

ADACOM

SECURITY
BUILT ON TRUST



CyberSynthGuard: Synthesizing Security through AI-Driven XDR
Brilliance

Security Challenges and Threat Landscape

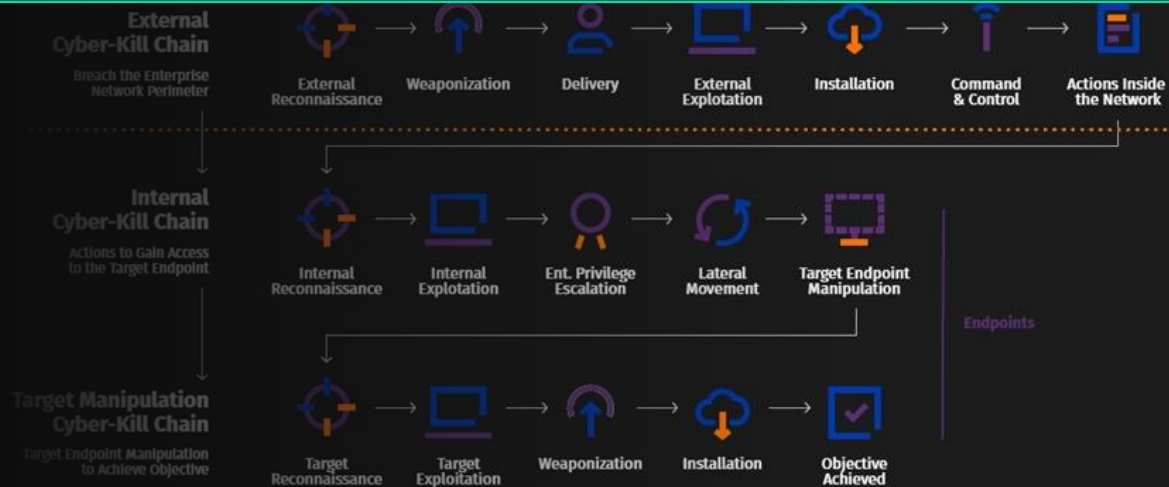





Rise of AI-Directed Cyberattacks

Hackers will use AI to analyze attack strategies, thereby enhancing their likelihood of success. Also, they will use AI to heighten the speed, scale and scope of their activities

