.

- Dateityp – Der allgemeine Typ der heruntergeladenen Datei. Eine Liste der Dateitypen finden Sie unter [Registerkarte „Eindeutig“](#).
- Konfidenz – Gibt die Wahrscheinlichkeit an, dass die heruntergeladene Datei böswillig ist. Da das System erweiterte Heuristiken verwendet, um unbekannte Bedrohungen zu erkennen, kann die erkannte Bedrohung in einigen Fällen einen niedrigeren Konfidenzwert haben, wenn die Menge der für diese spezifische Bedrohung verfügbaren Informationen begrenzt ist.
- SHA1 – Der SHA1-Hash der Datei.

Malware-Identifikation

Eine Übersicht über die erkannte Malware wird angezeigt. Klicken Sie für weitere Details auf den Link [Analysebericht](#), um den Analysebericht anzuzeigen. Weitere Informationen finden Sie unter [Verwenden des Analyseberichts](#).

- Antivirusklasse – Eine Bezeichnung, die die Antivirusklasse der heruntergeladenen Datei definiert.
- Antivirusfamilie – Eine Bezeichnung, die die Antivirusfamilie der heruntergeladenen Datei definiert.
- Malware – Eine Bezeichnung, die den Malware-Typ der heruntergeladenen Datei definiert. Wenn die Bezeichnung über das  verfügt, klicken Sie auf das Symbol, um die Beschreibung in einem Popup-Fenster anzuzeigen.
- Verhaltensübersicht – Das erkannte Verhalten der heruntergeladenen Datei. Wenn viele Daten vorhanden sind, wird standardmäßig eine Teilliste angezeigt. Klicken Sie auf [Erweitern](#), um weitere Details anzuzeigen. Schalten Sie die Option erneut um, indem Sie auf [Weniger](#) klicken.

Öffnen in ...

Um die heruntergeladene Datei in einem bestimmten Dienst zu öffnen, klicken Sie auf eines der Symbole für die Anbieter. Standardmäßig wird hier eine Teilliste der Anbieter angezeigt.

Details herunterladen

Die Details der heruntergeladenen Datei werden angezeigt. Klicken Sie für weitere Details auf den Link [Analysebericht](#), um den Analysebericht anzuzeigen. Weitere Informationen finden Sie unter [Verwenden des Analyseberichts](#).

Info	Beschreibung
Dateiname	Der Ressourcenpfad zur heruntergeladenen Datei.
URL	Die vollständige URL zur heruntergeladenen Datei.
Erste Erkennung	Der Zeitstempel, wann die heruntergeladene Datei zum ersten Mal angezeigt wurde. Wenn mehrere Instanzen dieser Datei vorhanden sind, ist dies ein Bereich von Zeitstempeln.
Heruntergeladen von	Die IP-Adresse des Quellservers.

Info	Beschreibung
Protokoll	Das Protokoll, das zum Übertragen der heruntergeladenen Datei vom Quellserver verwendet wurde.
Benutzer-Agent	Falls verfügbar, wird die Zeichenfolge des Benutzer-Agent für die Downloadanforderung angezeigt.

Seitenleiste für die Nachweiszusammenfassung von Signaturen

Die Seitenleiste **Nachweiszusammenfassung** für den Nachweistyp „Signatur“ wird angezeigt, wenn Sie in der Spalte „Nachweis“ der Registerkarte **Bedrohungen** auf den Link „Signatur“ klicken.

Klicken Sie auf **Referenzereignis >**, um auf die Seite **Ereignisprofil** und die vollständigen Details des zugehörigen Ereignisses zuzugreifen.

Eine kurze Beschreibung der Nachweise wird bereitgestellt.

Bedrohungsdetails

Die folgenden Details werden zu der Bedrohung bereitgestellt.

Detail	Beschreibung
Bedrohung	Name des erkannten Sicherheitsrisikos.
Bedrohungsklasse	Name der erkannten Sicherheitsrisikoklasse.
Aktivität	Zeigt, falls vorhanden, die erkannte aktuelle Aktivität der Bedrohung an.
Konfidenz	Gibt die Wahrscheinlichkeit an, dass die erkannte Bedrohung böswillig ist. Bei Ereignissen, bei denen Analyseergebnisse angezeigt werden, z. B. bei einem Dateidownload, wird eine Punktzahl angezeigt.
Erste Erkennung 	Ein Diagramm mit dem Zeitstempel, wann der Nachweis zum ersten und letzten Mal angezeigt wurde.
Letzte Erkennung	Die Dauer wird unterhalb des Diagramms angezeigt.

Datenverkehrsdetails

Das Widget **Referenzereignis-Datenverkehr** bietet einen Überblick über den beobachteten Datenverkehr zwischen den an dem referenzierten Ereignis beteiligten Hosts. Mindestens ein an dem Ereignis beteiligter Host ist ein überwachter Host. Der kommunizierende Host kann ein überwachter Host oder ein externes System sein.

Der Pfeil gibt die Datenverkehrsrichtung zwischen den Hosts an.

Für jeden Host wird die IP-Adresse angezeigt. Bei einem lokalen Host wird die Adresse als Link angezeigt, auf den Sie klicken können, um die Hostprofilseite anzuzeigen. Möglicherweise wird eine Geostandort-Flag  oder ein  Symbol angezeigt. Es können mehrere angezeigt werden. Falls verfügbar, wird ein Hostname angezeigt. Alle auf den Host angewendeten Host-Tags werden angezeigt. Wenn verfügbar, klicken Sie auf das Symbol , um die Hostdetails im Popup-Fenster **WHOIS** anzuzeigen. Einzelheiten dazu finden Sie unter [WHOIS-Popup-Fenster](#).

Übersicht zum Detektor

Es wird eine Übersicht über den Detektor angezeigt. Klicken Sie für weitere Details auf den Link **Weitere Details >**, um das **Detektor-Pop-Up**-Fenster anzuzeigen. Einzelheiten dazu finden Sie unter [Popup-Fenster der Detektor-Dokumentation](#).

- Detektortyp – Der Name des Detektors.
- Ziel – Kurze Beschreibung des Ziels des Detektors.
- IDS-Regel: Klicken Sie auf den Link **Regel anzeigen (falls verfügbar)**, um das **Detektor-Popup**-Fenster anzuzeigen. Weitere Informationen finden Sie unter [Popup-Fenster der Detektor-Dokumentation](#). Sie kann eine IDS-Regel enthalten.

Hostprofil: Registerkarte „Ereignisse“

Auf der Registerkarte **Ereignisse** der Seite **Hostprofil** werden Informationen zur Erkennung und zu Ereignissen angezeigt.

Erkennungsereignisse

Die Liste der Erkennungsereignisse zeigt die Ereignisse an, die die NSX Network Detection and Response-Anwendung im Zusammenhang mit dem ausgewählten Host gefunden hat. Diese Ereignisse bilden einen Teil der Vorfälle, die auch für den Host aufgelistet werden.

Passen Sie die Anzahl der angezeigten Zeilen an. Die Standardeinstellung ist 30 Einträge. Verwenden Sie das Symbol mit dem < und dem >, um durch mehrere Seiten zu navigieren.

Die Spalten, die in der Liste angezeigt werden sollen, können durch Klicken auf das Symbol mit den **≡** angepasst werden.

Jede Zeile zeigt eine Zusammenfassung eines Ereignisses an. Klicken Sie auf eine beliebige Stelle in einer Eingabezeile, um auf die Seitenleiste **Ereignisübersicht** zuzugreifen.

Die Liste der Erkennungsereignisse enthält die folgenden Spalten.

Spaltenname	Beschreibung
Zeitstempel	Gibt die Startzeit des Ereignisses an. Die Zeit wird in der aktuell ausgewählten Zeitzone angezeigt. Die Liste wird nach Zeitstempel sortiert, standardmäßig in absteigender Reihenfolge (neuestes Ereignis oben). Sie können die Symbole verwenden, um die Liste in aufsteigendem Reihenfolge zu sortieren (ältestes Ereignis oben) oder um zur Standardeinstellung zurückzuwechseln.
Host	Der Host im überwachten Netzwerk, das an diesem Ereignis beteiligt ist. In dieser Spalte werden die IP-Adresse, der Hostname oder die Bezeichnung des Hosts angezeigt, abhängig von Ihren aktuellen Anzeigeeinstellungen.
Andere IP	IP-Adresse und Port des Hosts, der mit diesem Ereignis verknüpft ist. Beispiel: 203.0.113.115:80 gibt an, dass die IP-Adresse 203.0.113.115 über Port 80 kontaktiert wurde. Das System versucht, die IP-Adresse zu lokalisieren. Wenn dies erfolgreich ist, zeigt ein kleines Flag-Symbol das Land an, das diese IP-Adresse möglicherweise hostet. Ein Lokales Netzwerk-Symbol wird für lokale Hosts verwendet.
Anderer Host	Der Hostname oder die IP-Adresse des bösartigen/verdächtigen Eintrags.
Bedrohung	Name der erkannten Bedrohungsklasse.

Spaltenname	Beschreibung
Bedrohungsklasse	Name der erkannten Bedrohungsklasse.
Auswirkung	<p>Der Auswirkungswert gibt die kritische Stufe der erkannten Bedrohung an und liegt zwischen 1 und 100:</p> <ul style="list-style-type: none"> ■ Bedrohungen ab 70 werden als kritisch betrachtet. ■ Bedrohungen zwischen 30 und 69 gelten als mittleres Risiko. ■ Bedrohungen zwischen 1 und 29 gelten als harmlose Bedrohungen. <p>Wenn das Symbol für die  angezeigt wird, bedeutet dies, dass das Artefakt blockiert wurde.</p> <p>Klicken Sie auf das Symbol , um die Liste nach Auswirkungen zu sortieren.</p>

Info-Erkennungsereignisse

Die Liste der Info-Erkennungsereignisse zeigt **INFO**-Ereignisse an, die mit dem ausgewählten Host verbunden sind. Diese Liste enthält dieselben Spalten wie die Liste der Erkennungsereignisse.

Hostprofil: Registerkarte „Dateidownloads“

Die Registerkarte **Dateidownloads** auf der Seite **Hostprofil** der NSX Network Detection and Response-Benutzeroberfläche zeigt die vom Host heruntergeladenen schädlichen Dateien mit Details zu ihrem Inhalt und den entsprechenden Bedrohungsstufen an.

Das Textfeld für die **Schnellsuche** oberhalb der Liste bietet eine Suchfunktion, die direkt nach der Eingabe ausgeführt wird. Es filtert die Zeilen in der Liste und zeigt nur die Zeilen an, die in einem beliebigen Feld Text enthalten, der mit der Abfragezeichenfolge übereinstimmt.

Die Spalten, die in der Liste angezeigt werden sollen, können durch Klicken auf das Symbol  angepasst werden.

Jede Zeile ist eine Zusammenfassung einer heruntergeladenen Datei. Klicken Sie auf das -Symbol (oder an einer beliebigen Stelle in einer Eingabezeile), um Details der heruntergeladenen Datei anzuzeigen.

Die Liste ist nach Punktzahl sortiert und enthält die folgenden Spalten.

Spaltenname	Beschreibung
Zeitstempel	Der Zeitstempel der Erkennung des Dateidownloads
Host	Der Host, der die Datei heruntergeladen hat.
Sensor	Der Sensor, der den Dateidownload erkannt hat.
Kontaktierte IP	Die IP-Adresse des kontaktierten Hosts.
Speicherort	Für einen Download ist dies die URL der Datei im unterstützten Format. Beispielsweise \\127.0.0.2\samba_share\1128dedb.exe für einen SMB-Download oder http://www.example.com/download/example.zip für einen HTTP-Download. Für einen Upload wird „Hochladen“ angezeigt.
Dateiname	Der Name der heruntergeladenen Datei.
MD5	Der MD5-Hash der heruntergeladenen Datei.

Spaltenname	Beschreibung
Typ	Der allgemeine Dateityp der heruntergeladenen Datei. Unter Registerkarte „Eindeutig“ finden Sie die Liste der aktuell unterstützten Typen.
AV-Klasse	Eine Bezeichnung, die die Antivirenklasse der heruntergeladenen Datei definiert. Wenn die Bezeichnung über ein  verfügt, können Sie auf dieses Symbol klicken, um eine Beschreibung in einem Pop-up-Fenster zu erhalten.
Malware	Eine Bezeichnung, die den Malware-Typ der heruntergeladenen Datei definiert. Wenn die Bezeichnung über ein  verfügt, können Sie auf dieses Symbol klicken, um eine Beschreibung in einem Pop-up-Fenster zu erhalten.
Bewertung	<p>Die der heruntergeladenen Datei durch die Analyse zugewiesene Punktzahl gibt den kritischen Grad der erkannten Bedrohung an und reicht von 0-100:</p> <ul style="list-style-type: none"> ■ Bedrohungen ab 70 werden als kritisch betrachtet. ■ Bedrohungen, die zwischen 30 und 69 liegen, gelten als mittelschweres Risiko. ■ Bedrohungen, die zwischen 1 und 29 liegen, gelten als ungefährlich. <p>Einzelheiten zum Kern der Bösartigkeit und zur Risikoeinschätzung finden Sie unter Analysebericht: Registerkarte „Übersicht“.</p> <p>Wenn das  angezeigt wird, bedeutet dies, dass das Artefakt blockiert wurde. Die Liste wird in absteigender Reihenfolge sortiert (die kritischsten Bedrohungen oben). Klicken Sie auf den , um die Liste in aufsteigender Reihenfolge zu sortieren (am wenigsten kritische Bedrohungen oben). Klicken Sie dann auf den , um zur Standardeinstellung zurückzukehren.</p>

Arbeiten mit der Seite „Ereignisse“

Die Seite **Ereignisse** enthält Informationen zu einzelnen Ereignissen, die die NSX Network Detection and Response-Anwendung in Ihrem NSX-T Data Center-Netzwerk erkannt hat.

Die Seite besteht aus mehreren Widgets, die mithilfe der Informationen in [Kennenzulernen der NSX Network Detection and Response-Benutzeroberfläche](#) verwaltet werden können.

Die Registerkarte **Netzwerk** auf der Seite **Ereignisse** besteht aus Widgets, mit denen Sie die von der NSX Network Detection and Response-Anwendung gemeldeten Netzwerkerkennungsergebnisse überprüfen, verwalten und priorisieren können.

Globale Ereigniszuzuordnung

Das Widget **Globale Ereigniszuzuordnung** bietet einen visuellen Überblick über die Geolocations der aggregierten Ereignisse.

Es markiert den ungefähren Speicherort der anderen Hosts, die an dem von der NSX Network Detection and Response-Anwendung erkannten Ereignis beteiligt sind. Die Markierungsfarbe stellt die Ereigniswirkung dar. Die Markierungsgröße stellt die Anzahl der betroffenen Hosts dar.

Ereignisse ohne bestimmten Speicherort sind von dieser Zuordnung ausgeschlossen.

Um mehr über die Bedrohungen und Hosts zu erfahren, die an diesem bestimmten Standort dargestellt werden, klicken Sie auf eine Markierung auf der Zuordnung.

Im angezeigten Popup-Fenster **Standortdetails** können Sie den ungefähren Standort, die Bedrohungen und die Zielhosts für das ausgewählte Ereignis anzeigen. Klicken Sie neben jedem Eintrag auf das Symbol , um Filter auf die Liste anzuwenden, die auf der Seite **Ereignisse** angezeigt wird.

Erkannte Bedrohungen auf der Seite „Ereignisse“

Das Widget **Erkannte Bedrohungen** auf der Seite **Ereignisse** bietet eine Visualisierung aller Arten von Bedrohungsklassen und Bedrohungen, die die NSX Network Detection and Response-Anwendung in Ihrem Netzwerk erkannt hat.

Indem Sie auf das Rechteck für eine bestimmte Bedrohungsklasse klicken, können Sie die darin enthaltenen Bedrohungen in derselben Visualisierung weiter untersuchen. Wenn Sie eine bestimmte Bedrohung auswählen, zeigt das System Details zu dieser bestimmten Bedrohung und deren Aktivität in Ihrem Netzwerk an.

Hinweis Wenn Sie zu den einzelnen Bedrohungen navigieren, wird die Liste **Erkennungsereignisse** durch Ihre Auswahl angepasst. Wenn Sie dagegen die Filter verwenden, um die angezeigte Liste der Ereignisse einzuschränken, werden die im Widget **Erkannte Bedrohungen** enthaltenen Ereignisse ebenfalls gefiltert.

Bedrohungsklasse

Die erste Ansicht zeigt die Bedrohungsklassen an, die in Ihrem Netzwerk erkannt wurden, ähnlich der folgenden Abbildung.



Die Rechtecke stellen die Bedrohungsklassen dar, die in Ihrem Netzwerk erkannt wurden. Die Größe jedes Rechtecks wird basierend auf der Anzahl der Ereignisse für jede erkannte Bedrohungsklasse skaliert. Die Farben der Blöcke geben den Schweregrad der Bedrohung an.

Die Liste auf der rechten Seite des Widgets zeigt die Liste der am häufigsten erkannten Bedrohungen an. Wenn Sie auf ein Element in der Liste zeigen, werden in einem Popup-Fenster weitere Informationen über die Bedrohung, ihre Klasse und die Anzahl der Ereignisse sowie betroffene Hosts angezeigt.

Wenn Sie auf ein bestimmtes Rechteck für eine Bedrohungsklasse zeigen, wird ein Popup-Fenster angezeigt. Es zeigt die Bedrohungsklasse, die Anzahl der eindeutigen Bedrohungen und eine Aufschlüsselung der Anzahl der Ereignisse und der teilnehmenden Hosts an. Wenn Sie auf das Popup-Fenster oder das Rechteck klicken, können Sie einen Drilldown zu den eindeutigen Bedrohungen durchführen, aus denen die ausgewählte Bedrohungsklasse besteht.

Eindeutige Bedrohungen

Die nachfolgende Ansicht zeigt die Bedrohungen an, aus denen die ausgewählte Bedrohungsklasse besteht. Die Rechtecke werden basierend auf der Anzahl der Ereignisse für jede erkannte Bedrohung skaliert, und die Farben geben den Schweregrad der Bedrohung an.

Wenn Sie den Mauszeiger über eine bestimmte Bedrohung bewegen, wird ein Popup-Fenster angezeigt. Es zeigt die Bedrohung und eine Aufschlüsselung der Anzahl der Ereignisse und der teilnehmenden Hosts an. Wenn Sie auf das Popup-Fenster oder das Rechteck klicken, um die Bedrohung auszuwählen, wird auf der rechten Seite des Widgets die Option **Bedrohungsdetails** angezeigt.

Bedrohungsdetails

Der Abschnitt „Bedrohungsdetails“ enthält die folgenden Informationen:

- **BEDROHUNG:** Der Name der Bedrohung.
- **KLASSE:** Der Name der Bedrohungsklasse.
- **MAX. AUSWIRKUNG:** Die maximale Auswirkung von Ereignissen, die für die Bedrohung erkannt wurden.
- **EREIGNISSE:** Die Anzahl der erkannten Ereignisse.
- **HOSTS:** Die Anzahl der Zielhosts. Um die Liste „Hosts“ anzuzeigen, klicken Sie auf den Zahlenlink. Weitere Informationen finden Sie unter [Hostliste](#).
- **ERSTE ERKENNUNG/LETZTE ERKENNUNG:** Ein Balkendiagramm, das die Zeitstempel der Bedrohung anzeigt. Die Dauer wird unten angezeigt.

Verwenden von Filtern auf der Seite „Ereignisse“

Die NSX Network Detection and Response-Anwendung bietet einen Filtermechanismus, mit dem Sie sich auf bestimmte Ereignisinformationen konzentrieren können, die für Sie von Interesse sind. Die Verwendung von Filtern ist optional.

Verfahren

- 1 Klicken Sie auf der Seite **Ereignisse** auf das , um das Widget **Filter** zu erweitern.
- 2 Klicken Sie auf eine beliebige Stelle im Textfeld **Filter auf** und wählen Sie ein Element im Dropdown-Menü aus.

Sie können aus den folgenden verfügbaren Filtern auswählen. Um den Fokus der angezeigten Informationen weiter einzuschränken, können Sie mehrere Filter kombinieren.

Filtername	Beschreibung
Ereignisergebnis	Wählen Sie Alle oder Info im Dropdown-Menü aus. Standardmäßig werden Ereignisse angezeigt, bei denen ein Zusammenhang mit einer Bedrohung festgestellt wurde. Wenn Sie Info auswählen, werden nur die Ereignisse berücksichtigt, die selbst informationsbezogen sind. Indem Sie diese Ereignisse verfolgen, können Sie einen weiteren Einblick in die Aktivitäten in Ihrem Netzwerk erhalten.
Home-Netzwerk	Schränken Sie die angezeigten Ereignisse mit Hilfe des Dropdown-Menüs auf die Einstellung Home-Netzwerk ein. Wählen Sie Nur Home-Netzwerk für Ereignisse innerhalb Ihres definierten Home-Netzwerks aus. Wählen Sie Nur nicht identifizierte Netzwerke für Ereignisse von unbekannten Hosts aus.
Host-IP	Schränken Sie die angezeigten Ereignisse auf eine bestimmte Quell-IP-Adresse, einen IP-Adressbereich oder einen CIDR-Block ein. Geben Sie einen gültigen Wert in das Textfeld Host-IP ein.
Hostname	Schränken Sie die angezeigten Ereignisse auf einen bestimmten Hostnamen als Quelle ein. Der vollständige Hostname oder die Bezeichnung muss angegeben werden.
Vorfall-ID	Zeigen Sie Ereignisse an, die zum angegebenen Vorfall gehören. Eine Vorfall-ID ist ein numerischer Eintrag, z. B. 73142. Eine gültige Vorfall-ID muss angegeben werden.
Minimale Auswirkung	Anzeige der Ereignisse, die den minimalen Auswirkungswert aufweisen. Der Bereich liegt zwischen 1 und -100.
Anderer Host	Beschränken Sie die angezeigten Ereignisse auf einen bestimmten Hostnamen.
Andere Host-IP	Beschränken Sie die angezeigten Ereignisse auf eine bestimmte Host-IP-Adresse. Die IP-Adresse kann als eine oder mehrere IP-Adressen, CIDR-Blöcke (z. B. 192.168.0.0/24) oder IP-Adressbereiche (z. B. 1.1.1.5-1.1.1.9) eingegeben werden.
Port	Zeigen Sie Ereignisse mithilfe eines bestimmten TCP/UDP-Ports an. Um die angezeigten Ereignisse weiter zu filtern, können Sie dies mit dem Filter Transport kombinieren.
Priorität	Schränken Sie die angezeigten Ereignisse nach dem Prioritätsstatus ein. Wählen Sie im Dropdown-Menü Infektionen , Überwachungsliste oder Belästigungen aus. Einzelheiten dazu finden Sie unter Infektionen im Zeitverlauf .
Bedrohung	Schränken Sie die angezeigten Vorfälle auf eine bestimmte Bedrohung ein. Wählen Sie eine Bedrohung aus dem Dropdown-Menü aus. Das Menü wird mit einer Liste katalogisierter Bedrohungen vorausgefüllt. Verwenden Sie die Suchfunktion oben im Menü, um schnell einen Bedrohungsnamen zu finden.
Bedrohungsklasse	Schränken Sie die Anzeige auf eine bestimmte Klasse von Ereignissen ein. Wählen Sie die Bedrohungsklasse aus dem Dropdown-Menü. Das Menü ist mit einem Katalog von Klassen vorausgefüllt.
Transport	Zeigen Sie Ereignisse mithilfe eines bestimmten Transportschichtprotokolls an. Wählen Sie TCP oder UDP im Dropdown-Menü aus.

3 Um die ausgewählten Filter anzuwenden, klicken Sie auf **Anwenden**.

Das System wendet die ausgewählten Filter an und aktualisiert die Ereignisliste.

4 (Optional) Um einen einzelnen Filter zu löschen, klicken Sie neben dem Eintrag auf die Schaltfläche **ENTFERNEN**. Um alle ausgewählten Filter zu löschen, klicken Sie auf das Symbol **X** rechts neben dem Widget **Filter**.

Das Widget **Filter** wird ausgeblendet, wenn Sie alle ausgewählten Filter löschen.

Erkennungsereignisse

Das Widget **Erkennungsereignisse** bietet einen Überblick über die einzelnen Ereignisse, die die NSX Network Detection and Response-Anwendung erkannt hat.

Ein Ereignis stellt eine sicherheitsrelevante Aktivität dar, die im überwachten Netzwerk aufgetreten ist. Ein Ereignis kann mehrere Datenflüsse umfassen (z. B. TCP-Verbindungen), stellt aber einen einzelnen Aktivitätstyp dar, der über einen kurzen Zeitraum (höchstens eine Stunde) stattfindet.

Wenn der ausgewählte Zeitraum heute (Standardeinstellung) enthält, aktualisiert das Widget seine Ereignisliste alle 5 Minuten. Neue Ereignisse werden grün hervorgehoben. Die Farbe verschwindet nach einigen Sekunden.

Das Feld **Schnellsuche** über der Liste bietet eine schnelle, von Ihnen eingegebene Suche. Es filtert die Zeilen in der Liste und zeigt nur die Zeilen an, die in einem beliebigen Feld Text enthalten, der mit der Abfragezeichenfolge übereinstimmt.

Aktualisieren Sie die Ereignisliste manuell, indem Sie auf die Schaltfläche **Jetzt Update durchführen** klicken.

Passen Sie die Anzahl der Zeilen an, die angezeigt werden sollen. Standardmäßig werden 30 Einträge angezeigt. Es können bis zu 1000 Ereignisse angezeigt werden. Es kann jedoch zu einer erheblichen Verzögerung für das System führen, wenn eine große Anzahl von Ereignissen abgerufen wird. Verwenden Sie die Symbole und , um durch mehrere Seiten zu navigieren.

