Windows

Continuous Threat Protection:

Defense-in-depth, Swiss Cheese, Machine Learning (oh, and Microsoft Security)

Paul Huijbregts
Microsoft

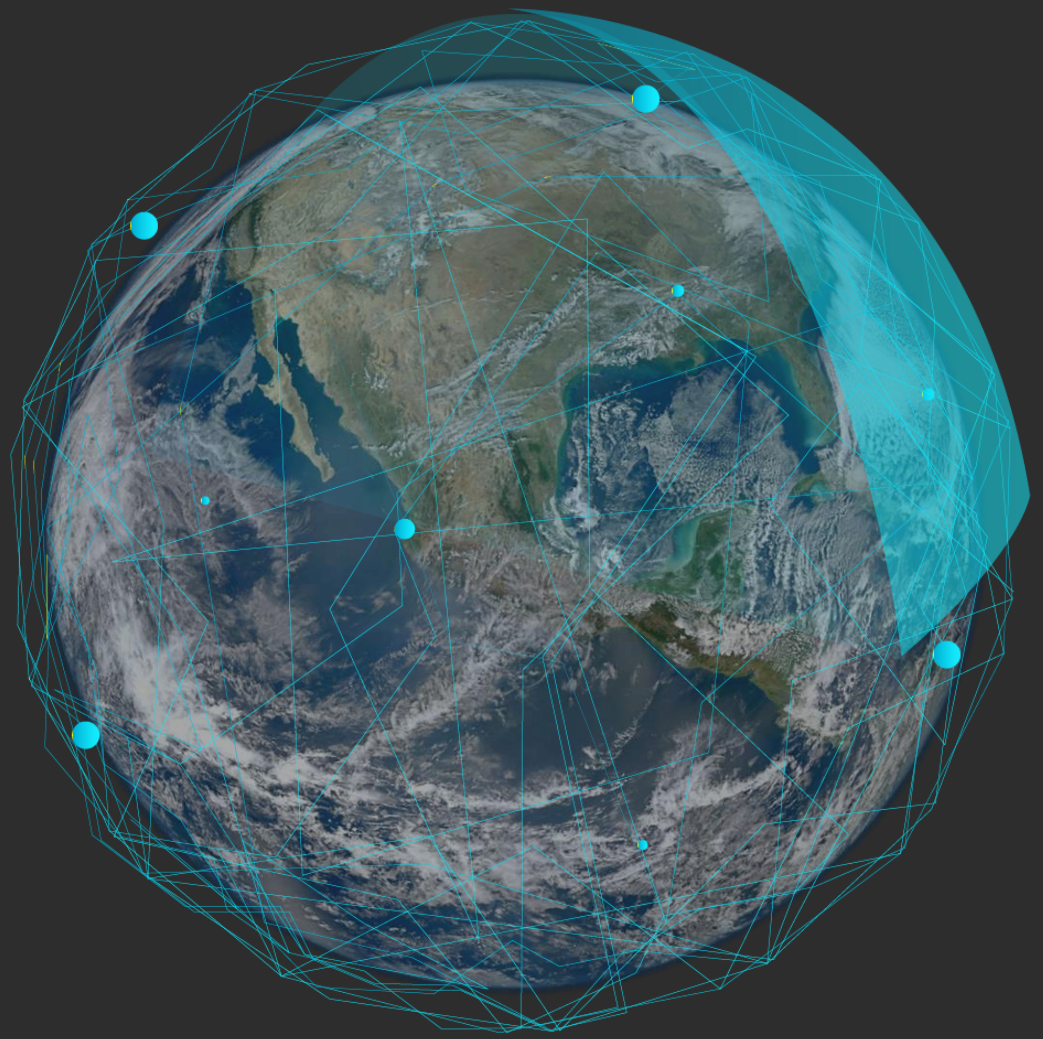
Data-driven security insights

Machine Learning

Intelligent Automation

Cloud Scale

What if this is your corporate network?



Defense in depth (computing)

From Wikipedia, the free encyclopedia

For the military strategy, see Defence in depth.

This article **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed. *(April 2012) (Learn how and when to remove this template message)*

Defense in depth (also known as **Castle Approach**[*citation needed*]) is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of *personnel*, *procedural*, *technical* and *physical* security for the duration of the system's life cycle.

Swiss cheese model

From Wikipedia, the free encyclopedia

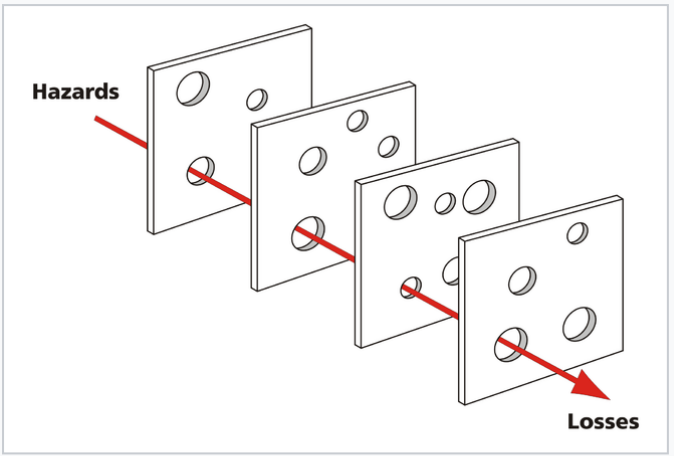
(Redirected from Swiss Cheese model)

Risk management

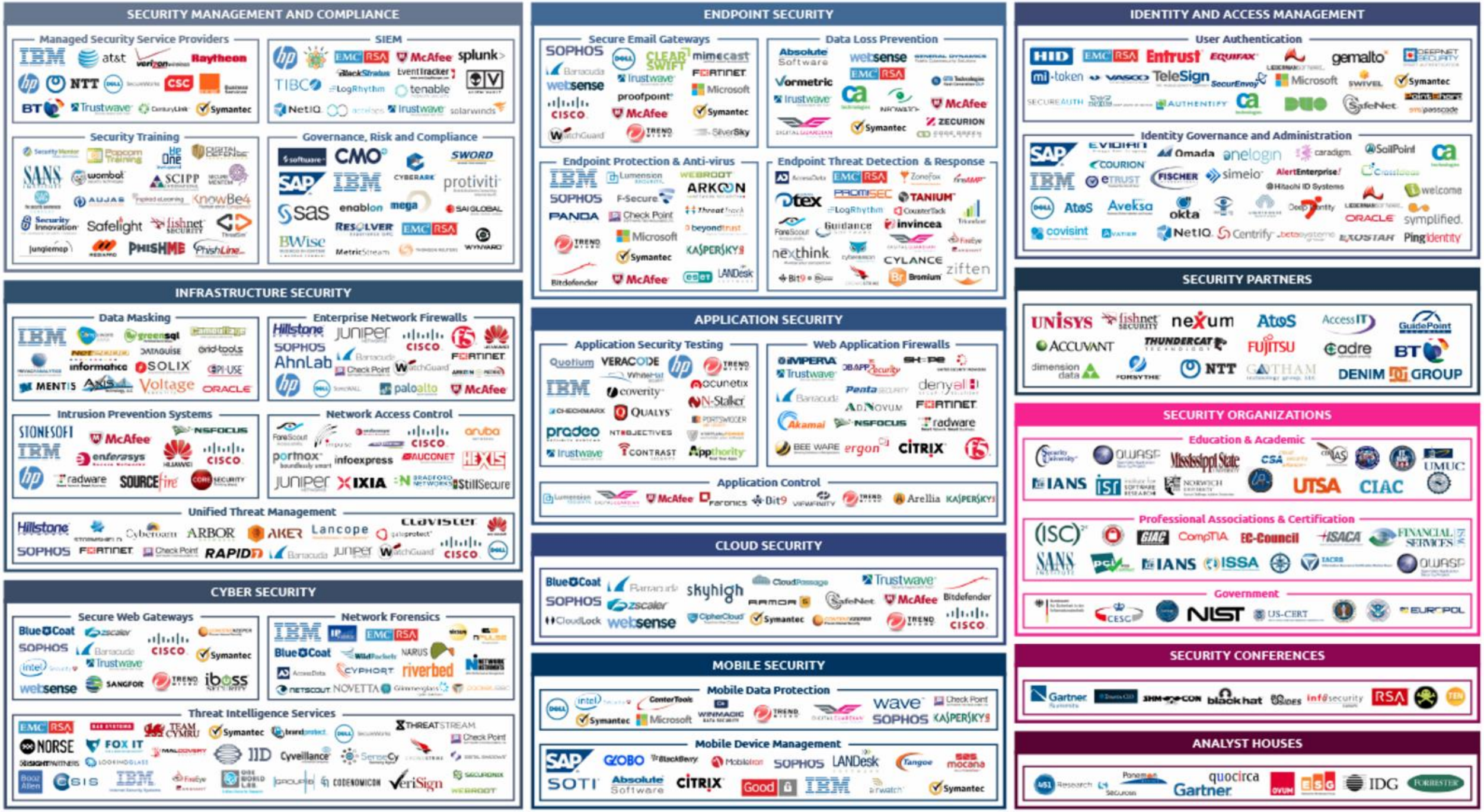
The **Swiss cheese model** of accident causation is a model used in risk analysis and risk management, including aviation safety, engineering, healthcare, emergency service organizations, and as the principle behind layered security, as used in computer security and defense in depth. It likens human systems to multiple slices of swiss cheese, stacked side by side, in which the risk of a threat becoming a reality is mitigated by the differing layers and types of defenses which are "layered" behind each other. Therefore, in theory, lapses and weaknesses in one defense do not allow a risk to materialize, since other defenses also exist, to prevent a single point of failure. The model was originally formally propounded by Dante Orlandella and James T. Reason of the University of Manchester,[1] and has since gained widespread acceptance. It is sometimes called the **cumulative act effect**.