Ransomware: Stealthy Exploits and AI Battlefields





Vulnerabilities
continue to expand



Phishing attacks based on
AI continue to plague
businesses



Supply Chain and critical infrastructure attacks

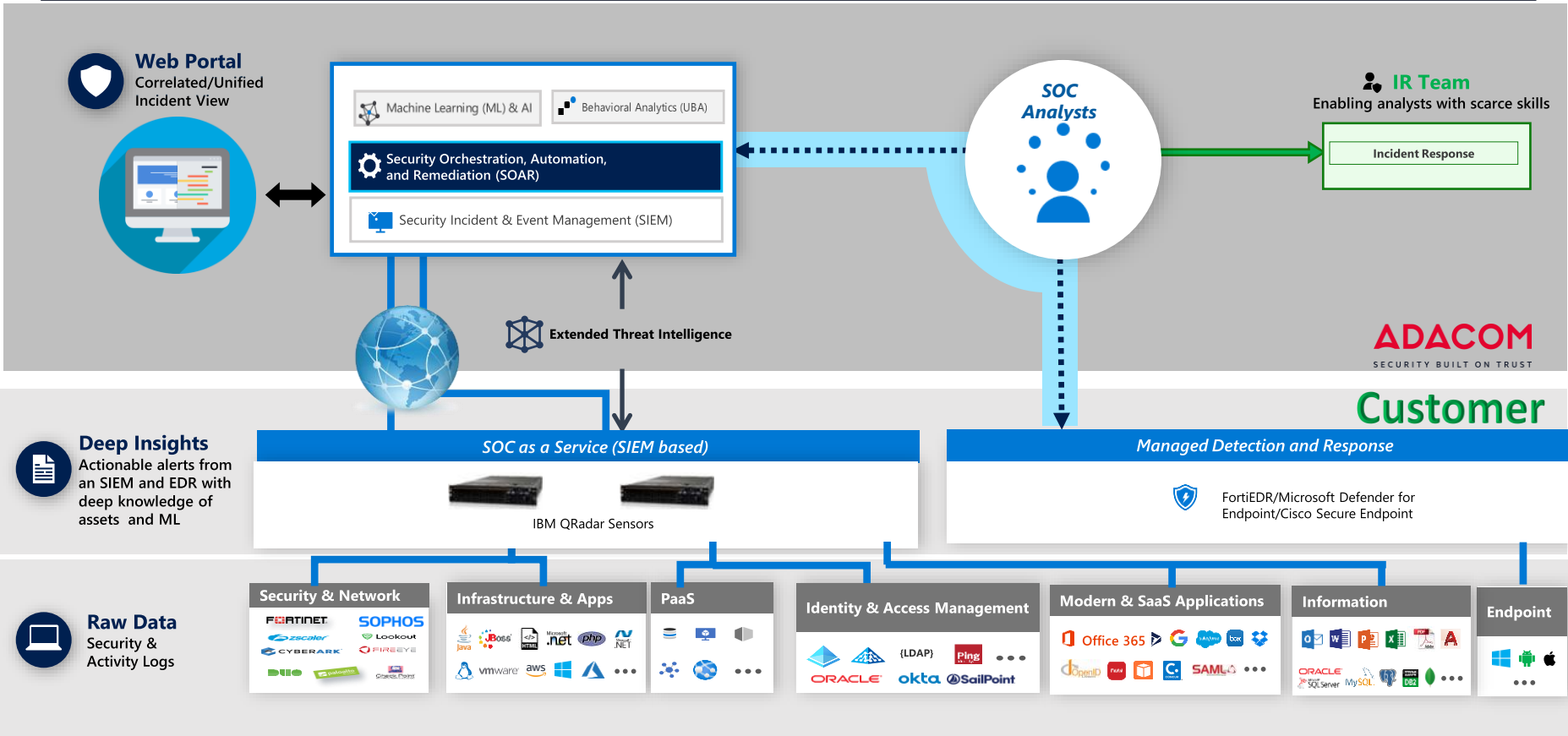


Hackers will Target the Cloud
to Access AI Resources

AI-Driven XDR Services

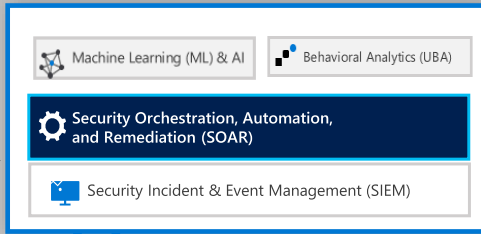


SOCaaS (SIEM based) and MDR

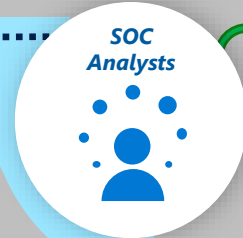


AI-Driven XDR Operation Model

Web Portal
Correlated/Unified Incident View



Extended Threat Intelligence



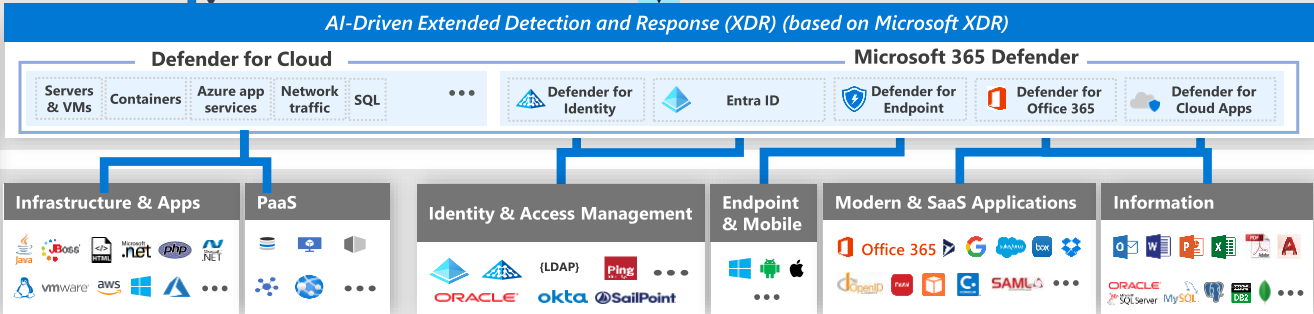
IR Team
Enabling analysts with scarce skills



Deep Insights
Actionable alerts from an XDR tool with deep knowledge of assets and ML



Raw Data
Security & Activity Logs



Customer

Microsoft Azure
Search resources, services, and docs
admin@contoso.com
CONTOSO

Home > Azure Sentinel

Azure Sentinel - Overview

Search (Ctrl+F)

Last week (1/21/2018-1/27/2018)

8.2M ↑ 978.4K

EVENTS

39 ↑ 6

ALERTS

18 ↑ 4

INCIDENTS

INCIDENTS BY STATUS

NEW (7) | IN-PROGRESS (4) | CLOSED (RESOLVED) (4) | CLOSED (ISSUES) (3)

Events and alerts over time

ALERTS 89

CEF 315K

SECURITY EVENTS 121K

AZURE AD 110K

OTHERS (5) 106K

Recent incidents

- User logged in to critical assets 9 Alerts
- Suspicious process execution after co... 9 Alerts
- Computers with cleaned event logs 8 Alerts
- Remote procedure call (RPC) attempts 8 Alerts

Potential malicious events

MALICIOUS IPS EVENTS 82K

OUTBOUND 4K ▲

INBOUND 78K ▲

Most anomalous data sources

- Azure AD
- Office
- SecurityEvents

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 >](#)

GENERAL

- Overview
- Logs

THREAT MANAGEMENT

- Incidents
- Dashboards
- User analytics
- Hunting
- Notebooks

CONFIGURATION

- Getting started
- Data collection
- Analytics
- Playbooks
- Community
- Workspace

Incidents

📧 Email notification

Most recent incidents and alerts

↓ Export

🔍 Search for name or ID

🔧 Customize columns

📅 6 Months

Filter set: 📄 Save

Status: **New**, **In progress**

Alert severity: **High**, **Medium**, **Low**

Service/detection sources: **Any**


➕ Add filter

🔄 Reset all

<input type="checkbox"/>	Incident name	Incide...	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service sources	Detection sources
<input type="checkbox"/>	> E2E Mde Streaming Detection Rule on one end...	222	whakapapa	High		Exfiltration	whakapa-dc.whakapa.alpir 1/1		Endpoint	Custom detection
<input type="checkbox"/>	> E2E Mde Streaming Detection Rule on one end...	220	whakapapa	High		Exfiltration	whakapa-win11t.whakapa 1/1		Endpoint	Custom detection
<input type="checkbox"/>	> Impossible travel activity involving one user	219		Medium		Initial access	jasuri 2 Apps 1/1		Microsoft Defender for...	Microsoft Defender for...
<input type="checkbox"/>	> Attempts to sign in to disabled accounts involi...	216		Medium		Initial access	Jonathan Wolcott 1/1		Microsoft Sentinel	Scheduled detection
<input type="checkbox"/>	> SAP financial process manipulation (attack disr...	190	Attack Disruption	High	2 investigation states	Initial access, Defense ...	Cameron White 27/27		Microsoft Defender for...	Microsoft Defender for...
<input type="checkbox"/>	> SAP non existent decoy account has been used ...	192		High		Credential access	MICHAELP 1/1		Microsoft Sentinel	NRT rules
<input type="checkbox"/>	> Human-operated ransomware attack was launc...	181	Ransomware +6	High	3 investigation states	Execution, Persistence, ...	4 Devices 4 Accounts 26/32		Endpoint, Identity, Def...	EDR, Antivirus, Microso...
<input type="checkbox"/>	> Suspicious 'GenRansom' behavior was detected...	186	whakapapa	Low		Suspicious activity	whakapa-win10s.whakapa 1/1		Endpoint	Antivirus
<input type="checkbox"/>	> Suspicious 'GenRansom' behavior was detected...	185	whakapapa	Low		Suspicious activity	whakapa-win10r.whakapa 1/1		Endpoint	Antivirus
<input type="checkbox"/>	> E2E Mde Streaming Detection Rule on one end...	223	whakapapa	High		Exfiltration	whakapa-win10s.whakapa 1/1		Endpoint	Custom detection
<input type="checkbox"/>	> E2E Mde Streaming Detection Rule on one end...	221	whakapapa	High		Exfiltration	whakapa-win11t.whakapa 1/1		Endpoint	Custom detection

Microsoft 365 Defender
Search

- Home
- Incidents & alerts
- Hunting
- Actions & submissions
- Threat intelligence
- Secure score
- Learning hub
- Trials
- Partner catalog
- Assets
- Devices
- Identities
- Endpoints
- Vulnerability management
- Partners and APIs
- Evaluation & tutorials
- Configuration management