Jede Zeile zeigt eine Zusammenfassung eines Ereignisses an. Klicken Sie auf eine beliebige Stelle in einer Eingabezeile, um auf die Seitenleiste **Ereignisübersicht** zuzugreifen.

Die Liste der Ereignisse enthält die folgenden Spalten.

Spaltenname	Beschreibung
Zeitstempel	Gibt die Startzeit des Ereignisses an. Die Zeit wird in der aktuell ausgewählten Zeitzone angezeigt. Die Liste wird nach Zeitstempel sortiert, standardmäßig in absteigender Reihenfolge (neuestes Ereignis oben). Sie können die Symbole verwenden, um die Liste in aufsteigendem Reihenfolge zu sortieren (ältestes Ereignis oben) oder um zur Standardeinstellung zurückzuwechseln. Klicken Sie auf das , um die Liste nach Zeitstempel zu sortieren.
Host	Der Host im überwachten Netzwerk, das an diesem Ereignis beteiligt ist. In dieser Spalte werden die IP-Adresse, der Hostname oder die Bezeichnung des Hosts angezeigt, abhängig von Ihren aktuellen Anzeigeeinstellungen. Klicken Sie neben dem Host auf das Symbol Bearbeiten , um das Popup-Fenster Bezeichnungs-/Stummschaltungs-Host zu öffnen.
Andere IP	IP-Adresse und Port des Hosts, der mit diesem Ereignis verknüpft ist. Beispiel: 203.0.113.115:80 gibt an, dass die IP-Adresse 203.0.113.115 über Port 80 kontaktiert wurde. Das System versucht, die IP-Adresse zu lokalisieren. Wenn dies erfolgreich ist, zeigt ein kleines Flag-Symbol das Land an, das diese IP-Adresse möglicherweise hostet. Ein Lokales Netzwerk-Symbol wird für lokale Hosts verwendet.
Anderer Host	Der Hostname oder die IP-Adresse des bösartigen/verdächtigen Eintrags.
Bedrohung	Name der erkannten Bedrohung oder des Sicherheitsrisikos.

Spaltenname	Beschreibung
Bedrohungsklasse	Name der erkannten Bedrohungsklasse.
Auswirkung	<p>Der Auswirkungswert gibt die kritische Stufe der erkannten Bedrohung an und liegt zwischen 1 und 100:</p> <ul style="list-style-type: none"> ■ Bedrohungen ab 70 werden als kritisch betrachtet. ■ Bedrohungen zwischen 30 und 69 gelten als mittleres Risiko. ■ Bedrohungen zwischen 1 und 29 gelten als harmlose Bedrohungen. <p>Wenn das  angezeigt wird, weist es darauf hin, dass das Artefakt blockiert wurde.</p> <p>Klicken Sie auf das , um die Liste nach Auswirkungen zu sortieren.</p>

Seitenleiste „Ereignisübersicht“

Sie greifen auf die Seitenleiste **Ereignisübersicht** zu, wenn Sie im Widget **Erkennungsereignisse** auf der Seite NSX Network Detection and Response**Ereignisse** auf eine Eingabezeile klicken.

Im folgenden Abschnitt wird beschrieben, was auf dieser Seitenleiste angezeigt wird. Nach dem oberen Abschnitt werden in den nachfolgenden Abschnitten unterstützende Daten angezeigt. Einige Abschnitte werden nur angezeigt, wenn relevante Daten verfügbar sind.

Oberster Abschnitt

Der Anfang der Seitenleiste enthält Folgendes:

- Um die Seitenleiste zu schließen, klicken Sie auf das Symbol zum .
- Um das Ereignis auf der Seite **Ereignisprofil** anzuzeigen, klicken Sie auf **Details >**. Weitere Informationen hierzu finden Sie unter [Seite „Ereignisprofil“](#).
- Falls verfügbar, wird eine kurze Beschreibung des Ereignisses bereitgestellt. Sie enthält eine Erklärung darüber, warum das System dieses Ereignis markiert hat, identifiziert die mit diesem Ereignis verbundene Bedrohung oder Malware und beschreibt kurz die erkannte Aktivität.

Bedrohungsdetails

Dieser Abschnitt enthält die folgenden Informationen.

Name der Bedrohungsdetails	Beschreibung
Bedrohung	Name des erkannten Sicherheitsrisikos.
Bedrohungsklasse	Name der erkannten Sicherheitsrisikoklasse.
Ereigniserkennung	<p>Der Name des Ereigniserkennungsgeräts. Klicken Sie auf den Link, um das Popup-Fenster Detektor anzuzeigen. Einzelheiten dazu finden Sie unter Popup-Fenster der Detektor-Dokumentation.</p> <p>Wenn kein Detektor für das Ereignis vorhanden ist, wird dieser Abschnitt nicht angezeigt.</p>

Name der Bedrohungsdetails	Beschreibung
Auswirkung	<p>Der Wert der Auswirkung gibt die kritische Stufe der erkannten Bedrohung an und liegt zwischen 1 und 100.</p> <ul style="list-style-type: none"> ■ Bedrohungen ab 70 werden als kritisch betrachtet. ■ Bedrohungen zwischen 30 und 69 gelten als mittleres Risiko. ■ Bedrohungen zwischen 1 und 29 gelten als harmlose Bedrohungen.
Aktion	Eine Liste der vom Sensor durchgeföhrten Aktionen (z. B. alle blockierenden Aktivitäten, ob das Ereignis protokolliert wird, ob Datenverkehr erfasst wurde oder ein Malware-Download extrahiert wurde).
Ergebnis	<p>Das Ergebnis des Ereignisses. In den meisten Fällen ist dies „Erkennung“.</p> <p>Für Info-Ereignisse und Ereignisse, die vom Info-Status heraufgestuft wurden, gibt eine zusätzliche Bezeichnung den Grund für den Status bzw. die Statusänderung an. Wenn Sie den Mauszeiger über die Bezeichnung bewegen, wird ein Popup-Fenster mit zusätzlichen Details zur Ursache angezeigt.</p>
Erste Erkennung Letzte Erkennung	<p>Ein Diagramm mit dem Zeitstempel, wann der Nachweis zum ersten und letzten Mal angezeigt wurde.</p> <p>Die Informationen zur Dauer werden unterhalb des Diagramms angezeigt.</p>

Ereignisdatenverkehr

Das Widget **Ereignisdatenverkehr** bietet einen Überblick über den Datenverkehr, der zwischen den am Ereignis beteiligten Hosts beobachtet wird. Mindestens ein an dem Ereignis beteiligter Host ist ein überwachter Host. Der kommunizierende Host kann ein überwachter Host oder ein externes System sein. Ein Link zum Anzeigen des erfassten Datenverkehrs wird angezeigt, wenn die Daten verfügbar sind.

Der Pfeil gibt die Datenverkehrsrichtung zwischen den Hosts an.

Für jeden Host wird die IP-Adresse angezeigt. Wenn der Host lokal ist, handelt es sich bei der Adresse um einen Link, auf den Sie klicken können, um die Seite **Hostprofil** anzuzeigen.

Möglicherweise wird ein Geostandort-Flag,  oder  angezeigt. Es werden möglicherweise mehrere Symbole angezeigt. Falls verfügbar, wird ein Hostname angezeigt. Falls aus der DHCP-Datenverkehrsüberwachung verfügbar, wird die MAC-Adresse des Hosts angezeigt. Alle auf den Host angewendeten Host-Tags werden angezeigt. Falls verfügbar, klicken Sie auf das , um die Hostdetails im Popup-Fenster **WHOIS** anzuzeigen.

Ereignisnachweis

Im Abschnitt „Ereignisnachweis“ werden verschiedene Aktionen aufgelistet, die bei der Analyse des Ereignisses beobachtet wurden. Klicken Sie für weitere Details auf den Link **Ereignisdetails**, um den Ereignisnachweis anzuzeigen.

Zu den Aktionen gehören „Signatur“, „Reputation“, „Ungewöhnliches Verhalten“, „Dateidownload“, „URL-Pfad-Übereinstimmung“, „Verifizierung“, „Anomalie“ usw. Falls angegeben, klicken Sie auf den Link, um das entsprechende **Detektor**-Popup-Fenster anzuzeigen. Für jede Aktion wird ein Konfidenzwert angezeigt.

Malware-Identifikation

Wenn die NSX Malware-Schutz-Anwendung aktiviert ist, wird eine Zusammenfassung der erkannten Malware angezeigt. Klicken Sie für weitere Details auf den Link **Analysebericht**  , um den Analysebericht anzuzeigen. Weitere Informationen hierzu finden Sie unter [Verwenden des Analyseberichts](#).

Detailname	Beschreibung
Antiviruskategorie	Eine Bezeichnung, die die Antivirenklasse der heruntergeladenen Datei definiert.
Antivirusfamilie	Eine Bezeichnung, die die Antivirusfamilie der heruntergeladenen Datei definiert.
Malware	Eine Bezeichnung, die den Malware-Typ der heruntergeladenen Datei definiert. Wenn die Bezeichnung über ein  verfügt, können Sie darauf klicken, um eine Pop-up-Beschreibung zu erhalten.
Verhaltensübersicht	Das erkannte Verhalten der heruntergeladenen Datei. Wenn viele Daten vorhanden sind, wird standardmäßig eine Teilliste angezeigt. Klicken Sie auf Erweitern  , um weitere Details anzuzeigen. Schalten Sie die Option erneut um, indem Sie auf Weniger  klicken.

Ereignis-URLs

Im Abschnitt „Ereignis-URLs“ werden alle URLs angezeigt, die im Ereignis erkannt wurden. Dieser Abschnitt wird nur angezeigt, wenn das Ereignis einer URL zugeordnet ist.

Ereignismetadaten

Im Abschnitt „Ereignismetadaten“ werden die folgenden Daten angezeigt.

Datenname	Beschreibung
Zugehöriger Vorfall	Klicken Sie auf das  , um den zugehörigen Vorfall anzuzeigen, sofern verfügbar.
Verbindungen	Die Anzahl der Verbindungen, die im Ereignis enthalten sind.
Zugehörige Aktivität	Klicken Sie auf das  , um die zugehörige Aktivität anzuzeigen, sofern verfügbar.

WHOIS-Popup-Fenster

Das Popup-Fenster **WHOIS** zeigt Registrierungsinformationen und andere Details zur IP-Adresse oder zum Hostnamen des Hosts an, den Sie untersuchen.

Es verfügt über die folgenden zwei Registerkarten.

Zusammenfassung

Auf der Registerkarte **ZUSAMMENFASSUNG** werden die folgenden Informationen über die IP-Adresse oder den Hostnamen angezeigt.

- Datumsinformationen – Das Datum, an dem die Domäne registriert wurde, das Datum, an dem der Domänendatensatz aktualisiert wurde, und, falls verfügbar, das Ablaufdatum der Domäne.

- Organisation – Der Name der Organisation, die E-Mail-Adressen der Organisation, das Land der Organisation (Ländercode), die Telefonnummern der Organisation, der Name des Absenders und die Kontaktliste.
- Netzwerk – Der Netzwerkname, der IP-Adressbereich, die AS-Liste, die autoritativen Namensserver und die übergeordneten Netzwerke.

Rohdatensatz

Auf der Registerkarte **ROHDATENSATZ** werden die WHOIS-Daten in ihrer Rohform angezeigt.

Informationen nicht verfügbar

Wenn das Popup-Fenster **WHOIS** eine Warnung anzeigt, dass Informationen für die angegebene IP-Adresse oder den angegebenen Hostnamen nicht verfügbar sind, können Sie es mit einem Drittanbieter versuchen. Klicken Sie zum Nachschlagen des Hosts auf **Im externen Tool anzeigen** unten rechts im Popup-Fenster.

Hinweis Die Schaltfläche des Drittanbieters ist immer verfügbar.

Popup-Fenster der Detektor-Dokumentation

Das Popup-Fenster **Detektor-Dokumentation** enthält detaillierte Informationen über den NSX Network Detection and Response-Detektor, der den Ereignisnachweis lieferte. Ziel ist es, Sie bei der Bestimmung der Konfidenz zu unterstützen, die Sie in diesem Detector platzieren können.

In der Dokumentation werden mindestens einige der folgenden Details angezeigt.

Detailname	Beschreibung
Ziel	Kurze Beschreibung des Ziels des Detektors.
ATT&CK-Kategorisierung	Falls zutreffend wird ein Link zur MITRE ATT&CK-Technik bereitgestellt.
Kurzübersicht zum Detektor	Eine detaillierte technische Beschreibung des Detektors und seines Betriebs.
IDS-Regel	Eine allgemeine Darstellung der Erkennungslogik, die von einer NSX Network Detection and Response-Netzwerksignatur verwendet wird. Die Regelsyntax steht in losem Zusammenhang mit der in https://suricata.readthedocs.io/en/latest/rules/index.html definierten Suricata-Signatursprache. Eine Regel besteht aus einem oder mehreren Klauselsätzen, in der Regel aus einer einzelnen Klausel, die jeweils Schlüssel-Wert-Paare enthält. Wenn eine Regel mehrere Klauseln enthält, werden diese nummeriert, wobei der ersten Klausel „IF:“ und jeder nachfolgenden Klausel „AND THEN IF:“ vorangestellt wird. Die verschiedenen Klauselsätze werden sequenziell auf Daten ausgewertet, die zum selben Flow gehören. Zeigen Sie auf ein beliebiges Schlüssel-Wert-Paar, um ein relevantes Hilfe-Popup-Fenster anzuzeigen.
Falsch-positive Ergebnisse	Eine Beschreibung der Möglichkeit des Detektors, falsch positive Ergebnisse zu generieren.
Falsch-negative Ergebnisse	Die Annahmen, die dazu führen können, dass der Detektor falsch-negative Ergebnisse verursacht.

Seite „Ereignisprofil“

Der Zugriff auf die Seite **Ereignisprofil** erfolgt über die Schaltfläche **Details** ➤ oben in der Seitenleiste **Ereignisübersicht**.

Oben in der Ansicht gibt es eine Reihe von Steuerelementen und Schaltflächen:

- Klicken Sie auf **Ereignisse**, um eine Dropdown-Liste ähnlicher Funktionen anzuzeigen. Klicken Sie auf das -Symbol neben jeder Funktion, um das **Ziel**, den **Zielport**, die **Quell-IP**, das **Transportprotokoll**, die **Bedrohungsklasse** und den **Bedrohungstyp** auszuwählen. Klicken Sie dann auf **Ereignisse anzeigen** 🔍, um die ausgewählten Ereignisse in einer neuen Registerkarte anzuzeigen.
- Klicken Sie auf **Warnung verwalten**, um die Seitenleiste **Warnung verwalten** zu starten. Verwenden Sie diese Funktion, um unbedenkliche Ereignisse zu unterdrücken oder herabzustufen, wie z. B. Test- oder blockierende Ereignisse des Systems, oder um benutzerdefinierte Bewertungen auf bestimmte Ereignisse anzuwenden. Einzelheiten dazu finden Sie unter [Arbeiten mit der Sidebar „Warnung verwalten“](#).
- Klicken Sie auf das Symbol , um alle Felder zu reduzieren, oder auf das Symbol , um alle Felder zu erweitern.

Ereignisübersicht

Der obere Abschnitt bietet einen visuellen Überblick über die Bedrohung oder Malware, die die NSX Network Detection and Response-Anwendung erkannt hat, und zeigt die Bedrohungsklasse und die Auswirkungsbewertung für die Bedrohung an.

Ereignisübersicht

Der Abschnitt **Ereignisübersicht** enthält eine Erklärung, warum die NSX Network Detection and Response-Anwendung dieses Ereignis markiert hat, identifiziert die mit diesem Ereignis verbundene Bedrohung oder Malware, beschreibt kurz die erkannte Aktivität und zeigt unterstützende Daten an.

Falls über den NSX Advanced Threat Prevention-Cloud-Dienst verfügbar, wird eine ausführliche Erklärung des Ereignisses und der Gründe, warum es als bösartig eingestuft wird, oben im Abschnitt **Ereignisübersicht** angezeigt.

Serverblock

Der Serverblock zeigt die folgenden Daten an.

Daten	Beschreibung
Hostname	Falls verfügbar, der FQDN des Servers.
IP-Adresse	<p>Die IP-Adresse des -Servers. Möglicherweise wird ein Geostandort-Flag angezeigt. Wenn das Symbol  vorhanden ist, klicken Sie auf den Link, um weitere Details auf der Seite Hostprofil anzuzeigen.</p> <p>Falls verfügbar, klicken Sie auf das Symbol , um die Reputations-Tags des Clients anzuzeigen.</p> <p>Falls verfügbar, klicken Sie auf das Symbol , um Registrierungsinformationen und andere Daten zum Host im Popup-Fenster WHOIS anzuzeigen.</p>
MAC-Adresse	Falls verfügbar, die MAC-Adresse des Servers. Diese Adresse wird aus der Überwachung des DHCP-Datenverkehrs bezogen und ist einer der Datenpunkte, die das System zum Generieren eines eindeutigen HostID-Eintrags verwendet, der einem bestimmten Host im Netzwerk unabhängig von seiner IP-Adresse zugeordnet wird.

Clientblock

Der Clientblock zeigt die folgenden Daten an.

Daten	Beschreibung
Hostname	Falls verfügbar, der FQDN des Clients.
IP-Adresse	<p>Die IP-Adresse des Clients. Möglicherweise wird ein Geostandort-Flag angezeigt. Falls verfügbar, klicken Sie auf die Adresse oder das Symbol , um die Seite Hostprofil anzuzeigen.</p> <p>Falls verfügbar, klicken Sie auf das Symbol , um die Reputations-Tags des Clients anzuzeigen.</p> <p>Falls verfügbar, klicken Sie auf das Symbol , um Registrierungsinformationen und andere Daten zum Host im Popup-Fenster WHOIS anzuzeigen.</p>
MAC-Adresse	Falls verfügbar, die MAC-Adresse des Clients. Diese Adresse wird aus der Überwachung des DHCP-Datenverkehrs bezogen und ist einer der Datenpunkte, die das System zum Generieren eines eindeutigen HostID-Eintrags verwendet, der einem bestimmten Host im Netzwerk unabhängig von seiner IP-Adresse zugeordnet wird.

Ereignismetadaten

Im Abschnitt „Ereignismetadaten“ werden die folgenden Daten angezeigt.

Daten	Beschreibung
Ergebnis der Überprüfung	<p>Gibt das Ereignisergebnis an. Folgende Werte sind möglich.</p> <ul style="list-style-type: none"> ■ Blockiert: Die Bedrohung wurde von der NSX Network Detection and Response-Anwendung oder von einer Drittanbieteranwendung blockiert. ■ Fehlgeschlagen: Die Bedrohung konnte ihr Ziel nicht erreichen. Dies kann darauf zurückzuführen sein, dass der C&C-Server offline ist, der Angreifer Codierungsfehler gemacht hat usw. ■ Erfolgreich: Es wurde festgestellt, dass die Drohung ihr Ziel erreicht hat. Dies könnte bedeuten, dass sein Anmeldeversuch beim C&C-Server abgeschlossen wurde und Daten vom böswilligen Endpoint empfangen wurden. <p>Wenn das Ereignisergebnis unbekannt ist, wird dieses Feld nicht angezeigt.</p>
Name des Prüfers	Der Name des Ereignisprüfers. Klicken Sie auf den Link, um auf das Popup-Fenster Prüferdokumentation zuzugreifen.

Daten	Beschreibung
Nachricht des Prüfers	Eine Nachricht vom Prüfer, die weitere Informationen zu dem Ergebnis liefert, z. B. welche Drittanbieteranwendung die Gefährdung blockiert hat.
Sensor	Der Sensor, der das Ereignis erkannt hat.
Verbindungen	Die Anzahl der Verbindungen, die im Ereignis enthalten sind.
Aktion	Eine Liste der vom Sensor durchgeföhrten Aktionen (z. B. alle blockierenden Aktivitäten, ob das Ereignis protokolliert wird, ob Datenverkehr erfasst wurde oder ein Malware-Download extrahiert wurde).
Angemeldete Benutzer	Eine Liste der Benutzer, die in den protokollierten Datensätzen erkannt wurden.
Ergebnis	Das Ergebnis des Ereignisses. In den meisten Fällen ist das Ergebnis ERKENNUNG. Für INFO-Ereignisse und Ereignisse, die vom INFO-Status heraufgestuft wurden, gibt eine zusätzliche Bezeichnung den Grund für den Status bzw. die Statusänderung an. Wenn Sie den Mauszeiger über die Bezeichnung bewegen, wird ein Popup-Fenster mit zusätzlichen Details zur Ursache angezeigt.
Zugehöriger Vorfall	Ein Permalink zu einem korrelierten Vorfall. Durch Klicken auf den Link  wird die Seite Vorfallprofil in einer neuen Browserregisterkarte geöffnet. Bei diesem Ereignis kann es sich um eine Reihe von eng miteinander verbundenen Ereignissen handeln, die automatisch mit einem Vorfall korreliert wurden.
Ereignis-ID	Zeigen Sie das Ereignis auf der Seite Netzwerkereignisdetails an. Der Link wird auf einer neuen Browserregisterkarte geöffnet.
Startzeit	Ein Zeitstempel für den Beginn des Ereignisses.
Endzeit	Ein Zeitstempel für das Ende des Ereignisses.

Erfasste Malware

Der Abschnitt „Erfasste Malware“ enthält Informationen aus der dynamischen Analyse, die auf der bösartigen Softwareinstanz durchgeführt wurde, die sich auf das Ereignis bezieht.

Sie können auf detaillierte technische Informationen darüber zugreifen, was die Malware tut, wie sie funktioniert und welche Art von Risiko sie darstellt. Weitere Informationen zu den angezeigten Details finden Sie unter [Verwenden des Analyseberichts](#).

Hinweis Wenn für das Ereignis keine bösartige Software erkannt wurde, wird dieser Abschnitt nicht angezeigt.

Ereignsnachweis

Der Abschnitt „Ereignsnachweis“ enthält Details zu den Aktionen, die bei der Analyse des Ereignisses beobachtet wurden.

Zu den Aktionen können schädliche Dateidownloads, Netzwerksignatur für bekannte Bedrohungen entspricht, die Ausführung einer Domänennamensaflösung einer blockierten Malware-Domäne, ein bekannter ungültiger URL-Pfad usw. gehören.

Falls verfügbar, klicken Sie auf den Detector-Link, um das Popup-Fenster [Popup-Fenster der Detektor-Dokumentation](#) anzuzeigen. Weitere Informationen finden Sie ebenfalls unter [Informationen zu Nachweisen](#).

Hostreputation

Der Abschnitt „Hostreputation“ enthält Informationen zu bekannten bösartigen Hosts oder URL-Reputationseinträgen, die im Ereignis angezeigt werden.

Hinweis Wenn der Host über keinen bekannten Verlauf verfügt, wird dieser Abschnitt nicht angezeigt.

Anomaliedaten

In diesem Abschnitt werden die Netflow- oder passiven DNS-Einträge angezeigt, die das Anomalieereignis ausgelöst haben.

Je nach der festgestellten Anomalie trägt er den Titel **DNS-Anomaliedaten** oder **Netflow-Anomaliedaten**.

Es können zusätzliche Informationen angegeben werden, z. B. die IP-Adressen oder Ports, die als anomale eingestuft wurden. Wenn eine große Anzahl von Elementen betroffen ist, können Sie auf das **+ #**, um alle Elemente anzuzeigen.

Hinweis Wenn für das Ereignis keine Anomalien festgestellt wurden, wird dieser Abschnitt nicht angezeigt.

Bedrohungsbeschreibung

Der Abschnitt „Bedrohungsbeschreibung“ enthält eine detaillierte Beschreibung der Bedrohung im Zusammenhang mit dem Ereignis.

Risikominderung

Der Abschnitt „Risikominderung“ enthält detaillierte Anweisungen zum Entfernen schädlicher Software und anderer empfohlener Prozesse, die nach dem Ereignis bereinigt werden sollen.

Hinweis Wenn kein bekannter Risikominderungsprozess für das Ereignis vorhanden ist, wird dieser Abschnitt nicht angezeigt.

Verwalten der Seite „Vorfälle“

Auf der Seite **Vorfälle** werden die Vorfälle und deren unterschiedliche Gefährdungsbewertungen angezeigt. Sie können die Widgets auf der Seite verwenden, um die von der NSX Network Detection and Response-Anwendung gemeldeten Vorfälle zu überprüfen, zu verwalten und zu priorisieren.

Die Seite besteht aus mehreren Widgets, die mithilfe der Informationen in [Kennenzulernen der NSX Network Detection and Response-Benutzeroberfläche](#) verwaltet werden können.

