CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Technologien und Tools

Intrusion Detection Systeme (IDS)

IDS-Systeme überwachen den Netzwerkverkehr auf Anomalien und verdächtige Aktivitäten. Sie können in Echtzeit Alarme auslösen, wenn potenzielle Bedrohungen erkannt werden. Bekannte IDS-Systeme sind Snort, Suricata und Zeek (früher bekannt als Bro).

Intrusion Detection Systeme (IDS)

Intrusion Detection Systeme (IDS)

Netzwerküberwachung:

- IDS überwachen den Datenverkehr in Netzwerken, um verdächtige Aktivitäten oder Anomalien zu erkennen.

Signaturbasierte Erkennung:

- IDS verwenden vordefinierte Signaturen oder Muster von bekannten Angriffen, um potenzielle Bedrohungen zu identifizieren.

Verhaltensbasierte Erkennung:

- Einige IDS analysieren das normale Verhalten des Netzwerks und identifizieren Abweichungen davon, was auf unbekannte Bedrohungen hinweisen kann.

Intrusion Detection Systeme (IDS)

Hostbasierte Erkennung:

- Diverse IDS sind auf einzelnen Hosts oder Systemen installiert und überwachen Aktivitäten auf diesen Geräten, um Anomalien oder Angriffe zu erkennen.

Protokollanalyse:

- IDS analysieren Protokolle und Protokolldateien, um Angriffe oder verdächtige Ereignisse zu identifizieren.

Korrelationsanalyse:

- Einige IDS können Ereignisse aus verschiedenen Quellen korrelieren, um komplexere Angriffsmuster zu erkennen.

Endpoint Detection and Response (EDR) Lösungen

EDR-Lösungen bieten erweiterte Funktionen zur Überwachung und Untersuchung von Endpunktgeräten. Sie können Angriffe auf Endgeräte erkennen und darauf reagieren. Beispiele für EDR-Tools sind CrowdStrike, Carbon Black und SentinelOne.

Endpoint Detection and Response (EDR) Lösungen

Endpoint Detection and Response (EDR) Lösungen

Endpunktüberwachung:

- EDR-Lösungen überwachen die Endpunkte (z. B. Computer, Laptops, Server) in einem Netzwerk in Echtzeit.

Verhaltensanalyse:

- Sie analysieren das Verhalten von Endpunkten, um verdächtige Aktivitäten oder Anomalien zu erkennen, die auf Sicherheitsvorfälle hinweisen könnten.

Bedrohungserkennung:

- EDR-Lösungen verwenden fortschrittliche Algorithmen und Signaturen, um bekannte und unbekannte Bedrohungen zu identifizieren.

Endpoint Detection and Response (EDR) Lösungen

Datenkorrelation:

- Sie korrelieren Informationen von verschiedenen Endpunkten und Netzwerkquellen, um ein umfassendes Bild von Bedrohungen zu erstellen.

Automatisierte Reaktion:

- EDR-Lösungen können automatisch auf erkannte Bedrohungen reagieren, z. B. das Isolieren eines infizierten Endpunkts oder das Blockieren von schädlichem Datenverkehr.

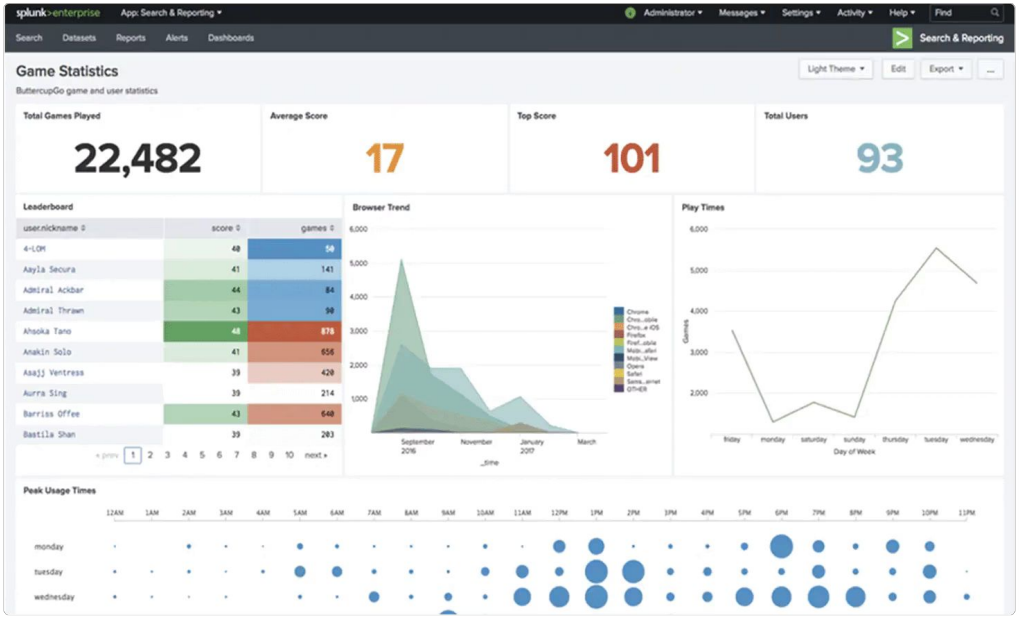
Bewegungsverfolgung:

- Sie verfolgen die Bewegung von Malware oder Bedrohungen innerhalb des Netzwerks und auf verschiedenen Endpunkten

SIEM-Systeme

SIEM-Systeme (Security Information and Event Management) erfassen und korrelieren Sicherheitsereignisse aus verschiedenen Quellen. Sie bieten einen Überblick über die Sicherheitslage einer Organisation und können bei der Identifizierung von Bedrohungen helfen. Beispiele für SIEM-Tools sind Splunk, ELK Stack (Elasticsearch, Logstash, Kibana) und QRadar von IBM.

SIEM-Systeme



SIEM-Systeme

Datenaggregation:

- SIEM-Systeme sammeln und aggregieren Sicherheitsdaten aus verschiedenen Quellen, einschließlich Netzwerken, Anwendungen, Endpunkten und Protokolldateien.

Echtzeitanalyse:

- Sie analysieren Sicherheitsereignisse in Echtzeit, um verdächtige Aktivitäten oder Anomalien zu erkennen.

Regelbasierte Erkennung:

- SIEM-Systeme verwenden vordefinierte Regeln und Schwellenwerte, um auf bekannte Angriffe und Verhaltensweisen zu reagieren.

SIEM-Systeme

Protokollanalyse:

- Sie analysieren Protokolldaten, um Einblicke in die Aktivitäten auf Systemen und im Netzwerk zu gewinnen.

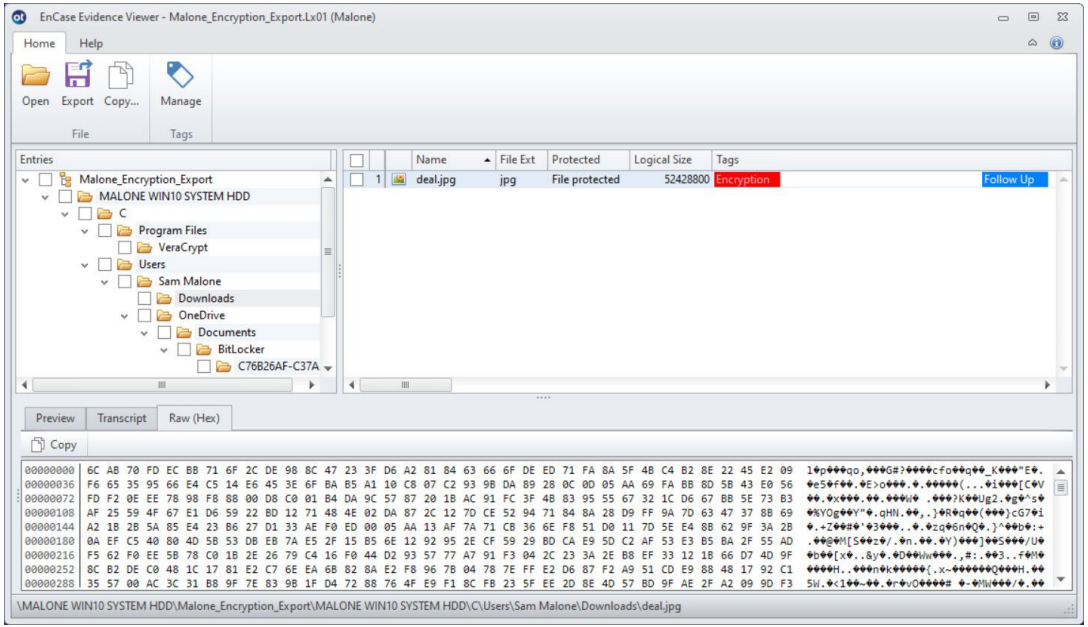
Reaktion und Automatisierung:

- SIEM-Systeme können automatisierte Reaktionsmaßnahmen auslösen, um auf Bedrohungen zu reagieren, z. B. das Blockieren von verdächtigem Datenverkehr.