Ilona Padilla
Software Engineer | Microsoft | Dept: Security

HONEYTOKEN

Confirm user compromised

Overview
Alerts (2)
Observed in organization
Timeline

Entity details

User threat

Azure AD Identity risk level ▲ High

Observed in organization

Last Seen	First Seen
5/29/2023	4/13/2023
Lateral movement paths	Devices
0	3
Groups	Locations
2	0

Incidents and Alerts


2 alerts over 2 incidents

Open alerts by severity

Medium

[View all alerts](#)

Investigation priority score over the last 2 weeks



■ Above 90% compared to the organization

Investigation Priority

Score: 35 (High)

Alerts

Risk Activities

User's score compared to the organization 100/100

Active Directory account controls

<input checked="" type="checkbox"/> Password never expires	<input type="checkbox"/> Trusted for delegation
<input type="checkbox"/> Smartcard required	<input type="checkbox"/> Password expired
<input type="checkbox"/> Empty password allowed	<input type="checkbox"/> Plain text password stored
<input type="checkbox"/> Cannot be delegated	<input type="checkbox"/> DES encryption only
<input type="checkbox"/> Kerberos pre-authenticatio...	<input type="checkbox"/> Account disabled

Microsoft Microsoft 365 Defender

Alerts > Possible lateral movement

Part of incident: Multi-stage incident involving Execution & Collection on multiple endpoints reported by multiple sources
[View incident page](#)

workstation6 Risk level ■ ■ ■ High

Windows10 SecCapNinja

seccxp\pgustavo

CIO

SECCXP\KDickens

Account Manager

ALERT STORY

5:12:09 AM	Image load vaultcli.dll	⋮
	⚡ Possible attempt to steal credentials ■ ■ ■ High ● Detected ● Resolved ⋮	
5:12:10 AM	powershell.exe executed a script	⌵
5:12:10 AM	powershell.exe executed a script	⌵
5:12:10 AM	powershell.exe executed a script	⌵
5:12:10 AM	Network connect Outbound connection from 192.168.2.6:49158 to 192.168.2.5:445 Remote device: adfs01.seccxp...	⋮
	⚡ Possible lateral movement ■ ■ ■ Medium ● Detected ● New ⋮	
5:12:10 AM	powershell.exe executed a script	⌵
5:12:10 AM	powershell.exe executed a script	⌵
5:12:11 AM	powershell.exe executed a script	⌵
5:12:11 AM	powershell.exe executed a script	⌵
5:12:49 AM	powershell.exe read lsass.exe process memory	⌵
5:11:05 AM	svchost.exe process performed User Account Discovery by invoking powershell.exe	⌵
	⚡ Suspicious User Account Discovery ■ ■ ■ Low ● Detected ● New ⋮	

⚡ **Possible lateral movement**

■ ■ ■ Medium
 ● Detected
 ● New

[Manage alert](#) ⋮

Details Recommendations

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state ⌵

Classification: Not Set Assigned to: bgajzler@microsoft.com

[Set Classification](#)

Alert details ⌵

Category: Lateral movement MITRE ATT&K Techniques
T1570: Lateral Tool Transfer+5 More
[View all techniques](#)

Detection source: Microsoft 365 Defender Service source: Microsoft Defender for Endpoint


Detection status: ● Detected Detection technology: -

Office 365 | Security & Compliance

Home > Policy


- Home
- Alerts
- Permissions
- Classifications
- Data loss prevention
- Data governance
- Threat management
- Dashboard
- Explorer
- Attack simulator
- Review
- Policy
- Campaigns

Anti-malware




Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

ATP safe attachments




Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.

ATP safe links




Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.

Anti-spam




Protect your organization's email from spam, including what actions to take if spam is detected.

DKIM



Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.

ATP anti-phishing



Protect your users from impersonation-based phishing attacks.



Cloud Discovery

Updated on Feb 19, 2022, 4:54 PM

Dashboard | Discovered apps | Discovered resources | IP addresses | Users | Devices

Win10 Endpoint Users | Last 30 days | Actions



App categories

<1-5 of 37 | Traffic

Sanctioned Unsanctioned Other



Discovered apps

<1-15 of 231 | View all apps | All categories | Traffic

Sanctioned Unsanctioned Other



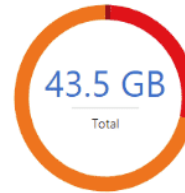
Cloud Discovery open alerts

+ Create policy

0 Cloud Discovery alerts | 0 Suspicious use alerts

Risk levels

All categories | by Traffic



Traffic from high risk apps
 Traffic from medium risk apps
 Traffic from low risk apps
 Configure score metric