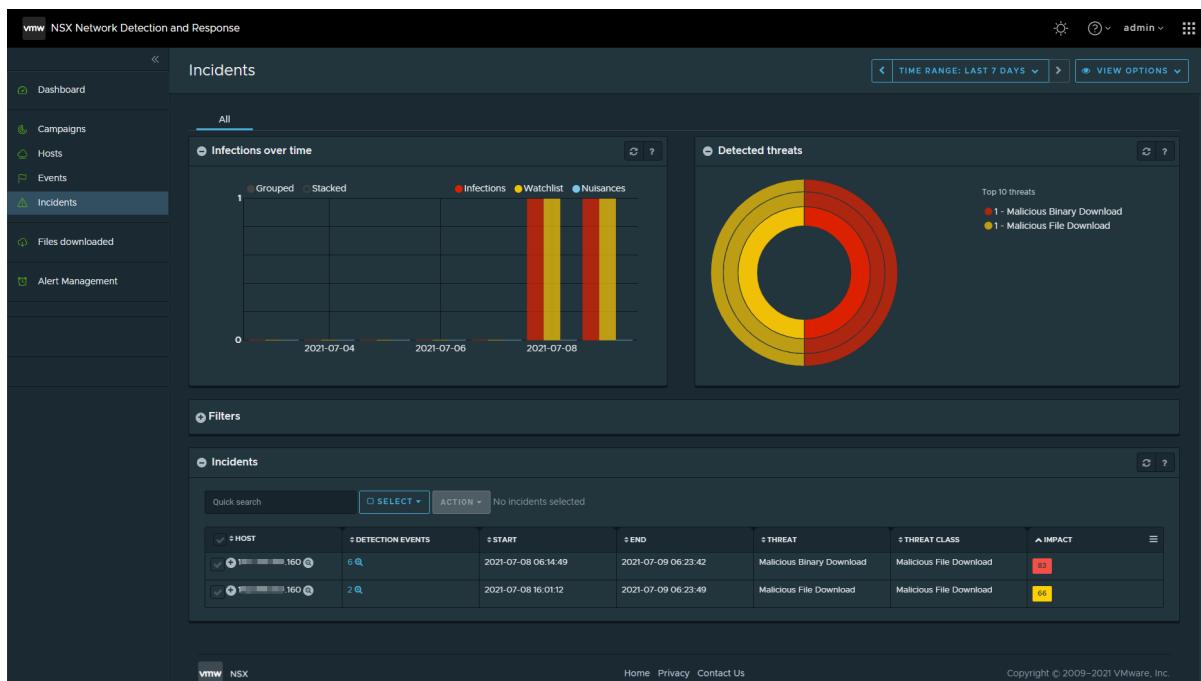
In der NSX Network Detection and Response-Anwendung ist ein Vorfall eine Zusammenfassung von Erkennungsereignissen aus einer einzelnen Bedrohung, die auf einer einzelnen Arbeitslast im überwachten Netzwerk erkannt wird.

Die NSX Network Detection and Response-Anwendung meldet nicht nur Sicherheitsereignisse. Ein Vorfall kann aus einem einzelnen Ereignis oder aus vielen Ereignissen bestehen, die automatisch korreliert und als eng mit der System-Bedrohungs-Engine verbunden erkannt wurden. Beispielsweise kann die Seite **Vorfälle** alle ausgehenden Verbindungen zum Befehls- und Steuerungskanal der Malware, alle verdächtigen DNS-Lookups (z. B. Anfragen für automatisch generierte, zugehörige Malware-Domänen) und ausführliche Beschreibungen jedes registrierten Sicherheitsereignisses gemeldet werden.

Auf der Seite **Vorfälle** können Sie die folgenden Aufgaben ausführen.

- Alle auftretenden Vorfälle effizient verfolgen.
- Schnell eine Liste der betroffenen Hosts anzeigen.
- Anhand verschiedener Ansichten Prioritäten für Bedrohungen nach deren Auswirkungen und Schweregrad setzen.
- Einen detaillierten Überblick über die für jeden Vorfall registrierten Ereignisse erhalten und auf Beschreibungen von Bedrohungen und Schadensbegrenzungen zugreifen.
- Vorfälle schließen oder öffnen.
- Betroffene Hosts als bereinigt markieren oder löschen.
- Die gemeldeten Bedrohungen für bestimmte Hosts filtern.

Die folgende Abbildung ist ein Beispiel für die Seite **Vorfälle**, auf der die Registerkarte **Alle** angezeigt wird.



Infektionen im Zeitverlauf

Das Widget **Infektionen im Zeitverlauf** bietet einen grafischen Überblick über die verschiedenen Arten von Vorfällen, die im Netzwerk entdeckt wurden. Die x-Achse zeigt die Zeit und die y-Achse die Anzahl der von Vorfällen eines bestimmten Typs betroffenen Hosts.

Es gibt drei verschiedene Arten von Vorfällen.

Vorfalltyp	Beschreibung
Infektionen	Dies sind Vorfälle, die als kritisch erkannt wurden. Diesen Vorfällen wurde eine Auswirkungspunktzahl von 70 oder höher zugewiesen und sie werden in Rot angezeigt.
Watchlist	Hierbei handelt es sich um Vorfälle, bei denen festgestellt wurde, dass sie ein mittleres Risiko aufweisen. Solche Vorfälle weisen zwar auf ein potenzielles Risiko hin, müssen aber nicht unbedingt sofort behandelt werden. Sie werden genau beobachtet, falls neue Nachweise auftauchen, die ihren Status ändern. Diesen Vorfällen wurde eine Auswirkungspunktzahl von 30 bis 69 zugewiesen und sie werden in Orange angezeigt.
Belästigungen	Dies sind Vorfälle, die als gering oder ohne Risiko betrachtet werden. In der Regel handelt es sich dabei um potenziell unerwünschte/riskante Aktivitäten, die nicht unbedingt auf eine Gefährdung oder Infektion des überwachten Netzwerks hindeuten. Diesen Vorfällen wurde eine Auswirkungsbewertung von weniger als 30 zugewiesen, und sie werden blau angezeigt.

Sie können die verschiedenen Ereignistypen ein- oder ausblenden, indem Sie auf die jeweiligen Namen in der Legende am oberen Rand des Diagramms klicken.

Wenn Sie auf einen Balken im Diagramm zeigen, wird in einem Popup-Fenster die Anzahl der Hosts im Netzwerk angezeigt, die von den entsprechenden Vorfällen betroffen sind.

Wenn Sie auf einen Balken klicken, werden der Zeitbereich und der Vorfallstyp entsprechend aktualisiert. Das Dashboard zeigt nur Informationen zu diesem Vorfalltyp am ausgewählten Tag an.

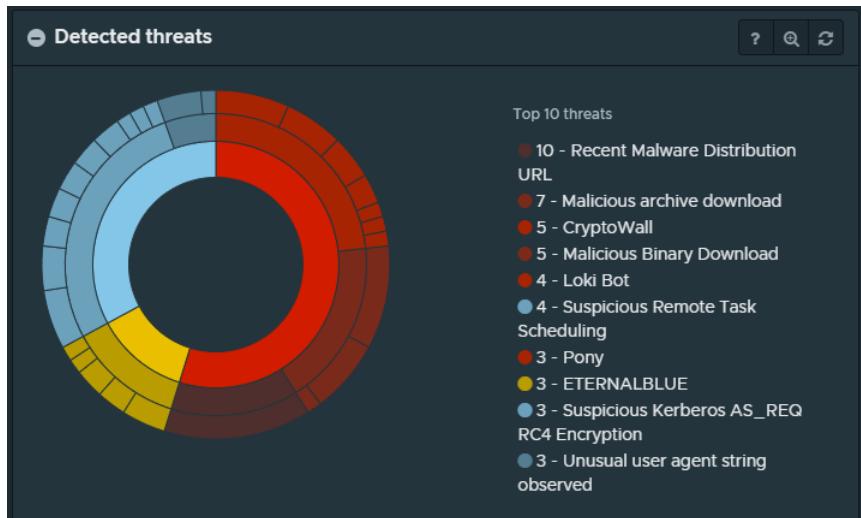
Zum Rückgängigmachen des Zooms müssen Sie den Zeitbereich zurücksetzen. Beachten Sie, dass dadurch der Vorfalltyp ausgewählt bleibt. Um das Dashboard zurückzusetzen, verwenden Sie die Schaltfläche „Zurück“ in Ihrem Browser.

In der Standardansicht werden die Vorfälle gruppiert angezeigt. Klicken Sie auf **Gestapelt**, um die Vorfälle in einer gestapelten Darstellung anzuzeigen. Klicken Sie auf die **Gruppiert**, um zur gruppierten Anzeige zurückzukehren.

Erkannte Bedrohungen

Das Widget **Erkannte Bedrohungen** bietet eine grafische Übersicht über die verschiedenen Arten von Bedrohungen, die die NSX Network Detection and Response-Anwendung im Netzwerk erkannt hat.

Die Bedrohungsinformationen werden in einem mehrschichtigen Kreis angezeigt, ähnlich wie in der folgenden Abbildung.



Die Unterteilungen der Kreise stellen die Anzahl der Hosts dar, die von den angezeigten Vorfalltypen betroffen sind. Die Bewegung zu den äußeren Kreisen bietet eine präzisere Granularität und spezifischere Informationen.

- Der innere Ring zeigt die drei verschiedenen Arten von Vorfällen an.

Vorfalltyp	Beschreibung
Infektionen	Dies sind Vorfälle, die die NSX Network Detection and Response-Anwendung als kritisch festgestellt hat. Diesen Vorfällen wurde eine Auswirkungsbewertung von 70 oder höher zugewiesen, und sie werden in Rot angezeigt.
Watchlist	Hierbei handelt es sich um Vorfälle, bei denen die NSX Network Detection and Response-Anwendung ein mittleres Risiko festgestellt hat. Solche Vorfälle weisen zwar auf ein potenzielles Risiko hin, erfordern aber möglicherweise keine sofortige Aufmerksamkeit. Sie werden genau überwacht, falls neue Nachweise ihren Status ändern. Diesen Vorfällen wird eine Auswirkungsbewertung von 30 bis 69 zugewiesen, und sie werden gelb angezeigt.
Belästigungen	Dies sind Vorfälle, die als gering oder ohne Risiko betrachtet werden. In der Regel handelt es sich dabei um potenziell unerwünschte/riskante Aktivitäten, die nicht unbedingt auf eine Gefährdung oder Infektion des überwachten Netzwerks hindeuten. Diesen Vorfällen wurde eine Auswirkungsbewertung von weniger als 30 zugewiesen, und sie werden blau angezeigt.

- Im mittleren Ring wird die Bedrohungsklasse zusammen mit der Anzahl der relevanten Vorfälle für jeden Typ von Mandanten angezeigt. Bedrohungsklassen umfassen Befehls- und Steuerungsserver, Downloads bösartiger Dateien, Crypto-Miner und vieles mehr.
- Der äußere Ring stellt die einzelnen Bedrohungsfamilien dar, die im Netzwerk erkannt werden. Bedrohungsfamilien umfassen Ransomware, bösartige Binärdateien usw.

Wenn Sie auf das Diagramm zeigen, zeigt das Widget den Bedrohungsnamen und eine Anzahl der Hosts an, auf denen die NSX Network Detection and Response-Anwendung die Bedrohung beobachtet hat.

Wenn Sie auf ein Element im Diagramm klicken, wird die Ansicht vergrößert und zeigt weitere Details zum ausgewählten Informationstyp an. Durch erneutes Klicken auf das Element wird die Ansicht wieder vergrößert.

Wenn Sie im inneren Ring auf einen Vorfalltyp klicken, vergrößert sich die Diagrammansicht und zeigt die entsprechenden Vorfälle im mittleren und äußeren Ring an. Wenn Sie im mittleren Ring auf eine Bedrohungsklasse klicken, wird die Diagrammansicht vergrößert und zeigt die entsprechenden Bedrohungsfamilien an. Wenn Sie auf den äußeren Ring klicken, wird die Diagrammansicht vergrößert und zeigt Details zur ausgewählten Bedrohung an.

Die Legende auf der rechten Seite des Widgets liefert eine Anzahl der Vorkommen der am häufigsten erkannten Bedrohungen. Wenn Sie auf ein Element in der Legende zeigen, enthält ein Popup-Fenster weitere Informationen zur Bedrohungsklasse, zur Anzahl der Vorfälle und zur Anzahl der betroffenen Hosts. Wenn Sie auf das Element klicken, wird die Diagrammansicht für den ausgewählten Bedrohungstyp vergrößert und bietet weitere kontextbezogene Informationen.

Verwenden von Filtern auf der Seite „Vorfälle“

NSX Network Detection and Response bietet einen Filtermechanismus, der es Ihnen ermöglicht, sich auf bestimmte, für Sie interessante Informationen zu konzentrieren. Die Verwendung von Filtern ist optional.

Verfahren

- 1 Klicken Sie auf der Seite **Vorfälle** auf das Symbol  um das Widget **Filter** zu erweitern.
- 2 Klicken Sie auf eine beliebige Stelle im Textfeld **Filter auf** und wählen Sie ein Element im Dropdown-Menü aus.

Sie können aus den folgenden verfügbaren Filtern auswählen. Um den Fokus der angezeigten Informationen weiter einzuschränken, können Sie mehrere Filter kombinieren.

Filtername	Beschreibung
Aktivitäten-UUID	Schränken Sie die angezeigten Einträge durch die Aktivitäten-UUID ein. Dies ist eine 32-stellige hexadezimale Zeichenfolge, z. B. 7dabc0fc9b3f478a850e1089a923df3a. Alternativ können Sie die Zeichenfolge <code>null</code> eingeben, um Datensätze auszuwählen, die zu keiner Aktivität gehören.
Home-Netzwerk	Schränken Sie die angezeigten Einträge durch die Einstellung Home-Netzwerk ein. Wählen Sie im Dropdown-Menü Nur Home-Netzwerk oder Nicht identifizierte Netzwerke aus.
Host-IP	Beschränken Sie die angezeigten Einträge auf eine bestimmte Quell-IP-Adresse, einen bestimmten IP-Adressbereich oder einen CIDR-Block. Geben Sie den Wert in das Textfeld ein.
Hostname	Beschränken Sie die angezeigten Einträge anhand des Hostnamens. Der vollständige Hostname oder die Bezeichnung muss angegeben werden.
Priorität	Schränken Sie die angezeigten Einträge nach dem Prioritätsstatus ein. Wählen Sie im Dropdown-Menü Infektionen , Überwachungsliste oder Belästigungen aus.
Gelesen	Schränken Sie die angezeigten Einträge nach ihrem Gelesenstatus ein. Wählen Sie im Dropdown-Menü Gelesen oder Ungelesen aus.
Status	Schränken Sie die angezeigten Einträge nach ihrem Status ein. Wählen Sie Geschlossen oder Offen im Dropdown-Menü aus.

Filtername	Beschreibung
Bedrohung	<p>Schränken Sie die angezeigten Einträge auf eine bestimmte Bedrohung ein. Wählen Sie eine Bedrohung aus dem Dropdown-Menü aus. Das Menü wird mit einer Liste katalogisierter Bedrohungen vorausgefüllt.</p> <p>Verwenden Sie die Suchfunktion oben im Menü, um schnell einen Bedrohungsnamen zu finden.</p>
Bedrohungsklasse	<p>Schränken Sie die angezeigten Einträge auf eine bestimmte Bedrohungsklasse ein. Wählen Sie die Bedrohungsklasse aus dem Dropdown-Menü. Das Menü ist mit einem Katalog von Klassen vorausgefüllt, von denen einige unten aufgeführt sind. Verwenden Sie die Suchfunktion oben im Menü, um schnell einen Klassennamen zu finden.</p> <ul style="list-style-type: none"> ■ Adware: Malware, die auf einem infizierten Computer Werbung anzeigt oder herunterlädt. ■ Klickbetrug: Klickbetrug zielt auf Pay-per-Click-Online-Werbung ab. ■ Befehl und Steuerung: Ein infizierter Computer gehört zu einem Botnet und kann von einem Angreifer aus der Ferne gesteuert werden. ■ Drive-by: Ein Angreifer versucht, eine Sicherheitslücke auf dem Computer auszunutzen, um zusätzliche Malware auf dem Zielsystem zu installieren. ■ Exploit-Toolkit: Erkennung eines Exploit-Toolkits, das einen Drive-by-Download-Angriff versucht hat ■ Fake-AV: Gefälschte Antiviren-Software oder andere Arten betrügerischer Sicherheitssoftware, die darauf abzielt, Ihre Benutzer zu täuschen oder in die Irre zu führen. ■ Inaktives C&C: Der Befehls- und Steuerungsserver für dieses spezifische Botnet ist inaktiv. ■ VMware-Blockierungstest: Die Domäne block.lastline.com wird verwendet, um die Blockierung von Netzwerkverbindungen zu testen. Die ausgewählten Ereignisse gehören zu dieser Klasse. ■ VMware-Test: Die Domäne test.lastline.com wird verwendet, um die Funktionalität des Setups zu testen, und die ausgewählten Ereignisse gehören zu dieser Klasse. ■ Download bösartiger Dateien, Malwareverteilung und Malware-Download: Die IP-Adresse oder Domäne hostet bösartige ausführbare Dateien. ■ Sinkhole: Ein Sinkhole wird von einer legitimen Organisation betrieben, stellt also keine Bedrohung dar. Allerdings können Hosts, die versuchen, einen solchen Host zu kontaktieren, infiziert werden. ■ Spyware: Malware, die versucht, vertrauliche Informationen zu entwenden. ■ suspicious-dns: Verdächtige DNS-Domänen sind Domänen, die von Malware kontaktiert werden, die auf infizierten Computern ausgeführt wird. Unsere proprietären Techniken konnten diese Domänen proaktiv als böswillig identifizieren. ■ Unbekannt: Ein unbekanntes Sicherheitsrisiko wurde erkannt.

- 3 Um die ausgewählten Filter anzuwenden, klicken Sie auf **Anwenden**.
- 4 (Optional) Um einen einzelnen Filter zu löschen, klicken Sie neben dem Eintrag auf die Schaltfläche – **Entfernen**. Um alle ausgewählten Filter zu löschen, klicken Sie auf das Symbol  rechts neben dem Widget **Filter**.

Das Widget **Filter** wird ausgeblendet, wenn Sie alle ausgewählten Filter löschen.

Vorfallsliste

Ein Vorfall ist eine sicherheitsrelevante Aktivität, die von NSX Network Detection and Response im überwachten Netzwerk festgestellt wurde. Ein Vorfall kann aus einem einzelnen Ereignis oder einer Reihe von Ereignissen bestehen, die automatisch korreliert wurden und als eng miteinander verbunden erkannt wurden. Die Liste der Vorfälle zeigt die registrierten Vorfälle mit ihren entsprechenden Bedrohungsstufen an.

Sie können alle gemeldeten Vorfälle sehen, die als kritisch eingestuft wurden, die Sie im Auge behalten sollten oder die in Ihrem Netzwerk als störend empfunden werden. Kritische Vorfälle müssen ohne Verzögerung behandelt werden. Der Umgang mit kritischen Vorfällen ist äußerst riskant und erhöht die Wahrscheinlichkeit, dass auch andere Hosts in Ihrem Netzwerk kompromittiert werden.

Vorfälle, die Sie noch nicht untersucht haben, werden als ungelesen markiert, während diejenigen, die Sie bereits untersucht haben, als gelesen markiert sind. Sie haben die Möglichkeit, Vorfälle auszuwählen und Aktionen daran durchzuführen, wie z. B. sie als gelesen oder ungelesen zu markieren. Sie können auch ausgewählte Vorfälle schließen oder öffnen.

Das Textfeld für die **Schnellsuche** oberhalb der Liste bietet eine Suchfunktion, die direkt nach der Eingabe ausgeführt wird. Es filtert die Zeilen in der Liste und zeigt nur die Zeilen an, die in einem beliebigen Feld Text enthalten, der mit der Abfragezeichenfolge übereinstimmt.

Verwenden Sie das Dropdown-Menü **AUSWÄHLEN** für eine detaillierte Auswahl. Mit diesen Optionen können Sie **alle sichtbaren Vorfälle** auswählen oder die **Auswahl löschen**. Sie können auch die Vorfälle **Gelesen (aktuelle Seite)** oder **Ungelesen (aktuelle Seite)** auswählen. Sie können auch auf das Symbol **Bearbeiten** in der Titelzeile klicken, um alle sichtbaren Nachrichten auszuwählen.

Verwenden Sie das Dropdown-Menü **AKTION**, um die ausgewählten Vorfälle zu aktualisieren: **Als gelesen markieren**, **Als ungelesen markieren**, **Schließen** oder **Öffnen**.

Passen Sie die Anzahl der Zeilen an, die angezeigt werden sollen. Die Standardeinstellung ist 20 Einträge. Verwenden Sie das Symbol mit dem < und das Symbol mit dem >, um durch mehrere Seiten zu navigieren.

Die Spalten, die in der Liste angezeigt werden sollen, können durch Anklicken des Symbols **Zusätzlicher Inhalt** angepasst werden.

Jede Zeile ist eine Zusammenfassung eines Vorfalls. Klicken Sie auf das **Plussymbol** (oder an einer beliebigen Stelle in einer Eingabezeile), um auf die Vorfalldetails zuzugreifen. Um eine Meldungszeile auszuwählen, klicken Sie auf das Symbol **Bearbeiten**.

Die Liste ist nach Auswirkungen sortiert und enthält die folgenden Spalten.

Spalte	Beschreibung
Host	<p>Der von diesem Vorfall betroffene Host. In dieser Spalte wird die IP-Adresse, der Hostname oder die Bezeichnung des Hosts angezeigt, je nach dem aktuellen Popup-Fenster Anzeigeeinstellungen.</p> <p>Klicken Sie auf das  um die Seite mit dem Hostprofil aufzurufen, die Details über den Host anzeigt.</p> <p>Klicken Sie auf das Symbol , um die Liste nach Hostinformationen zu sortieren.</p>
Erkennungsereignisse	<p>Anzahl der Ereignisse, aus denen dieser Vorfall besteht. Dies ist ein Link, der eine Ereignisanzahl und das  anzeigt. Wenn Sie auf diesen Link klicken, wird die Seite Ereignisse gefiltert, um nur Ereignisse für diesen Vorfall anzuzeigen.</p> <p>Klicken Sie auf das Symbol , um die Liste nach Ereignissen zu sortieren.</p>
Start	<p>Startzeit des Vorfalls.</p> <p>Klicken Sie auf das Symbol , um die Liste nach Startzeit zu sortieren.</p>
Ende	<p>Endzeit des Vorfalls.</p> <p>Klicken Sie auf das Symbol , um die Liste nach Endzeit zu sortieren.</p>
Bedrohung	<p>Name des erkannten Sicherheitsrisikos.</p> <p>Klicken Sie auf das Symbol , um die Liste nach Bedrohung zu sortieren.</p>
Bedrohungsklasse	<p>Name der erkannten Sicherheitsrisikoklasse.</p> <p>Klicken Sie auf das Symbol Sortieren, um die Liste nach Bedrohungsklasse zu sortieren.</p>
Auswirkung	<p>Der Auswirkungswert gibt die kritische Stufe der erkannten Bedrohung an und liegt zwischen 1 und 100:</p> <ul style="list-style-type: none"> ■ Bedrohungen ab 70 werden als kritisch betrachtet. ■ Bedrohungen, die zwischen 30 und 69 liegen, gelten als mittelschweres Risiko. ■ Bedrohungen, die zwischen 1 und 29 liegen, werden als ungefährlich eingestuft. <p>Wenn das Symbol Stopp angezeigt wird, weist es darauf hin, dass das Artefakt blockiert wurde. Die Liste ist in abnehmender Reihenfolge der Auswirkungen sortiert (die kritischsten Vorfälle stehen an erster Stelle). Klicken Sie auf das Symbol , um die Liste in aufsteigender Reihenfolge zu sortieren (die am wenigsten kritischen Vorfälle ganz oben), und klicken Sie dann auf das Symbol Winkel nach unten , um zur Standardeinstellung zurückzukehren.</p>

Vorfallsdetails

Wenn Sie auf eine beliebige Stelle in einer Vorfallszeile klicken, wird die Ansicht „Vorfallsdetails“ innerhalb der Vorfallssumme erweitert.

Oben in den Vorfalldetails sind mehrere Schaltflächen vorhanden:

- Klicken Sie auf die Schaltfläche mit dem , um den Vorfall zu schließen.
- Verwenden Sie das Dropdown-Menü **Aktion**, um eine Aktion für den Vorfall durchzuführen:
 - Wenn der Vorfall noch nicht geschlossen ist, wählen Sie **Vorfall schließen**  aus. Wählen Sie andernfalls **Vorfall öffnen**.

- Wenn der Vorfall noch nicht gelesen ist, wählen Sie **Als gelesen markieren**. Wählen Sie andernfalls **Als ungelesen markieren** aus.
- Wählen Sie **Bedrohung ignorieren**. Die Bedrohungsdetails werden im Menüelement aufgelistet. Die Auswahl dieses Elements zeigt an, dass das Vorhandensein dieser bestimmten Bedrohung auf dem Host nicht von Interesse ist. Daher werden alle Vorfälle, bei denen diese Bedrohung auf diesem Host erkannt wird, automatisch geschlossen.
- Wählen Sie **Host <Host> als bereinigt markieren**. Das System markiert den Host, der an dem Vorfall beteiligt ist, als bereinigt. Infolgedessen werden alle Vorfälle auf diesem Host geschlossen.
- Wenn Sie auf das  **Vorfalldetails anzeigen** klicken, wird der Inhalt der Seite **Vorfallprofil** in einer neuen Browserregisterkarte angezeigt.
- Wenn Sie auf **Warnung verwalten** klicken, wird die Seitenleiste **Warnung verwalten** geöffnet. Verwenden Sie diese Funktion, um unbedenkliche Ereignisse im Zusammenhang mit dem angegebenen Vorfall zu unterdrücken oder herabzustufen, z. B. den Systemtest oder blockierende Vorfälle. Weitere Informationen finden Sie unter [Arbeiten mit der Sidebar „Warnung verwalten“](#).
- Klicken Sie auf das  **Als gelesen markieren**, um den Vorfall zu markieren. Die Schaltfläche wechselt zu **Als ungelesen markieren**, wodurch Sie den Lesestatus zurücksetzen können.

Vorfallsübersicht

Der obere Abschnitt bietet eine visuelle Übersicht über die erkannte Bedrohung und zeigt die Auswirkungspunktzahl an.

Vorfallsdetails

Das Widget **Vorfallsdetails** zeigt detaillierte Netzwerkinformationen über den Vorfall an. Sie enthält die folgenden Daten.

Spalte	Beschreibung
Quell-IP	Die IP-Adresse der Vorfallsquelle. Klicken Sie auf das  , um die Seite Aktivität für Host anzuzeigen. Klicken Sie auf das  , um die Quelle auf der Seite Netzwerkanalyse anzuzeigen.
Quellhost	Falls verfügbar, der FQDN der Vorfallsquelle.
Ereignisse	Die Anzahl der Ereignisse, aus denen dieser Vorfall besteht.
Vorfall-ID	Ein Permalink zur Seite Vorfallprofil . Der Link wird in einer neuen Registerkarte/einem neuen Browserfenster geöffnet.
Aktivitäts-ID	Ein Permalink zur Seite „Aktivitäten“. Der Link wird auf einer neuen Browserregisterkarte geöffnet.
Auswirkung	Die vom System auf diesen Vorfall angewendete Auswirkungspunktzahl.
Startzeit	Ein Zeitstempel für den Beginn des Vorfalls.

Spalte	Beschreibung
Endzeit	Ein Zeitstempel für das letzte aufgezeichnete Ereignis des Vorfalls.
Status	Zeigt an, ob der Vorfall geschlossen wurde.

Nachweise

Das erweiterte Widget **Nachweis** zeigt die Liste der Ereignisse an, die von NSX Network Detection and Response erkannt wurden.

Die Spalten, die in der Liste angezeigt werden sollen, können durch Klicken auf das Symbol mit den  angepasst werden.

Jede Zeile ist eine Zusammenfassung eines Nachweiseintrags und enthält die folgenden Spalten.

Spalte	Beschreibung
Erste Erkennung	Zeitstempel des ersten Auftretens dieses Ereignisses.
Letzte Erkennung	Zeitstempel des letzten Auftretens dieses Ereignisses.
Bedrohung	Name des erkannten Sicherheitsrisikos.
Bedrohungsklasse	Name der erkannten Sicherheitsrisikoklasse.
Auswirkung	Die auf diesen Vorfall angewendete Auswirkungspunktzahl.
Nachweise	Die Nachweiskategorie für diesen Vorfall. Der Titel des Blocks mit den Nachweisdetails wird von der Kategoriebezeichnung abgeleitet.
Subjekt	Das Artefakt, in der Regel eine Datei, die analysiert wird.
Verweis	Ein Permalink zur Ereignisseite. Der Link wird auf einer neuen Browserregisterkarte geöffnet.

Nachweisdetails

Klicken Sie auf das  (oder an einer beliebigen Stelle in einer Vorfalleintragszeile), um den Block mit den Nachweisdetails anzuzeigen.

Der Titel des Blocks mit den Nachweisdetails wird vom Nachweistyp abgeleitet. Beispiel: Reputationsnachweis.

In diesem Abschnitt werden detailliertere Informationen zu den Nachweisen angezeigt. Sie enthält die folgenden Daten.

Daten	Beschreibung
Bedrohung	Name des erkannten Sicherheitsrisikos.
Bedrohungsklasse	Name der erkannten Sicherheitsrisikoklasse.
Auswirkung	Die auf diesen Vorfall angewendete Auswirkungspunktzahl.
Detektor	Falls vorhanden, wird das NSX Network Detection and Response-Modul angezeigt, das die Bedrohung identifiziert hat. Klicken Sie auf den Link, um das Popup-Fenster „Detektor“ anzuzeigen. Siehe Popup-Fenster der Detektor-Dokumentation .
Netzwerkereignis anzeigen	Ein Permalink zur Ereignisseite. Der Link wird auf einer neuen Browserregisterkarte geöffnet.

Daten	Beschreibung
Netzwerkereignis anzeigen	Ein Permalink zur Ereignisseite. Der Link wird auf einer neuen Browserregisterkarte geöffnet.
Erste Erkennung	Zeitstempel des ersten Auftretens dieses Ereignisses.
Letzte Erkennung	Zeitstempel des letzten Auftretens dieses Ereignisses.
Schweregrad	Eine Schätzung, wie kritisch die erkannte Bedrohung ist. Beispielsweise wird eine Verbindung zu einem Befehl und einem Steuerungsserver in der Regel als hoher Schweregrad betrachtet, da die Verbindung potenziell schädlich ist.
Konfidenz	Gibt die Wahrscheinlichkeit an, dass die erkannte individuelle Bedrohung böswillig ist. Da das System fortschrittliche Heuristiken verwendet, um unbekannte Bedrohungen zu erkennen, kann die erkannte Bedrohung in einigen Fällen einen niedrigeren Konfidenzwert haben, wenn die Menge der für diese spezifische Bedrohung verfügbaren Informationen begrenzt ist.
Subjekt	Falls vorhanden, wird das Artefakt (in der Regel eine Datei) angezeigt, das gerade analysiert wird.

Weitere Informationen finden Sie unter [Informationen zu Nachweisen](#).

Arbeiten mit der Seite „Heruntergeladene Dateien“

Die Seite **Dateien heruntergeladen** enthält Registerkarten mit Informationen zu den Dateien, die in Ihr NSX-T Data Center-Netzwerk heruntergeladen wurden.

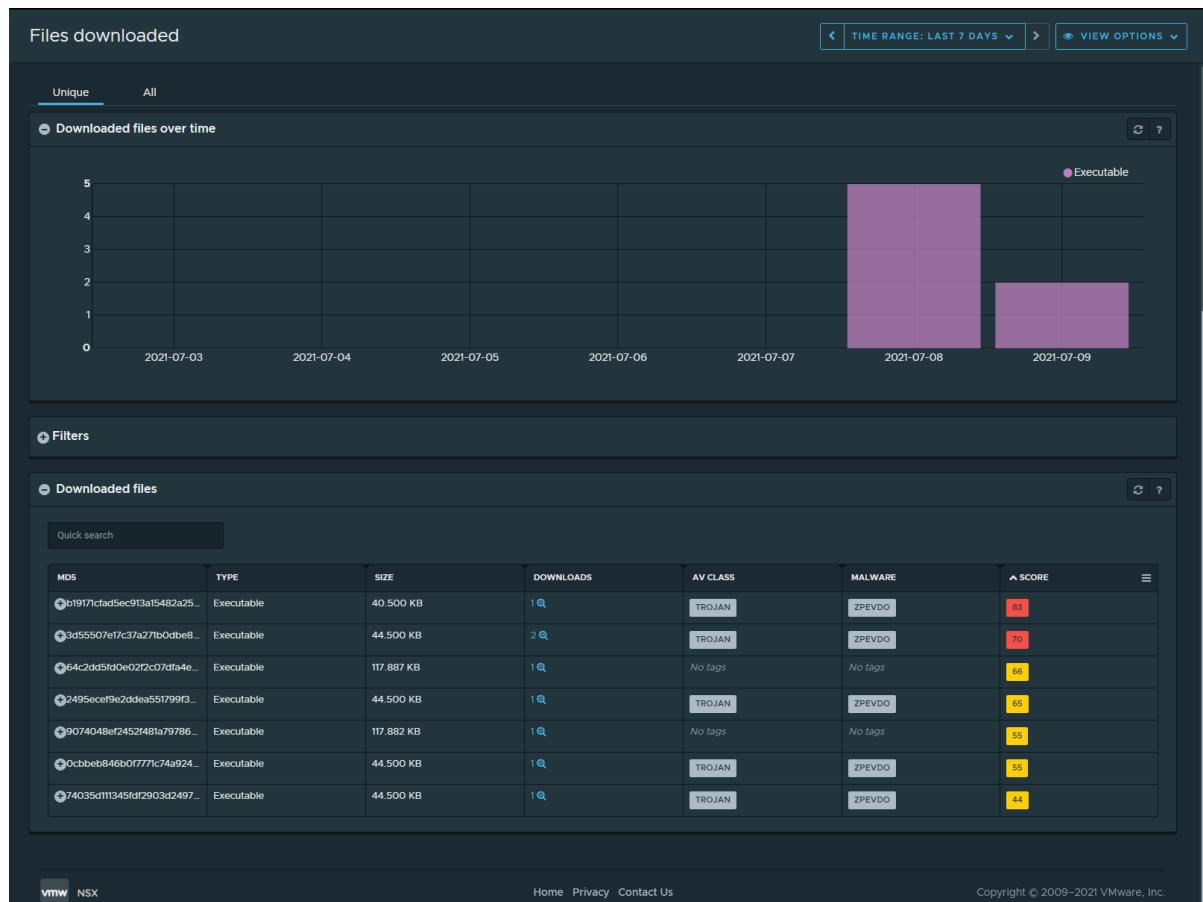
Die Seite besteht aus mehreren Widgets, die mithilfe der Informationen in [Kennenzlernen der NSX Network Detection and Response-Benutzeroberfläche](#) verwaltet werden können.

Die Seite bietet eine allgemeine Ansicht der Anzahl von Dateien verschiedener Typen, die im Netzwerk heruntergeladen wurden. Darüber hinaus können Sie die Details einzelner Downloads einsehen, einschließlich Zugriff auf die vollständigen Berichte der durchgeföhrten Analyse.

Die folgenden Registerkarten werden auf dieser Seite angezeigt.

- Auf der Registerkarte **Eindeutig** werden eindeutige Dateidownloads im Netzwerk angezeigt, die analysiert wurden.
- Auf der Registerkarte **Alle** werden alle Instanzen von Dateidownloads angezeigt, die NSX Network Detection and Response im Netzwerk analysiert. Einige der angezeigten Dateien sind Wiederholungen.

Die folgende Abbildung zeigt ein Beispiel für die Seite **Heruntergeladene Dateien**.



Registerkarte „Eindeutig“

Auf der Registerkarte **Eindeutig** auf der Seite **Heruntergeladene Dateien** von NSX Network Detection and Response werden die einzelnen Dateidownloads im Netzwerk angezeigt, die analysiert wurden.

Heruntergeladene Dateien im zeitlichen Verlauf

Das Widget **Heruntergeladene Dateien** bietet einen Überblick über die Anzahl der Dateien, die während des angegebenen Zeitraums im überwachten Netzwerk heruntergeladen wurden. Das Diagramm ist ein tägliches Histogramm der heruntergeladenen Dateien, gruppiert nach dem übergeordneten Dateityp.

Das Widget zeigt nur eindeutige Dateidownloads an, die analysiert wurden.

Im Folgenden sind die angezeigten Dateitypen aufgeführt.

Dateityp	Beschreibung
Archiv	Archivformate, wie z. B. ZIP oder RAR.
Dokument	Enthält andere Arten von Office-Dokumenten.
Ausführbare Datei	Binäre Anwendungsformate, wie z. B. Windows Portable Executable.

Dateityp	Beschreibung
Java	Java-Anwendung oder -Applet.
Medien	Flash-Datei von Macromedia (Adobe).
Sonstiges	Anderes erkanntes Dateiformat.
PDF	Dateien im Portable Document Format.
Skript	Ein ausführbares Skript, z. B. JavaScript, Python usw.
Unbekannt	Unbekannter Dateityp.

Verwenden von Filtern auf der Seite „Heruntergeladene Dateien“

NSX Network Detection and Response bietet einen Filtermechanismus, mit dem Sie sich auf bestimmte Informationen zu heruntergeladenen Dateien konzentrieren können, die für Sie von Interesse sind. Die Verwendung von Filtern ist optional.

Verfahren

- 1 Klicken Sie auf der Seite **Heruntergeladene Dateien** auf das , um das Widget **Filter** zu erweitern.
- 2 Klicken Sie auf eine beliebige Stelle im Textfeld **Filter auf** und wählen Sie ein Element im Dropdown-Menü aus.

Sie können aus den folgenden verfügbaren Filtern auswählen. Um den Fokus der angezeigten Informationen weiter einzuschränken, können Sie mehrere Filter kombinieren.

Filtername	Beschreibung
Analyse-Tags	Schränken Sie die angezeigten Dateien durch ihre Analyse-Tags ein. Hierbei handelt es sich um Bezeichnungen, die einer Datei oder URL von der Systemanalyse zugewiesen werden. Sie können eine Bedrohung oder eine Bedrohungsklasse identifizieren oder sich auf ein bestimmtes bösartiges Verhalten beziehen, das erkannt wurde.
Analyst-UUID	Schränken Sie die angezeigten Dateien auf die Systemanalyse-UUID für die heruntergeladene Datei ein. Dies ist ein interner eindeutiger Bezeichner für die Analyse einer Datei.
Anwendungsprotokoll	Beschränken Sie angezeigte Dateien, die über eines der angegebenen Protokolle übertragen werden. Unterstützte Werte sind HTTP/HTTPS, FTP und SMB.
Kontaktierte IP	Beschränken Sie die angezeigten Dateien auf die IP-Adresse, von der die Datei heruntergeladen wurde. Wie der Host-IP-Filter unterstützt auch dieser IP-Adressen, CIDR-Blöcke oder IP-Adressbereiche.
Dateitypfilter	Beschränken Sie die angezeigten Dateien auf einen oder mehrere Dateitypen auf hoher Ebene. Weitere Informationen finden Sie in der Liste der Dateitypen (oben).
Dateien	Wählen Sie Bösartig aus, um die angezeigten Dateien auf bösartige Dateien zu beschränken. Dies sind Dateien, die bei der Systemanalyse eine Punktzahl von 70 oder mehr (von 100) erhalten haben.
Host-IP	Beschränken Sie die angezeigten Dateien auf die IP-Adresse des Hosts im Netzwerk, von dem die Datei heruntergeladen wurde. Dieser Filter unterstützt die Auswahl einer oder mehrerer IP-Adressen, CIDR-Blöcke (z. B. 192.168.0.0/24) oder IP-Adressbereiche (z. B. 192.168.1.5-192.168.1.9).

Filtername	Beschreibung
HTTP-Host	<p>Beschränken Sie die angezeigten Dateien auf den/die Hostname(n), von dem die Datei heruntergeladen wurde.</p> <p>Hinweis Dieser Wert wird aus dem HTTP-Host-Header in der HTTP-Anforderung extrahiert, mit der die Datei heruntergeladen wurde. Daher unterliegt er der Kontrolle des Clients und kann von einer bösartigen Software gefälscht werden, z. B. von einer Malware-Binärdatei, die bereits auf einem infizierten Host ausgeführt wird.</p>
MD5	Beschränken Sie die angezeigten Dateien auf den MD5-Hash der heruntergeladenen Datei.
Mindestpunktzahl	Beschränken Sie die angezeigten Dateien auf diejenigen, denen die Systemanalyse eine höhere Punktzahl als den von Ihnen gewählten Wert (von 1-100) zugewiesen hat.

- 3 Um die ausgewählten Filter anzuwenden, klicken Sie auf **Anwenden**.
- 4 (Optional) Um einen einzelnen Filter zu löschen, klicken Sie neben dem Eintrag auf die Schaltfläche **ENTFERNEN**. Um alle ausgewählten Filter zu löschen, klicken Sie auf das Symbol **X** rechts neben dem Widget **Filter**.

Das Widget **Filter** wird ausgeblendet, wenn Sie alle ausgewählten Filter löschen.

Eindeutige Liste heruntergeladener Dateien

In der Liste **Heruntergeladene Dateien** werden alle einzelnen Dateien angezeigt, die von Hosts im Netzwerk heruntergeladen und vom NSX Advanced Threat Prevention-Dienst verarbeitet wurden.

Das Textfeld für die **Schnellsuche** in der oberen linken Ecke der Liste bietet eine schnelle Suchfunktion, die direkt nach der Eingabe ausgeführt wird. Es filtert die Zeilen in der Liste und zeigt nur die Zeilen mit Text in einer Spalte an, die mit der Abfragezeichenfolge übereinstimmt, die Sie im Suchtextfeld eingegeben haben.

Um die in der Liste angezeigten Spalten anzupassen, klicken Sie auf das  in der oberen rechten Ecke der Liste.

Sie können die Anzahl der Zeilen, die angezeigt werden sollen, anpassen. Die Standardeinstellung ist 20 Einträge. Verwenden Sie das Symbol mit dem  und das Symbol mit dem , um durch mehrere Seiten zu navigieren.

Jede Zeile ist eine Zusammenfassung einer heruntergeladenen Datei. Klicken Sie auf das  oder an einer beliebigen Stelle in einer Eingabezeile, um auf eine detaillierte Ansicht der heruntergeladenen Datei zuzugreifen.

Die Liste ist nach Punktzahl sortiert und enthält die folgenden Spalten.

Spaltenname	Beschreibung
MD5	Der MD5-Hash der heruntergeladenen Datei.
Typ	<p>Der allgemeine Dateityp der heruntergeladenen Datei. Unterstützte Typen sind derzeit:</p> <ul style="list-style-type: none"> ■ Archiv – Archivformate wie ZIP oder RAR ■ Dokument – Enthält andere Arten von Office-Dokumenten ■ Ausführbare Datei – Binäre Anwendungsformate, wie z. B. Windows Portable Executable ■ Java – Java-Anwendung oder -Applet ■ Medien – Flash-Datei von Macromedia (Adobe) ■ Andere – Anderes erkanntes Dateiformat ■ PDF – Dateien im Portable Document Format ■ Skript – Ein ausführbares Skript wie JavaScript, Python und andere ■ Unbekannt – Unbekannter Dateityp
Größe	Größe der heruntergeladenen Datei in Byte.
Downloads	<p>Anzahl der Downloads der Datei durch Hosts im Netz.</p> <p>Die angezeigte Nummer und das  sind ein Link zur detaillierten Download-Seite. Der Link übergibt einen Analyse-UUID-Filter, der die Ansicht auf Downloads dieser spezifischen Datei beschränkt.</p>
AV-Klasse	<p>Eine Bezeichnung, die die Antivirenklasse der heruntergeladenen Datei definiert. Wenn die Bezeichnung über ein  verfügt, können Sie in einem Popup-Fenster auf dieses Symbol klicken, um eine Beschreibung zu erhalten.</p>
Malware	<p>Eine Bezeichnung, die den Malware-Typ der heruntergeladenen Datei definiert. Wenn die Bezeichnung über ein  verfügt, können Sie in einem Popup-Fenster auf dieses Symbol klicken, um eine Beschreibung zu erhalten.</p>
Bewertung	<p>Die der heruntergeladenen Datei durch die Analyse zugewiesene Punktzahl gibt den kritischen Grad der erkannten Bedrohung an und reicht von 0-100:</p> <ul style="list-style-type: none"> ■ Bedrohungen ab 70 werden als kritisch betrachtet. ■ Bedrohungen zwischen 30 und 69 gelten als mittleres Risiko. ■ Bedrohungen zwischen 1 und 29 gelten als harmlose Bedrohungen. <p>Einzelheiten zum Kern der Bösartigkeit und zur Risikoeinschätzung finden Sie unter Analysebericht: Registerkarte „Übersicht“.</p> <p>Wenn das  angezeigt wird, bedeutet dies, dass das Artefakt blockiert wurde. Die Liste wird in absteigender Reihenfolge sortiert (die kritischsten Bedrohungen oben). Klicken Sie auf den , um die Liste in aufsteigender Reihenfolge zu sortieren (am wenigsten kritische Bedrohungen oben). Klicken Sie dann auf den , um zur Standardeinstellung zurückzukehren.</p>

Details zu heruntergeladenen Dateien

Die Detailansicht der heruntergeladenen Dateien wird in der Liste **Heruntergeladene Dateien** erweitert.

Je nachdem, welche Registerkarte Sie auf der Seite **Heruntergeladene Dateien** ausgewählt haben, wird eine Teilmenge der folgenden verfügbaren Details angezeigt.

Detailname	Beschreibung
Analysebericht	Klicken Sie auf den Link oder das  , um den Analysebericht in einer neuen Registerkarte anzuzeigen.
Dateityp	Der allgemeine Typ der heruntergeladenen Datei. Eine Liste der Dateitypen finden Sie unter Heruntergeladene Dateien im zeitlichen Verlauf .
Details zum Dateityp	Falls verfügbar, finden Sie hier weitere Details zum Dateityp. Beispiel: PE executable, application, 32-bit, Intel i386 oder Zip archive data.
Dateiname	Falls verfügbar, finden Sie hier den Namen der Datei.
Heruntergeladen	Für Downloads vom Typ Eindeutig wird hiermit die Anzahl der Downloads der Datei durch Hosts im Netzwerk angegeben. Klicken Sie auf die Zahl oder das  , um die Dateidownloads auf der Download-Seite anzuzeigen. Der Link übergibt einen Analyse-UUID-Filter, der die Ansicht auf Downloads der jeweiligen Datei beschränkt.
Heruntergeladen von	Die IP-Adressen der Hosts im Netzwerk, die die Datei heruntergeladen haben. Falls verfügbar, klicken Sie auf das  , um Registrierungsinformationen und andere Daten zum Host unter WHOIS-Popup-Fenster anzuzeigen.
URL	Die URL des Dateidownloads. Dies ist eine UTF-8-codierte Unicode-Zeichenfolge.
URL	Die Raw-URL des Dateidownloads. Wenn die URL Nicht-ASCII-Zeichen enthält, werden diese sowie der umgekehrte Schrägstrich selbst mit einem umgekehrten Schrägstrich codiert.
Protokoll	Netzwerkprotokolle, die zum Herunterladen der Datei verwendet werden. HTTP/HTTPS, FTP oder SMB.
Heruntergeladen von	IP-Adresse des kontaktierten Hosts. Falls verfügbar, klicken Sie auf das  , um Registrierungsinformationen und andere Daten zum Host in den WHOIS-Popup-Fenster anzuzeigen.
HTTP-Host	Falls verfügbar, der Domänenname des kontaktierten Hosts. Dieser Name kann von anderen Daten, einschließlich der IP-Adresse, abgeleitet werden. Falls verfügbar, klicken Sie auf das  , um Registrierungsinformationen und andere Daten zum Host unter WHOIS-Popup-Fenster anzuzeigen.
Benutzer-Agent	Die Zeichenfolge des Benutzer-Agent, die aus der HTTP/HTTPS-Anforderung extrahiert wurde.
Erster Download	Bei eindeutigen Downloads der Zeitstempel der ersten aufgezeichneten Erkennung des Dateidownloads.
Letzter Download	Bei eindeutigen Downloads der Zeitstempel der neuesten Erkennung des Dateidownloads.
Zeitstempel	Der Zeitstempel der Erkennung des Dateidownloads.
Dateigröße	Größe der Datei in Byte.
MD5	Der MD5-Hash der heruntergeladenen Datei.
SHA 1	Der SHA1-Hash der heruntergeladenen Datei.
Übermittlungsstatus	Gibt an, warum die heruntergeladene Datei nicht zur vollständigen Analyse übermittelt wurde. Dies ist in der Regel auf Vorabfilterung oder andere Gründe zurückzuführen. Fahren Sie mit der Maus über das  , um ein Popup-Fenster mit weiteren Informationen anzuzeigen.

Detailname	Beschreibung
Analyst-UUID	Der eindeutige Bezeichner, der vom NSX Advanced Threat Prevention-Dienst nach der Verarbeitung der heruntergeladenen Datei zurückgegeben wurde.
Ereignis-ID	Ein Link zum zugehörigen Ereignis für den Dateidownload. Klicken Sie auf die ID oder das  , um das Ereignis anzuzeigen. Weitere Informationen hierzu finden Sie unter Erkennungsereignisse .

Analyseübersicht

Der Abschnitt „Analyseübersicht“ enthält eine Übersicht über die Ergebnisse der Analyse einer heruntergeladenen Datei durch den NSX Advanced Threat Prevention-Dienst.

Um den vollständigen Analysebericht in einer neuen Registerkarte zu öffnen, klicken Sie auf das . Siehe [Verwenden des Analyseberichts](#).

Um die erkannte Datei auf Ihren lokalen Computer herunterzuladen, klicken Sie auf der rechten Seite des Bildschirms auf das . Wählen Sie im Dropdown-Menü **Datei herunterladen** oder **Als ZIP herunterladen** aus.

Wenn Sie **Als ZIP herunterladen** auswählen, wird das Popup-Fenster **Datei als ZIP herunterladen** angezeigt, in dem Sie aufgefordert werden, ein optionales Kennwort für das Archiv anzugeben. Klicken Sie auf **Download**, um das Herunterladen der .ZIP-Datei abzuschließen.

Wichtig Mit der NSX Network Detection and Response-Anwendung können Sie erkannte Dateien nur unter bestimmten Bedingungen herunterladen.

Wenn das Artefakt als geringes Risiko betrachtet wird, wird das  und Sie können es auf Ihren lokalen Computer herunterladen.

Wenn das Artefakt als riskant betrachtet wird, wird das  nur angezeigt, wenn Ihre Lizenz über die `ALLOW_RISKY_ARTIFACT_DOWNLOADS`-Funktion verfügt.

Sie müssen sich bewusst sein, dass das Artefakt beim Öffnen möglicherweise Schaden anrichten kann.

Die NSX Network Detection and Response-Benutzeroberfläche zeigt möglicherweise das Popup-Fenster **Warnung: Bösartige Datei wird heruntergeladen** an. Klicken Sie auf die Schaltfläche **Ich stimme zu**, um die Bedingungen zu akzeptieren und die Datei herunterzuladen.

Bei bösartigen Artefakten empfiehlt es sich, die Datei in ein ZIP-Archiv einzuschließen, um zu verhindern, dass andere Lösungen, die Ihren Datenverkehr überwachen, die Bedrohung automatisch inspizieren.

Wenn Sie nicht über die `ALLOW_RISKY_ARTIFACT_DOWNLOADS`-Funktion verfügen und die Möglichkeit benötigen, bösartige Artefakte herunterzuladen, wenden Sie sich an den [VMware Support](#).

Klicken Sie auf das  und , um die Abschnitte auf der Registerkarte zu erweitern und zu reduzieren.

Der Abschnitt „Analyseübersicht“ enthält eine Zusammenfassung der Analyseergebnisse einer Datei oder URL, die vom NSX Advanced Threat Prevention-Dienst analysiert wird. Im Abschnitt werden die folgenden Daten angezeigt.

- MD5 – Der MD5-Hash der Datei. Um nach anderen Instanzen dieses Artefakts in Ihrem Netzwerk zu suchen, klicken Sie auf <Suchsymbol>.
- SHA 1 – Der SHA 1-Hash der Datei.
- SHA 256 – Der SHA 256-Hash der Datei.
- MIME-Typ – Die Bezeichnung, die zur Identifizierung des Datentyps in der Datei verwendet wird.
- Übermittlung – Der Zeitstempel für die Übermittlung

Der Abschnitt „Bedrohungsstufe“ beginnt mit einer Zusammenfassung der Analyseergebnisse: Der md5-Hash der Datei wurde als bösartig/gutartig eingestuft.

Anschließend werden die folgenden Daten angezeigt:

Risikobewertung

In diesem Abschnitt werden die Ergebnisse der Risikobewertung angezeigt.

- Punktzahl für die Böswilligkeit – Legt einen Wert von 100 fest.
- Risikoschätzung – Eine Schätzung der Risiken, die durch dieses Artefakt verursacht werden:
 - Hoch – Dieses Artefakt stellt ein kritisches Risiko dar, das Sie mit Priorität beheben müssen. Bei diesen Subjekten handelt es sich in der Regel um Trojanerdateien oder Dokumente, die Exploits enthalten, was zu größeren Kompromittierungen des infizierten Systems führt. Die Risiken sind vielfältig: von Informationsverlusten bis hin zu Systemstörungen. Diese Risiken werden teilweise aus dem erkannten Aktivitätstyp abgeleitet. Der Schwellenwert für die Punktzahl für diese Kategorie ist in der Regel größer als 70.
 - Mittel – Dieses Artefakt stellt ein langfristiges Risiko dar, das Sie genau überwachen müssen. Es kann sich um eine Webseite mit verdächtigen Inhalten handeln, die potenziell zu Drive-by-Angriffen führt. Es kann sich auch um eine Adware oder ein gefälschtes Antivirenprodukt handeln, das keine unmittelbare ernsthafte Bedrohung darstellt, aber Probleme mit der Funktion des Systems verursachen kann. Der Schwellenwert für die Punktzahl für diese Kategorie liegt in der Regel zwischen 30 und 70.
 - Niedrig – Dieses Artefakt wird als gutartiges Artefakt betrachtet, und Sie können es ignorieren. Der Schwellenwert für die Punktzahl für diese Kategorie liegt in der Regel unter 30.
- Antivirenklasse – Die Antiviren- oder Malware-Klasse, zu der das Artefakt gehört. Zum Beispiel ein Trojanisches Pferd, ein Wurm, Adware, Ransomware, Spyware und so weiter.

- Antivirus-Familie – Die Antivirus- oder Malware-Familie, zu der das Artefakt gehört. Beispiel: Valyria, Darkside usw. Um nach anderen Instanzen dieser Familie zu suchen, klicken Sie auf das Suchsymbol.

Analyseübersicht

Die angezeigten Informationen sind nach Schweregrad sortiert und enthalten die folgenden Eigenschaften:

- Schweregrad – Eine Punktzahl zwischen 0 und 100 der Böswilligkeit der Aktivitäten, die während der Analyse des Artefakts erkannt wurden. Die zusätzlichen Symbole geben die Betriebssysteme an, auf denen das Artefakt ausgeführt werden kann.
- Typ – Die Typen von Aktivitäten, die während der Analyse des Artefakts erkannt wurden. Diese Typen beinhalten:
 - Autostart – Möglichkeit zum Neustarten nach dem Herunterfahren einer Maschine.
 - Deaktivieren – Möglichkeit, kritische Komponenten des Systems zu deaktivieren.
 - Evasion – Möglichkeit, die Analyseumgebung zu umgehen.
 - Datei – Verdächtige Aktivität über das Dateisystem.
 - Arbeitsspeicher – Verdächtige Aktivität innerhalb des Systemarbeitsspeichers.
 - Netzwerk – Verdächtige Aktivität auf Netzwerkebene.
 - Reputation – Bekannte Quelle oder von der Organisation des Unternehmens signiert.
 - Einstellungen – Möglichkeit, kritische Systemeinstellungen dauerhaft zu ändern.
 - Signatur – Böswillige Identifizierung von Subjekten.
 - Diebstahl – Fähigkeit, auf sensible Informationen zuzugreifen und diese möglicherweise weiterzugeben.
 - Tarnung – Fähigkeit, von Benutzern unbemerkt zu bleiben.
 - Im Hintergrund – Erkennung eines ungefährlichen Subjekts.
- Beschreibung – Eine Beschreibung, die jedem Aktivitätstyp entspricht, der während der Analyse des Artefakts erkannt wurde.
- ATT&CK-Taktiken – Die MITRE ATT&CK-Phase oder -Phasen eines Angriffs. Mehrere Taktiken werden durch Kommas getrennt.
- ATT&CK-Techniken – Die beobachteten Aktionen oder Tools, die ein böswilliger Akteur verwenden kann. Mehrere Methoden werden durch Kommas getrennt.
- Links – Um nach anderen Instanzen dieser Aktivität zu suchen, klicken Sie auf das Suchsymbol.

Zusätzliche Artefakte

In diesem Abschnitt werden zusätzliche Artefakte (Dateien und URLs) aufgelistet, die während der Analyse des übermittelten Beispiels beobachtet und wiederum für eine eingehende Analyse übermittelt wurden. Dieser Abschnitt enthält die folgenden Eigenschaften:

- Beschreibung – Beschreibt das zusätzliche Artefakt.
- SHA1 – Der SHA1-Hash des zusätzlichen Artefakts.
- Inhaltstyp – Der MIME-Typ des zusätzlichen Artefakts.
- Punktzahl – Die Punktzahl für die Böswilligkeit des zusätzlichen Artefakts. Um den zugeordneten Analysebericht anzuzeigen, klicken Sie auf .

Entschlüsselte Befehlszeilenargumente

Wenn während der Analyse PowerShell-Skripts ausgeführt wurden, entschlüsselt das System diese Skripts, damit die Argumente in lesbare Form zur Verfügung stehen.

Drittanbiertools

Ein Link zu einem Bericht über das Artefakt im Portal „VirusTotal“.

Registerkarte „Alle“

Auf der Registerkarte **Alle** werden alle Instanzen von Dateidownloads angezeigt, die in Ihrem NSX-T Data Center-Netzwerk analysiert wurden.

Heruntergeladene Dateien im Zeitverlauf auf der Registerkarte „Alle“

Das Widget **Heruntergeladene Dateien** auf der Registerkarte **Alle** bietet einen Überblick über die Anzahl der Dateien, die in dem überwachten Netzwerk im angegebenen Zeitbereich heruntergeladen wurden. Das Diagramm ist ein tägliches Histogramm der heruntergeladenen Dateien, gruppiert nach dem übergeordneten Dateityp.

Das Widget zeigt alle analysierten Dateidownloads an.

Eine Liste der Dateitypen finden Sie unter [Heruntergeladene Dateien im zeitlichen Verlauf](#).

Verwenden von Filtern auf der Seite „Heruntergeladene Dateien“

NSX Network Detection and Response bietet einen Filtermechanismus, mit dem Sie sich auf bestimmte Informationen zu heruntergeladenen Dateien konzentrieren können, die für Sie von Interesse sind. Die Verwendung von Filtern ist optional.

Verfahren

- 1 Klicken Sie auf der Seite **Heruntergeladene Dateien** auf das , um das Widget **Filter** zu erweitern.
- 2 Klicken Sie auf eine beliebige Stelle im Textfeld **Filter auf** und wählen Sie ein Element im Dropdown-Menü aus.

Sie können aus den folgenden verfügbaren Filtern auswählen. Um den Fokus der angezeigten Informationen weiter einzuschränken, können Sie mehrere Filter kombinieren.

Filtername	Beschreibung
Analyse-Tags	Schränken Sie die angezeigten Dateien durch ihre Analyse-Tags ein. Hierbei handelt es sich um Bezeichnungen, die einer Datei oder URL von der Systemanalyse zugewiesen werden. Sie können eine Bedrohung oder eine Bedrohungsklasse identifizieren oder sich auf ein bestimmtes bösartiges Verhalten beziehen, das erkannt wurde.
Analyst-UUID	Schränken Sie die angezeigten Dateien auf die Systemanalyse-UUID für die heruntergeladene Datei ein. Dies ist ein interner eindeutiger Bezeichner für die Analyse einer Datei.
Anwendungsprotokoll	Beschränken Sie angezeigte Dateien, die über eines der angegebenen Protokolle übertragen werden. Unterstützte Werte sind HTTP/HTTPS, FTP und SMB.
Kontaktierte IP	Beschränken Sie die angezeigten Dateien auf die IP-Adresse, von der die Datei heruntergeladen wurde. Wie der Host-IP-Filter unterstützt auch dieser IP-Adressen, CIDR-Blöcke oder IP-Adressbereiche.
Dateitypfilter	Beschränken Sie die angezeigten Dateien auf einen oder mehrere Dateitypen auf hoher Ebene. Weitere Informationen finden Sie in der Liste der Dateitypen (oben).
Dateien	Wählen Sie Bösartig aus, um die angezeigten Dateien auf bösartige Dateien zu beschränken. Dies sind Dateien, die bei der Systemanalyse eine Punktzahl von 70 oder mehr (von 100) erhalten haben.
Host-IP	Beschränken Sie die angezeigten Dateien auf die IP-Adresse des Hosts im Netzwerk, von dem die Datei heruntergeladen wurde. Dieser Filter unterstützt die Auswahl einer oder mehrerer IP-Adressen, CIDR-Blöcke (z. B. 192.168.0.0/24) oder IP-Adressbereiche (z. B. 192.168.1.5-192.168.1.9).
HTTP-Host	Beschränken Sie die angezeigten Dateien auf den/die Hostname(n), von dem die Datei heruntergeladen wurde. Hinweis Dieser Wert wird aus dem HTTP-Host-Header in der HTTP-Anforderung extrahiert, mit der die Datei heruntergeladen wurde. Daher unterliegt er der Kontrolle des Clients und kann von einer bösartigen Software gefälscht werden, z. B. von einer Malware-Binärdatei, die bereits auf einem infizierten Host ausgeführt wird.
MD5	Beschränken Sie die angezeigten Dateien auf den MD5-Hash der heruntergeladenen Datei.
Mindestpunktzahl	Beschränken Sie die angezeigten Dateien auf diejenigen, denen die Systemanalyse eine höhere Punktzahl als den von Ihnen gewählten Wert (von 1-100) zugewiesen hat.

- 3 Um die ausgewählten Filter anzuwenden, klicken Sie auf **Anwenden**.
- 4 (Optional) Um einen einzelnen Filter zu löschen, klicken Sie neben dem Eintrag auf die Schaltfläche **ENTFERNEN**. Um alle ausgewählten Filter zu löschen, klicken Sie auf das Symbol **X** rechts neben dem Widget **Filter**.

Das Widget **Filter** wird ausgeblendet, wenn Sie alle ausgewählten Filter löschen.

Liste der heruntergeladenen Dateien auf der Registerkarte „Alle“

In der Liste **Heruntergeladene Dateien** werden alle Dateien angezeigt, die von Hosts im Netzwerk heruntergeladen und vom NSX Advanced Threat Prevention-Dienst verarbeitet wurden.

Das Textfeld für die **Schnellsuche** in der oberen linken Ecke der Liste bietet eine schnelle Suchfunktion, die direkt nach der Eingabe ausgeführt wird. Es filtert die Zeilen in der Liste und zeigt nur die Zeilen mit Text in einer Spalte an, die mit der Abfragezeichenfolge übereinstimmt, die Sie im Suchtextfeld eingegeben haben.

Um die in der Liste angezeigten Spalten anzupassen, klicken Sie auf das  in der oberen rechten Ecke der Liste.

Sie können die Anzahl der Zeilen, die angezeigt werden sollen, anpassen. Die Standardeinstellung ist 20 Einträge. Verwenden Sie das Symbol mit dem  und das Symbol mit dem , um durch mehrere Seiten zu navigieren.

Jede Zeile ist eine Zusammenfassung einer heruntergeladenen Datei. Klicken Sie auf das  oder an einer beliebigen Stelle in einer Eingabezeile, um auf eine detaillierte Ansicht der heruntergeladenen Datei zuzugreifen.

Weitere Informationen zur detaillierten Ansicht der heruntergeladenen Dateien finden Sie unter [Details zu heruntergeladenen Dateien](#).

Die Liste wird nach den Zeitstempelinformationen sortiert und enthält die folgenden Spalten.

Spaltenname	Beschreibung
Zeitstempel	Der Zeitstempel der Erkennung des Dateidownloads.
Host	Der Host, der die Datei heruntergeladen hat.
Kontaktierte IP	IP-Adresse des kontaktierten Hosts.
Speicherort	Für einen Download ist dies die URL der Datei im unterstützten Format. Beispielsweise <code>\127.0.0.2\samba_share\1128dedb.exe</code> für einen SMB-Download oder <code>http://www.example.com/download/example.zip</code> für einen HTTP-Download. Für einen Upload wird „Hochladen“ angezeigt.
MD5	Der MD5-Hash der heruntergeladenen Datei.
Typ	Der allgemeine Typ der heruntergeladenen Datei. Die Liste der Dateitypen finden Sie unter Heruntergeladene Dateien im zeitlichen Verlauf .
AV-Klasse	Eine Bezeichnung, die die Antivirenklasse der heruntergeladenen Datei definiert. Wenn die Bezeichnung über das  verfügt, können Sie darauf klicken, um eine Popup-Beschreibung zu erhalten.
Malware	Eine Bezeichnung, die den Malware-Typ der heruntergeladenen Datei definiert. Wenn die Bezeichnung über das  verfügt, können Sie darauf klicken, um eine Popup-Beschreibung zu erhalten.
Bewertung	Die Bewertung, die der heruntergeladenen Datei mittels NSX Intelligence-Analyse zugewiesen wurde. Klicken Sie auf  , um die Liste nach Bewertung zu sortieren. Wenn  angezeigt wird, weist dies darauf hin, dass das Artefakt blockiert wurde.

Verwenden der Seite „Warnungsmanagement“

Auf der Seite **Warnungsmanagement** werden die Regeln für die Verwaltung von Warnungen in NSX Network Detection and Response angezeigt.

NSX Network Detection and Response vergleicht die Ereignisse mit den benutzerdefinierten Filtern, die in diesen Regeln enthalten sind. Übereinstimmende Ereignisse werden in der NSX Network Detection and Response-Benutzeroberfläche in `INFO`-Ereignisse (Herabstufen) umgewandelt, gelöscht oder basierend auf der ausgewählten Aktion einem benutzerdefinierten Auswirkungswert zugewiesen.

In der Liste **Benutzerdefinierte Regeln** werden die Warnungsregeln definiert.

Das Textfeld für die Schnellsuche oberhalb der Liste bietet eine Suchfunktion, die direkt nach der Eingabe ausgeführt wird. Es filtert die Zeilen in der Liste und zeigt nur die Zeilen an, die in einer beliebigen Spalte Text enthalten, der mit der Suchanfrage übereinstimmt.

Klicken Sie auf das Symbol rechts auf der Seite, um eine neue Warnungsregel hinzuzufügen. Die Sidebar **Warnung verwalten** wird angezeigt. Einzelheiten dazu finden Sie unter [Arbeiten mit der Sidebar „Warnung verwalten“](#).

Sie können die Anzahl der Zeilen, die angezeigt werden sollen, anpassen. Die Standardeinstellung ist 25 Einträge. Um durch mehrere Seiten zu navigieren, verwenden Sie die Paginierungssymbole.

Die Liste ist nach der Spalte „Zuletzt geändert“ sortiert und enthält die folgenden Informationen.

Spaltenname	Beschreibung
Regelname	<p>Der Name der Warnungsregel.</p> <p>Um die Liste nach Regelnamen zu sortieren, klicken Sie auf das Symbol in der Kopfzeile der Liste.</p>
Ausdruck	<p>Der übereinstimmende Ausdruck der Regel ist eine Reihe von Filtern, die mit Ereignissen abgeglichen werden. Der Ausdruck kann abgeschnitten werden, wenn er zu lang ist. Erweitern Sie die Zeile, um den vollständigen Inhalt der Regel anzuzeigen, indem Sie auf das Symbol oder auf eine beliebige Stelle der Eingabezeile klicken.</p> <p>Um die Liste nach Ausdruck zu sortieren, klicken Sie auf das Symbol in der Kopfzeile der Liste.</p>
Regelaktion	<p>Die Regelaktion definiert, was mit einem Ereignis zu tun ist, das mit dem Ausdruck übereinstimmt: <code>demote</code> das Ereignis an <code>INFO</code>, <code>suppress</code> das Ereignis oder weisen Sie einen benutzerdefinierten <code>impact</code>-Wert von 1 bis 100 zu. Die Aktion wird möglicherweise abgeschnitten, wenn sie zu lang ist. Erweitern Sie die Zeile, um den vollständigen Inhalt der Regel anzuzeigen, indem Sie auf das Symbol (oder eine beliebige Stelle in der Eingabezeile) klicken.</p> <p>Der Regelname wird als benutzerdefiniertes Tag an die Aktion angehängt, z. B. <code>tag:network_event=rule_name</code>.</p> <p>Um die Liste nach Regelaktion zu sortieren, klicken Sie auf das Symbol in der Kopfzeile der Liste.</p>
Zuletzt geändert	Datum und Uhrzeit der letzten Änderung der Regel.
Aktionen	<p>Um die Regel anzuzeigen/zu bearbeiten, klicken Sie auf . Die Seitenleiste Warnung verwalten wird angezeigt, damit Sie die Regel anzeigen oder Änderungen daran vornehmen können.</p> <p>Um die Regel zu entfernen, klicken Sie auf .</p>

Arbeiten mit der Sidebar „Warnung verwalten“

Mit der Sidebar **Warnung verwalten** können Sie eine Regel erstellen, die mit allen nachfolgenden Ereignissen abgeglichen wird, die von NSX Network Detection and Response erkannt werden. Wenn ein Ereignis mit einer Regel übereinstimmt, wird die Regelaktion angewendet.

Zugriff auf die Sidebar

Sie können auf die Sidebar **Warnung verwalten** auf eine der folgenden Arten zugreifen.

- Klicken Sie auf einer beliebigen Registerkarte auf der Seite **Hostprofil** auf die Schaltfläche **Hostaktionen** und wählen Sie dann „Warnung verwalten“ aus dem Pulldown-Menü aus. Der Seitenleistenbereich wird dann mit den entsprechenden Filtern vorbelegt. Sie können diese Einträge bearbeiten.
- Klicken Sie auf der Seite **Hostprofil** auf die Registerkarte **Bedrohungen**. Klicken Sie auf einer Bedrohungskarte auf **Weitere Schritte** und wählen Sie im Pulldown-Menü **Warnung verwalten** aus.
- Wählen Sie in der Ansicht **Informationendetails** einen bestimmten Vorfall aus und klicken Sie auf **Warnung verwalten**.
- Klicken Sie auf der Seite **Warnungsmanagement** im Widget  auf das Symbol **Regel hinzufügen**,

Die Seite **Warnungen verwalten** besteht aus drei separaten Bereichen: FILTER, AKTIONEN und REGEL ÜBERPRÜFEN. Jeder Bereich wird angezeigt, je nachdem, in welchem Schritt des Vorgangs „Regel erstellen“ oder „Regel bearbeiten“ Sie sich gerade befinden.

Sie können die Sidebar **Warnung verwalten** schließen indem Sie in der oberen rechten Ecke auf **X** klicken. Wenn Sie Änderungen vorgenommen haben, müssen Sie das Schließen der Sidebar bestätigen.

Um eine Regel zu erstellen oder zu bearbeiten, müssen Sie drei Schritte in der Sidebar **Warnung verwalten** ausführen.

Schritt 1: Filter erstellen oder bearbeiten

Die Registerkarte **Filters** verfügt über zwei Bearbeitungsmodi, die Sie beim Arbeiten mit Filtern verwenden können: Standard und Erweitert. Sie können Filter in beiden Modi erstellen oder bearbeiten.

- Um den Modus Erstellen/Bearbeiten in den erweiterten Modus umzuschalten, klicken Sie oben in der Sidebar auf die Registerkarte **Erweitert**.
- Um wieder zum Standardmodus zu wechseln, klicken Sie auf die Registerkarte **Standard** (siehe jedoch den [wichtigen Hinweis](#)).

Um einen Filter im Standardmodus zu erstellen, führen Sie die folgenden Schritte aus.

- 1 Klicken Sie auf **Neuen Filter hinzufügen+**.
- 2 Wählen Sie im Dropdown-Menü Filtereinträge einen Filter aus.

Die Filter sind in vier Kategorien unterteilt: Quelle, URL, Erkennung und Datei. Weitere Informationen zu diesen Kategorien finden Sie im Abschnitt „Attributeinträge“ in [Syntax für Warnungsregeln](#).

- 3 Legen Sie je nach ausgewähltem Regeltyp dessen Wert fest. Dazu kann es erforderlich sein, auf einen Schalter zu klicken, einen Wert einzugeben, ein Element aus einem Pulldown-Menü auszuwählen oder ähnliches.

Scrollen Sie zum Bearbeiten der Filter durch die Liste, wählen Sie einen Filter aus und ändern Sie die entsprechenden Werte. Löschen Sie einen unerwünschten Filter, indem Sie ihn anklicken. Sie können auch weitere Filter auswählen.

Um Filter im erweiterten Modus zu erstellen, füllen Sie das Textfeld **Übereinstimmender Ausdruck** aus und fügen Sie einen Filter hinzu oder bearbeiten Sie ihn mit der Syntax für Warnregeln.

Beispiel:

```
(network_event.relevant_host_ip: 10.154.115.91 OR network_event.relevant_host_ip:  
10.1.1.1-10.255.255.255) AND NOT  
(network_event.server_port: 53 OR network_event.server_port: 65535) OR  
(network_event.other_host_hostname: block.lastline.com) AND  
(network_event.threat: Lastline blocking test)
```

Wichtig Normalerweise können Sie zwischen den beiden Bearbeitungsmodi der Sidebar hin- und herschalten. Wenn jedoch der von Ihnen erstellte oder bearbeitete Filter für den übereinstimmenden Ausdruck vom Standardmodus nicht unterstützt wird, ist der Link **Standard** deaktiviert, und auf der Registerkarte **FILTER** wird standardmäßig der erweiterte Editor angezeigt.

Schritt 2: Definieren der Aktion

Nachdem Sie einen Filter definiert oder bearbeitet haben, klicken Sie zum Definieren der Regelaktionen in der unteren rechten Ecke auf **Aktionen definieren**. Der Bereich **Aktionen** verfügt über zwei Bearbeitungsmodi: Grundlegende Aktionen (Standard) und Erweiterte Aktionen:

- Klicken Sie auf die Registerkarte **Erweiterte Aktionen** oben in der Sidebar, um den Erstellungs-/Bearbeitungsmodus in den erweiterten Modus zu versetzen.
- Klicken Sie auf den Link **Grundlegende Aktionen**, um wieder zum Standardmodus zu wechseln.

Im Bereich **Aktionen** im Modus „Grundlegende Aktionen“ gibt es zwei Schalter: **Warnung verwalten** und **Benutzerdefinierte Auswirkung (1-100)**.

Aktion unterdrücken

- 1 Klicken Sie auf den Schalter **Warnung verwalten**.
- 2 Wählen Sie aus dem Dropdown-Menü die Option **Zu INFO-Ereignis herabstufen** (Standard) oder **Löschen**.

Die Aktion „Herabstufen“ wandelt nachfolgende Netzwerkereignisse, die mit der Regel übereinstimmen, in **INFO**-Ereignisse um. Beachten Sie, dass Sie **INFO** mit dem Filter für das Ereignisergebnis auswählen müssen.

Die Aktion „Löschen“ löscht die übereinstimmenden Ereignisse aus dem Benutzerportal.

Warnung Auf alle gelöschten Ereignisse kann nicht mehr zugegriffen werden.

Benutzerdefinierte Auswirkung

- 1 Klicken Sie auf die Umschaltoption **Benutzerdefinierte Auswirkung (1-100)**.
- 2 Klicken Sie auf das Optionsfeld, um **Definierter Bereich** oder **Einzelwert** auszuwählen.
Wenn Sie **Definierter Bereich** ausgewählt haben, geben Sie mindest- und maximalwerte in die entsprechenden Textfelder ein. Wenn Sie **Einzelwert** ausgewählt haben geben Sie den Wert in das Textfeld ein.

Sie können die Aktionen auch im Bereich „Erweiterte Aktionen“ definieren.

- 1 Klicken Sie auf die Registerkarte **Erweiterte Aktionen**.
- 2 Fügen Sie im Textfeld eine Aktion mithilfe der Syntax der Warnungsregeln hinzu oder bearbeiten Sie sie.

Beispiel:

```
demote:outcome=TEST
```

oder

```
impact:min_impact=12,impact:max_impact=22
```

Nachdem Sie die Aktion ausgewählt haben, klicken Sie auf **Regel überprüfen** um mit dem nächsten Schritt fortzufahren.

Um die ausgewählten Filter zu korrigieren, klicken Sie auf **Filter** um zum vorherigen Fensterbereich **Filter** zurückzukehren.

Schritt 3: Regel überprüfen

Im Bereich „Regel überprüfen“ können Sie Ihre Warnungsregel überprüfen.

- 1 Geben Sie in das Textfeld Regelname einen Namen ein.
Wenn Sie eine vorhandene Regel bearbeiten, können Sie den Namen nicht ändern.
- 2 (Optional) Verwenden Sie das Dropdown-Menü, um eine Lizenz auszuwählen.
Dieses Dropdown-Menü ist deaktiviert, wenn Sie die Sidebar **Warnung verwalten** auf der Seite **Warnungsmanagement** gestartet haben oder wenn Sie eine vorhandene Regel bearbeiten.
- 3 Überprüfen Sie im Abschnitt **Regelübersicht** die ausgewählten Filter, die aufgelistet sind.

Wenn die Registerkarte **Filter** im Standardmodus belassen wurde, besteht die Übersicht aus einer Liste der ausgewählten Filter. Jeder Filter wird mit seinem Namen und seinen Werten angezeigt. Beispiel:

```
Rule summary
SERVER IP
12.6.6.6/32
RELEVANT HOST SILENCED
1
THREAT(S)
Torn rat
THREAT CLASS
Malicious file execution
```

Wenn die Registerkarte **Filter** im erweiterten Modus belassen wurde, wird in der Übersicht der übereinstimmende Ausdruck angezeigt. Beispiel:

```
Rule summary
(network_event.server_ip: 12.6.6.6/32) AND
(network_event.relevant_host_whitelisted: 1)
AND (network_event.threat: Torn RAT) AND
(network_event.threat_class: Malicious File
Execution)
```

Wenn die Registerkarte **Aktionen** im Modus „Grundlegende Aktionen“ belassen wurde, wird in der Übersicht die Aktion angezeigt. Beispiel:

```
SUPPRESSION ALERT
Demote to INFO event
```

Wenn sich die Registerkarte **Aktionen** im Modus „Erweiterte Aktionen“ belassen wurde, wird in der Übersicht die Aktion angezeigt. Beispiel:

```
ACTION
impact:min_impact=12,impact:max_impact=22
```

- 4 (Optional) Um die ausgewählten Regeltypen zu korrigieren, klicken Sie auf **Regel bearbeiten** um zur vorherigen Seite zurückzukehren.
- 5 Wenn Sie fertig sind, klicken Sie auf **Regel erstellen**, um die Regel abzuschließen, oder klicken Sie auf **Regel aktualisieren** wenn Sie eine vorhandene Regel bearbeiten.

Syntax für Warnungsregeln

Sie verwenden die Syntax für Warnungsregeln, um die Aktionen zu definieren, die NSX Network Detection and Response durchführen müssen, wenn Ereignisse einem Filter entsprechen.

Eine Warnungsregel besteht aus zwei Teilen: übereinstimmender Ausdruck und Aktionen.

Übereinstimmender Ausdruck

Eine Kombination aus Klauseln, die eine Bedingung für die Attribute eines Objekts ausdrücken.

Ein übereinstimmender Ausdruck hat das folgende Format: `object_type . attribute_type: [relation]value`

Der übereinstimmende Ausdruck besteht aus den folgenden vier Teilen.

Teilname	Beschreibung
object_type	<p>Der Objekttyp, der abgeglichen werden soll. Der folgende Datensatztyp wird unterstützt:</p> <ul style="list-style-type: none"> ■ <code>network_event</code> <p>Der Objekttyp und sein Attribut sind durch einen Punkt (.) getrennt.</p>
attribute_type	<p>Das Attribut, das abgeglichen werden soll (siehe Attributeinträge).</p> <p>Der <code>object_type.attribute_type</code> wird durch einen Doppelpunkt (:) von [relation] und value getrennt.</p>
[relation]	<p>Die Beziehung zwischen dem Objekt und seinem Attribut sowie der Wert, auf den abgeglichen werden soll. Wenn keine Beziehung angegeben ist, ist „Gleichheit“ die Standardeinstellung. Unterstützte Beziehungstypen sind folgende:</p> <ul style="list-style-type: none"> ■ Gleichheit (:) ■ Größer als oder gleich (>, >=) ■ Kleiner als oder gleich (<, <=)
Wert	Der Wert, der mit dem <code>object_type.attribute_type</code> der eingehenden Ereignisse abgeglichen werden soll.

Mehrere übereinstimmende Ausdrücke werden durch die logischen Operatoren `AND`, `OR` und `NOT` getrennt.

Aktionen

Eine oder mehrere Änderungen, die für das Objekt durchgeführt werden müssen.

Eine Aktion hat das folgende Format: `action : target = value`

Die Aktion besteht aus drei Teilen:

Teilname	Beschreibung
Aktion	Die auszuführende Aktion (siehe Unterstützte Aktionen). Die Aktion und ihr Ziel werden durch einen Doppelpunkt (:) getrennt.
Ziel	Das unterstützte Ziel.
Wert	Der optionale Wert, der auf das Ziel angewendet werden soll.

Mehrere Aktionen werden durch ein Komma (,) getrennt und in derselben Reihenfolge angewendet, in der sie definiert wurden.

Attributeinträge

In der folgenden Liste werden die verschiedenen Attributeinträge beschrieben, die Sie beim Erstellen oder Aktualisieren neuer Filter verwenden können. Die Attribute werden in die folgenden fünf Kategorien unterteilt.

QUELLE

Attribut „Quelle“	Beschreibung
client_ip	Entspricht einer IP-Adresse oder einem IP-Adressbereich. Der Adresswert muss exakt übereinstimmen. (network_event.client_ip: 142.42.1.6/24)
other_host_hostname	Entspricht dem Hostnamen des anderen Hosts, der dem Ereignis zugeordnet ist. Platzhaltervergleiche werden unterstützt: * für mehrere Zeichen, ? für einzelne Zeichen. Sie müssen die Platzhalterzeichen mit einem Escape-Zeichen (\) versehen, um mit einem literalen * oder ? übereinzustimmen. (network_event.other_host_hostname: host.example.com)
other_host_in_homenet	Bei „true“ wird eine Übereinstimmung erzielt, wenn sich die IP-Adresse des anderen mit dem Ereignis verbundenen Hosts im Home-Netzwerk befindet. Erwartet einen booleschen Wert. (network_event.other_host_in_homenet: false)
other_host_ip	Entspricht einer IP-Adresse oder einem IP-Adressbereich. Der Adresswert muss exakt übereinstimmen. (network_event.other_host_ip: 10.10.4.2)
other_host_tag	Entspricht einem Host-Tag. Wählen Sie ein vorhandenes Host-Tag aus. (network_event.other_host_tag: tag)
relevant_host_in_homenet	Bei „true“ wird eine Übereinstimmung erzielt, wenn sich die IP-Adresse des entsprechenden mit dem Ereignis verbundenen Hosts im Home-Netzwerk befindet. Erwartet einen booleschen Wert. (network_event.relevant_host_in_homenet: true)
relevant_host_ip	Entspricht einer IP-Adresse oder einem IP-Adressbereich. Der Adresswert muss exakt übereinstimmen. (network_event.relevant_host_ip: 42.6.7.0/16)
relevant_host_tag	Entspricht einem Host-Tag. Wählen Sie ein vorhandenes Host-Tag aus. (network_event.relevant_host_tag: tag)
relevant_host_whitelisted	Entspricht einer stillgelegten Quell-IP-Adresse. Erwartet einen booleschen Wert. (network_event.relevant_host_whitelisted: true)
server_ip	Entspricht einer IP-Adresse oder einem IP-Adressbereich. Der Adresswert muss exakt übereinstimmen. (network_event.server_ip: 12.6.6.6)
server_port	Entspricht einer Portnummer. Es werden ganzzahlige Vergleiche durchgeführt: Gleichheit, Ungleichheit, größer-als, kleiner-als, usw. (network_event.server_port: 7777)
transport_protocol	Entspricht entweder „TCP“ oder „UDP“. (network_event.transport_protocol: UDP)

URL

Attribut „URL“	Beschreibung
full_url	<p>Entspricht mindestens einer URL im Ereignis. Platzhaltervergleiche werden unterstützt: * für mehrere Zeichen, ? für einzelne Zeichen. Sie müssen die Platzhalterzeichen mit einem Escape-Zeichen (\) versehen, um mit einem literalen * oder ? übereinzustimmen.</p> <p>Beispiel: Das Zeichen für die Abfragezeichenfolge ? muss mit einem Escape-Zeichen (\?) versehen werden:</p> <pre>(network_event.full_url: https://www.example.com/resource/path\? r=start&v=cK5G8fPmWeA)</pre>
normalized_url	<p>Entspricht mindestens einer normalisierten URL (einer URL ohne Abfragezeichenfolge) im Ereignis. Platzhaltervergleiche werden unterstützt: * für mehrere Zeichen, ? für einzelne Zeichen. Sie müssen die Platzhalterzeichen mit einem Escape-Zeichen (\) versehen, um mit einem literalen * oder ? übereinzustimmen.</p> <pre>(network_event.normalized_url: https://www.example.com/resource/path/)</pre>
resource_path	<p>Entspricht mindestens einem URL-Ressourcenpfad im Ereignis. Platzhaltervergleiche werden unterstützt: * für mehrere Zeichen, ? für einzelne Zeichen. Sie müssen die Platzhalterzeichen mit einem Escape-Zeichen (\) versehen, um mit einem literalen * oder ? übereinzustimmen.</p>

ERKENNUNG

Attribut „Erkennung“	Beschreibung
custom_ids_rule_id	<p>Entspricht einer ID für eine IDS-Regel. Der numerische Wert muss exakt übereinstimmen.</p> <pre>(network_event.custom_ids_rule_id: 987654321)</pre>
detector	<p>Entspricht dem Namen/eindeutigen Bezeichner des Moduls, das das Ereignis erkannt hat. Der Zeichenfolgenwert muss exakt übereinstimmen.</p> <pre>(network_event.detector: llrules:1532130206460)</pre>
event_outcome	<p>Entspricht entweder „ERKENNUNG“ oder „INFO“.</p> <pre>(network_event.event_outcome: DETECTION)</pre>
event_type	<p>Entspricht einem der Folgenden: „BINARYDOWNLOAD“, „DNS“, „DNSANOMALY“, „DYNAMICIP“, „HTTPANOMALY“, „IDS“, „IP“, „LLANTARULE“, „NETFLOW“, „NETFLOWANOMALY“, „NETWORK“, „TLSANOMALY“ oder „URL“.</p> <pre>(network_event.event_type: IDS)</pre>
llanta_rule_uuid	<p>Entspricht der UUID einer Systemregel. Der numerische Wert muss exakt übereinstimmen.</p> <pre>(network_event.llanta_rule_uuid: b579caaec719415cb04f925f8f187cb0)</pre>
operation	<p>Entspricht einem der Folgenden: „BLOCK“, „INFO“, „LOG“ oder „TEST“.</p> <pre>(network_event.operation: BLOCK)</pre>

Attribut „Erkennung“	Beschreibung
threat	Entspricht einer gültigen Zeichenfolge, die eine Bedrohung definiert. Platzhaltervergleiche werden unterstützt: * für mehrere Zeichen, ? für einzelne Zeichen. Sie müssen die Platzhalterzeichen mit einem Escape-Zeichen (\) versehen, um mit einem literalen * oder ? übereinzustimmen. (network_event.threat: Torn RAT)
threat_class	Entspricht einer Bedrohungsklasse. Der Zeichenfolgenwert muss exakt übereinstimmen. (network_event.threat_class: Malicious File Execution)

DATEI

Dateiattribut	Beschreibung
av_class	Entspricht mindestens einem av_class-Analyse-Tag. Der Zeichenfolgenwert muss exakt übereinstimmen. (network_event.av_class: exploit)
file_category	Entspricht einer der unterstützten Dateikategorien. Der Zeichenfolgenwert muss exakt übereinstimmen. (network_event.file_category: Java)
file_md5	Entspricht einer gültigen MD5-Summe. (network_event.file_md5: bb4f64ddfb8704d2bf69b0216be7f837)
file_sha1	Entspricht einer gültigen SHA 1-Summe. (network_event.file_sha1: c3e266ede7f6fec7a021a4ae0edf248848d5ae06)
file_size	Entspricht einer Dateigröße in Byte. Es muss eine gültige Ganzzahl sein. Es werden ganzzahlige Vergleiche durchgeführt: Gleichheit, Ungleichheit, größer-als, kleiner-als, usw. (network_event.file_size: > 1042249837)
file_type	Entspricht einer gültigen Zeichenfolge, die einen Dateityp definiert. Platzhaltervergleiche werden unterstützt: * für mehrere Zeichen, ? für einzelne Zeichen. Sie müssen die Platzhalterzeichen mit einem Escape-Zeichen (\) versehen, um mit einem literalen * oder ? übereinzustimmen. (network_event.file_type: ?xecutable)
malware	Entspricht mindestens einem av_family- oder lastline_malware-Analyse-Tag. Der Zeichenfolgenwert muss exakt übereinstimmen. (network_event.malware: emotet)
malware_activity	Entspricht mindestens einem Aktivitätsanalyse-Tag. Der Zeichenfolgenwert muss exakt übereinstimmen. (network_event.malware_activity: Execution: Spawning Powershell with too many parameters)

SONSTIGE

Name eines sonstigen Attributs	Beschreibung
custom_tag	Entspricht einem benutzerdefinierten Tag, das Ereignissen zugewiesen ist. Der Zeichenfolgenwert muss exakt übereinstimmen. (network_event.custom_tag: tagged_event)

Unterstützte Aktionen

Im Folgenden finden Sie die Aktionen, die Sie beim Definieren von Regeln verwenden können.

Aktionsname	Beschreibung
demote	Stuft das Ergebnis des übereinstimmenden Ereignisses in einen anderen Modus herab. Unterstützte Ziele: <code>outcome</code> . Zulässige Werte: „INFO“ oder „TEST“.
impact	Legen Sie eine Unter- oder Obergrenze für die Auswirkungen eines Ereignisses fest. Unterstützte Ziele: <ul style="list-style-type: none">■ <code>impact</code>: Legt den unteren und den oberen Grenzwert auf denselben Wert fest.■ <code>max_impact</code>: Legt die Obergrenze für <code>impact</code> fest. Kleiner oder gleich Wert.■ <code>min_impact</code>: Legt die untere Grenze für <code>impact</code> fest. Größer oder gleich dem Wert. Zulässige Werte: eine Ganzzahl zwischen 1 und 100.
suppress	Unterdrückt alle Bedrohungen für das übereinstimmende Ereignis. Dies führt dazu, dass es als falsch positiv mit einer Auswirkung von null (0) bewertet wird, wodurch das Ereignis effektiv gelöscht wird. Unterstützte Ziele: <code>network_event</code> . Zulässige Werte: keine.
tag	Weisen Sie dem übereinstimmenden Ereignis ein benutzerdefiniertes Tag zu. Unterstützte Ziele: <code>network_event</code> . Zulässige Werte: eine gültige Zeichenfolge.

Verwenden des Analyseberichts

Der von NSX Network Detection and Response erstellte Analysebericht enthält detaillierte Ergebnisse einer Analyse, die vom NSX Advanced Threat Prevention-Dienst in einer übermittelten Datei durchgeführt wurde.

Neben der Böswilligkeitsbewertung enthält der Bericht auch wichtige Informationen über die Aktivität des Analysesubjekts. Die beschriebene Aktivität stellt die Grundlage der NSX Network Detection and Response-Bedrohungsbeurteilung und -bewertung.

Der Analysebericht wird auf der Registerkarte **Übersicht** gestartet.

Analysebericht: Registerkarte „Übersicht“

Die Registerkarte **Übersicht** auf der Seite **Analysebericht** der NSX Network Detection and Response-Benutzeroberfläche bietet eine Zusammenfassung der Analyseergebnisse für die vom NSX Advanced Threat Prevention-Dienst analysierte Datei.

Um die erkannte Datei auf Ihren lokalen Computer herunterzuladen, klicken Sie auf der rechten Seite des Bildschirms auf das . Wählen Sie im Dropdown-Menü **Datei herunterladen** oder **Als ZIP herunterladen** aus.

Wenn Sie **Als ZIP herunterladen** auswählen, wird das Popup-Fenster **Datei als ZIP herunterladen** angezeigt, in dem Sie aufgefordert werden, ein optionales Kennwort für das Archiv anzugeben. Klicken Sie auf **Download**, um das Herunterladen der .ZIP-Datei abzuschließen.

Wichtig Mit der NSX Network Detection and Response-Anwendung können Sie erkannte Dateien nur unter bestimmten Bedingungen herunterladen.

Wenn das Artefakt als geringes Risiko betrachtet wird, wird das  und Sie können es auf Ihren lokalen Computer herunterladen.

Wenn das Artefakt als riskant betrachtet wird, wird das  nur angezeigt, wenn Ihre Lizenz über die `ALLOW_RISKY_ARTIFACT_DOWNLOADS`-Funktion verfügt.

Sie müssen sich bewusst sein, dass das Artefakt beim Öffnen möglicherweise Schaden anrichten kann.

Die NSX Network Detection and Response-Benutzeroberfläche zeigt möglicherweise das Popup-Fenster **Warnung: Bösartige Datei wird heruntergeladen** an. Klicken Sie auf die Schaltfläche **Ich stimme zu**, um die Bedingungen zu akzeptieren und die Datei herunterzuladen.

Bei bösartigen Artefakten empfiehlt es sich, die Datei in ein ZIP-Archiv einzuschließen, um zu verhindern, dass andere Lösungen, die Ihren Datenverkehr überwachen, die Bedrohung automatisch inspizieren.

Wenn Sie nicht über die `ALLOW_RISKY_ARTIFACT_DOWNLOADS`-Funktion verfügen und die Möglichkeit benötigen, bösartige Artefakte herunterzuladen, wenden Sie sich an den [VMware Support](#).

Abschnitt „Analyseübersicht“

Hinweis Wenn beim NSX Advanced Threat Prevention-Dienst während der Dateianalyse Fehler aufgetreten sind, wird ein hervorgehobener Block angezeigt. Er enthält eine Liste der aufgetretenen Fehler.

Der Abschnitt „Analyseübersicht“ enthält eine Zusammenfassung der Analyseergebnisse einer Datei oder URL, die vom NSX Advanced Threat Prevention-Dienst analysiert wird. Im Abschnitt werden die folgenden Daten angezeigt.

- MD5 – Der MD5-Hash der Datei. Um nach anderen Instanzen dieses Artefakts in Ihrem Netzwerk zu suchen, klicken Sie auf <Suchsymbol>.
- SHA 1 – Der SHA 1-Hash der Datei.
- SHA 256 – Der SHA 256-Hash der Datei.
- MIME-Typ – Die Bezeichnung, die zur Identifizierung des Datentyps in der Datei verwendet wird.
- Übermittlung – Der Zeitstempel für die Übermittlung

Abschnitt „Bedrohungsstufe“

Der Abschnitt „Bedrohungsstufe“ beginnt mit einer Zusammenfassung der Analyseergebnisse:
Der md5-Hash der Datei wurde als bösartig/gutartig eingestuft.

Anschließend werden die folgenden Daten angezeigt:

Risikobewertung

In diesem Abschnitt werden die Ergebnisse der Risikobewertung angezeigt.

- Punktzahl für die Böswilligkeit – Legt einen Wert von 100 fest.
- Risikoschätzung – Eine Schätzung der Risiken, die durch dieses Artefakt verursacht werden:
 - Hoch – Dieses Artefakt stellt ein kritisches Risiko dar, das Sie mit Priorität beheben müssen. Bei diesen Subjekten handelt es sich in der Regel um Trojanerdateien oder Dokumente, die Exploits enthalten, was zu größeren Kompromittierungen des infizierten Systems führt. Die Risiken sind vielfältig: von Informationsverlusten bis hin zu Systemstörungen. Diese Risiken werden teilweise aus dem erkannten Aktivitätstyp abgeleitet. Der Schwellenwert für die Punktzahl für diese Kategorie ist in der Regel größer als 70.
 - Mittel – Dieses Artefakt stellt ein langfristiges Risiko dar, das Sie genau überwachen müssen. Es kann sich um eine Webseite mit verdächtigen Inhalten handeln, die potenziell zu Drive-by-Angriffen führt. Es kann sich auch um eine Adware oder ein gefälschtes Antivirenprodukt handeln, das keine unmittelbare ernsthafte Bedrohung darstellt, aber Probleme mit der Funktion des Systems verursachen kann. Der Schwellenwert für die Punktzahl für diese Kategorie liegt in der Regel zwischen 30 und 70.
 - Niedrig – Dieses Artefakt wird als gutartiges Artefakt betrachtet, und Sie können es ignorieren. Der Schwellenwert für die Punktzahl für diese Kategorie liegt in der Regel unter 30.
- Antivirenklasse – Die Antiviren- oder Malware-Klasse, zu der das Artefakt gehört. Zum Beispiel ein Trojanisches Pferd, ein Wurm, Adware, Ransomware, Spyware und so weiter.
- Antivirus-Familie – Die Antivirus- oder Malware-Familie, zu der das Artefakt gehört. Beispiel: Valyria, Darkside usw. Um nach anderen Instanzen dieser Familie zu suchen, klicken Sie auf das Suchsymbol.

Analyseübersicht

Die angezeigten Informationen sind nach Schweregrad sortiert und enthalten die folgenden Eigenschaften:

- Schweregrad – Eine Punktzahl zwischen 0 und 100 der Böswilligkeit der Aktivitäten, die während der Analyse des Artefakts erkannt wurden. Die zusätzlichen Symbole geben die Betriebssysteme an, auf denen das Artefakt ausgeführt werden kann.

- Typ – Die Typen von Aktivitäten, die während der Analyse des Artefakts erkannt wurden. Diese Typen beinhalten:
 - Autostart – Möglichkeit zum Neustarten nach dem Herunterfahren einer Maschine.
 - Deaktivieren – Möglichkeit, kritische Komponenten des Systems zu deaktivieren.
 - Evasion – Möglichkeit, die Analyseumgebung zu umgehen.
 - Datei – Verdächtige Aktivität über das Dateisystem.
 - Arbeitsspeicher – Verdächtige Aktivität innerhalb des Systemarbeitsspeichers.
 - Netzwerk – Verdächtige Aktivität auf Netzwerkebene.
 - Reputation – Bekannte Quelle oder von der Organisation des Unternehmens signiert.
 - Einstellungen – Möglichkeit, kritische Systemeinstellungen dauerhaft zu ändern.
 - Signatur – Böswillige Identifizierung von Subjekten.
 - Diebstahl – Fähigkeit, auf sensible Informationen zuzugreifen und diese möglicherweise weiterzugeben.
 - Tarnung – Fähigkeit, von Benutzern unbemerkt zu bleiben.
 - Im Hintergrund – Erkennung eines ungefährlichen Subjekts.
- Beschreibung – Eine Beschreibung, die jedem Aktivitätstyp entspricht, der während der Analyse des Artefakts erkannt wurde.
- ATT&CK-Taktiken – Die MITRE ATT&CK-Phase oder -Phasen eines Angriffs. Mehrere Taktiken werden durch Kommas getrennt.
- ATT&CK-Techniken – Die beobachteten Aktionen oder Tools, die ein böswilliger Akteur verwenden kann. Mehrere Methoden werden durch Kommas getrennt.
- Links – Um nach anderen Instanzen dieser Aktivität zu suchen, klicken Sie auf das Suchsymbol.

Zusätzliche Artefakte

In diesem Abschnitt werden zusätzliche Artefakte (Dateien und URLs) aufgelistet, die während der Analyse des übermittelten Beispiels beobachtet und wiederum für eine eingehende Analyse übermittelt wurden. Dieser Abschnitt enthält die folgenden Eigenschaften:

- Beschreibung – Beschreibt das zusätzliche Artefakt.
- SHA1 – Der SHA1-Hash des zusätzlichen Artefakts.
- Inhaltstyp – Der MIME-Typ des zusätzlichen Artefakts.
- Punktzahl – Die Punktzahl für die Böswilligkeit des zusätzlichen Artefakts. Um den zugeordneten Analysebericht anzuzeigen, klicken Sie auf .

Entschlüsselte Befehlszeilenargumente

Wenn während der Analyse PowerShell-Skripts ausgeführt wurden, entschlüsselt das System diese Skripts, damit die Argumente in lesbärerer Form zur Verfügung stehen.

Drittanbiertools

Ein Link zu einem Bericht über das Artefakt im Portal „VirusTotal“.

Analysebericht: Registerkarte „Bericht“

Die auf der Registerkarte **Bericht** angezeigten Informationen ändern sich je nach Art der von NSX Network Detection and Response analysierten Datei.

Um einen Bericht anzuzeigen, klicken Sie auf den Pfeil nach unten auf der Registerkarte **Bericht** und wählen Sie einen der verfügbaren Berichte aus.

Klicken Sie auf das und , um die Abschnitte auf der Registerkarte zu erweitern und zu reduzieren.