Forensiksoftware

Ermöglichen die Untersuchung von Daten auf betroffenen Systemen und die Extraktion von Beweisen. Beispiele für solche Software sind EnCase, FTK (Forensic Toolkit) und Autopsy.

Forensiksoftware



Forensiksoftware

Datensammlung:

- Forensiksoftware sammelt digitale Beweise von verschiedenen Quellen, einschließlich Festplatten, Speichermedien, Netzwerken und Cloud-Diensten.

Datenextraktion:

- Sie ermöglicht die Extraktion von Daten aus verschiedenen Dateiformaten, Betriebssystemen und Anwendungen, ohne die Integrität der Beweise zu beeinträchtigen.

Forensiksoftware

Datenaufbereitung:

- Die Software bereitet die gesammelten Daten für die forensische Analyse vor, einschließlich der Entfernung von Duplikaten und der Organisation der Informationen.

Metadatenanalyse:

- Sie analysiert Metadaten wie Zeitstempel, Dateiverläufe und Zugriffsrechte, um Einblicke in die Aktivitäten und Ereignisse zu gewinnen.

Dateisignaturprüfung:

- Forensiksoftware überprüft Dateisignaturen und Hash-Werte, um die Integrität und Authentizität von Dateien sicherzustellen.

Automatisierungs- und Orchestrierungstools

Diese Tools helfen bei der Automatisierung von Routineaufgaben und Abläufen in der Incident Response, was die Effizienz des Teams verbessert. Beispiele sind Ansible, Puppet und verschiedene SOAR (Security Orchestration, Automation, and Response)-Plattformen.

Automatisierungs- und Orchestrierungstools

Automatisierungs- und Orchestrierungstools

Automatisierung von Aufgaben:

- Automatisieren wiederholbare Aufgaben und Abläufe in der IT-Sicherheit, wie die Bereitstellung von Sicherheitsupdates oder das Blockieren von schädlichem Datenverkehr.

Integration von Sicherheitswerkzeugen:

- Sie ermöglichen die Integration verschiedener Sicherheitswerkzeuge und -systeme, um eine nahtlose Zusammenarbeit zu gewährleisten und Sicherheitsprozesse zu optimieren.

Automatisierungs- und Orchestrierungstools

Workflow-Management:

- Automatisierungs- und Orchestrierungstools ermöglichen die Erstellung und Verwaltung von Workflow-Prozessen, um Aufgaben und Abläufe zu strukturieren und zu steuern.

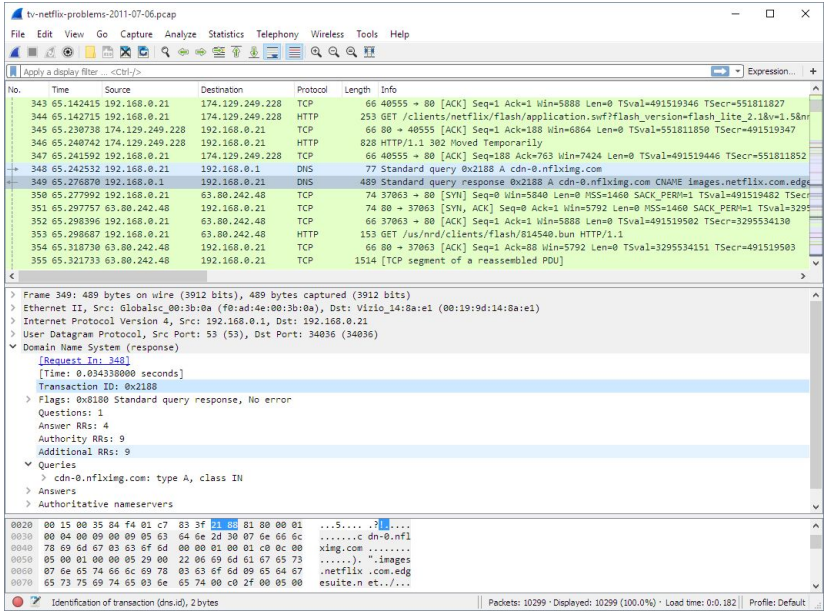
Integration von KI und Machine Learning:

- Einige Tools integrieren künstliche Intelligenz (KI) und maschinelles Lernen, um fortschrittliche Analyse und Vorhersage von Sicherheitsvorfällen zu ermöglichen.