Top entities

View all users | User | by Traffic

There's no relevant data to display

Microsoft Defender for Cloud | Overview

Showing 102 subscriptions

Search

Subscriptions What's new

General

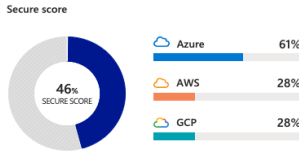
Overview

- Getting started
- Recommendations
- Attack path analysis
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems
- Cloud Security
 - Security posture
 - Regulatory compliance
 - Workload protections
 - Firewall Manager
 - DevOps security (preview)
- Management
 - Environment settings
 - Security solutions
 - Workflow automation

102 Azure subscriptions
49 AWS accounts
114 GCP projects
36588 Assessed resources
370 Active recommendations
141 Attack paths
2895 Security alerts

Security posture

237/244 Unassigned recommendation
21/43 Overdue recommendations
141 Attack paths



[Explore your security posture >](#)

Regulatory compliance

Microsoft cloud security benchmark
9 of 63 passed controls

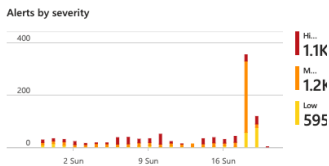
Lowest compliance regulatory standards by passed controls

AWS PCI DSS 3.2.1 Classic	0/40
AWS CIS 1.2.0 Classic	0/43
Reserve Bank of India IT Framework for NBFC	2/21

[Improve your compliance >](#)

Workload protections

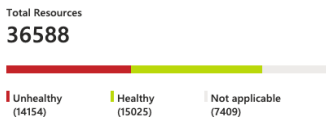
Resource coverage
86% For full protection, enable 15 resource plans



[Enhance your threat protection capabilities >](#)

Inventory

Unmonitored VMs
122 To better protect your organization, we recommend installing agents



[Explore your resources >](#)

Upgrade to new Defender CSPM plan

Defender Cloud Security Posture Management (CSPM) provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize, and reduce risk. Defender CSPM is available in addition to the free foundational security posture capabilities turned on by default in Defender for Cloud.

[Click here to upgrade >](#)

Defender EASM

Protect your organization with a holistic view of your internet security posture. Microsoft Defender EASM discovers assets across all your first- and third-party internet-exposed infrastructure, identifying potential vulnerabilities and compliance risks for remediation.

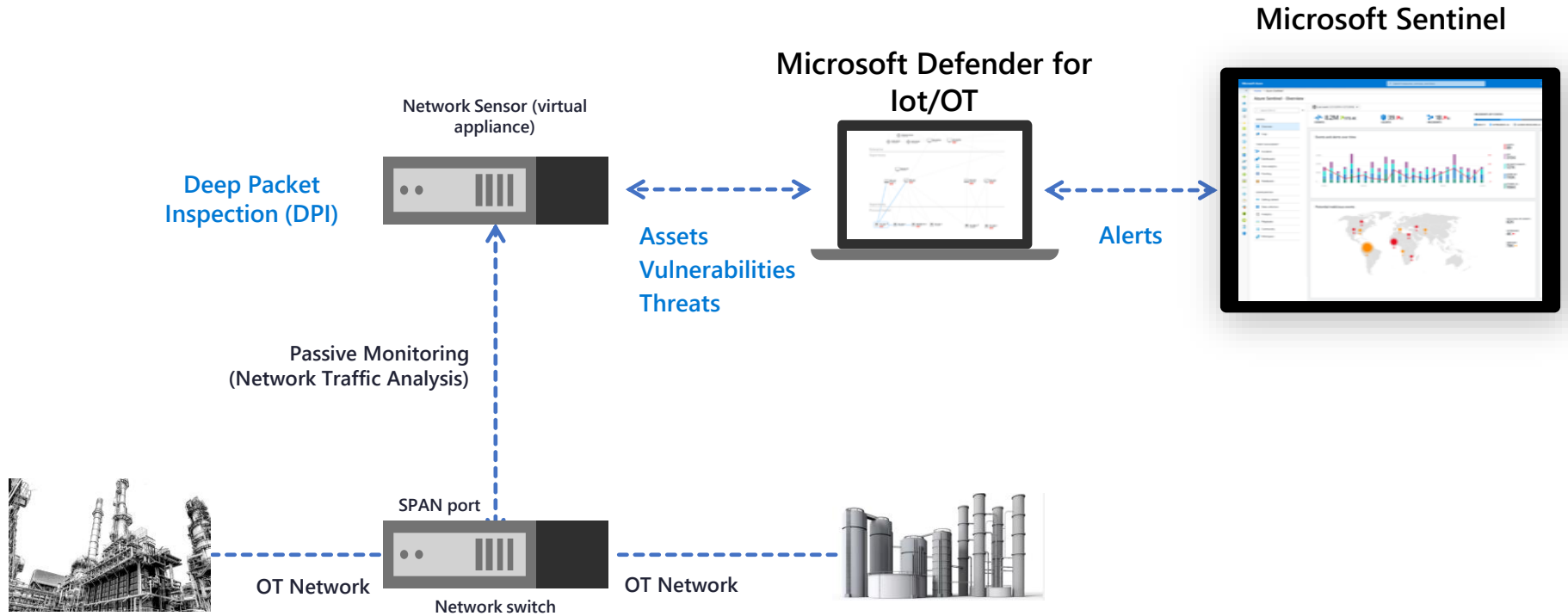
[Explore assets in Defender EASM >](#)

Defender for Cloud community

Join the Defender for Cloud community on GitHub to share knowledge and interact with other customers and experts. The community is a great place to learn and provide feedback.

[View Azure Community >](#)

Microsoft Defender for IoT/OT



Extended Threat Intelligence





Attack Surface Management

- An attack surface is the sum of an organization's attacker-exposed assets, whether these digital assets are secure or vulnerable, known or unknown, in active use or not
- An organization's attack surface changes continuously over time, and includes digital assets that are on-premises, in the cloud, as well as those in third-party vendors' environments

Digital Risk Protection

Digital Risk Protection (DRP) service protects against external threats and continually identifies where your assets are exposed whilst providing sufficient context to understand the risk and options for remediation. Monitor for Data leaks, Brand compromise, Account takeovers, Fraud campaigns etc





Threat Intelligence

- Strategic
- Tactical
- Operational

Artificial Intelligence



Microsoft Azure Search resources, services, and docs (G+)

Home > Azure Sentinel | Incidents >

Investigation

Undo Redo

Human operated ransomware attack High Severity New Status Unassigned Owner 9/04/2020, 4:06:50 PM Last incident update time

ZScaler traffic matched to known malicious...

SystemAlertId
e16cff2c-e5b2-5ed3-b4d9-2bee33a04cea

Tactics
Impact

AlertDisplayName
ZScaler traffic matched to known malicious threat intelligence

Description
Identifies a match from ZScaler network activity to any IP-address IoC from Threat Intelligence

ConfidenceLevel
Unknown

Severity
Medium

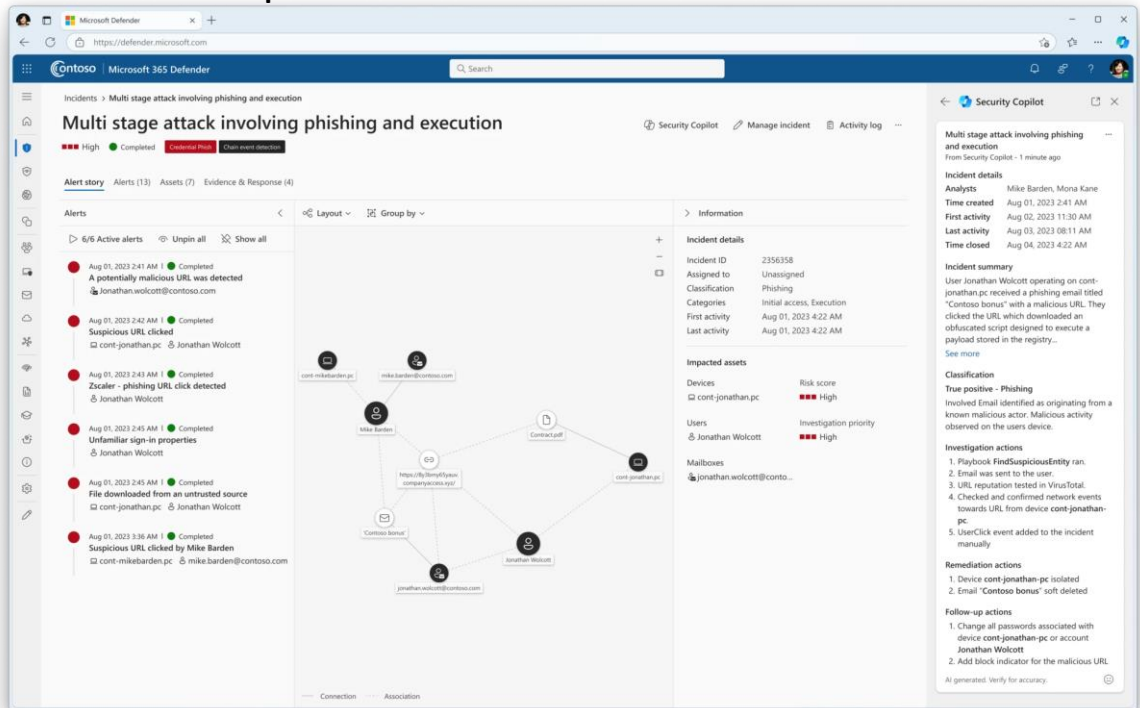
VendorName
Microsoft

ProductName

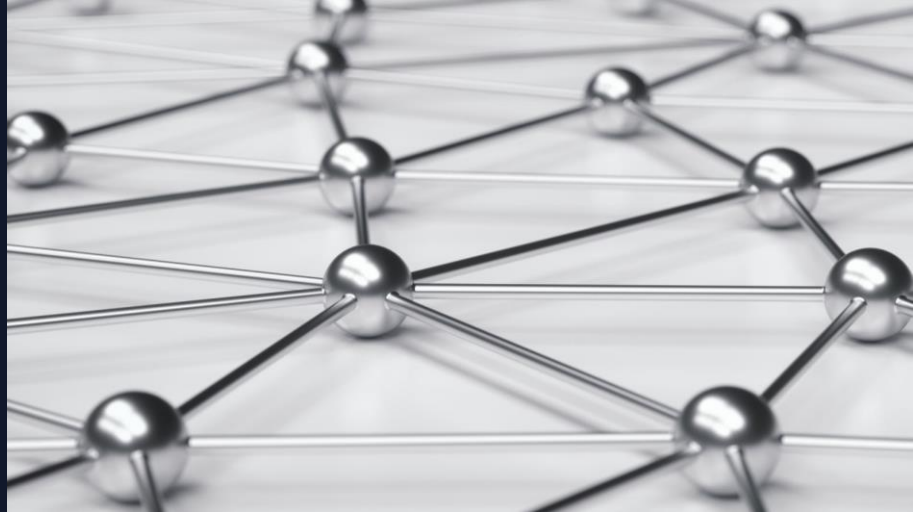
[View playbooks](#)

Timeline
Info
Entities
Help

- Incident summaries with a single click
- Guided response to incidents at machine speed
- Natural language queries to simplify hunting
- Real-time malware analysis
- Threat intelligence



Process Automation & Orchestration (SOAR)



Automation rules (Preview) Active playbooks **Playbook templates (Preview)**

Search by name

Trigger : All

Logic Apps Connectors : All

Entities : All

Tags : All

Name ↑↓	Trigger ↑↓	Logic Apps Connectors	Entities	Tags	Last modified ↑↓
Prompt User - Alert	Microsoft Sentinel Alert	Azure AD +3	Account	Remediation	07/14/21, 12:00 AM
Prompt User - Incident	Microsoft Sentinel Incident ...	Azure AD +3	Account	Remediation	07/14/21, 12:00 AM
Reset-AADUserPassword	Microsoft Sentinel Incident ...	Office 365 Outlo... +2	Account	Remediation	07/14/21, 12:00 AM
Reset-AADUserPassword	Microsoft Sentinel Alert	Office 365 Outlo... +2	Account	Remediation	07/14/21, 12:00 AM
Response on Okta user from Tea...	Microsoft Sentinel Incident ...	OktaCustomCon... +2	Account	Remediation	07/28/21, 12:00 AM
IN USE Restrict MDE App Execut...	Microsoft Sentinel Incident ...	Microsoft Defen... +1	Host	Remediation	07/14/21, 12:00 AM
Restrict MDE Domain	Microsoft Sentinel Incident ...	Microsoft Sentinel	DNS	Remediation	07/14/21, 12:00 AM
IN USE Restrict MDE FileHash	Microsoft Sentinel Incident ...	Microsoft Sentinel	FileHash	Remediation	07/14/21, 12:00 AM
Restrict MDE Ip Address	Microsoft Sentinel Incident ...	Microsoft Sentinel	IP	Remediation	07/14/21, 12:00 AM
IN USE Restrict MDE Url	Microsoft Sentinel Incident ...	Microsoft Sentinel	URL	Remediation	07/14/21, 12:00 AM
Run MDE Antivirus	Microsoft Sentinel Incident ...	Microsoft Defen... +1	Host	Remediation	07/14/21, 12:00 AM
Send basic email	Microsoft Sentinel Incident ...	Office 365 Outlo... +1		Notification	07/14/21, 12:00 AM
IN USE Send email with formatt...	Microsoft Sentinel Incident ...	Office 365 Outlo... +1		Notification	07/14/21, 12:00 AM
Sync Jira from Sentinel - Create i...	Microsoft Sentinel Incident ...	Azure Key Vault +1		Sync	07/20/21, 12:00 AM
Sync Jira to Sentinel - Assigned ...	Microsoft Sentinel Incident ...	Azure Key Vault +1		Sync	07/20/21, 12:00 AM
Sync Jira to Sentinel - public com...	Microsoft Sentinel Incident ...	Microsoft Sentinel		Sync	07/20/21, 12:00 AM
Sync Jira to Sentinel - Status	Microsoft Sentinel Incident ...	Microsoft Sentinel		Sync	07/20/21, 12:00 AM
Unisolate MDE Machine	Microsoft Sentinel Incident ...	Microsoft Defen... +1	Host	Remediation	07/14/21, 12:00 AM