Abschnitt „Analyseinformationen“

Der Abschnitt **Analyseinformationen** enthält wichtige Informationen zu der Analyse, auf die sich der aktuelle Bericht bezieht:

- Analysegegenstand: Der MD5-Hash der Datei.
- Analysetyp: Der Typ der durchgeföhrten Analyse:
 - Dynamische Analyse unter Microsoft Windows 10: Der NSX Advanced Threat Prevention-Dienst hat das Analysesubjekt in einer simulierten Windows 10-Umgebung unter Verwendung der NSX Network Detection and Response-Sandbox ausgeführt. Das System überwacht das Verhalten der Datei und ihre Interaktionen mit dem Betriebssystem auf Anzeichen für verdächtiges oder bösartiges Verhalten.
 - Dynamische Analyse unter Microsoft Windows 7: Der NSX Advanced Threat Prevention-Dienst hat das Analysesubjekt in einer simulierten Windows 7-Umgebung unter Verwendung der NSX Network Detection and Response-Sandbox ausgeführt. Das System überwacht das Dateiverhalten und dessen Interaktionen mit dem Betriebssystem und sucht nach verdächtigen oder böswilligen Indikatoren.
 - Dynamische Analyse im instrumentierten Chrome-Browser: Der NSX Advanced Threat Prevention-Dienst untersuchte das Analysesubjekt (z. B. eine HTML-Datei oder eine URL) mithilfe des instrumentierten Browsers, der auf Google Chrome basiert. Der instrumentierte Browser gibt das Verhalten des realen Browsers originalgetreu wieder und lässt sich daher nicht leicht durch einen Fingerabdruck von bösartigem Content infizieren.
 - Dynamische Analyse im emulierten Browser: Der NSX Advanced Threat Prevention-Dienst prüft das Analysesubjekt (z. B. eine HTML-Datei oder eine URL) mithilfe des emulierten Browsers. Der emulierte Browser kann dynamisch verschiedene Browser-„Persönlichkeiten“ emulieren (z. B. durch Ändern seiner user-agent oder durch Variieren

der APIs, die er bereitstellt). Diese Funktion ist nützlich bei der Analyse von bösartigem Content, der auf bestimmte Browsertypen oder Versionen abzielt. Der Nachteil dieser Art von Analyse ist, dass dieser Browser weniger realistisch ist und möglicherweise durch bösartige Inhalte erkannt werden kann.

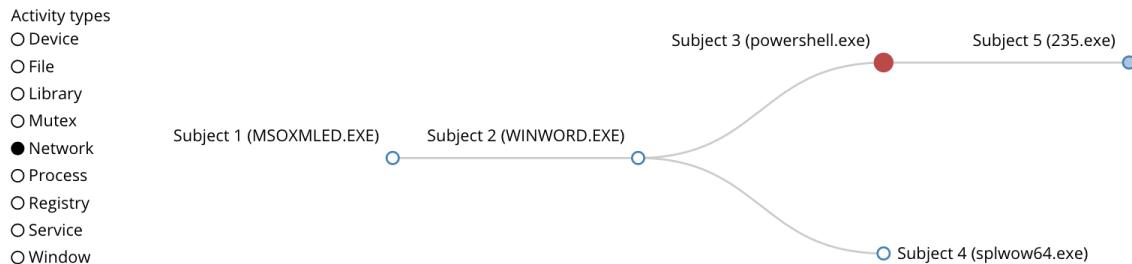
- Dynamische Analyse in einem simulierten Datei-Viewer: Der NSX Advanced Threat Prevention-Dienst inspiziert das Analysesubjekt (z. B. eine PDF-Datei) mithilfe des simulierten Datei-Viewers. Der Viewer kann eingebettete Inhalte und Links erkennen.
- Aufblasen des Archivs: Der NSX Advanced Threat Prevention-Dienst hat das Analysesubjekt (ein Archiv) aufgeblasen, seinen Inhalt extrahiert und den Inhalt, sofern er von einem geeigneten Typ ist, zur Analyse übermittelt.
- Verwendetes Kennwort: Sofern verfügbar, wird das Kennwort angegeben, das der NSX Advanced Threat Prevention-Dienst zur erfolgreichen Entschlüsselung der Probe verwendet hat.

Widget „Analysebeziehungen“

Für eine einzige Analyse muss der NSX Advanced Threat Prevention-Dienst möglicherweise mehrere Subjekte überwachen.

Beispielsweise kann die ursprüngliche Anwendung während einer Dateianalyse mehrere Prozesse starten. Ebenso werden während einer URL-Analyse möglicherweise mehr URLs referenziert und abgerufen.

In diesem Fall generiert NSX Network Detection and Response das Widget **Übersicht der Analysesubjekte**, das eine grafische Darstellung der Beziehung zwischen den einzelnen Analysesubjekten bietet, die der NSX Advanced Threat Prevention-Dienst während der Analyse überwacht hat.



Das Widget zeigt einen Knoten für jedes Analysesubjekt an. Zwei Knoten sind durch eine Kante verbunden, wenn während der Analyse eine Interaktion zwischen den entsprechenden Analysesubjekten festgestellt wurde (z. B. wenn ein Prozess einen anderen Prozess gestartet hat).

Auf der linken Seite des Widgets befindet sich eine Legende der Aktivitäten, die während der Analyse beobachtet wurden. Klicken Sie auf das Optionsfeld neben einem Aktivitätsnamen, um die Analysesubjekte hervorzuheben, die diese bestimmte Aktivität angezeigt haben. Sie können auch einen Satz von Aktivitäten auswählen.

Klicken Sie auf einen Knoten, um die nachfolgenden zugehörigen Knoten auszublenden.

Durch Doppelklicken auf einen Knoten gelangen Sie zu dem Abschnitt des Berichts mit detaillierten Informationen zum entsprechenden Analysesubjekt.

Analysedateibericht

In den **Analysesubjekt**-Abschnitten werden detaillierte Informationen über die Datei(en) angezeigt, die in der Probe enthalten sind oder auf die bei der Verarbeitung durch den NSX Advanced Threat Prevention-Dienst zugegriffen wurde.

Um den Abschnitt zu erweitern, klicken Sie auf das .

Für eine ausführbare Datei werden die folgenden Daten angezeigt:

- Name: Der Name der ausführbaren Datei, falls verfügbar.
- MD5: Der MD5-Hash der Datei.
- SHA1: Der SHA 1-Hash der Datei.
- Dateityp: Der Typ der ausführbaren Datei, z. B. PE executable, application, 32-bit, Intel i386.
- Dateigröße: Die Dateigröße.
- Befehlszeile: Die vollständige Befehlszeile, einschließlich aller Argumente oder Optionen.
Beispiel: C:\Users\ExampleUser\AppData\Local\Temp\exe_malware.exe.
- Ausführungskontext: Die von der ausführbaren Datei aufgerufene Berechtigungsebene.
- Architektur: Die Architektur der ausführbaren Datei.
- Analysegrund: Der Grund für den Beginn der Verarbeitung der Datei.

Analysedateiaktivitäten

Die **Analysesubjekt**-Abschnitte zeigen die tatsächliche Aktivität der Probe an, wie sie vom NSX Advanced Threat Prevention-Dienst erfasst wurde.

Diese Abschnitte enthalten das ursprünglich analysierte Subjekt und die von der Analyseumgebung verfolgten zusätzlichen Subjekten, die entweder vom ursprünglichen Subjekt erzeugt wurden oder weil das ursprüngliche Subjekt seinen Speicher manipuliert hat.

Hinweis Nicht alle diese Aktivitäten sind für eine bestimmte Probe vorhanden.

Klicken Sie auf das Symbol , um jeden der folgenden Abschnitte zu erweitern.

Abschnittsname	Beschreibung
Konsole-E/A	Daten, die in Konsolen-Handles geschrieben werden (Dateideskriptoren für Standardeingabe und Standardausgabe).
Entschlüsselte Befehlszeilenargumente	Die Argumente bösartiger PowerShell-Skripts sind häufig verschlüsselt oder verschleiert. Wenn ein Skript während der Analyse ausgeführt wurde, entschlüsselt das VMware-Backend das Skript und stellt die Argumente in einer besser lesbaren Form zur Verfügung.

Abschnittsname	Beschreibung
Geräte-E/A	Geräte-E/A Liste der E/A-Vorgänge, die vom Subjekt während der Laufzeit versucht wurden. Für jeden Vorgang werden das Zielgerät und der Steuerungscode aufgezeichnet.
Treiberaktivität	Liste der Treiber, auf die das Subjekt während der Laufzeit zugreift. Die folgenden Vorgänge werden aufgezeichnet: Laden und Entladen.
Ausnahmen	Liste der vom Subjekt während der Laufzeit ausgeführten Skripts. Für jede Zeile gibt es einen Eintrag für den Namen, den TYP und den INTERPRETER. Sie können die Liste nach einer beliebigen Spalte sortieren.
Ausgeführte Skripts	Liste der vom Subjekt während der Laufzeit ausgeführten Skripts. Für jede Zeile gibt es einen Eintrag für den Namen, den TYP und den INTERPRETER. Sie können die Liste nach einer beliebigen Spalte sortieren.
Dateisystemaktivität	Liste der Dateien, auf die das Subjekt während der Laufzeit zugreift. Die folgenden Vorgänge werden aufgezeichnet: Lesen, Schreiben, Umbenennen, Löschen. Für geschriebene Dateien werden die neue Größe und der MD5-Hash der Datei aufgezeichnet.
Bibliotheken	Liste der Bibliotheksdateien, die vom Subjekt während der Laufzeit geladen wurden.
Arbeitsspeicherinhalte	Beachtenswerte Daten im Programmarbeitsspeicher. Das System extrahiert z. B. IPs, Domänen und URLs während der Analyse.
Mutex-Aktivität	Liste der Mutex-Sperren, auf die das Subjekt während der Laufzeit zugegriffen hat. Die folgenden Vorgänge werden aufgezeichnet: Erstellen und Öffnen.
Netzwerkaktivität	Liste der Netzwerkkonversationen, an denen das Subjekt während der Laufzeit beteiligt war. Die folgenden Konversationstypen werden aufgezeichnet: Kommunikation über FTP, HTTP, IRC, SMTP und andere Arten von UDP/TCP-Protokollen. DNS-Anforderungen und Remotedatei-Downloads werden ebenfalls aufgezeichnet.
Prozessinteraktionen	Liste der Prozessinteraktionen, die das Subjekt während der Laufzeit versucht hat. Die folgenden Vorgänge werden aufgezeichnet: Prozesserstellung, Thread-Erstellung, Lesen und Schreiben von Arbeitsspeicher.
Registrierungsaktivität	Liste der Registrierungsschlüssel und -werte, auf die das Subjekt während der Laufzeit zugreift. Die folgenden Vorgänge werden aufgezeichnet: Lesen, Schreiben, Löschen und Überwachen.
Dienstaktivität	Liste der Dienste, auf die das Subjekt während der Laufzeit zugreift. Die folgenden Vorgänge werden aufgezeichnet: Starten, Beenden, Ändern von Parametern.
Fensteraktivität	Liste der vom Subjekt während der Laufzeit geöffneten Fenster.

Analysedateiartefakte

Im Abschnitt **Ereignisbericht** werden zusätzliche Artefakte angezeigt, die der NSX Advanced Threat Prevention-Dienst während der Probenverarbeitung erfasst.

Diese Artefakte sind im Bericht enthalten, damit Sie sie anzeigen können.

Paketerfassung

Wenn das Subjekt Netzwerddatenverkehr generiert hat, wird dieser Datenverkehr erfasst und im Widget „Erfasster Datenverkehr“ angezeigt.

Extrahierte Dateien

Für ein vergrößerndes Archiv wird eine Liste der Inhalte angezeigt. Jede Zeile zeigt den Mime-Typ, das Tag (gibt die Art der Analyse an), die Beschreibung, den Dateinamen (falls im Archiv verfügbar) und die Bewertung des Artefakts. Eine Bewertung wird nur angezeigt, wenn das Artefakt analysiert wurde. In diesem Fall wird auch ein Link zu seinem Bericht bereitgestellt.

Wenn beim NSX Advanced Threat Prevention-Dienst beim Entpacken eines Archivs ein Fehler aufgetreten ist, wird eine Warnung angezeigt, die auf die Fehlerbedingung hinweist. Zu den Fehlern gehören Überschreitung der maximalen Dateigröße, Überschreitung der maximalen Tiefe und Überschreitung der maximalen Anzahl an untergeordneten Aufgaben.

Generierte Dateien

Während der Analyse kann die Probe verschiedene Dateien generieren. Diese Dateien werden in einer nach PATH sortierten Liste angezeigt.

- PATH: Der Pfad des Artefakts im Dateisystem.
- TYPE: Der ermittelte Dateityp. Um die Liste nach Dateityp zu sortieren, klicken Sie auf **TYPE**.

Klicken Sie auf das Symbol , um eine Zeile zu erweitern. Es werden Daten für MD5, SHA 1, Größe (Bytes), Packer und Signaturen angezeigt. Möglicherweise sind nicht für alle Felder Daten verfügbar.

Entschlüsselte Befehlszeilenargumente

Die Argumente bösartiger PowerShell-Skripts sind häufig verschlüsselt oder verschleiert. Wenn während der Analyse ein Skript ausgeführt wurde, entschlüsselt der NSX Advanced Threat Prevention-Dienst es und stellt seine Argumente in einer für den Menschen besser lesbaren Form zur Verfügung. Diese Argumente werden in einer Liste mit dem Analysesubjekt und dem entschlüsselten Skript angezeigt.

Analyse-URL-Bericht

Im Abschnitt **Analysedetails** werden die tatsächlichen Aktivitäten des Analysesubjekts angezeigt, wie sie vom NSX Advanced Threat Prevention-Dienst erfasst wurden. Eine Aktivität wird verwendet, um eine Bewertung ihres Typs zu ermitteln.

Die folgenden Aktivitäten werden in diesem Abschnitt **Analysedetails** angezeigt.

Aktivitätstyp	Beschreibung
Netzwerkaktivität	Hier werden alle URLs aufgelistet, die während der Analyse besucht wurden, sowie zusätzliche Webinhalte, die vom Subjekt angefordert wurden oder darin enthalten sind. Jede zusätzliche URL wird zusammen mit ihrem Inhaltstyp, dem Server-Statuscode, der Server-IP-Adresse, den Hashes der Antwortinhalte (MD5 und SHA1), der Länge der Antwortinhalte und dem Zeitpunkt der Anforderung (Startzeit, Endzeit und Dauer in Millisekunden) aufgezeichnet.
Ressourcen	Listet lokale Ressourcen auf, auf die während der URL-Analyse über das <code>res protocol</code> zugegriffen wurde. Böswillige Webseiten greifen manchmal auf lokale Ressourcen zu, um die Ausführungsumgebung zu untersuchen. Beispielsweise, um festzustellen, ob bestimmte Programme installiert sind. Dieser Abschnitt wird nur angezeigt, wenn während der Analyse Ressourcenereignisse aufgetreten sind.
Codeausführungsaktivität	Listet den Code auf, der während der Analyse ausgeführt wurde. Insbesondere wird interessanter Code angezeigt, der statisch in einer Ressource enthalten war (mit Hilfe eines <code><script></code> -Tags), sowie der gesamte Code, der während der URL-Analyse dynamisch generiert und ausgeführt wurde. Bösartiger Code wird oft zur Laufzeit generiert, um statische Signaturen zu umgehen und seine Analyse komplizierter zu machen. <ul style="list-style-type: none"> ■ Statischer JavaScript-Code: Wird nur angezeigt, wenn während der Analyse relevante Ereignisse aufgetreten sind. ■ Dynamischer JavaScript-Code: Der Bericht gibt an, ob während der Analyse keine Ereignisse aufgetreten sind. ■ HTML-Code: Code, der dem Dokument dynamisch über Funktionen wie <code>document.write()</code> hinzugefügt wurde. Ansonsten zeigt der Bericht an, dass bei der Analyse keine Ereignisse aufgetreten sind.
Ausgeblendete iFrames	Listet ausgeblendete HTML-Tags auf, wie z. B. <code>iframe</code> , die während der Navigation erkannt wurden. Ausgeblendete Elemente werden manchmal auf kompromittierten Seiten verwendet, um bösartigen Code von Websites von Drittanbietern einzuschleusen. Dieser Abschnitt wird nur angezeigt, wenn während der Analyse ausgeblendete Tags erkannt wurden.
Arbeitsspeicherinhalte	Listet die Zeichenfolgen auf, die während der Analyse gefunden wurden. Dieser Abschnitt wird nur angezeigt, wenn bei der Analyse Zeichenfolgen gefunden wurden.
Textinhalt	Zeigt den textuellen Inhalt an, der aus einem Dokument extrahiert wurde. Dieser Abschnitt wird nur angezeigt, wenn bei der Analyse Text gefunden wurde, nur PDF-Analyse.
Links in Dokumenten	Zeigt die Links an, die in analysierten Dokumenten gefunden wurden. Dieser Abschnitt wird nur angezeigt, wenn während der Analyse Links gefunden wurden.
Plug-Ins	Listet jede Verwendung von gängigen Browser-Plug-Ins auf. Aufrufe dieser Plug-Ins werden aufgezeichnet, und der Bericht enthält die Details zu den aufgerufenen Methoden und den übergebenen Argumenten.
Applets	Zeigt die Java-Applets an, die während der URL-Analyse heruntergeladen wurden. Dieser Abschnitt wird nur angezeigt, wenn während der Analyse Applets gefunden wurden.
Exploits	Die Analyseumgebung ist in der Lage, in Analysesubjekten enthaltenen Shellcode zu erkennen. Erkannte Shellcodes werden extrahiert und im Hexadezimalformat in den Bericht aufgenommen.
Shellcode	Die Analyseumgebung ist in der Lage, in Analysesubjekten enthaltenen Shellcode zu erkennen. Erkannte Shellcodes werden extrahiert und im Hexadezimalformat in den Bericht aufgenommen.

Aktivitätstyp	Beschreibung
Prozesse	Listet die Prozesse auf, die während der URL-Analyse erzeugt wurden. Dieser Abschnitt wird nur angezeigt, wenn während der Analyse erzeugte Prozesse gefunden wurden.
Abgelegte Dateien	Listet Dateien auf, die während der URL-Analyse auf der Systemfestplatte gespeichert wurden. Dieser Abschnitt wird nur angezeigt, wenn bei der Analyse Dateivorgänge aufgetreten sind.

NSX Intelligence-Vorgänge und -Verwaltung

6

Es gibt Tools, mit denen Sie Vorgänge ausführen können, die Ihnen bei der Verwaltung der NSX Intelligence-Funktion in Ihrer NSX-T-Umgebung helfen.

Die folgenden Themen helfen Ihnen, den Zugriff auf die NSX Intelligence-Funktion zu verwalten, den Status der NSX Intelligence-Anwendung zu überwachen oder Informationen über NSX Intelligence-Objekte zu finden.

Dieses Kapitel enthält die folgenden Themen:

- [Rollenbasierte Zugriffssteuerung in NSX Intelligence](#)
- [Erfassen von NSX Intelligence-Support-Paketen](#)
- [Suche nach NSX Intelligence-Einheiten](#)
- [Verwalten der NSX Intelligence-Einstellungen](#)
- [Verwalten der privaten IP-Bereiche für NSX Intelligence](#)

Rollenbasierte Zugriffssteuerung in NSX Intelligence

Die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) hilft Ihnen dabei, den Zugriff auf NSX Intelligence nur auf bestimmte autorisierte Benutzer zu beschränken.

Da auf die NSX Intelligence-Funktionen über die NSX Manager-Benutzeroberfläche zugegriffen wird, werden dieselben integrierten NSX-T Data Center-Rollen, die den Benutzern zugewiesen sind, für NSX Intelligence-RBAC verwendet und jede Rolle verfügt über bestimmte Berechtigungen. Informationen zur Zuweisung von Rollen für Benutzer finden Sie im *Administratorhandbuch für NSX-T Data Center*.

Um die integrierten NSX-T Data Center-Rollen anzuzeigen, navigieren Sie zu **System > Benutzerverwaltung > Rollen**.

Rollen und Berechtigungen

Im Folgenden sind die Arten von Berechtigungen aufgeführt, die in der NSX Intelligence-Funktion erzwungen werden. In der Liste enthalten sind die Abkürzungen für die Berechtigungen, die in der Tabelle [Tabelle 6-1. NSX Intelligence – Rollen und Berechtigungen](#) verwendet werden.

- Vollständiger Zugriff (Full Access, FA) – Für Empfehlungen beinhaltet der vollständige Zugriff die Möglichkeit, Empfehlungen zu lesen, zu starten, erneut zu starten, zu aktualisieren, zu löschen und zu veröffentlichen.
- Ausführen (Execute, E)
- Lesen (Read, R)
- Keine

Die NSX Intelligence-Funktion erkennt die folgenden integrierten Rollen. Sie können keine neuen Rollen hinzufügen, da benutzerdefinierte RBAC-Rollen NSX Intelligence-Funktionen nicht unterstützen. Ebenfalls in der Liste enthalten sind die Abkürzungen für die Rollen, die in der Tabelle [Tabelle 6-1. NSX Intelligence – Rollen und Berechtigungen](#) verwendet werden.

- Auditor (A)
- Unternehmens-Admin (Enterprise Admin, EA)
- GI (Guest Introspection) Partner-Admin (GIA)
- LB (Load Balancer) Admin (LBA)
- LB-Operator (LB Operator, LBO)
- NETX (Netzwerk-Introspektion) Partner-Admin (NIA)
- Netzwerk-Admin (Network Admin, NA)
- Netzwerkbetreiber (Network Operator, NO)
- Sicherheits-Admin (Security Admin, SA)
- Sicherheitsbeauftragter (Security Operator, SO)
- Support-Paket-Collector (Support Bundle Collector, SBC)
- VPN-Admin (VPN Admin, VPNA)

Die folgende Tabelle zeigt die Berechtigungen, die jede integrierte Rolle für die verschiedenen NSX Intelligence-Vorgänge hat.

Tabelle 6-1. NSX Intelligence – Rollen und Berechtigungen

Vorgang	E												VP
	A	A	SA	SO	NA	NO	SBC	GIA	NIA	LBA	LBO	NA	
Aktivieren Sie die NSX Intelligence-Funktion auf der NSX Application Platform.	F A	R	R	R	Kein e								
Konfigurieren Sie NSX Intelligence-Datenerfassungseinstellungen auf Hosts oder Hostclustern mithilfe von System > NSX Intelligence	F A	R	FA	R	Kein e								
Arbeiten Sie mit dem Dashboard Sicherheit > Verdächtiger Datenverkehr > Erkennungsereignisse .	F A	R	FA	R	Kein e								
Konfigurieren Sie die Detektoren in Sicherheit > Verdächtiger Datenverkehr > Detector-Definitionen .	F A	R	FA	R	Kein e								
Visualisieren Sie Datenverkehrsflows über Planen und Fehler beheben > Entdecken und Ergreifen von Aktionen .	F A	R	R	R	R	R	Kein e						
Arbeiten Sie mit NSX-Empfehlungen über Planen und Fehler beheben > Empfehlungen .	F A	R	FA	R	Kein e								
Generieren Sie ein Support-Paket über System > Support-Paket .	F A	R	Kein e	Kein e	Kein e	Kein e	FA	Kein e	Kein e	Kein e	Kein e	Kein e	Kein e
Führen Sie ein Upgrade der NSX Intelligence-Funktion mithilfe der NSX Application Platform durch.	F A	R	Kein e										
Suchen Sie Flows über die Suchleiste.	F A	R	R	R	R	R	Kein e						
Suchen Sie eine Empfehlung über die Suchleiste.	F A	R	R	R	Kein e								

Erfassen von NSX Intelligence-Support-Paketen

Sie können Support-Pakete von Ihrer NSX Intelligence-Funktion über die NSX Manager-Benutzeroberfläche erfassen. Sie können das Paket auf Ihr lokales System herunterladen oder einen Remotedateiserver hochladen.

Die Inhalte der Support-Paketdatei enthalten keine Daten zu Netzwerkschlüssel-Flows und keine Empfehlungsdaten.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://<nsx-manager-ip-address>` mit Unternehmensadministratorrechten bei einem NSX Manager an.
- 2 Wählen Sie **System > Support-Paket**.
- 3 Wählen Sie auf der Seite **Anforderungspaket** die Option **NSX Application Platform** im Dropdown-Menü **Typ** aus.
- 4 Wählen Sie im Bereich **Verfügbar** den Dienst aus, für den das Support-Paket erfasst werden soll.
- 5 Um den bzw. die ausgewählten Dienst(e) in den Bereich **Ausgewählt** zu verschieben, klicken Sie auf das Symbol >.
- 6 Behalten Sie im Textfeld **Protokollalter (Tage)** den Standardwert **Alle** bei oder geben Sie eine bestimmte Anzahl von Protokollen ein, die in das Support-Paket aufgenommen werden sollen.
- 7 Um anzugeben, dass die Kerndateien und die Überwachungsprotokolldateien im Support-Paket enthalten sein sollen, wählen Sie für **Core-Dateien und Überwachungsprotokolle einbeziehen** die Option **Ja** aus.
Stellen Sie sicher, dass Sie die Informationen unter dem Schalter lesen und verstehen, was es bedeutet, wenn Sie die Kerndateien und Überwachungsprotokolle ein- bzw. ausschließen.
- 8 (Optional) Aktivieren Sie das Kontrollkästchen **Paket auf Remote-Dateiserver hochladen**, wenn Sie das Support-Paket auf einen Remotedateiserver hochladen möchten.
 - a Geben Sie die IP-Adresse oder den Hostnamen des zu verwendenden Remotedateiservers, Ports und Protokolls an.
 - b Geben Sie den Benutzernamen und das Kennwort für den Remotedateiserver an.
 - c Geben Sie den absoluten Zielpfad ein, zu dem das Paket auf den Remoteserver hochgeladen werden soll.
 - d Wenn Sie möchten, dass NSX Manager das Paket hochlädt, stellen Sie die Option für **Upload durch Manager** entsprechend ein.
- 9 Klicken Sie auf **Paketerfassung starten**.
- 10 Überwachen Sie den Status des Paketerfassungsvorgangs.
Auf der Seite **Status** wird der Fortschritt der Support-Paketerfassung angezeigt. Wenn die Erfassung erfolgreich abgeschlossen wurde, wird die Größe des Pakets neben **Support-Paket** angezeigt. In der Tabelle **Details** werden die Informationen zu allen unterstützten Support-Paketen angezeigt, die erfolgreich generiert wurden bzw. nicht abgeschlossen werden konnten.
- 11 Um das Support-Paket in einem lokalen Ordner zu speichern, klicken Sie auf **Herunterladen**. Wenn Sie das Kontrollkästchen **Paket auf Remote-Dateiserver hochladen** ausgewählt haben, wird das Support-Paket auf den von Ihnen angegebenen Dateiserver hochgeladen.