Although the Swiss cheese model is respected and considered to be a useful method of relating concepts, it has been subject to criticism that it is used too broadly, and without enough other models or support.[2]

Contents [hide]



The Swiss cheese model of accident causation illustrates that, although many layers of defense lie between hazards and accidents, there are flaws in each layer that, if aligned, can allow the accident to occur.


SECURITY MANAGEMENT AND COMPLIANCE
Managed Security Service Providers
SIEM
Security Training
Governance, Risk and Compliance
INFRASTRUCTURE SECURITY
Data Masking
Enterprise Network Firewalls
Intrusion Prevention Systems
Network Access Control
Unified Threat Management
CYBER SECURITY
Secure Web Gateways
Network Forensics
Threat Intelligence Services
ENDPOINT SECURITY
Secure Email Gateways
Data Loss Prevention
Endpoint Protection & Anti-virus
Endpoint Threat Detection & Response
APPLICATION SECURITY
Application Security Testing
Web Application Firewalls
Application Control
CLOUD SECURITY
MOBILE SECURITY
Mobile Data Protection
Mobile Device Management
IDENTITY AND ACCESS MANAGEMENT
User Authentication
Identity Governance and Administration
SECURITY PARTNERS
SECURITY ORGANIZATIONS
Education & Academic
Professional Associations & Certification
Government
SECURITY CONFERENCES
ANALYST HOUSES

Designing for failure – the mindshift

THEN

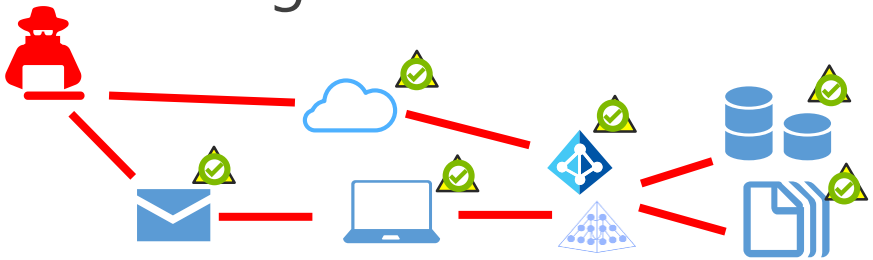
Reliability: Designed not to fail

Prevent: Every possible attack

NOW

Resilience: Designed to recover quickly

Assume Compromise: Protect, Detect, & Respond along the kill chain



Zero trust networking

Offensive Security Research

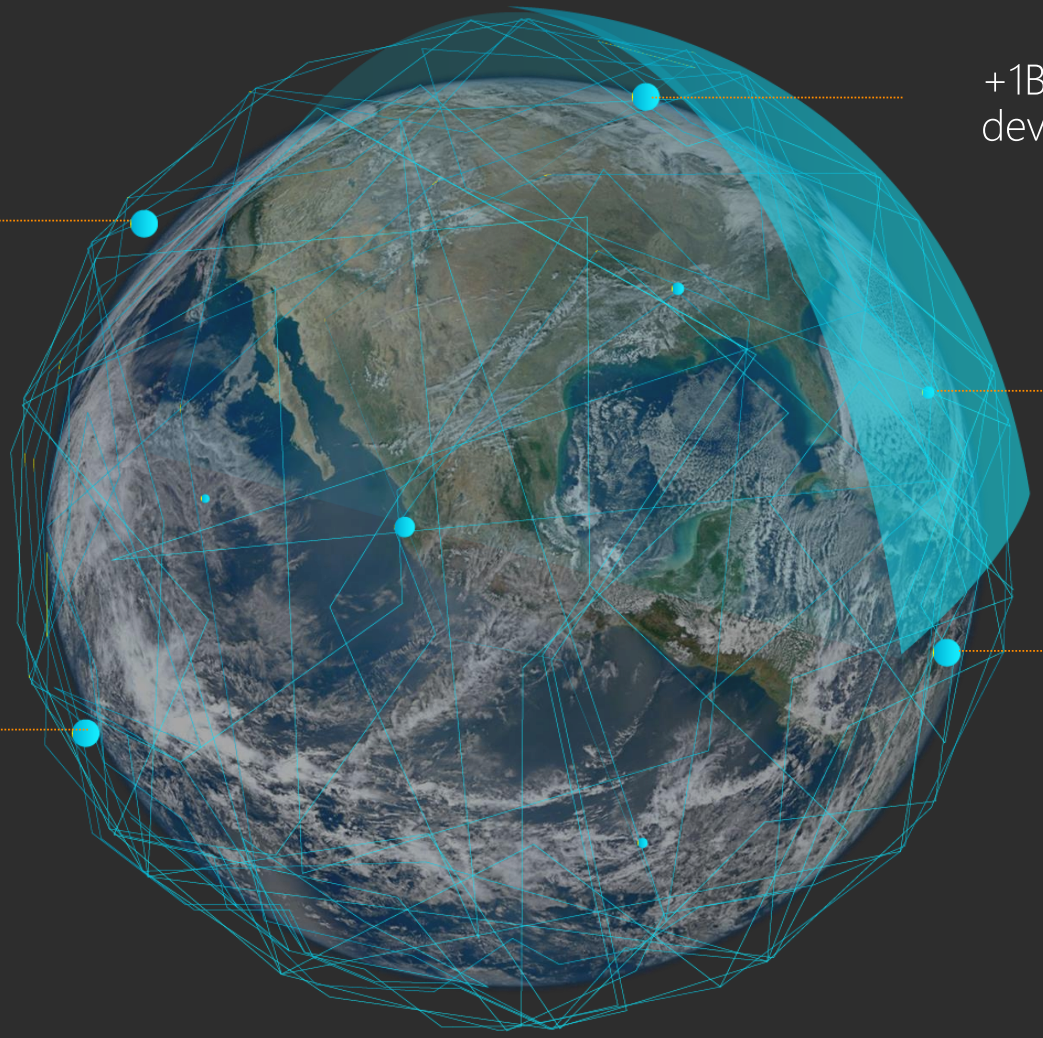
MICROSOFT OFFENSIVE SECURITY RESEARCH

in Azure Active Directory, Azure Information Protection, Microsoft 365, Windows Defender Advanced Threat Protection, Identity and Access Management, Security Management, Security Strategies, Threat Protection, Best Practices and How-Tos, Industry Trends

The traditional perimeter-based network defense is obsolete. Perimeter-based networks operate on the assumption that all systems within a network can be trusted. However, today's increasingly mobile workforce, the migration towards public cloud services, and the adoption of Bring Your Own Device (BYOD) model make perimeter security controls irrelevant. Networks that fail to evolve from traditional defenses are vulnerable to breaches: an attacker can compromise a single endpoint within the trusted boundary and then quickly expand foothold across the entire network.

personnel files of almost 22 million people who had undergone background investigations.

THE MICROSOFT **INTELLIGENT SECURITY GRAPH**



+1B Windows devices updated

200+ global cloud consumer and commercial services

300B monthly authentications

18+ billion Bing web pages scanned

200B e-mails analyzed

Data-driven security insights

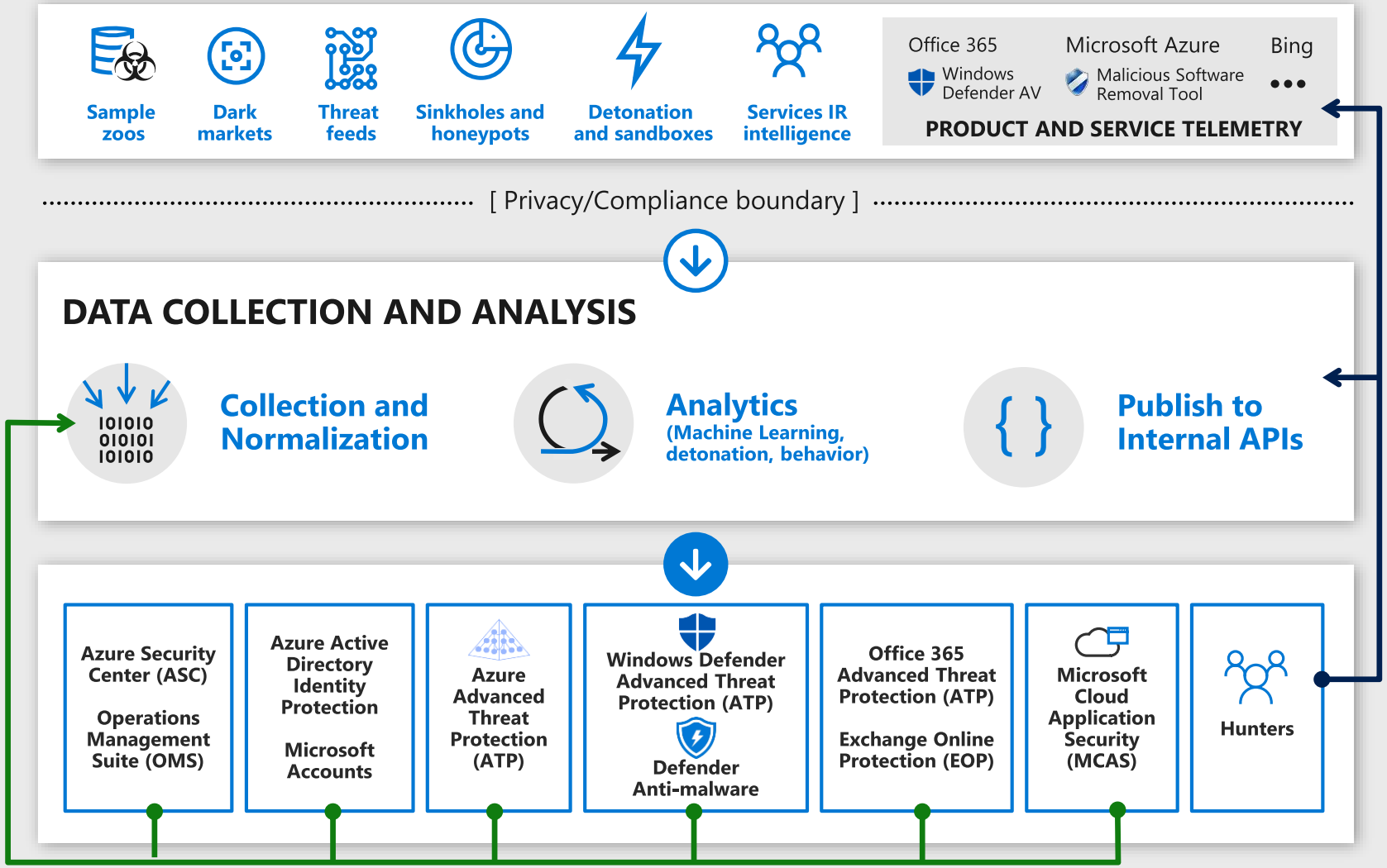
Machine Learning

Intelligent Automation

Cloud Scale

Data-driven security insights

Inside The Intelligent Security Graph



- Products instrumented to strict privacy/compliance standards
  See Microsoft Trust Center
- Analytics help fuel new discoveries
- Products send data to graph
- Products use Interflow APIs to access results
- Products generate data which feeds back into the graph
- Hunters identify attacks, improve analytics, feed back into product design

Home
Alerts
Monitoring & reports
Secure score
Hunting
Classification
Policies
Permissions
More resources

Prevent

Microsoft Secure Score

Total score: 179/555

This score reflects the collective security state of your identities, data, devices, apps, and infrastructure.

Updated 10/02/2018

Identity	77 / 224
Data	46 / 116
Device	36 / 195
App	20 / 20
Infrastructure	No data available

Improve your score | View history

Identity protection

54 users at risk

Updated 12/31/2018

High risk | Medium risk | Low risk

View all users

Device compliance

35% devices noncompli...

Intune device compliance status

Noncompliant | In grace period
Compliant | Not evaluated

See compliance issues

Cloud App Security - OAuth apps

248 privileged apps

Apps that users gave permissions to. Discovered by Cloud App Security

Updated 6:20 pm today

High | Medium | Low

App	Permission level
Boomerang	High
Yesware email tracking	High
Jira for Outlook	High
Pickit Free Images	Medium
officeatwork Template Chooser	Medium
MyScript Math Sample	Medium

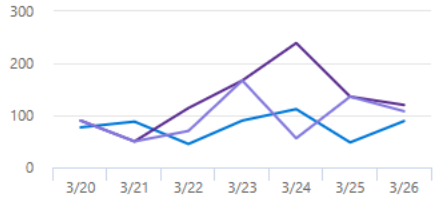
Show more

Device malware detections

15 unresolved malware

Active | Action failed | Allowed
Not executed

DLP policy matches



PCI Data Security Standard (PCI DSS)
U.S. Health Insurance Portability and Accountability ...
General Data Protection Regulation (GDPR)

Infrastructure protection overview

80% subscriptions cove...

138 resources protected by Azure Security Center

44 unhealthy resources	6 minutes ago
2 attacked resources	6 minutes ago

Microsoft Threat Protection

Need help? | Feedback

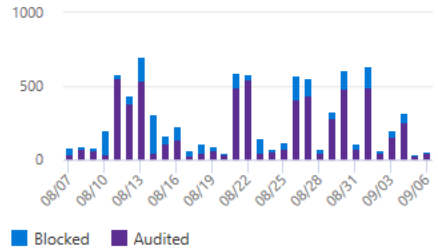
Home
Alerts
Monitoring & reports
Secure score
Hunting
Classification
Policies
Permissions
More resources

Attack surface reduction rule detections

Possible malware or breach activity on your devices

8.3k detections
145 unique files
6k affected devices

Detections over time



View detections | Add exclusions

Attack surface reduction rules

28% devices use ASR rules to block threats

Configuration for behaviorial rules from Windows Defender ATP that reduce the attack surface of your devices

Block mode | Audit mode | Off

Device settings by rule

Block executable content from email client and webmail	Block all Office applications from creating child processes
Block Office applications from creating executable content	Block Office applications from injecting code into other pr...
Block JavaScript or VBScript from launching downloaded e...	Block execution of potentially obfuscated scripts
Block Win32 API calls from Office macro	Block executable files from running unless they meet a pre...
Use advanced protection against ransomware	Block credential stealing from the Windows local security a...
Block process creations originating from PSExec and WMI ...	Block untrusted and unsigned processes that run from USB
Block Office communication application from creating chil...	Block Adobe Reader from creating child processes

Block mode | Audit mode | Off

View detections | Manage configuration

Device protection

34 devices at risk

Device	Risk level
tocohen1	High
tocohen2	Moderate
tocohen3	Low
tocohen4	High
tocohen5	High
tocohen6	High
tocohen7	High
tocohen8	High
tocohen9	High

View details

Device threat analytics

Assess your defenses against high-profile threats

Get interactive reports on Windows Defender ATP about emerging threats and outbreaks. Assess the impact on your network, contain active threats, and improve organizational resilience.

View threat analytics

GADOLINIUM / FoggyBrass	12 / 16
Dofoil / CoinMiner	10 / 13
Zacinlo(Detrahere)	1 / 7
EternalBlue endures	2 / 4
Emotet distributes Trickbot	3 / 3

Device compliance

35% devices noncompli...

Intune device compliance status

Noncompliant | In grace period
Compliant | Not evaluated

See compliance issues

Device malware detections

15 unresolved malware

Active | Action failed | Allowed
Not executed

Types of malware on devices

Malware on devices

Devices with malware detections

Users with malware

Need help? | Feedback

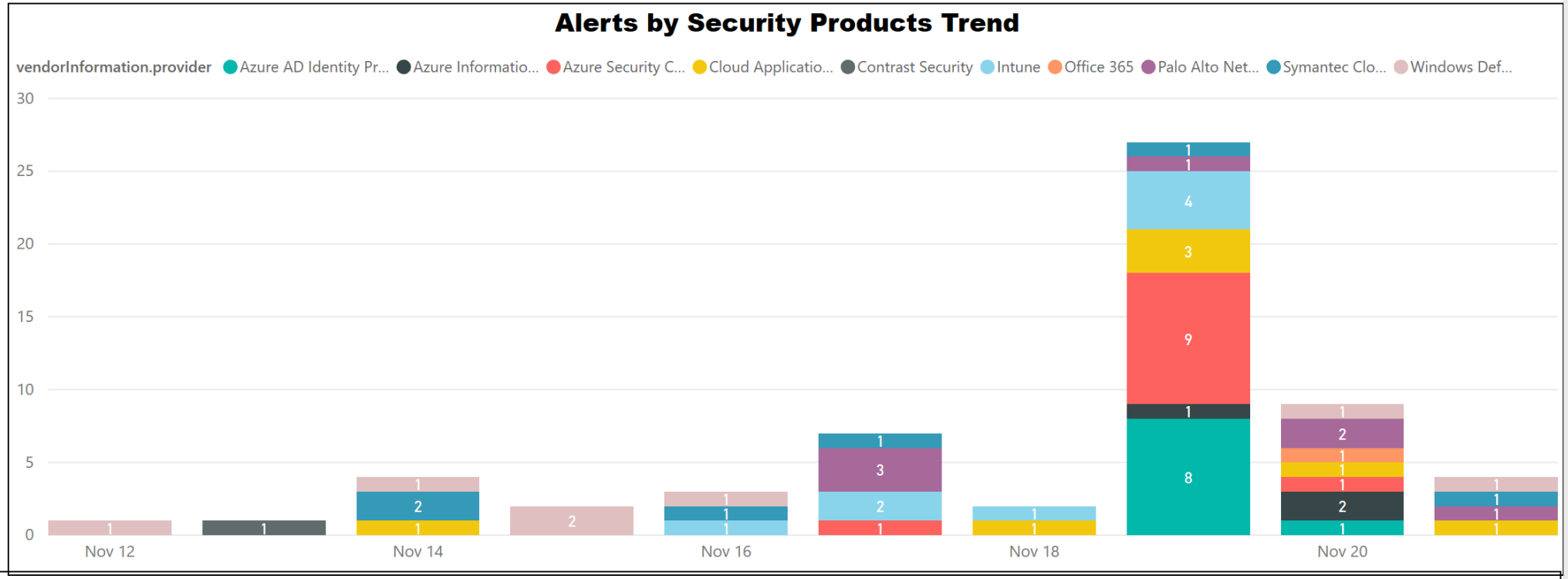
70

Count of id

eventDateTime

Last 6 Months

8/27/2018 - 2/26/2019

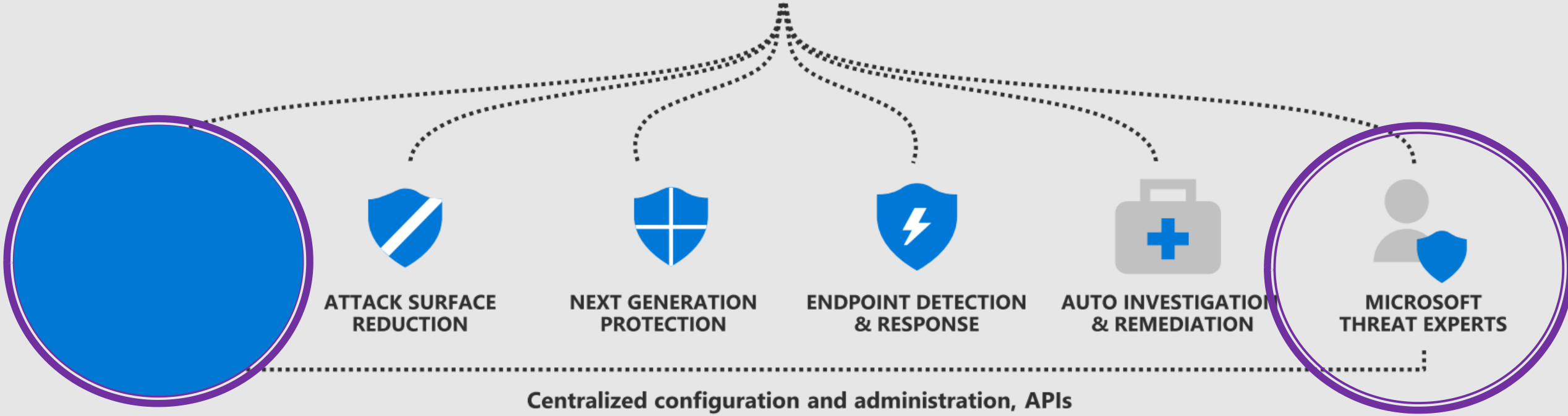


eventDateTime	createdDateTime	Delay (hrs)	vendorInformation.provider	id	category	title	description
11/21/2018 9:09:32 PM	11/21/2018 9:09:32 PM	0.00	Symantec Cloud Workload Protection	5F637F63-1BAA-4F6A-A2C8-31AA81C087F4	MONITORING	Unsecured Instances Detected	Agent is not yet installec
11/21/2018 3:31:00 PM	11/21/2018 9:14:09 AM	-6.28	Windows Defender ATP	EF76CDE9-C3C4-4A83-9707-9EF003C379BB	Social Engineering	Right-to-Left-Override (RLO) technique observed	Attackers can implant th used for hiding purpose
11/21/2018 1:34:00 PM	11/21/2018 2:33:00 PM	0.98	Cloud Application Security	E21C584F-EA0B-34D9-8DD6-4DABF442A232	repeatedShareActivity	Mass share	The user "Douglas Fife@
11/21/2018 10:16:36 AM	11/21/2018 10:16:36 AM	0.00	Palo Alto Networks	53C7E3B0-8470-424C-BD40-2C9C3F9EFB81	data	Data Filtering Alert	Data Filtering Alert: Docu
11/20/2018 10:07:37 PM	11/20/2018 10:07:37 PM	0.00	Illumio VEN	41CB1B5D-F295-40B3-8B18-DFC4AA85531E	blockedTraffic	Blocked Traffic	Traffic blocked by the de
11/20/2018 10:02:38 PM	11/20/2018 10:02:38 PM	0.00	Illumio VEN	27F4011B-1E2B-43FC-B7DA-53E79785D9D5	blockedTraffic	Blocked Traffic	Traffic blocked by the de
11/20/2018 10:02:37 PM	11/20/2018 10:02:37 PM	0.00	Illumio	93619956-A013-44FE-8BB5-AFED47BBF654	unauthorizedAccess	User Authentication Failed	multiple failed login atte

Alerts by Security Products Trend | Alerts by Security Categories Trend | Alert - Slicers

Windows Defender
Advanced Threat Protection

Built-in. Cloud-powered.



Threat and Vulnerability Manag

https://securitycenter.windows.com/tvm_dashboard

Windows Defender Security Center

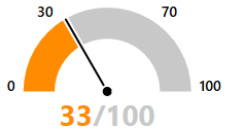
Search (File, IP, URL, Machine, User)

Threat & Vulnerability Management dashboard

Organization exposure score

Exposure score

This score reflects the current exposure associated with machines in your organization



Low 0-29 Medium 30-69 High 70-100

WDATP configuration score

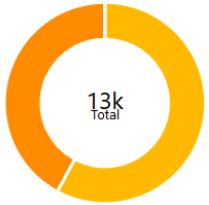
Configuration score: 522/690

This score reflects the collective security configuration posture of your machines across OS, Application, Network, Accounts and Security Controls

Application	63/148
OS	149/183
Network	52/64
Accounts	7/12
Security controls	251/283

Machine exposure distribution

Exposure distribution



High Medium Low

Top vulnerable software

Software	Weaknesses	Threats	Exposed machines
Windows 10	372		8.56k / 13k
Internet Explorer	113		8.56k / 13k
Edge	211		8.56k / 13k

Show more

Top exposed machines

Name	Exposure level
[redacted]	High
	High
	High

Show more

Top remediation activities

There are no active remediation activities.

Top security recommendations 8/97

Based on highest organizational exposure impact

Update Windows 10
8.56k Exposed machines
20.73 Software patch

Update Office
1.35k Exposed machines
3.86 Software patch

Turn on Attack Surface Reduction rules
13k Exposed machines
2.93 | 8.99 Configuration change

Turn on Application Guard
13k Exposed machines
2.87 | 8.99 Configuration change

Disable 'Domain controller: Allow server ...
13k Exposed machines
2.63 | 8.00 Configuration change

Enable 'Local Security Authority (LSA) pr...
13k Exposed machines
2.63 | 8.00 Configuration change

Set User Account Control (UAC) to autom...
13k Exposed machines
2.63 | 8.00 Configuration change

Disable 'Local Machine Run-Once'
13k Exposed machines
1.64 | 5.00 Configuration change

Show more

Targeted Attack Behaviors and Data Exfiltration Observed

This alert is part of incident (9724) Threat Experts

Automated investigation is not applicable to alert type

Actions

Severity: High
Category: Suspicious Activity
Detection source: Threat experts

Alert context

contoso\omkantor

First activity: 01.17.2019 | 13:55:26
Last activity: 01.17.2019 | 13:55:26

Status

State: Resolved
Classification: Not set

Assigned to: analyst@contoso.com

Description

Executive Summary

An advanced attack initiated from a successful phishing email launched by a user has been observed on two machines within your organization. From our preliminary investigation, two users opened emails with a malicious PDF file that caused the default browser to navigate to a malicious domain that then created a decoy PDF and a malicious DLL, which then communicated to a command and control server.

We recommend further investigation and actions be taken immediately in response to this threat.

Timeline of Observed Events

A breakdown of key events from the attack on the compromised machines is as follows:

1. (11/14/2018 9:59 AM UTC) User opened email in Outlook that contained the malicious PDF, which then causes the default browser to connect to a malicious domain and makes the browser create a .LNK and .ZIP file.
2. (11/14/2018 9:59 AM UTC) PowerShell opens the LNK and then creates the malicious payload utilizing Cobalt Strike, cyzfc.dat. PowerShell also creates a decoy PDF with the same name as the one opened in the email and launches it in AcroRd32.exe to make the user believe that the PDF was opened as expected.
3. (11/14/2018 9:59 AM UTC) PowerShell launches rundll32.exe which loads the cyzfc.dat payload, which connected to a malicious command and control server on port 443.

Recommended actions

Queries

This query will surface the compromised user for easier investigation on the entry point machine

```
ProcessCreationEvents | where EventTime between (datetime(11/14/2018 09:59:05)..datetime(11/14/2018 09:59:06)) and MachineId == "0b8b67d65e2912ac569894180dc82d3805880bd7"
| project AccountSid
```

Alert process tree

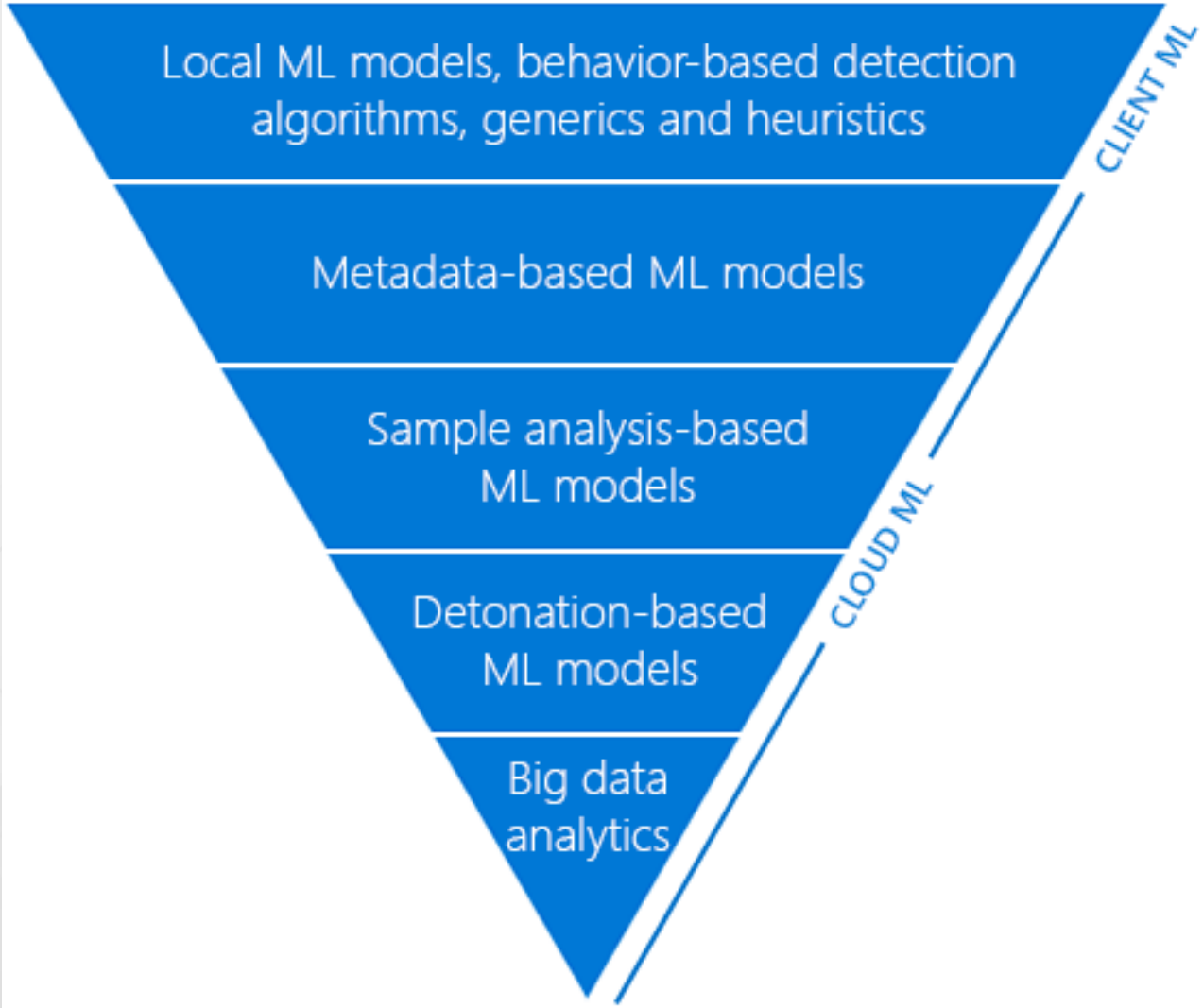
wininit.exe
services.exe

Data-driven security insights

Enable you to continuously improve your security posture by decreasing attack surface in a very targeted way

Machine learning

Application of layered ML defenses (EPP example)



Protection in milliseconds
Most common malware are blocked by high-precision detection in Windows Defender AV

Protection in milliseconds
ML-powered cloud rules evaluate suspicious files based on metadata sent by the Windows Defender AV client during query

Protection in seconds
A copy of the suspicious file is uploaded for inspection by multi-class ML classifiers

Protection in minutes
The suspicious file is executed in a sandbox for dynamic analysis by multi-class ML classifiers

Protection in hours
ML models and expert rules correlated signals from a vast network of sensors to automatically classify threats

win7fork12v9v3

Actions

Domain: kurosuke-coins.net
OS: Windows7 32-bit (Build 7601)
Machine IP addresses

Logged on users (last 30 days)

0

Interactive [0]
RemoteInteractive [0]
Other [0]

Medium Risk

Active alerts:

0	1	1	0
High	Medium	Low	Informational

Machine not found in Azure ATP

Machine reporting

First seen: 5 months ago
Last seen: a month ago

Alerts related to this machine

Last activity	Title	User	Severity	Status	Investigation State	Assigned to
12.17.2018 | 01:37:23	Suspicious sequence of exploration activities Reconnaissance		Low	New	Unsupported Alert Type	Not assigned
10.29.2018 | 10:38:36	Suspected credential theft activity Credential Stealing	kurosuke-coins.net\testuser1	Medium	New	Unsupported OS	Not assigned

Machine timeline

Value: Search in machine timeline
Information level: All
Event type: All
User account: All
Remove all filters

01.18.2019 | 18:54

Sep 2018 | Oct 2018 | Nov 2018 | Dec 2018 | Jan 2019 | Feb 2019 | Today

Export | 20 events per page | Older | Newer

Date	Event	Details	User
01.18.2019			
18:54:34	MsSenseS.exe loaded module Microsoft.VisualStudio.Tools.Applications.Hosting.v9.0.resources.dll	MonitoringHost.exe > MsSenseS.exe > Microsoft.VisualStudio.Tools.Applications.Hosting.v9.0.resources.dll	system
18:54:33	MsSenseS.exe loaded module Microsoft.VisualStudio.Tools.Applications.ServerDocument.v9.0.resources.dll	MonitoringHost.exe > MsSenseS.exe > Microsoft.VisualStudio.Tools.Applications.ServerDocument.v9.0.resources.dll	system
18:54:33	MsSenseS.exe loaded module Microsoft.VisualStudio.Tools.Applications.Adapter.v9.0.resources.dll	MonitoringHost.exe > MsSenseS.exe > Microsoft.VisualStudio.Tools.Applications.Adapter.v9.0.resources.dll	system
18:54:25	MsSenseS.exe loaded module Microsoft.Office.Tools.Common.v9.0.dll	MonitoringHost.exe > MsSenseS.exe > Microsoft.Office.Tools.Common.v9.	system

Security Center - Overview

Showing subscription 'Microsoft Azure Internal - Demo'

Search (Ctrl+/)

GENERAL
- Overview
- Getting started
- Events
- Search

POLICY & COMPLIANCE
- Coverage
- Secure score
- Security policy
- Regulatory Compliance (Prev...

RESOURCE SECURITY HYGIENE
- Recommendations
- Compute & apps
- Networking
- Data & storage
- Identity & access (Preview)
- Security solutions

ADVANCED CLOUD DEFENSE
- Adaptive application controls
- Just in time VM access
- File Integrity Monitoring

Subscriptions

Policy & compliance

Secure score

525 OF 845

Review your secure score >

Least compliant regulatory standards

SOC TSP	4 of 13 passed rules
ISO 27001	8 of 23 passed rules
Azure CIS	7 of 19 passed rules

Subscription coverage

1 TOTAL

Fully covered 0
Partially covered 1
Not covered 0

28 Covered resources

Make alert data available to your

You can make Security Cent connector

Set up SIEM connector >

Resource security hygiene

Recommendations

15 TOTAL

High Severity 9
Medium Severity 3
Low Severity 3

28 Unhealthy resources

Resource health monitoring

14 Compute & apps
3 Data & storage
10 Networking
1 Identity & access

Review and improve your secure s

Review and resolve security secure score and secure you

Learn more >

Threat protection

Security alerts by severity

13 TOTAL

High Severity 0
Medium Severity 13

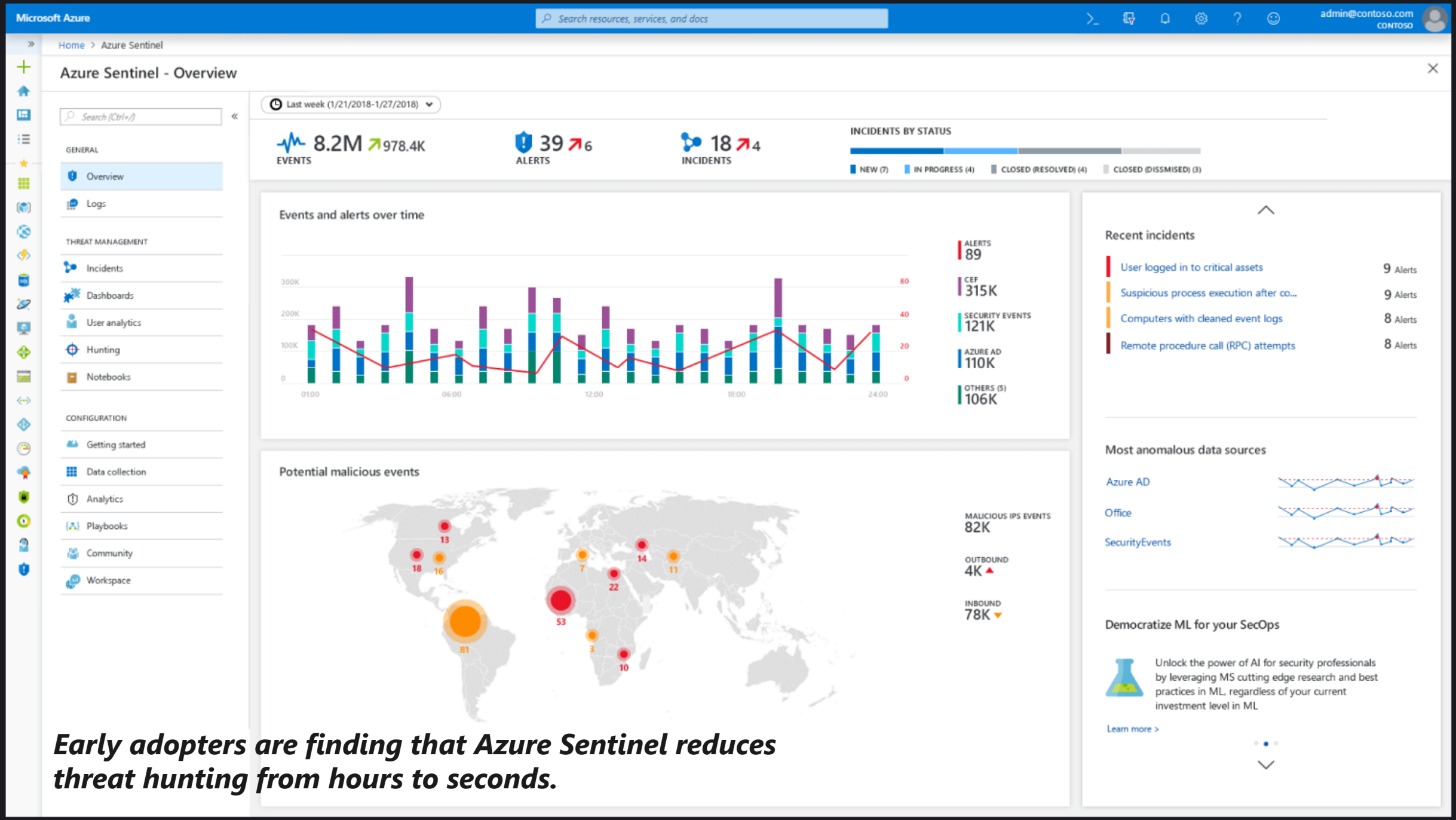
Security alerts over time

4
2
0

High severity 0
Medium severity 13

Most attacked resources

srv-web001
srv-web002



Early adopters are finding that Azure Sentinel reduces threat hunting from hours to seconds.

Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML

Learn more >

Machine learning

Helps protect you by looking for and protecting against what you cannot see

Intelligent automation

A malicious file was found on your machine

Investigation #9 is complete - Remediated

Started
Sep 7, 2018, 9:21:00 AM
Ended
Sep 7, 2018, 9:51:15 AM
Total pending time: 12s

00:30:15
Complete

Comments (0)

Investigation details

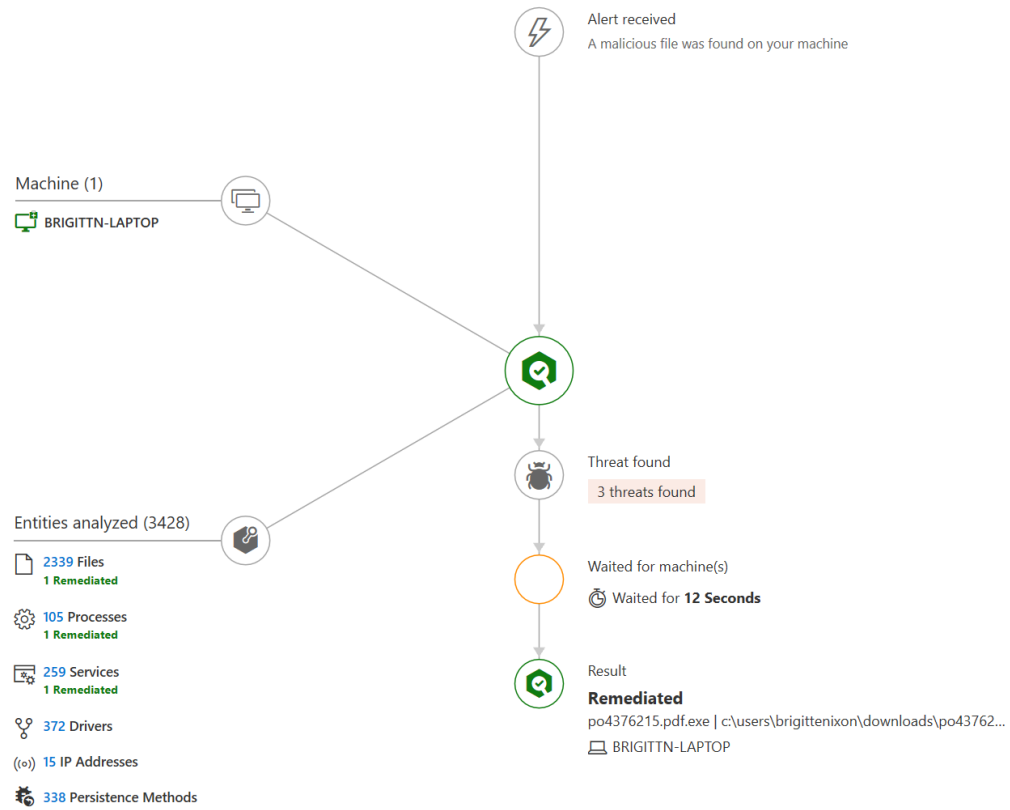
Status
Remediated
Malicious entities found were successfully re mediated.

Alert severity
High

Category
Malware

Detection source
EDR

Investigation graph | Alerts (1) | Machines (1) | Key findings (3) | Entities (3.43k) | Log (43)



Admin Center | Security and Compliance | Windows Defender Securit

https://protection.office.com

Office 365 | Security and Compliance

- Home
- Alerts
- Permissions
- Classifications
- Data loss prevention
- Data governance
- Threat Intelligence
  - Dashboard
  - Investigations
  - Users at risk
  - Attack Simulator
  - Explorer
  - Alerts
  - Threat tracker
- Mail flow
- Search and investigation
- Reports
- Service assurance

Home > Investigations > 11371

Weaponized URL in mail discovered by Office 365 ATP

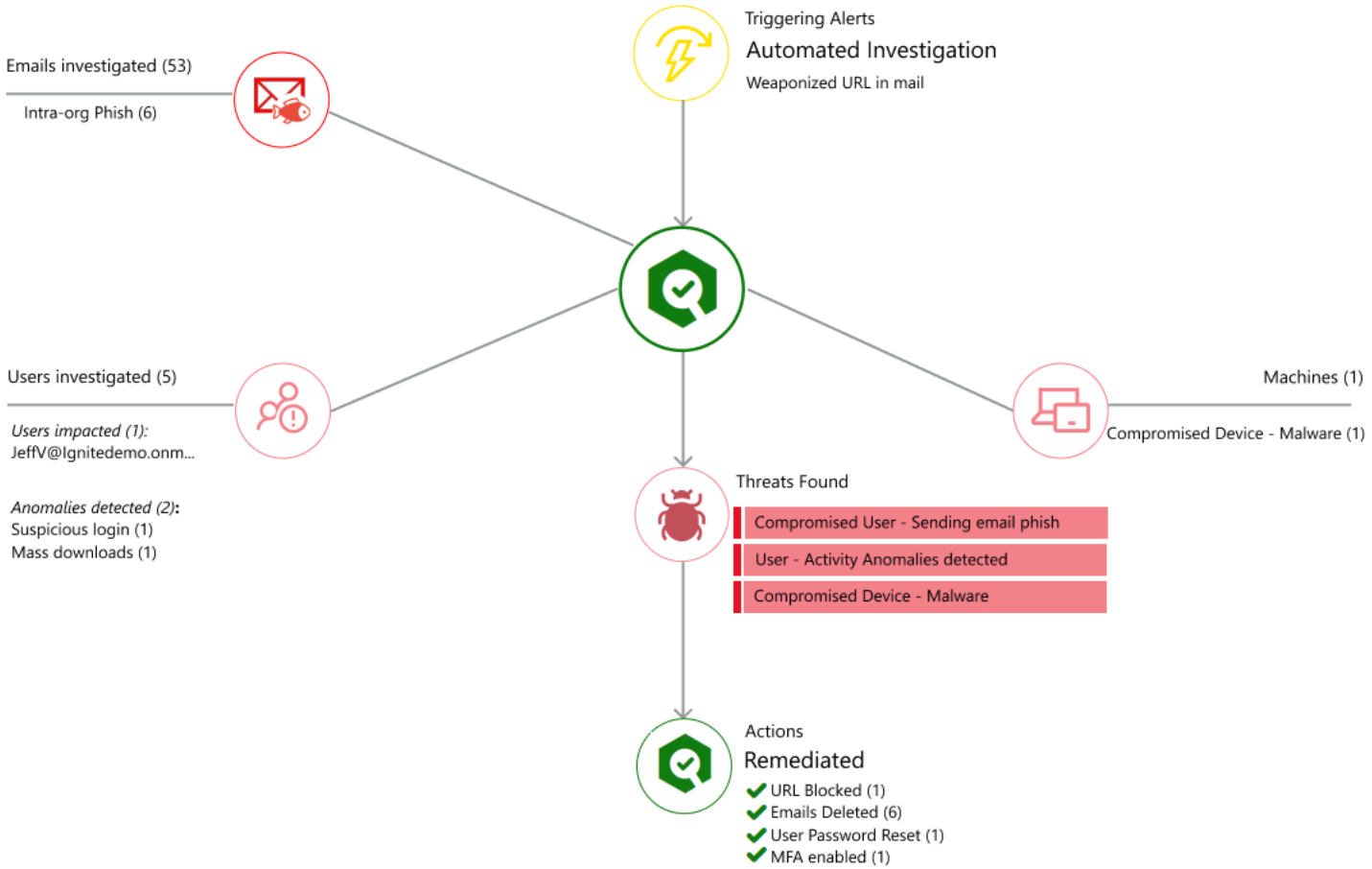
Investigation #11371 is complete - Remediated

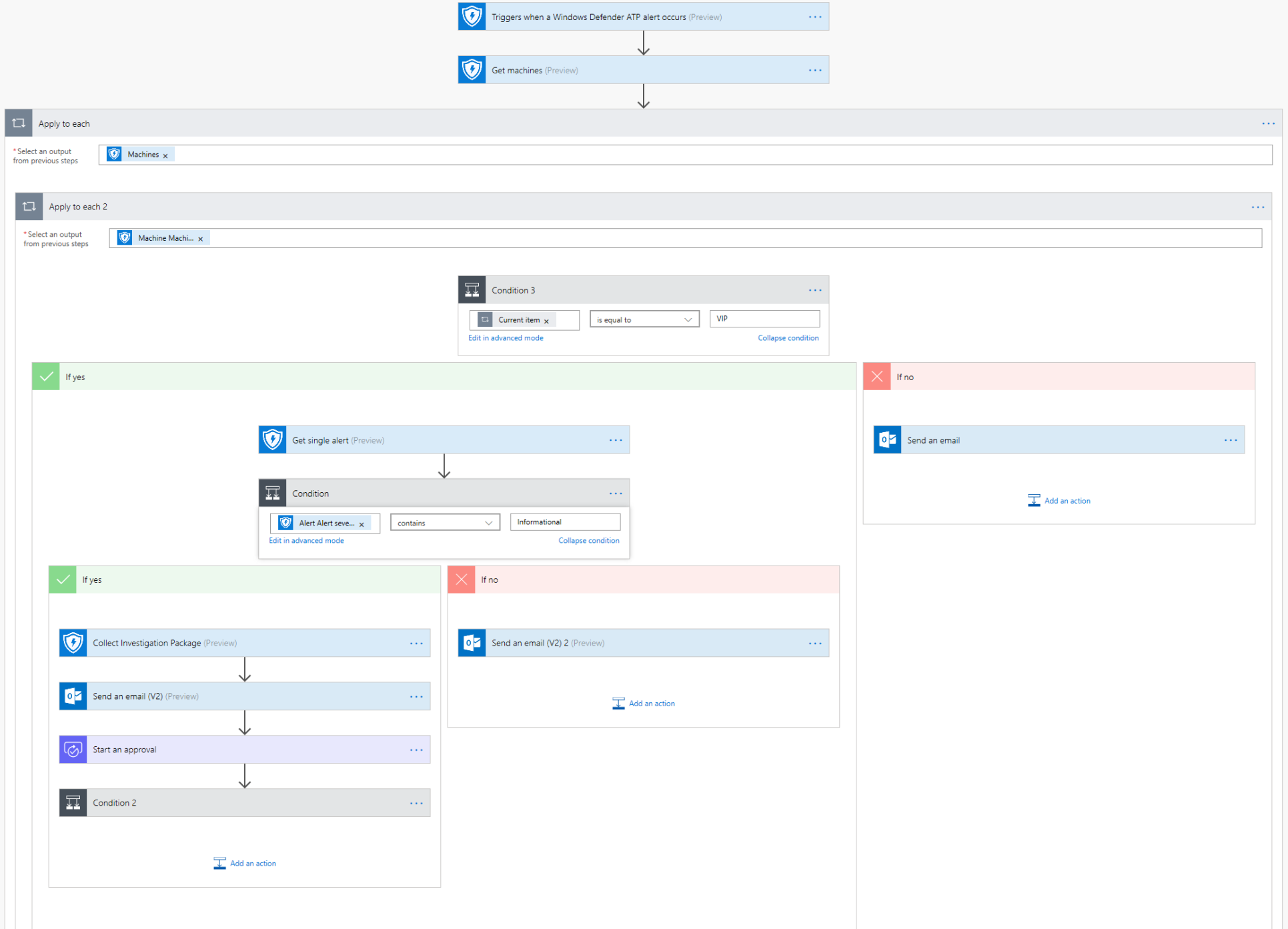
Started
Sep 19, 2018, 4:53:09 PM

Ended
Sep 19, 2018, 5:05:15 PM

0:12:06
Complete

Investigation graph | Alerts | Email | Users | Machines | Entities | Log | Actions

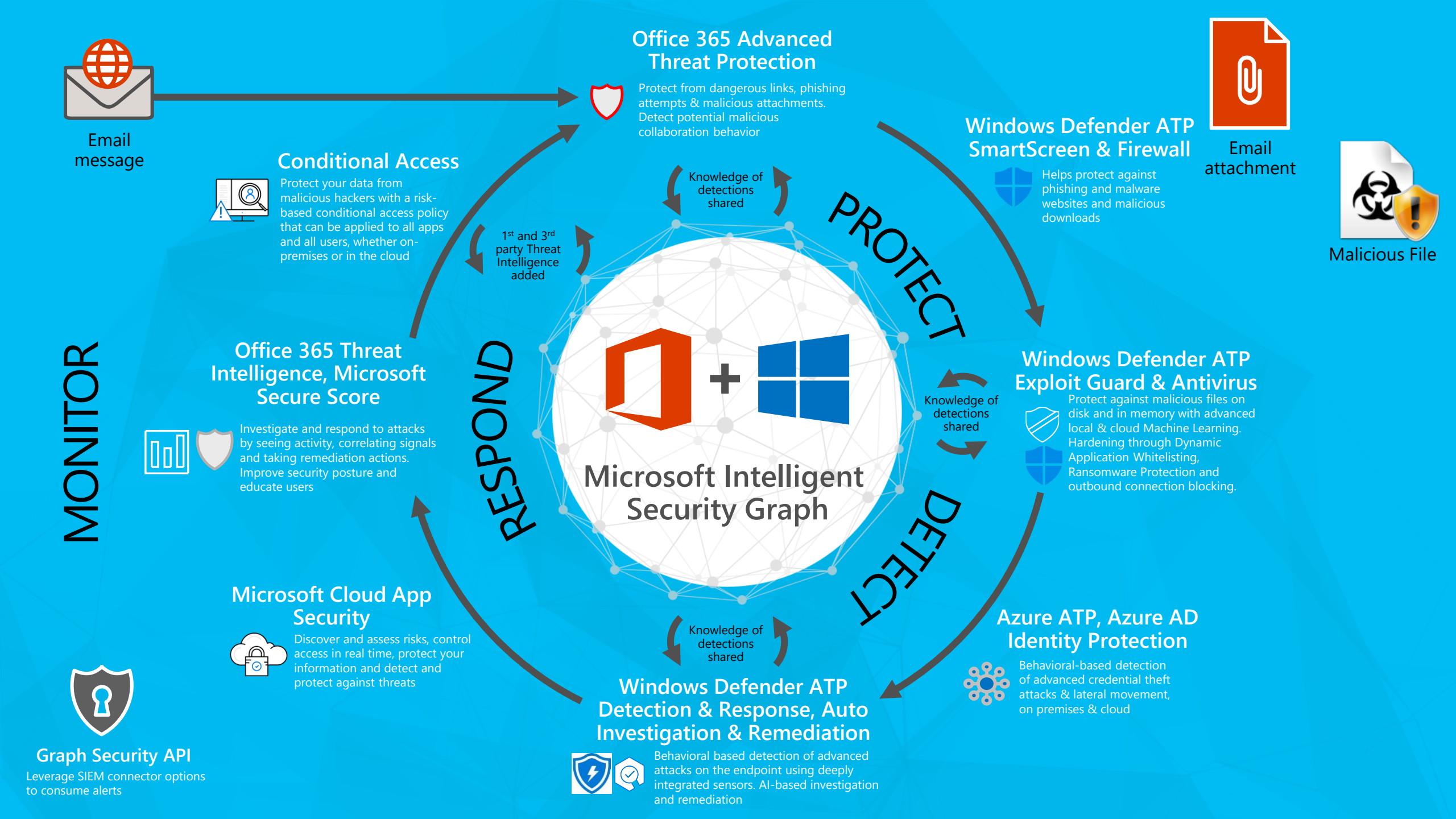


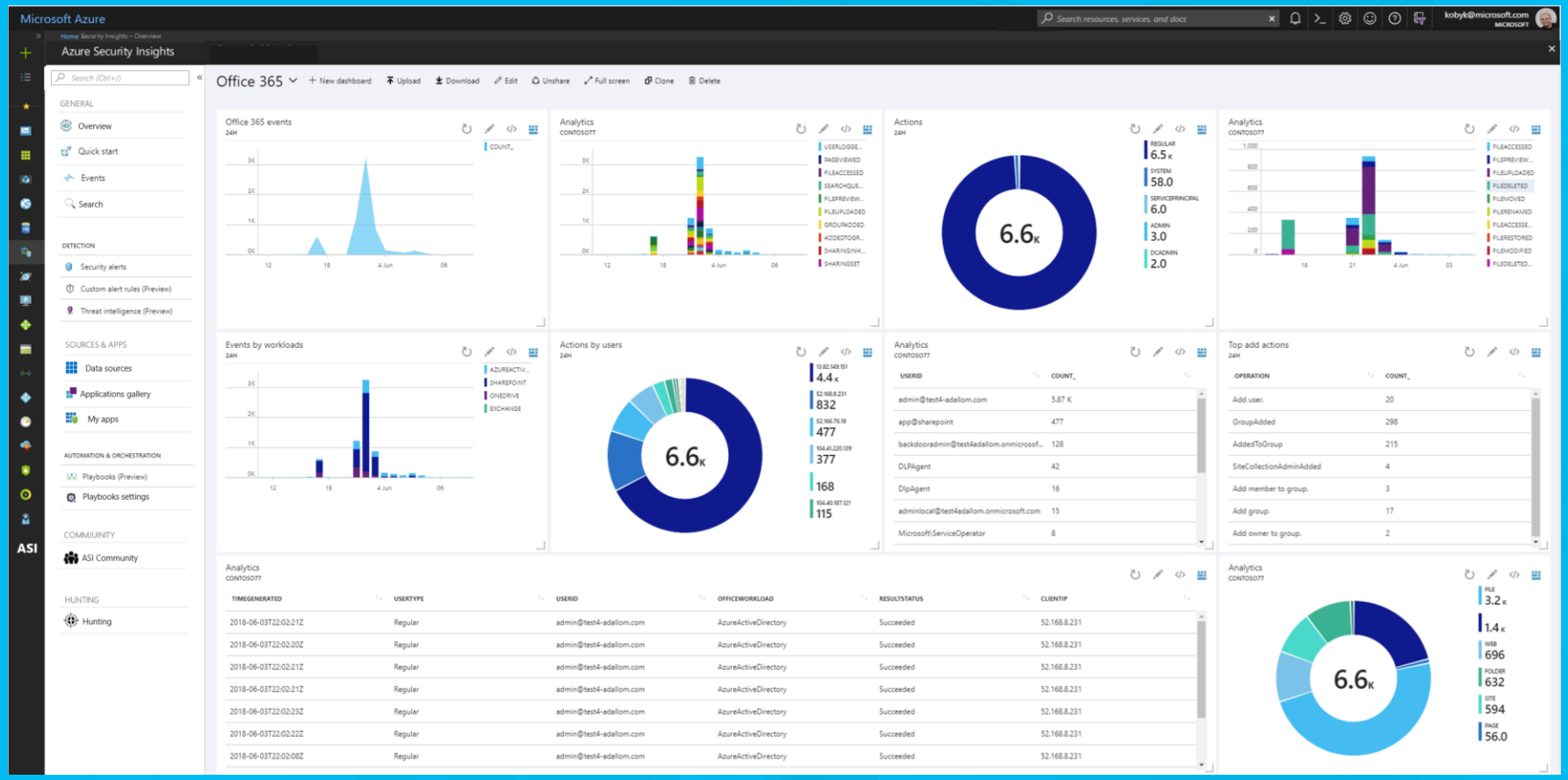

Triggers when a Windows Defender ATP alert occurs (Preview)
Get machines (Preview)
Apply to each
*Select an output from previous steps
Machines
Apply to each 2
*Select an output from previous steps
Machine Machi...
Condition 3
Current item
is equal to
VIP
Edit in advanced mode
Collapse condition
If yes
If no
Get single alert (Preview)
Condition
Alert Alert seve...
contains
Informational
Edit in advanced mode
Collapse condition
Send an email
Add an action
If yes
If no
Collect Investigation Package (Preview)
Send an email (V2) (Preview)
Start an approval
Condition 2
Send an email (V2) 2 (Preview)
Add an action
Add an action

Intelligent automation

Get you to the right conclusion faster, and helps you respond & recover quickly

Leveraging cloud scale


Email message
Office 365 Advanced Threat Protection
Protect from dangerous links, phishing attempts & malicious attachments. Detect potential malicious collaboration behavior
Email attachment
Malicious File
Windows Defender ATP SmartScreen & Firewall
Helps protect against phishing and malware websites and malicious downloads
Conditional Access
Protect your data from malicious hackers with a risk-based conditional access policy that can be applied to all apps and all users, whether on-premises or in the cloud
Knowledge of detections shared
1st and 3rd party Threat Intelligence added
PROTECT
DETECT
RESPOND
MONITOR
Microsoft Intelligent Security Graph
Knowledge of detections shared
Windows Defender ATP Exploit Guard & Antivirus
Protect against malicious files on disk and in memory with advanced local & cloud Machine Learning. Hardening through Dynamic Application Whitelisting, Ransomware Protection and outbound connection blocking.
Office 365 Threat Intelligence, Microsoft Secure Score
Investigate and respond to attacks by seeing activity, correlating signals and taking remediation actions. Improve security posture and educate users
Microsoft Cloud App Security
Discover and assess risks, control access in real time, protect your information and detect and protect against threats
Knowledge of detections shared
Azure ATP, Azure AD Identity Protection
Behavioral-based detection of advanced credential theft attacks & lateral movement, on premises & cloud
Windows Defender ATP Detection & Response, Auto Investigation & Remediation
Behavioral based detection of advanced attacks on the endpoint using deeply integrated sensors. AI-based investigation and remediation
Graph Security API
Leverage SIEM connector options to consume alerts



MONITOR?

SIEM

Security Incident Event Management

- Analytics
- Correlation
- Categorization
- Normalizing

SOAR!

Azure Sentinel

Security Orchestration, Automation & Response

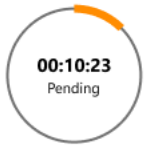
- Cloud born SIEM
- Better Integration
- Graph API based
- Fast Analytics
- Security Data Lake
- No Data on prem
- Workflow automation

Home
Alerts
Permissions
Classifications
Data loss prevention
Data governance
Threat Intelligence
Dashboard
Investigations
Users at risk
Attack Simulator
Explorer
Alerts
Threat tracker
Mail flow
Search and investigation
Reports
Service assurance

Malicious mail detected and removed by Office 365

Investigation #50ecc9 is pending action

Started
9/15/2017 12:46 PM



Pending time - 10 min

Investigation graph | Alerts (5) | **Email (23)** | Users (5) | Machines (2) | Entities (40) | Log (14) | Actions (13)

Export | Column options | Filter

The investigation has extracted different data from the original mail, then used this to find other email that have the same attributes.
- Distinct entities like files and URLs are investigated in detail and used to find indicators. Clusters that contain the same URL or file are called 'Indicator clusters' and get the verdict of the original file or URL.
- Source attributes like the sender, sending IP, body fingerprint and other items are used to emails that are similar. These similarity clusters are investigated and get the verdict based on threats detected on any of the similar emails.

View metadata for the original email that triggered the alert

Cluster	Value	Investigation Verdict	Threats/risks found	Recommended Action	Submissions	Delivery Verdict			Original Delivery Status				
						Total	Malware	Phish	Delivered	Zapped	Junked	Replaced	Blocked
URL	www.badsite.com	Phish	Phish URL Malicious URL clicks	Delete	0	6	-	-	6	-	-	-	-
IP, Sender	36.1.1.5 joe@gmall.com	Suspicious	Sender impersonation	Junk	0	10	-	1	9	-	-	-	1
Sender, Subject	joe@gmall.com, Negative Uber feedback received	Phish	Volume anomaly Sender impersonation	Delete	0	26	-	1	20	-	5	1	-

Admin Center | Security and Compliance | Windows Defender Securit

https://protection.office.com

Office 365 | Security and Compliance

- Home
- Alerts
- Permissions
- Classifications
- Data loss prevention
- Data governance
- Threat Intelligence
  - Dashboard
  - Investigations
  - Users at risk
  - Attack Simulator
  - Explorer
  - Alerts
  - Threat tracker
- Mail flow
- Search and investigation
- Reports
- Service assurance

Home > Investigations > 50ecc9

Malicious mail detected and removed by Office 365

Investigation #50ecc9 is pending action

Started
9/15/2017 12:46 PM

00:00:23
Pending

Pending time - 10 min

Investigation graph | Alerts (5) | Email (23) | **Users (5)** | Machines (2) | Entities (40) | Log (14) | Actions (13)

Export | Column options | Filter

Users	Risk Level	Risk Indicators	Risky Activities	Service
JeffV@Ignitedemo.onmicro...	High	Compromised user - phishing URL clicked User activity anomalies detected - suspicous login Exchange Web Service enabled Creation of mail forwarding rules	4	Exchange Online
RonH@Ignitedemo.onmicro...	High	Compromised user - phishing URL block override User activity anomalies detected - mass download Mail delegation enabled	3	Exchange Online SharePoint Online Exchange Online
JonD@Ignitedemo.onmicro...	Low	Intra-org email spike	1	Exchange Online
JaneE@Ignitedemo.onmicro...	Low	Clean	-	-
CarlD@Ignitedemo.onmicro...	Low	Clean	-	-

Home
Alerts
Permissions
Classifications
Data loss prevention
Data governance
Threat Intelligence
Dashboard
Investigations
Users at risk
Attack Simulator
Explorer
Alerts
Threat tracker
Mail flow
Search and investigation
Reports
Service assurance

Malicious mail detected and removed by Office 365

Investigation #50ecc9 is pending action

Started
9/15/2017 12:46 PM

00:00:23
Pending

Pending time - 10 min

Investigation graph | Alerts (4) | Emails (23) | Users (5) | Machines (2) | Entities (40) | Log (14) | Actions (13)

Export | Column options | Filter

Action	Description	Entity	Threats	Status	Execution start time	Duration
Email indicators extraction	Extract indicators from header, body and content of the email for investigation	Email	Email - Phish	Completed	09/19/18, 4:53:50 PM	15s
Email cluster identification	Email cluster analysis based on header, body, content and URLs	Email	Email - Malware	Completed	09/19/18, 4:54:52 PM	1:31m
On-demand detonation	On-demand detonation triggered with Office 365 ATP for emails, attachments and URLs	URL	Malicious URL	Completed	09/19/18, 4:55:02 PM	45s
Intra-org/Outbound anomaly investigation	Detect intra-org and outbound malware, phish or spam originating from users in your organization	Email	None	Completed	09/19/18, 4:59:52 PM	3:45m
URL clicks investigation	Investigate clicks from users protected by O365 ATP safe links in your organization.	URL	Phish URL click	Completed	09/19/18, 5:01:52 PM	2:15m
User activity investigation	Analyze user activity anomalies across Azure Active Directory and other Office 365 services including SharePoint, OneDrive, Teams, Yammer and PowerBI, including any detections from Microsoft Cloud App Security	User	Suspicious Login Mass downloads	Completed	09/19/18, 4:59:52 PM	5:24m
Sender domain investigation	On-demand check of domain reputation from Microsoft's ISG and external threat intelligence sources	Domain	Email - Phish	Completed	09/19/18, 4:56:02 PM	35s
Sender IP investigation	On-demand check of IP reputation from Microsoft's ISG and external threat intelligence sources	IP	Email - Phish	Completed	09/19/18, 4:56:02 PM	35s
Mail cluster volume analysis	Email cluster analysis based on outbound mail flow volume patterns	Email	None	Completed	09/19/18, 4:57:52 PM	5:55m
Admin user investigation	Analyze admin permissions and roles assigned to Office 365 user for Security and Compliance Center and Exchange Admin Center	User	None	Completed	09/19/18, 4:59:52 PM	35s
DLP violations investigation	Investigate any violations detected by Office 365 Data Loss Prevention (DLP)	File	Data Exfiltration	Completed	09/19/18, 5:00:52 PM	25s
Mail delegation investigation	Investigate mail delegation access for user mailboxes related to this investigation	User	Compromised user	Completed	09/19/18, 5:01:52 PM	10s
Mail forwarding rules investigation	Investigate any mail forwading rules for user mailboxes related to this investigation	User	Data Exfiltraiton	Completed	09/19/18, 4:59:12 PM	10s
OWA settings investigation	Investigate Outlook Web Access (OWA) configurations for user mailboxes related to this investigation	User	None	Completed	09/19/18, 5:02:52 PM	45s

Leveraging cloud scale

ensures reduced complexity, lower TCO and always enough capacity so you can absorb the blows

Data-driven security insights

continuously improve your security posture

Machine Learning

find and stop what you cannot see

Intelligent Automation

respond & recover - quickly

Cloud Scale

reduced complexity, always enough capacity