< Previous

Page 1

of 2

Next >

Send email with formatted incident report

Microsoft Sentinel Incid...
Trigger type

7/14/2021, 12:00:00 AM
Last update time

Description

This playbook will be sending email with formated incidents report (Incident title, severity, tactics, link,...) when incident is created in Microsoft Sentinel. Email notification is made in HTML.

Connectors in use

Microsoft Sentinel Office 365 Outlook

Prerequisites

An O365 account to be used to send email notification (The user account will be used in O365 connector (Send an email).) Link with company logo. No formatting since size is defined in the Playbook. Linke example - <https://azure.microsoft.com/svghandler/azure-sentinel>



Supported by
Community

GitHub template source
<https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks/Send-email-with-formatted-incident-report>

Create playbook

Home > Microsoft Sentinel

Microsoft Sentinel | Automation

Selected workspace: 'defenderloganalytics'

Search << + Create Refresh Automation health workbook Edit Enable Move up

News & guides

Search

Threat management

Incidents

Workbooks

Hunting

Notebooks

Entity behavior

Threat intelligence

MITRE ATT&CK (Preview)

Content management

Content hub (Preview)

Repositories (Preview)

Community

Configuration

Workspace manager (Preview)

Data connectors

Analytics

Watchlist

Automation

Settings

Automation rule

- Playbook with incident trigger
- Playbook with alert trigger
- Playbook with entity trigger
- Blank playbook

0 Enabled rules 3 Enabled playbooks More Content

playbooks Playbook templates (Preview)

No automation rules were found

What is it?

Automation rules allow you to centrally manage all the automation of incident handling. Automate and enable you to simplify complex workflows for your incident orchestration processes.

How does it work?

Automation rules are triggered by the creation of incidents. You can set conditions to govern when and on analytics rules. You can also set the order of actions and the rule's expiration time.

What does it do for you?



Automate incident configuration

Directly set incident status or severity, assign an owner, or add a tag when an incident is created, without the need for running a playbook.



Run playbooks on incidents

You can still run playbooks from your automation rules to integrate with other services

Incident Response



- Remote and on-site technical, incident command and advisory capability
- Incident response team experienced in common and uncommon cyber threat scenarios
- Incident-specific threat intelligence and insights into current adversary tradecraft
- Quick deployment of technologies and ADACOM security analytics as needed
- Attack Emulations, Hardening, RED Teaming Operations



- ↘ 150 Certifications
- ↘ > 80 Incident Investigations in 2023
- ↘ > 100 Worldwide Customers
- ↘ > 1.000 Use Cases
- ↘ 2 Security Operation Centers
- ↘ > 1.000 Critical & High-Risk Incidents per Month
- ↘ > 20 KPIs



SECURITY
BUILT ON TRUST

Call us before you need us

GREECE

25 Kreontos Str.,
104 42, Athens
+30 210 5193740

UNITED KINGDOM

8950 Fitness Lane,
Suite 100 Fishers, IN 46037
+44(0) 317 588 3131

CYPRUS

10 Katsoni Str.,
1082, Nicosia
+357 22 444 071