Suche nach NSX Intelligence-Einheiten

Die globale Suchfunktion in NSX-T Data Center erkennt NSX Intelligence-Schlüsselwörter.

Sie können die NSX Manager-Benutzeroberfläche nutzen, um nach Entitäten zu suchen, die zu NSX Intelligence gehören. Sie benötigen eine NSX Intelligence, die in NSX-T Data Center 3.0 oder höher aktiviert ist, damit die globale NSX Intelligence-Suchfunktion verfügbar ist.

Die Suchergebnisse basieren auf dem aktuellen Status der NSX-T Data Center-Konfiguration und legen keine Verlaufsdaten von NSX Intelligence offen.

Basierend auf den Suchkriterien können die Suchergebnisse Informationen zu mit NSX Intelligence verbundenen Entitäten enthalten, wie Gruppen, virtuelle Maschinen, Flows und Empfehlungen. Sie können diese Ergebnisse basierend auf einer oder mehreren zu den Entitäten gehörenden Eigenschaften filtern. Über die in den Suchergebnissen enthaltenen Verknüpfungen können Sie eine ausgewählte Ergebnisentität auf der NSX Intelligence-Visualisierungsarbeitsfläche anzeigen.

Die folgende Tabelle enthält die unterstützten NSX Intelligence-Ressourcentypen und deren Eigenschaften.

Unterstützter Ressourcentyp	Eigenschaften
recommendations	<ul style="list-style-type: none"> ■ context group path ■ context physical server display name ■ context physical server id ■ context vm display name ■ context vm external id ■ display name ■ effective physical server display name ■ effecive physical server id ■ effective vm display name ■ effective vm id ■ status <ul style="list-style-type: none"> ■ ANALYSIS_IN_PROGRESS ■ FAILED ■ PUBLISHED ■ READY_TO_PUBLISH ■ WAITING <p>Beispiel für die Suchabfrage:</p> <pre>recommendation where status = READY_TO_PUBLISH and context group display name = 'Linux'</pre>
flows	<ul style="list-style-type: none"> ■ active only ■ destination group display name ■ destination physical server display name ■ destination physical server id ■ destination vm display name ■ destination vm external id ■ flow type <ul style="list-style-type: none"> ■ ALLOWED ■ BLOCKED ■ UNPROTECTED ■ source group display name ■ source physical server display name ■ source physical server id ■ source vm display name ■ source vm external id <p>Beispiel für die Suchabfrage:</p> <pre>flows where source vm display name = 'Win10' and destination vm display name = 'AD Server'</pre>

Suchen von NSX Intelligence-Einheiten

Sie können mithilfe verschiedener unterstützter Kriterien nach NSX Intelligence-Einheiten suchen, wie Gruppen, virtuelle Maschinen, physische Server, Flows und Empfehlungen.

Die Ergebnistabelle enthält die nach Relevanz sortierten Suchergebnisse. Sie können die Ergebnisse weiter filtern, indem Sie in Ihrer Abfrage zusätzliche Suchkriterien angeben.

Hinweis Wenn Sonderzeichen in Ihrer Suchabfrage enthalten sind, die auch als Operatoren fungieren, müssen Sie davor jeweils einen umgekehrten Schrägstrich (\) einfügen. Die als Operatoren fungierenden Zeichen lauten wie folgt: +, -, =, &&, ||, <, >, !, (,), {, }, [,], ^, ", ~, ?, :, /, \.

Voraussetzungen

Sie müssen die Funktion NSX Intelligence 3.2 oder höher auf NSX-T Data Center 3.2 oder höher bereitgestellt haben.

Verfahren

- 1 Melden Sie sich über Ihren Browser unter `https://<nsx-manager-ip-address>` mit Unternehmensadministratorrechten bei einem NSX Manager an.
- 2 Geben Sie auf der **Startseite** ein Suchkriterium für eine NSX Intelligence-Einheit ein.

Bei der Eingabe Ihrer Suchkriterien unterstützt Sie die globale Suchfunktion, indem sie die entsprechenden Schlüsselwörter anzeigt.

Die Ergebnisse werden in einer Tabelle ähnlich der in der folgenden Abbildung aufgeführt.

The screenshot shows a search interface for NSX Intelligence. The search bar contains the query: "flows where flow type = UNPROTECTED and source vm external id = '501b1e8c-2a74-4ee9-8179-c9ccc2148f4f'". The results table has columns for Quelle (Source), Ziel (Destination), Dienste (Services), and Neuester Flow (Gegen die aktuelle Richtlinie) (Latest flow against current rule). There are two rows of data:

	Quelle	Ziel	Dienste	Neuester Flow (Gegen die aktuelle Richtlinie)	In Diagramm anzeigen
	Berechnen Gruppe	Berechnen Gruppe			
>	rhelvm2 RHELVM2_Group	rhelvm4 RHELVM4_Group	SSH... +2 More	● Allowed	
>	rhelvm2 Group-1 (REC 211109 10:2)	rhelvm4 RHELVM4_Group	SSH... +2 More	● Allowed	

At the bottom left is an "Aktualisieren" (Update) button, and at the bottom right is a status bar indicating "1 - 2 of 2 Flow(s)".

Sie können die einzelnen Zeilen erweitern, um weitere Details zu den Suchergebnissen anzuzeigen. Sie können auch auf die Verknüpfungen klicken, um zusätzliche Informationen zu einem bestimmten Attribut anzuzeigen. Wenn Sie auf das Diagrammsymbol und auf einen Link im Popup-Fenster klicken, werden auf der NSX Intelligence-Visualisierungsarbeitsfläche detailliertere Informationen angezeigt.

- 3 (Optional) Klicken Sie auf das Symbol , um Ihre Suchkriterien zu speichern.

- 4 Klicken Sie in der Suchleiste auf das Symbol für die erweiterte Suche  um die aktuellen und gespeicherten Suchabfragen anzuzeigen.
- 5 Klicken Sie auf **Letzte**, um eine Liste der zuletzt verwendeten Suchkriterien anzuzeigen.
Sie können auf die Suchkriterien klicken, damit die Ergebnisse im Ergebnisfenster angezeigt werden.
- 6 Klicken Sie auf **Gespeichert**, um alle gespeicherten Suchkriterien anzuzeigen.
- 7 (Optional) Klicken Sie auf **Alle löschen**, um Ihre erweiterten Suchkriterien zurückzusetzen.

Verwalten der NSX Intelligence-Einstellungen

Nachdem Sie die Funktion NSX Intelligence aktiviert haben, beginnt sie standardmäßig mit der Erfassung von Netzwerkdatenverkehrsdaten auf allen eigenständigen Hosts und Hostclustern. Bei Bedarf können Sie optional die Datenerfassung von einem eigenständigen Host oder Hostcluster beenden.

Im Abschnitt **Eigenständiger Host** der Registerkarte **Datenerfassung** in der Benutzeroberfläche **Systemeinstellungen > NSX Intelligence** werden nur die Hosts aufgelistet, die zu keinem Cluster gehören und die nicht von einem Compute Manager verwaltet werden. Im Abschnitt **Cluster** werden alle Cluster in Ihrer NSX-T-Umgebung aufgelistet.

Sie können die Datenerfassung für einen einzelnen Host, der zu einem Cluster gehört, nicht deaktivieren oder aktivieren. Sie können die Datenerfassung nur auf dem gesamten Cluster deaktivieren oder aktivieren, zu dem dieser Host gehört. Wenn die Datenerfassung für einen Cluster deaktiviert ist, beendet die **NSX Intelligence**-Anwendung die Datenerfassung auf allen Hosts, die zu diesem Cluster gehören. Wenn der Datenerfassungsmodus auf einem Cluster aktiviert ist, beginnt die **NSX Intelligence**-Anwendung gleichermaßen mit der Erfassung von Daten auf allen Hosts, die zu diesem Cluster gehören.

Wenn der Datenerfassungsmodus für einen eigenständigen Host deaktiviert ist und dieser Host zu einem Cluster hinzugefügt wird, dessen Datenerfassung aktiviert ist, beginnt die **NSX Intelligence**-Anwendung mit der Erfassung von Daten auf diesem Host, nachdem sie diesem Cluster hinzugefügt wurde. Wenn auf einem eigenständigen Host der Datenerfassungsmodus aktiviert ist und er einem Cluster hinzugefügt wird, dessen Datenerfassung deaktiviert ist, stoppt die **NSX Intelligence**-Anwendung die Datenerfassung auf diesem Host, nachdem sie diesem Cluster hinzugefügt wurde.

Voraussetzungen

- Die NSX Intelligence-Funktion muss auf der NSX Application Platform aktiviert werden. Einzelheiten dazu finden Sie unter *Aktivieren und Aktualisieren von VMware NSX Intelligence*.
- Sie müssen über die Benutzerrechte eines NSX-T Data Center Enterprise-Administrators verfügen.
- Mindestens eine gültige NSX Data Center Enterprise Plus Edition-Lizenz ist für Ihre NSX Manager-Sitzung gültig.

Verfahren

- 1 Melden Sie sich über Ihren Browser mit Unternehmensadministratorrechten bei einer NSX Manager-Appliance unter <https://<nsx-manager-ip-address>> an.
 - 2 Wählen Sie in der NSX Manager-Benutzeroberfläche **System** aus und wählen Sie im Abschnitt „Einstellungen“ die Option **NSX Intelligence** aus.
 - 3 Führen Sie einen der folgenden Schritte aus, um die Datenerfassung für einen oder mehrere Hosts zu verwalten.
 - a Um die Datenerfassung für den Datenverkehr zu beenden, wählen Sie den oder die Hosts im Abschnitt **Eigenständiger Host** aus, klicken Sie auf **Deaktivieren** und dann zum Bestätigen auf **Bestätigen**.
 - b Um die Datenerfassung für den Datenverkehr zu starten, wählen Sie den oder die Hosts aus, klicken Sie auf **Aktivieren** und dann zum Bestätigen auf **Bestätigen**.
- Abhängig vom festgelegten Datenerfassungsmodus aktualisiert das System den Wert **Erfassungsstatus** für jeden betroffenen Host auf **Deaktiviert** oder **Aktiviert**.
- 4 Führen Sie einen der folgenden Schritte aus, um die Datenerfassung für einen Host oder einen Hostcluster zu verwalten.
 - a Um die Datenerfassung für einen oder mehrere Cluster zu beenden, wählen Sie den oder die Cluster im Abschnitt **Cluster** aus, klicken Sie auf **Deaktivieren** und dann zum Bestätigen auf **Bestätigen**, wenn Sie dazu aufgefordert werden.
 - b Um die Datenerfassung für den Datenverkehr zu starten, wählen Sie den oder die Cluster aus, klicken Sie auf **Aktivieren** und dann zum Bestätigen auf **Bestätigen**, wenn Sie dazu aufgefordert werden.
- Abhängig vom festgelegten Datenerfassungsmodus aktualisiert das System den Wert **Erfassungsstatus** für jeden betroffenen Cluster auf **Deaktiviert** oder **Aktiviert**.

Verwalten der privaten IP-Bereiche für NSX Intelligence

Private IP-Bereiche werden verwendet, um verdächtigen Datenverkehr innerhalb von kontrollierten Netzwerksegmenten zu isolieren.

Sie können die privaten IP-Bereiche mithilfe der Registerkarte **Private IP-Bereiche** auf der Benutzeroberfläche **Allgemeine Sicherheitseinstellungen** verwalten. Diese privaten IP-Bereiche können von den Funktionen NSX Intelligence und NSX Network Detection and Response verwendet werden, wenn Sie eine der beiden Funktionen aktivieren.

Wenn Sie die NSX Network Detection and Response-Funktion aktivieren, lädt das System die Informationen zu privaten IP-Bereichen in die NSX Network Detection and Response-Funktion hoch, und einige der Korrelationsregeln für Eindringversuche verwenden diese Informationen.

- Um einen IPv4-IP-Bereich einzugeben, klicken Sie in das Textfeld „IPv4-IP-Bereich“ und geben Sie die Werte mithilfe des unter dem Feld angezeigten /IPv4-IP-CIDR-Notationsformats ein. Drücken Sie die Eingabetaste für jeden Eintrag und klicken Sie auf **Speichern**, wenn Sie fertig sind. Drücken Sie die Eingabetaste für jeden Eintrag und klicken Sie nach Abschluss auf **Speichern**.
- Um einen IPv6-IP-Bereich einzugeben, klicken Sie in das Textfeld „IPv6-IP-Bereich“ und geben Sie die Werte mithilfe des unter dem Feld angezeigten IPv6-CIDR-Notationsformats ein. Drücken Sie die Eingabetaste für jeden Eintrag und klicken Sie auf **Speichern**, wenn Sie fertig sind.

NSX Intelligence-Funktion kategorisiert eine IP-Adresse, die zu einer der im Dialogfeld aufgeführten CIDR-Notationen gehört, als private IP-Adresse. Jede IP-Adresse, die keiner dieser CIDR-Notationen angehört, wird als öffentliche IP-Adresse klassifiziert. Wenn die IP-Adresse Ihrer VM oder Ihres physischen Servers nicht unter eine dieser CIDR-Notationen fällt, sollten Sie Ihre CIDR-Notation mithilfe dieser Benutzeroberfläche **Private IP-Bereiche** hinzufügen.

Beheben von Problemen bei der Verwendung von NSX Intelligence

7

Wenn die NSX Intelligence-Funktion nicht mehr reagiert oder Sie weitere Details zu einer Fehlermeldung benötigen, die Sie während der Verwendung der NSX Intelligence-Funktion erhalten haben, können Sie bestimmte Befehle ausführen, um den Zustand der NSX Intelligence-Dienste abzurufen.

Sie können auch Support-Pakete zusammenstellen, die Sie und die VMware Support-Mitarbeiter beim Debugging von möglicherweise aufgetretenen Problemen unterstützen.

Dieses Kapitel enthält die folgenden Themen:

- Überprüfen des Status der NSX Intelligence-Funktion
- Vorhandensein herabgestufter Dienste nach einer erfolgreichen Aktivierung von NSX Intelligence
- Inkonsistenzen bei der inkrementellen Topologieberichterstellung
- Informationen zum FTP-Flow werden nach dem Anhalten der FTP-Sitzung weiterhin angezeigt.
- Ansicht "Gruppen" wird nicht mit Datenverkehrsflow-Daten aktualisiert

Überprüfen des Status der NSX Intelligence-Funktion

Wenn die NSX Intelligence-Funktion nicht mehr reagiert, überprüfen Sie den Status der NSX Application Platform-Dienste.

Problem

Die NSX Intelligence-Funktion reagiert nicht mehr, oder Sie erhalten eine Fehlermeldung, die angibt, dass die Funktion nicht wie erwartet funktioniert.

Ursache

Es ist möglich, dass einer oder mehrere der zugrunde liegenden NSX Application Platform-Dienste angehalten wurde oder sich nicht in einem fehlerfreien Zustand befindet. Die NSX Intelligence-Funktion wird auf der NSX Application Platform gehostet. Wenn sich einer der Dienste der Plattform nicht in einem fehlerfreien Zustand befindet, kann die NSX Intelligence-Funktion beeinträchtigt werden.

Lösung

Überprüfen Sie den NSX Intelligence-Status mithilfe des health-API-Aufrufs. Suchen Sie unter dem Schlüssel `intelligence` in der JSON-Ausgabe nach `services`. Weitere Informationen finden Sie im Dokument <http://developers.eng.vmware.com/apis/nsx-intelligence-&-application-platform/cluster/latest/napp/api/v1/platform/monitor/feature/health/get/>.

Vorhandensein herabgestufter Dienste nach einer erfolgreichen Aktivierung von NSX Intelligence

Die NSX Intelligence-Funktion wurde erfolgreich aktiviert, aber es sind einige herabgestufte Dienste vorhanden.

Problem

Die NSX Intelligence-Funktion wurde erfolgreich aktiviert, aber ihr Systemzustand wird als `TEILWEISE AKTIV` oder `INAKTIV` gemeldet. Diese Herabstufung des Systemzustands wird entweder unmittelbar nach der Aktivierung der NSX Intelligence-Funktion oder zu einem späteren Zeitpunkt in seinem Lebenszyklus gemeldet.

Ursache

Dies kann an einem der folgenden Gründe liegen.

- 1 Die Docker-Registrierung ist vom TKC- oder Upstream-Kubernetes-Worker-Knoten aus nicht erreichbar.
- 2 Der NSX Intelligence-Anwendungs-Pod konnte den Zustand `WIRD AUSGEFÜHRT` nicht erreichen.

Lösung

Wenden Sie sich an Ihren Kubernetes-Infrastrukturadministrator, um das Problem zu beheben. Die folgenden möglichen Lösungen entsprechen den zuvor im Abschnitt „Probleme“ aufgeführten Problemen.

- 1 Überprüfen Sie, ob alle gewünschten Pods gestartet werden können. Der Pod-Start hängt davon ab, ob die Docker-Registrierung erreichbar ist. Falls die Docker-Registrierung nicht erreichbar ist oder die Download-Aktion aus Authentifizierungs- oder Autorisierungsgründen fehlschlägt, kann der Kubernetes-Worker-Knoten das zum Ausführen der Arbeitslasten erforderliche Docker-Container-Image möglicherweise nicht herunterladen. Beheben Sie das Konnektivitätsproblem für die Docker-Registrierung, löschen Sie die NSX Intelligence-Funktion und versuchen Sie, sie erneut zu aktivieren.

- 2 Stellen Sie sicher, dass alle Pods den Status `Wird ausgeführt` erreichen und alle Aufträge erfolgreich abgeschlossen wurden. Sobald das Docker-Container-Image heruntergeladen wurde, müssen die Pods gestartet und ausgeführt werden können. Überprüfen Sie für Pods, die sich nicht im Status `Wird ausgeführt` befinden, die Ereignisse mit dem folgenden `describe`-Befehl.

```
napp-k describe pod <pod-name>
```

Überprüfen Sie die Protokolle für Aufträge, die nicht erfolgreich abgeschlossen wurden, mit dem folgenden Befehl.

```
napp-k logs <pod-name>
```

Wenn keine der bereitgestellten Lösungen funktioniert, wenden Sie sich an VMware Support, um weitere Unterstützung zu erhalten.

Inkonsistenzen bei der inkrementellen Topologieberichterstellung

Es kann zu Inkonsistenzen bei der Anzahl der VMs, physischen Servern, Gruppen oder Flows kommen, die in der Ansicht „Gruppen“ oder „Berechnungen“ angezeigt werden, wenn Sie die für lange Zeit angezeigte NSX Intelligence-Visualisierungsbenutzeroberfläche verlassen.

Problem

Wenn Sie die Ansicht „Gruppen“ oder „Berechnungen“ öffnen und die NSX Intelligence-Visualisierungsbenutzeroberfläche für eine lange Zeit geöffnet lassen, werden neue Ereignisse schrittweise gemeldet und in der Ansicht zusammengeführt. Während der inkrementellen Berichterstellung und Zusammenführung kommt es möglicherweise zu einigen Inkonsistenzen hinsichtlich der Anzahl an Gruppen, VMs oder physischen Servern. Wenn z. B. einige Konfigurationsänderungen vorhanden sind, wie Änderungen bei der Mitgliedschaft der Gruppen-VM, die während der inkrementellen Berichterstellung ausgelöst wurden, entstehen möglicherweise Inkonsistenzen bei den angezeigten Visualisierungen. Alle neuen Flows, die von den neu hinzugefügten Berechnungsentitäten generiert wurden, sind möglicherweise auch nicht in der aktuellen Ansicht enthalten.

Sie können möglicherweise die folgenden Inkonsistenzen in den dargestellten Visualisierungen beobachten.

- 1 Ein Knoten der Gruppe „Nicht kategorisiert“ zeigt eine falsche Anzahl von VMs an.
 - Die angezeigte Anzahl der VMs in der Gruppe „Nicht kategorisiert“ ist üblicherweise höher als die Anzahl der VMs, die bei einer erneuten Anzeige der Ansicht „Gruppen“ angezeigt wird.
 - Die angezeigte Anzahl der VMs in der Gruppe „Nicht kategorisiert“ ist üblicherweise höher als die Anzahl der angezeigten VMs, wenn Sie mit der rechten Maustaste auf den Knoten einer Gruppe klicken und **VM** auswählen.

- 2 Die Gruppe „Nicht kategorisiert“ zeigt bei einer Deep-Dive-Gruppenansicht eine inkonsistente Anzahl von VMs an.
 - Die Gruppe „Nicht kategorisiert“, die in einer Deep-Dive-Gruppenansicht angezeigt wird, zeigt möglicherweise mehr VMs als in einer neu geöffneten Deep-Dive-Gruppenansicht an.
 - Die Gruppe „Nicht kategorisiert“ in einer Deep-Dive-Gruppenansicht zeigt möglicherweise mehr VMs an als aufgelistet werden, wenn Sie mit der rechten Maustaste auf den Knoten der Gruppe „Nicht kategorisiert“ klicken und **VM** auswählen.
 - Eine VM erhält möglicherweise in der Gruppe „Nicht kategorisiert“ ein Live-Update, auch wenn sie vielleicht bereits zu einer anderen Gruppe hinzugefügt wurde.
- 3 In den Ansichten „Gruppen“ und „Berechnungen“ wird möglicherweise eine unbenannte VM angezeigt.
 - Dieses Problem tritt häufig bei VM-Mitgliedern auf, die zu der Gruppe „Unbekannt“ oder „Nicht kategorisiert“ gehören. Sie könnte eventuell auch in einer normalen Gruppe angezeigt werden.
- 4 Wenn die NSX Intelligence-Anwendung Datenverkehrsflows mit einer hohen Geschwindigkeit ausführt, wenn die Ansicht „Gruppen“ oder „Berechnungen“ angezeigt wird, werden die inkrementellen Visualisierungsupdates für die Ansicht möglicherweise verzögert.

Ursache

Bei der Berichterstellung der Echtzeitdaten gibt es derzeit einige bekannte Inkonsistenzen, die bei der inkrementellen Berichterstellung auftreten.

Lösung

Um alle Inkonsistenzen zu löschen, laden Sie die gesamte NSX Intelligence-Visualisierungsarbeitsfläche neu, indem Sie Ihren Webbrower aktualisieren.

Informationen zum FTP-Flow werden nach dem Anhalten der FTP-Sitzung weiterhin angezeigt.

Nach einem abrupten Beenden einer FTP-Sitzung werden die Informationen zum FTP-Flow für diese Sitzung weiterhin auf der NSX Intelligence-Visualisierungsbenuzeroberfläche angezeigt.

Problem

Wenn Sie eine FTP-Sitzung starten und in der Mitte der Sitzung Strg + C oder Strg + Z drücken, wird die FTP-Sitzung angehalten. Die Informationen zu diesem FTP-Flow werden jedoch für lange Zeit unter der Registerkarte **Aktive Flows** in der Tabelle „Flow-Details“ für die Gruppe angezeigt.

Ursache

Da die TCP-Sitzung nicht ordnungsgemäß angehalten wurde, ist die TCP-Leerlauf-Zeitüberschreitung immer noch wirksam. Die Zeitüberschreitung ist standardmäßig auf 12 oder 24 Stunden festgelegt.

Lösung

Um sicherzustellen, dass die Informationen zu FTP-Datenverkehrs-Flows nicht weiterhin auf der Registerkarte **Aktiver Flow** angezeigt werden, wenn die FTP-Sitzung abrupt beendet wird, legen Sie ein Sitzungs-Timerprofil mit einem kürzeren Zeitüberschreitungswert fest. Legen Sie das Profil auf die entsprechenden Gruppen fest. Weitere Informationen finden Sie unter dem Thema „Erstellen eines Sitzungstimers“ im *Administratorhandbuch für NSX-T Data Center*.

Ansicht "Gruppen" wird nicht mit Datenverkehrsflow-Daten aktualisiert

Nach einer erfolgreichen Migration von NSX Intelligence 1.2.x zu NSX Intelligence 3.2 oder höher werden die in der Ansicht „Gruppen“ angezeigten Datenverkehrsflow-Daten nicht aktualisiert.

Problem

In der Ansicht „Gruppen“ werden nicht die neuesten Datenverkehrsflow-Daten angezeigt.

Ursache

Innerhalb des Kubernetes-Clusternetzwerks, auf dem NSX Intelligence ausgeführt wird, liegt ein Netzwerkproblem vor.

Lösung

Nachdem das Kubernetes-Clusternetzwerk stabilisiert wurde, führen Sie einen der folgenden Schritte aus, um alle aktualisierten Datenverkehrsflow-Daten anzuzeigen, die während der Netzwerkinstabilität möglicherweise ausgelassen wurden.

- 1 Warten Sie, bis die Aktualisierungen der Datenverkehrsflow-Daten auf der NSX Intelligence-Arbeitsfläche angezeigt werden.

Sobald das Kubernetes-Clusternetzwerk stabil ist, synchronisiert NSX Intelligence alle Datenverkehrsflow-Daten mit NSX Manager und zeigt die aktuellen Datenverkehrsflow-Informationen in der Ansicht „Gruppen“ auf der NSX Intelligence-Arbeitsfläche an.
- 2 Wenn Sie eine Datensynchronisierung sofort erzwingen möchten, arbeiten Sie mit Ihrem Kubernetes-Infrastrukturadministrator zusammen, um den `nsx-config`-Pod neu zu starten. Sobald der `nsx-config`-Pod neu gestartet wurde und sich in einem stabilen Ausführungszustand befindet, wird eine Synchronisierung der Datenverkehrsflow-Daten ausgelöst und die Ansicht „Gruppen“ wird auf der NSX Intelligence-Arbeitsfläche aktualisiert.