Packet Capturing Tools

Diese Tools erfassen den Netzwerkverkehr und ermöglichen es den Analysten, den Datenverkehr im Detail zu analysieren. Bekannte Packet Capturing-Tools sind Wireshark und tcpdump.

Packet Capturing Tools



Packet Capturing Tools

Datenverkehrsaufzeichnung:

- Packet Capturing Tools erfassen den Datenverkehr, der über ein Netzwerk fließt, einschließlich Pakete, Protokolldaten und Kommunikation zwischen Geräten.

Protokollanalyse:

- Sie analysieren die erfassten Pakete, um Protokolldaten und Informationen über die Kommunikation zwischen Quell- und Zielgeräten zu extrahieren.

Paketfilterung:

- Ebenso bieten sie die Möglichkeit, den erfassten Datenverkehr anhand von Filtern oder Regeln zu filtern, um spezifische Informationen oder Protokolle zu isolieren.

Packet Capturing Tools

Rekonstruktion von Sitzungen:

- Sie ermöglichen die Rekonstruktion von Netzwerksitzungen, um den gesamten Kommunikationsverlauf zwischen Geräten zu visualisieren.

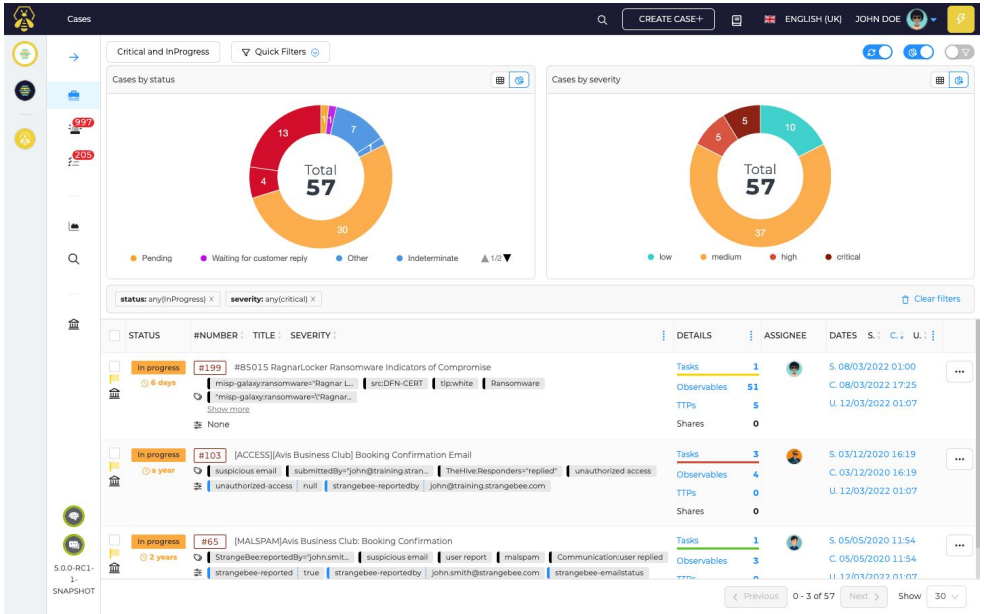
Fehleranalyse:

- Packet Capturing Tools helfen bei der Identifizierung von Netzwerkfehlern, Paketverlusten oder Latenzproblemen, die die Netzwerkleistung beeinträchtigen können.

Open Source Tools

Es gibt auch eine Vielzahl von Open-Source-Werkzeugen und Ressourcen für Incident Response. Diese können kostengünstige Alternativen zu kommerziellen Produkten sein und bieten oft eine aktive Community für Support und Weiterentwicklung. Einige Beispiele sind TheHive, MISP (Malware Information Sharing Platform & Threat Sharing), und OSSEC.

Open Source Tools



CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm