

Microsoft Sentinel & Azure Reference Architecture

Use Cases & Capabilities

Created by: Recorded Future Professional Services Solutions Architecture

Authored by: Adam Hirsch, Tom Davis

Published: June, 2023

Updated: September, 2024 Updated: September, 2024

Summary

This reference architecture aims to provide the reader with an understanding of the capabilities that can be achieved with Recorded Futures integration into the Microsoft Azure suite accompanied with use cases that our customers have implemented in the field.

The [Recorded Future V2 connector for Microsoft Azure](#) offers extensive capabilities that seamlessly integrate with a wide range of Microsoft's enterprise solutions, including Sentinel, Defender ATP, and Power Platform. By combining Recorded Future's comprehensive intelligence data sets with an organization's existing technology stack, and by leveraging external intelligence feeds, the connector optimizes performance and significantly reduces the time required to respond to threats. This can be achieved through correlation, orchestration, and automation processes that enable centralized threat prevention, detection, and hunting in the environment.

Recorded Future also provides connectors for [Identity](#) and [Sandbox](#).

Installation Guides:

- [Microsoft Sentinel](#)

General Recorded Future Integration statistics:



Resolve security threats 49% faster
Recorded Future delivers relevant cyber threat insights in real time – empowering you to identify threats faster



Improve security team capacity by 36%
Easily access the information you need, when you need it, to disrupt adversaries and reduce risk to your organization

Capabilities illustrated in this design are in their "current state". As more features and capabilities are released Recorded Future will update this design.

Professional Services Assistance

Recorded Future provides a custom Use Case Development service to identify and implement the capabilities outlined in this document and also develop new capabilities based on discovery workshops with customers.

For more information on Azure Use Case development, assistance with creation of custom Use Cases and implementation, please contact your sales representative and arrange a conversation with Professional Services at Recorded Future to see how we can help.

Index

Summary.....	1
Professional Services Assistance.....	1
Index.....	2
Integration.....	4
Integration Overview.....	4
Integration Data Flow.....	5
IOC Detection.....	5
With data ingested into the Log Analytics workspace, the following flow needs to be configured to start correlating.....	5
IOC Enrichment.....	5
Automation rules can be configured to trigger on each incident and enriches incidents with Recorded Future intelligence.....	5
Malware Sandbox Analysis (Sandbox).....	5
Logic Apps.....	6
Azure Capabilities.....	7
Capabilities Overview.....	7
SIEM - Sentinel Alert & Investigate.....	7
Problem.....	7
Solution.....	7
TIP - Sentinel - Centralized Threat Intelligence.....	8
Problem.....	8
Solution.....	8
Benefits.....	9
SOAR - Sentinel - Automate and Respond.....	10
Problem.....	10
Solution.....	10
EDR - Defender for Endpoint - Detect & Prevent.....	11
Problem.....	11
Solution.....	11
Use Cases.....	12
Correlation Dashboards.....	13
Use Case Summary.....	13
Procedure.....	13
Correlation Alerts.....	14
Use Case Summary.....	14
Procedure.....	14
Automated Incident Enrichment.....	15
Use Case Summary.....	15
Procedure.....	15
Threat Description / Scenario.....	15
Objective.....	15
Portal Alert Ingestion.....	16
Use Case Summary.....	16
Threat Description / Scenario.....	16
Procedure.....	16
Threat Map Seeded Hunting.....	17

Use Case Summary.....	17
Threat Description / Scenario.....	17
Procedure.....	17
Benefits.....	18
Retroactive Hunting.....	19
Use Case Summary.....	19
Threat Description / Scenario.....	19
Procedure.....	19
Benefits.....	19
Endpoint Proactive Blocking.....	20
Use Case Summary.....	20
Threat Description / Scenario.....	20
Procedure.....	20
Benefits.....	20
Identity Connector.....	21
Use Case Summary.....	21
Threat Description & Scenario.....	21
Procedure.....	21
Benefits.....	21
Sandbox Detonation.....	22
Use Case Summary.....	22
Threat Description & Scenario.....	22
Procedure.....	22
Benefits.....	22
Vulnerability Dashboard.....	23
Use Case Summary.....	23
Threat Description & Scenario.....	23
Procedure.....	23
Benefits.....	23
Automated Phishing Triage.....	24
Use Case Summary.....	24
Description.....	24
Procedure.....	24
Benefits.....	24
Sigma Rule Ingestion.....	25
Use Case Summary.....	25
Description.....	25
Procedure.....	25
Integration Conclusion.....	26
Summary.....	26
Requirements.....	26

Integration

Integration Overview

Security Operations teams require both External and Internal threat intelligence to rapidly identify and respond to known threats, eliminating the need for redundant analysis that specialized intelligence organizations have already performed. To accomplish this, a Recorded Future Connector, via a RESTful API, can be leveraged within [Logic Apps](#) and connect Recorded Future intelligence into Microsoft Sentinel [Threat Indicators](#).

This intelligence can then be leveraged by various solutions within the Azure platform, providing a wealth of performance benefits to Security Operations teams. Capabilities are expansive, including the ability to instantly comprehend threats associated with generated alerts and make swift decisions on priority and response. The connector supports multiple use cases, such as Threat Prevention, Threat Detection, and Incident Triage, and offers dedicated actions for pulling Recorded Future indicators and associated context, vulnerabilities, and Recorded Future alerts.

Microsoft Sentinel (SIEM) provides a platform for correlating events from both the Azure environment & infrastructure telemetry to provide enhanced detection of suspicious and malicious events. Combined with world-class threat intelligence, these events can be qualified to a high level of fidelity and auto-escalated to threat events due to the correlation of known malicious indicators, evidence and calculated risk score. On demand enrichment also provides hunters with the ability to quickly gain context related to suspicious indicators when hunting on the platform and provides analysts with contextual awareness when looking into related events.

Microsoft Sentinel (SOAR) provides the ability to orchestrate incident response for rapid actions to be taken via playbooks designed to act upon the events which generated the alert. Azure provides the capability to utilize existing technologies to enact the responses such as pushing Incidents to existing Incident Management platforms or Reactive blocks pushed to firewalls on the infrastructure.

Microsoft Sentinel (TIP) provides a central solution for managing vast amounts of threat data. It allows for the ingestion of intelligence from multiple sources, and its correlation with security events to improve threat detection. Sentinel TIP also enriches alerts with additional context for more accurate threat assessment. It tracks and proactively defends against threat actor tactics, techniques, and procedures (TTPs). The platform also handles Indicator of Compromise (IOC) management and integrates seamlessly with Azure's SIEM and SOAR functionalities for efficient threat hunting and automated response

Microsoft Defender for Endpoint (EDR) (*Formally Defender ATP*) Threat intelligence enables Defender for Endpoint to identify TTPs, suspicious events and known malicious events to generate alerts and proactively block events protecting the endpoint before the attackers leverage the foothold.

Microsoft Entra ID (IAM) - Microsoft Entra ID, previously known as Azure Active Directory, is a cloud-based identity and access management service that centralizes user identity management, enhances security with features like multi-factor authentication and conditional access, supports single sign-on, and integrates seamlessly with Microsoft services.

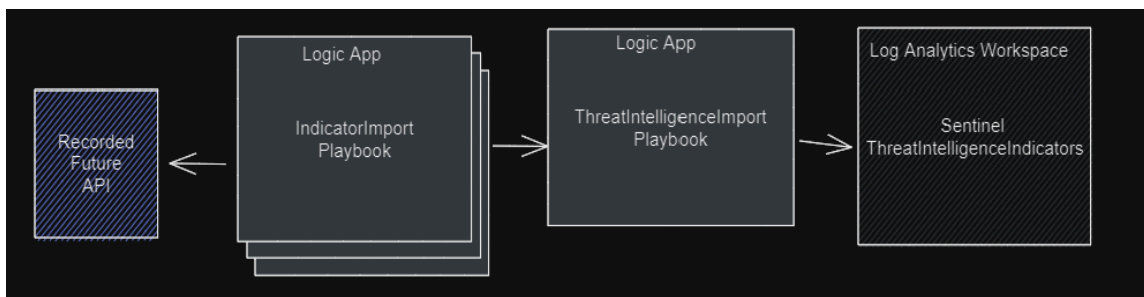
Ultimately, Microsoft Sentinel, in conjunction with Recorded Future, provides enriched, actionable insights for efficient and effective security operations, distributed throughout the ecosystem.

Integration Data Flow

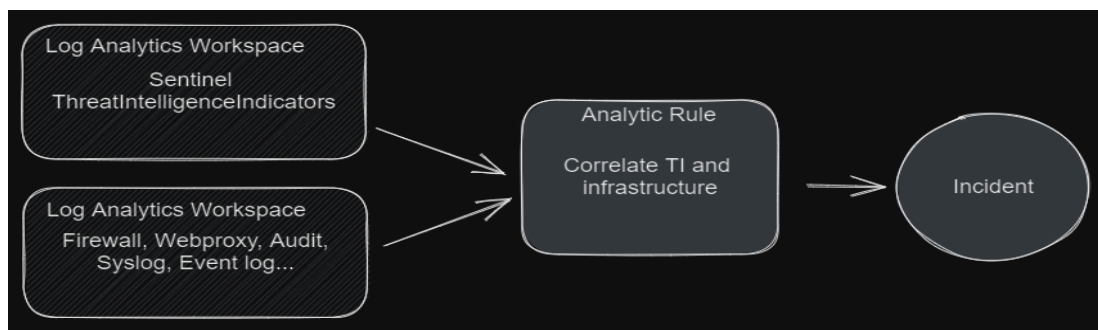
The following is from the Recorded Future Intelligence for Microsoft Sentinel installation guide found [here](#). Please utilize this resource for a deeper understanding of the integration technical specifics.

IOC Detection

Data flow depicting ingestion of Recorded Future Threat Intelligence feeds into the Log Analytics Workspace.

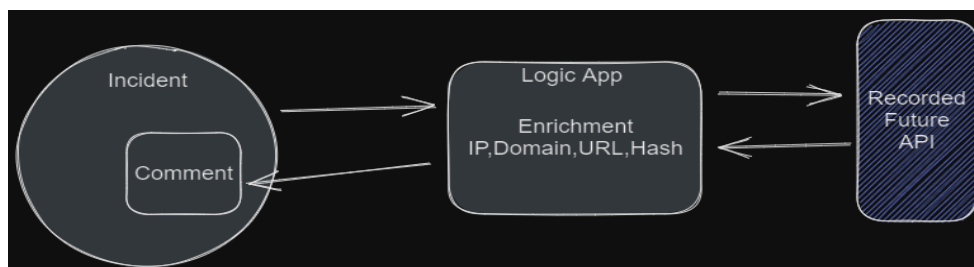


With data ingested into the Log Analytics workspace, the following flow needs to be configured to start correlating.



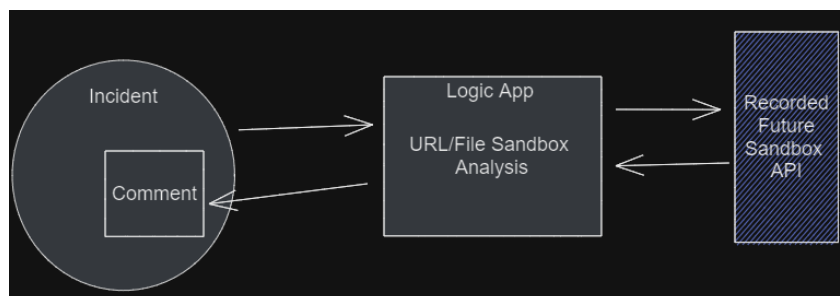
IOC Enrichment

Automation rules can be configured to trigger on each incident and enriches incidents with Recorded Future intelligence.



Malware Sandbox Analysis (Sandbox)

Uploads and detonates samples in Recorded future sandbox. Providing safe and immediate behavioral analysis, resulting in key artifacts being contextualized which can lead to faster triage.



Logic Apps

As seen in the dataflow above, Logic Apps are at the core of this integration, enabling the intelligence from the connector to propagate into the required places. Logic apps are the building blocks for automation in Azure, and are utilized for the Playbook development within Sentinel.

There is an extensive list of actions that can be performed using the connector to access Recorded Future's huge intelligence graph. Find below a list of the actions that can be performed using the connector.

Domain Enrichment	Domain Enrichment with Recorded Future data
Hash Enrichment	Hash Enrichment with Recorded Future data
IP Enrichment	IP Enrichment with Recorded Future data
Lookup Alert Notification	Lookup Alert Notification
Recorded Future RiskLists and SCF Download	Recorded Future RiskList & Security Control Feeds Download
Search Alert Notifications	Search Alert Notifications
Search Alert Rules	Search Recorded Future UI Alert Rules
SOAR API - Look up multiple entities	SOAR API - Look up multiple entities (Specific Access is Required)
URL Enrichment	URL Enrichment with Recorded Future data
Vulnerability Enrichment	Vulnerability Enrichment with Recorded Future data

Recorded Future Connector V2 Actions

Credential Lookup - Look up credential data for one or more users	Look up exposed credential data for a specific set of subjects
Credential Search - Search credential data for one or more domains	Search credential data exposed in data dumps and through malware logs

Recorded Future Identity Connector Actions

Get the full report	Get the full report on the submitted sample.
Get the full summary	Get the full summary on the submitted sample.
Submit file samples	Submit file samples to Recorded Future Sandbox.
Submit url samples	Submit url samples to Recorded Future Sandbox.

Recorded Future Sandbox Connector Actions

Azure Capabilities

Capabilities Overview

Integrating into the Azure suite of applications provides a unified approach to the Security Technology Stack. Azure fully supports third party applications while providing a defense in depth solution for Detection, Response & Defense. Combining Microsoft Azure with Recorded Future ensures the Defense in Depth technology stack is enhanced with world-class Intelligence.

SIEM - Sentinel Alert & Investigate

Recorded Future provides the intelligence to develop detection content with high fidelity and high confidence with a low rate of false positives. Correlating with additional telemetry provides the confidence to proactively take action on intelligence and enrichment of existing and new notables.

Problem

Alert volume, lack of context, difficulty prioritizing

SIEM detection rules frequently generate a lot of suspicious activity alerts with little room for maneuvering to ensure the alerts generated are high fidelity or confirmed threats. Tuning and configuring SIEM alerts takes time, patience and requires triage and investigation. Eventually, the rules become aged and no longer viable which can overwhelm the content development team with a stale repository of detection rules.

Solution

Centralize, Prioritize, Escalate

One of the primary benefits to implementing Recorded Future Intelligence into Microsoft Sentinel is increased alert fidelity. Augmenting existing use cases by combining Recorded Future's intelligence provides a solution to reduce false positives and increase fidelity and detection accuracy of known threat indicators.



Recorded Future Intelligence Indicators

TIP - Sentinel - Centralized Threat Intelligence

Problem

Stagnant, isolated, siloed threat intelligence


Numerous threat intelligence feeds often lack the context necessary to make informed judgments about the risk posed by specific indicators. Furthermore, outdated data can lead to high levels of false positives, diminishing the value of data within a Threat Intelligence Platform (TIP) for effective threat detection and incident prioritization.


Solution


Centralize & disseminate threat intelligence







Centralization and Dissemination of Intelligence are the keys to overcoming these challenges. Ingesting context-rich intelligence into a central repository not only provides a platform for storing sensitive internal incident data but also enables the identification of Tactics, Techniques, and Procedures (TTPs) and context correlation against third-party intelligence.

The Threat Intelligence application supports feed based and manual creation of Intelligence. The feeds are ingested from the Sentinels TI-Indicators and presented as a streamlined TIP solution centralizing indicators giving your SOC the ability to manage Threat Intelligence and apply it to alerting and correlation rules as shown in the below Use Cases.

 **376**
TI alerts

 **14K**
TI indicators

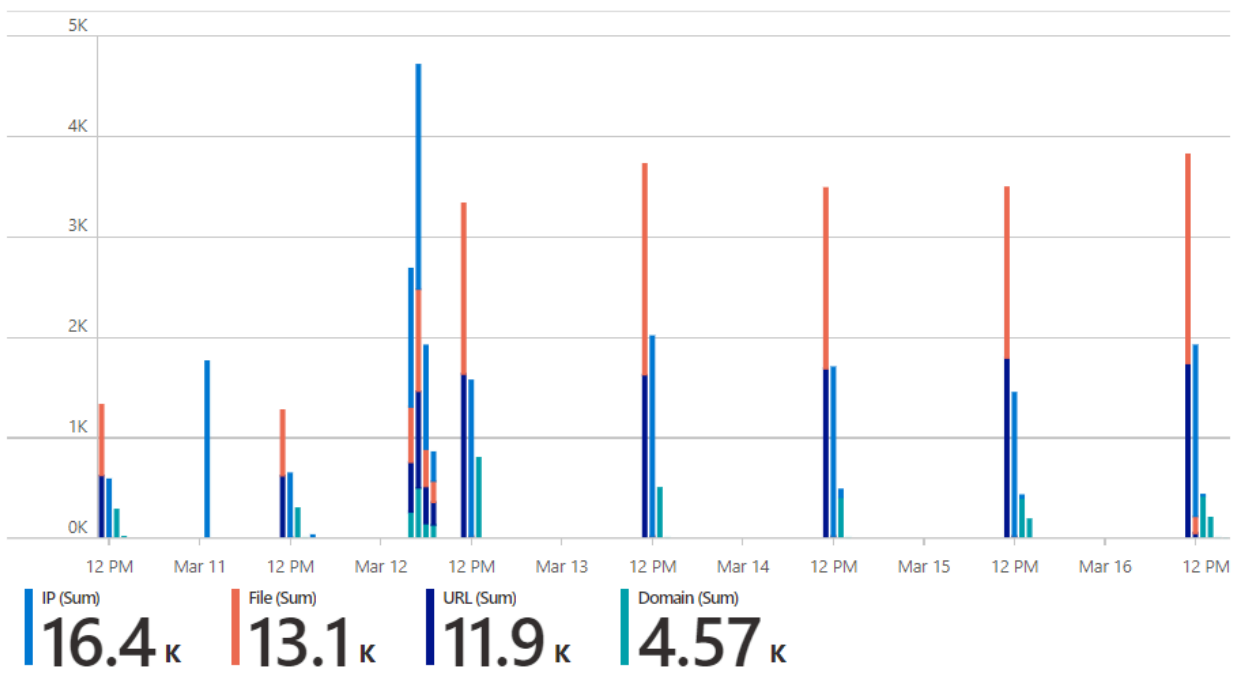
 **1**
TI sources

Search by name, values, description or tags						
Type : All Source : All Threat Type : All Confidence : All Valid Until : All						
<input type="checkbox"/> Name ↑↓	Values	Types	Source ↑↓	Confidence ↑↓	Alerts	Tags
<input type="checkbox"/> Custom Threat Intelligence	89.45.4.192	 ipv4-addr	SecurityGraph	99	0	...
<input type="checkbox"/> Custom Threat Intelligence	151.205.102.42	 ipv4-addr	SecurityGraph	99	0	...
<input type="checkbox"/> Custom Threat Intelligence	167.71.236.70	 ipv4-addr	SecurityGraph	99	0	...
<input type="checkbox"/> Custom Threat Intelligence	128.199.184.61	 ipv4-addr	SecurityGraph	99	0	...
<input type="checkbox"/> Custom Threat Intelligence	185.82.219.40	 ipv4-addr	SecurityGraph	99	0	...
<input type="checkbox"/> Custom Threat Intelligence	85.217.171.12	 ipv4-addr	SecurityGraph	99	0	...

Recorded Future Intelligence Indicators

There is a workbook available which shows metrics on Intelligence available to the Azure environment including such alerts as the number of times an alert has triggered per indicator per rule.

Indicators imported into Sentinel by indicator type and date



Recorded Future Intelligence Metrics within the Sentinel Threat Intelligence Workbook

Benefits

- Collect, Centralize and Tag Recorded Future threat intelligence
- Show metrics on Intelligence based Correlation alerts
- Create correlations with tags in the Threat Intelligence Workbook for the indicator

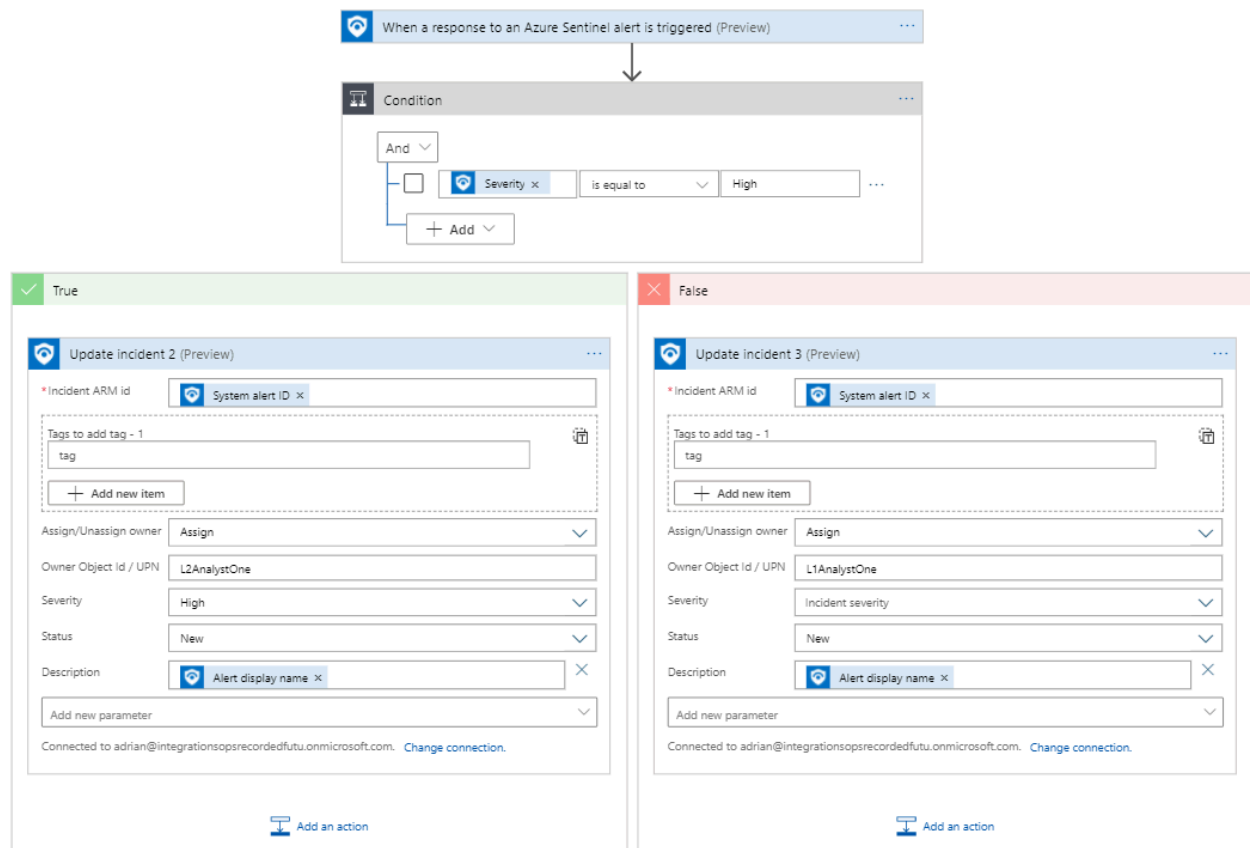
SOAR - Sentinel - Automate and Respond

Recorded Future's Intelligence context and related entities provides an invaluable method to utilize threat intelligence data within automation and orchestration playbooks to perform operations such as blocking, triaging, containment and hunting with a high level of confidence.

Problem

Too many alerts causing missed or delayed threats for extended periods

SOAR is largely advertised as a plug'n' play solution, however without trusted intelligence or well developed playbooks the solution can be cumbersome to achieve a high value result. Triage and Prioritization can be a long winded and tedious process for analyst teams to conduct and frequently leads to higher priority incidents being missed or actioned after extended dwell time for the attackers.



Playbook example to auto assign incident based on Priority

Solution

Response time, action with confidence, increase capabilities

SOAR provides outstanding capabilities to automate operational actions needed to contain, block, and triage at an unprecedented level. Recorded Future provides the capability to inject high confidence intelligence into playbooks designed to assist with Hunting, Triage, Prioritization and Proactive / Reactive blocking.

Leveraging Microsoft Sentinel's SOAR capabilities provides the intelligence to develop Detection and Response with a higher fidelity, faster response time and higher confidence level. Correlating with additional telemetry provides the confidence to proactively take action on events and provide enrichment to new and existing Events of Interest and Incident IOCs.

EDR - Defender for Endpoint - Detect & Prevent

Recorded Future data provides the confidence to block malicious activity directly on the endpoint via carving up the data into high fidelity, high confidence, high risk indicators. Alerts can also be generated for events which are considered suspicious or anomalous.

Problem

Remote users present a uniquely undetectable threat profile

Endpoints are commonly the first point of attack due to a lack of perimeter controls

- Users frequently work remotely effectively negating controls placed on the perimeter and ultimately making their own asset or personal home network the perimeter / or total removal of a perimeter via joining unsecured public wifi hotspots for example.
- Alerts are legion, analysts are often overwhelmed by the amount of alerts generated via correlation of telemetry and intelligence alerts which require urgent attention or in depth investigations.

Solution

Detect and Protect directly at the point of attack

- **Microsoft Defender for Endpoint (EDR)** has been positioned as the first line of defense for endpoints away from the protection of the business infrastructure and a last line of defense for endpoints which are connected to the infrastructure. In cases where the EDR is the first line of defense, world-class intelligence provides a much more robust protective layer to prevent a breach or at a minimum isolate the asset and prevent it rejoining the infrastructure network until it's been cleaned.
- Proactive protection at the endpoint as a perimeter (offline assets) helps to prevent assets becoming infected while away from the enterprise network, ensuring the foothold isn't leveraged.

Use Cases

The use cases section aims to provide real-world examples and applications of the Recorded Future V2 connector for Azure. These use cases serve as a guide for understanding how the connector can be integrated into various aspects of your cybersecurity strategy and leveraged to enhance your organization's security posture.

By exploring these use cases, you can gain insights into how the Recorded Future connector for Azure can be customized to fit your unique requirements, and discover new ways to utilize the connector's capabilities. Use cases can serve as seed ideas that inspire you to create tailored solutions for your specific needs, helping you maximize the value of the integration between Recorded Future and Azure.

We encourage you to use these use cases as a starting point, adapting and expanding on them as needed to fit your organization's specific objectives and challenges. As you become familiar with the connector for Azure and its capabilities, you will be better equipped to develop innovative solutions that enhance your security operations, threat detection, and incident response efforts.

These Use Cases reference targeted Use Cases for Recorded Future at a point in time. Use Cases may develop to provide additional benefits in the future.

Correlation Dashboards

Use Case Summary

Recorded Future has configured Microsoft Azure correlation dashboards, also known as [Azure Workbooks](#), that allows analysts to quickly identify threats, patterns, and trends by providing a single comprehensive view of Recorded Future threat data and top risk rules triggered by Domains in your environment.

Recorded Future provides Workbooks available on the [Azure Github repository](#).



This dashboard shows correlation for IP. Additional dashboards showing correlation for Domain, Hash and URL Risk Lists are also available. Analysts can also use the dashboard to generate reports, prioritize investigations, and gain a deeper understanding of their security environments.

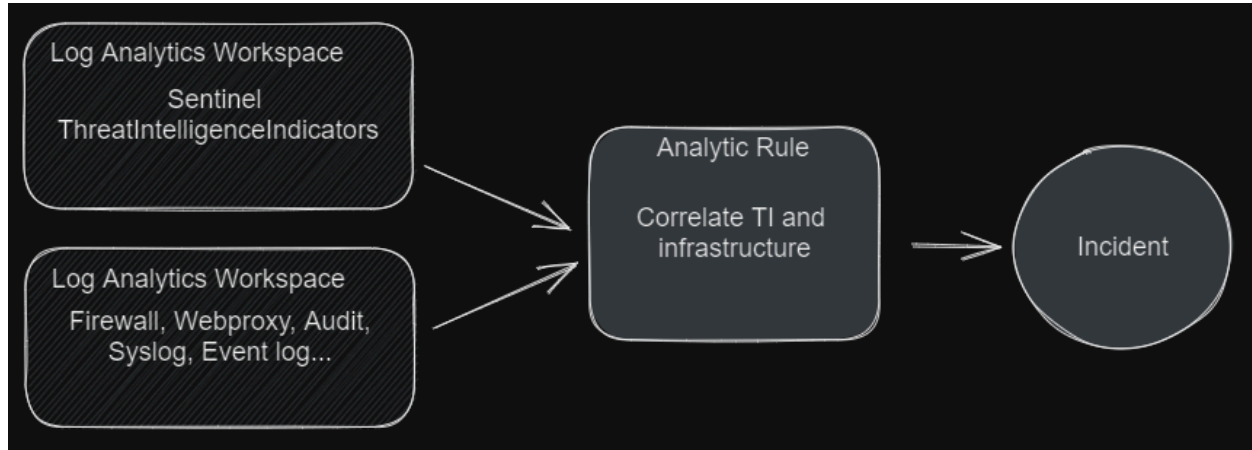
Procedure

- Setup:** Ingest Recorded Future data into the Threat Intelligence Indicator table and ensure your logs are formatted appropriately.
- Workbook Configuration:**
 - Select the source of your data within the "IOC_TYPE" Logs Table Parameter
 - Specify the specific field from the source where the IOC is.
 - Choose the RF Risk List to use.
 - Adjust timeframes to requirements.
- Enhanced Analysis:** Utilize the created dashboard for analysis. Clicking on specific Matches will open up risk rules triggered for that particular IOC enabling deeper analysis.

Correlation Alerts

Use Case Summary

Sentinel provides Use Cases which can natively utilize Intelligence fed into the Log Analytics Workspace as TI Indicators and correlate against these triggers in the solution. Also the ability to leverage the intelligence to prioritize and provide much needed context to operations teams for triage. This can help create a view to enhance the Use Cases, increase fidelity and reduce false positives.



+ Create Refresh Analytics efficiency workbook (Preview) Enable Disable Delete

12 Active rules LEARN MORE
About analytics rules

Rules by severity: High (6) | Medium (4) | Low (2) | Informational (0)

Active rules | Rule templates

Search:

Severity: All | Rule Type: All | Status: All | Tactics: All

SEVERITY	NAME	RULE TYPE	STATUS	TACTICS
High	Advanced Multistage Attack Detection	Fusion	Disabled	
High	Detect Requests to C&C Domains (High Score) - ...	Scheduled	Enabled	Comm...
High	Detect Traffic to Actively Communicatin C&C (Rel...	Scheduled	Enabled	Comm...
High	Detect Requests to Positive Malware Verdict URL...	Scheduled	Enabled	Executi...
High	Detect HASHes Observed in Underground Virus T...	Scheduled	Enabled	Executi...
High	Typosquatting Domain Detected - by Recorded F...	Scheduled	Enabled	PreAtt...
Medium	Detect Traffic to Actively Communicatin C&C (Hi...	Scheduled	Enabled	Comm...

Detect Traffic to Actively Communicatin C&C (Relat...)

High Severity | Enabled Status

Future Actively Communicating C&C Server Risklist, focused on indicators that are confirmed by Recorded Future as related/serving specific malware of interest for the company

Tactics: Command and Control

```

Rule query
| where Active == true
| where Description contains 'Recorded Future - IP - Actively Communicating C&C Server' and AdditionalInformation contains 'Cobalt Strike'
| join (

```

Microsoft Sentinel Recorded Future Correlations Events

Use Case correlation supports searching the Recorded Future evidence strings and manually added Tags from the Threat Intelligence table enabling searching for specific malware, threat actors or MITRE ATT&CK for example. Tagging Intelligence with previous Incident numbers provides a correlation of previous malicious activity to Intelligence.

Procedure

- Correlation Search:** Utilize Microsoft Sentinel's correlation capabilities to correlate against specific Recorded Future risk lists.
- Alert Generation:** Generate alerts based on the correlated telemetry and Recorded Future's intelligence.
- Incident Management:** Create incidents for identified threats, block indicators associated with malicious activity, and escalate incidents as required.

Automated Incident Enrichment

Playbooks found [here](#).

Use Case Summary

Recorded Future can provide automation playbooks which can extract entities from incidents and enrich these to provide in-line comments containing all of Recorded Future's intelligence for the indicator. Additionally, Recorded Future intelligence can be utilized within SOAR playbooks to provide the confidence via evidence-based risk scoring to make intelligence driven decisions.

Incident activity log

Activity logs content: All

Comment created from playbook - RecordedFuture-IOC_Enrichment-IP_Domain_URL_Hash
01/23/23, 02:16 AM

Recorded Future

Enriched Domain: **wpqqhshpps.in**

Risk Score: **94**

[Open IOC Intelligence Card \(Portal\)](#)

Triggered Risk Rules:

Risk_Rules	Severity	Evidence_Details
Recent C&C DNS Name	Very Malicious	1 sighting on 1 source: Bambenek Consulting C&C Blocklist.
Historically Reported Botnet Domain	Unusual	5 sightings on 1 source: External Sensor Data Analysis. wpqqhshpps.in is observed to be a botnet domain from which network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contacts.
Historically Reported as a Defanged DNS Name	Unusual	1 sighting on 1 source: @DGAFedAlerts. Most recent tweet: New mydoom Dom: wpqqhshpps.in IP: 35[1205][61][67] NS: https://t.co/R5eHbwsZt https://t.co/RakahsOTXS. Most recent link (Aug 26, 2022): https://twitter.com/DGAFedAlerts/statuses/1563211579478315014

Write a comment...

Close Comment

Automated enrichment enabling "IP Enrichment" on alerts within Sentinel

Procedure

- Incident Creation:** Sentinel will create alerts/incidents based on specific pre-configured rules.
- Automated Enrichment:** The Recorded Future Enrichment playbook will automatically trigger, extracting all IOCs from the incident.
- In-Line Comments:** Automatically the playbook will add the obtained intelligence to the incident, providing the analyst with greater context.

Threat Description / Scenario

Incidents are frequently littered with 'false positives' due to a number of factors and complexities in detecting threats. This can lead to extended dwell times for attackers as defenders are wasting time dealing with lower fidelity incidents—unaware of higher priority incidents in the queue.

Objective

- Automatically prioritize Incidents based on Intelligence led Incidents and Events
- Automatically enact mitigations related to high fidelity Intelligence led Incidents
- Escalation of Incidents based on risk and priority to ensure rapid response

Portal Alert Ingestion

Use Case Summary

Recorded Future offers UI-based alerts triggered by various customer needs, including credential leaks. This use case focuses on the ingestion of these alerts into Microsoft Sentinel, enabling immediate response and triage by operations teams.

The objective of this use case is to receive alerts related to credential leaks specific to an enterprise. By promptly ingesting these alerts into Microsoft Sentinel, organizations can rapidly triage, remediate, and verify suspicious activities associated with compromised accounts.

The screenshot displays the Microsoft Sentinel Recorded Future Alerts Dashboard and Details view. At the top, there are four summary cards: 'Open incidents' (5), 'New incidents' (5), 'Active incidents' (0), and 'Open incidents by severity' (High 3, Medium 2, Low 0, Informational 0). Below these is a search bar and filters for 'Severity: All' and 'Status: New, Active'. A table lists incidents with columns for Incident ID and Title. The first incident is 'Typosquatting Domain Detected - by Recorded Future' (ID: 590). A detailed view of this incident is shown on the right, including its description, alert product names (Azure Sentinel), and evidence (8 Events, 1 Alerts, 0 Bookmarks).

Incident ID	Title
590	Typosquatting Domain Detected - by Recorded Future
587	Detect Traffic to Actively Communicatin C&C (Related to specific Malware) - by Recorded Future
588	Detect Traffic to Actively Communicatin C&C (High Score) - by Recorded Future
586	Detect Requests to C&C Domains (High Score) - by Recorded Future
589	3rd Party Correlation/Alert - with Enrichment by Recorded Future

Microsoft Sentinel Recorded Future Alerts Dashboard and Details

Threat Description / Scenario

Every day, numerous corporate and personal credentials are illicitly traded on underground and dark web forums. Recorded Future actively monitors these sources to identify leaked credentials that belong to an organization. By alerting users the moment a credential is identified, Recorded Future helps enterprises maintain their security posture and take proactive action to protect their accounts and sensitive information.

Procedure

- Alert Generation in Recorded Future UI:** Recorded Future continuously monitors dark web and underground forums for leaked credentials and triggers alerts configured within the user interface, such as credential leaks.
- Ingestion into Microsoft Sentinel:** Configure Microsoft Sentinel to ingest the Recorded Future UI alerts, ensuring they are readily available for analysis and response.
- Alert Processing and Triage:** Analyze the ingested alerts within Microsoft Sentinel to identify credential leaks relevant to the enterprise. Triage involves assessing the scope, impact, and potential risk associated with the leaked credentials.
- Remediation and Verification:** Based on the analysis, perform appropriate actions such as disabling compromised accounts and/or resetting passwords to prevent unauthorized access and further potential attacks.

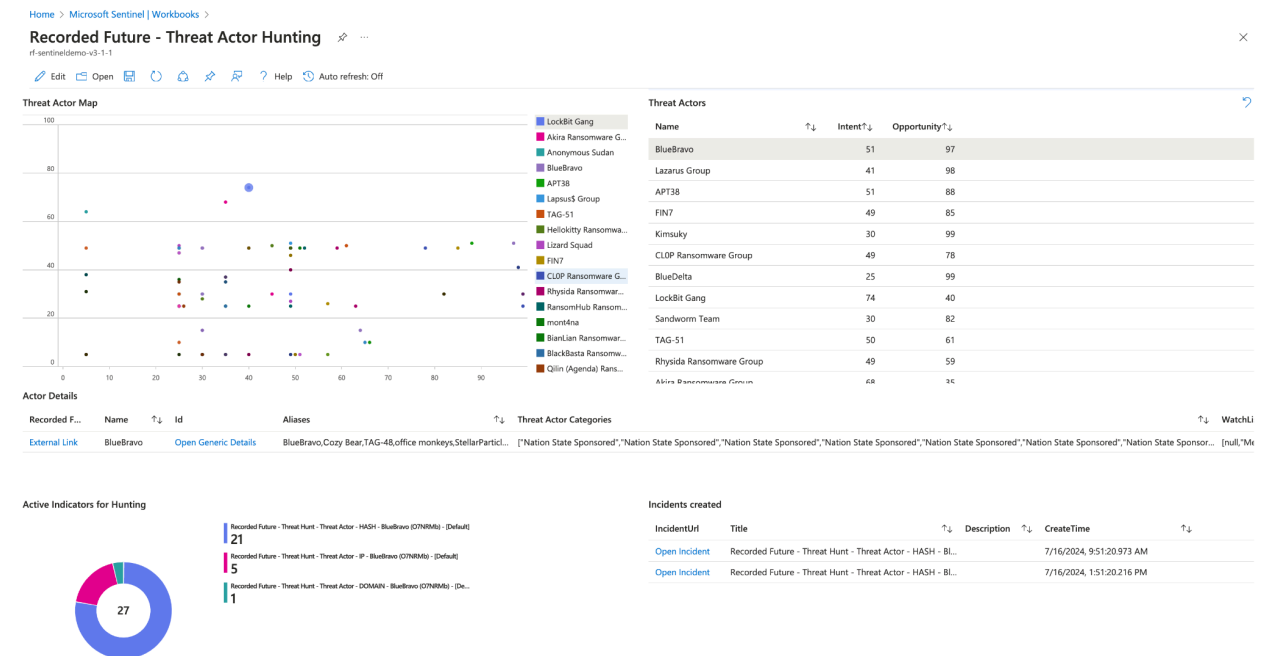
Threat Map Seeded Hunting

Support Article can be found [here](#).

Template playbook can be found [here](#).

Use Case Summary

This use case describes the process of leveraging the Recorded Future Connector for Azure to enhance threat hunting capabilities by utilizing the Recorded Future Threat Map as a seeding point for threat hunting. The objective is to identify and mitigate cyber threats proactively that may have evaded traditional security measures, Recorded Future Links Data can assist by providing Technical Links and Insikt Group Research Links to enhance the search for evasive malware with high fidelity data sets.



Threat Description / Scenario

The threat scenario involves potential cyber threats infiltrating the organization's network, bypassing traditional security measures. These can include APTs, malware, ransomware, or insider threats. The threat actors may aim to steal, alter, or destroy data, disrupt operations, or carry out other malicious activities.

Procedure

- Setup:** Configure the first logic app to fetch threat actor information from the Recorded Future's threat actor map daily. Set a threshold for threat actor scores.
- Threat Identification:** If a threat actor score exceeds the set threshold, the logic app queries Recorded Future's Links API for all relevant linked indicators (IPs, Hashes, Domains, and URLs) tied to that threat actor.
- Data Consolidation:** The identified indicators are then stored in the Microsoft Threat Intelligence (TI) database, labeled as 'Recorded Future Threat Actor Indicators'.
- Rule Application:** Implement an analytic rule that checks for correlations between threat actor indicators and internal telemetry data, such as firewall logs.
- Incident Creation:** If there's a match between the Recorded Future indicators and client logs, the analytic rule triggers the creation of an incident inside Microsoft Sentinel.
- Enrichment & Feedback:** The second logic app enriches the observables with Recorded Future context and sends incident data back to the Recorded Future Intelligence Cloud, which includes Incident title, MITRE Tactics, and threat actor name.

Benefits

- **Proactive Threat Hunting:** Enables proactive detection and mitigation of advanced cyber threats.
- **Contextualized Insights:** Offers enriched, contextualized threat intelligence insights, enhancing understanding of threat actor activities.
- **Efficient Response:** Accelerates incident response times through automated workflows.
- **Threat Prioritization:** Prioritizes threats based on validated and timely intelligence.
- **Continuous Improvement:** *Collective Insights, Feeds back the threat hunting results to Recorded Future's intelligence cloud for continuous monitoring and improvement of the threat hunting process.*

Retroactive Hunting

Use Case Summary

Performing retroactive threat hunting within the Azure platform involves leveraging a combination of SIEM, SOAR, and EDR solutions. This use case highlights the flexibility of the platform and the pivotal role that Recorded Future plays in automating these actions. By utilizing related entities and Recorded Future's Security Control Feeds (SCF), security teams can proactively detect and investigate high-risk indicators following a confirmed breach or incident, as well as identify evasive malware.

Threat Description / Scenario

Malware often employs multi-stage delivery techniques, making it challenging to detect and identify the core malware itself. However, Recorded Future's related entities provide crucial indicators tied to malicious events associated with malware. For example, identifying command-and-control (C2) activity related to a remote access trojan (RAT) can help pinpoint infected assets that may have evasive malware present.

Procedure

1. **Event Triggering (SIEM/EDR):** Detect malware on the wire or via EDR solutions, triggering an event indicating a potential breach or infection.
2. **Automated Investigation (SOAR):** Utilize the SOAR to identify all related indicators and entities associated with the initial event or infected asset.
3. **Recorded Future Integration:** Leverage Recorded Future's related entities and SCF feeds to enrich the investigation, identifying additional high-risk entities or indicators related to the incident.
4. **Threat Analysis and Response:** Analyze the gathered information, prioritize high-risk entities, and take appropriate response actions, such as quarantining infected assets, blocking C2 communication, or inciting incident response procedures.

Benefits

- **Proactive Threat Detection:** Utilize related entities and Recorded Future's SCF feeds to proactively identify potential threats and indicators of compromise.
- **Automated Investigation:** Streamline the investigation process by leveraging SOAR solutions to gather and analyze related indicators and entities.
- **Evasive Malware Detection:** Identify evasive malware by correlating related entities with known indicators.
- **Enhanced Incident Response:** Improve incident response capabilities by quickly identifying and prioritizing high-risk entities based on related indicators and Recorded Future risk score.

Endpoint Proactive Blocking

Use Case Summary

Endpoints are rapidly becoming the new perimeter as remote working becomes more and more popular. Having the ability to detect and respond to threats at the endpoint is crucial to protecting the enterprise. Recorded Future provides the intelligence to ensure malicious indicators can be proactively blocked and suspicious indicators are logged and investigated efficiently when the endpoints are rejoined to the domain.

The screenshot displays the Microsoft Defender for Endpoint console. On the left, the 'Indicators' section shows a table of IP addresses with columns for IP address, Application, Action, Alert severity, Scope, Expires on (UTC), and Title. The first row is selected, showing IP address 59.110.168.221 with an 'Alert and block' action, 'Informational' severity, and 'All devices' scope. On the right, the 'IP' indicator details panel is open, showing the 'Response Action' set to 'Alert and block' and the 'Alert title' as 'Indicator of type IpAddress'. The 'Alert severity' is set to 'Informational' and the 'Description' is 'Recorded Future - IP - C&C Security Control Feed'.

IP address	Application	Action	Alert severity	Scope	Expires on (UTC)	Title
59.110.168.221		Alert and block	Informational	All devices	Mar 17, 2021	Indicator of type IpAddress
31.208.244.153		Alert and block	Informational	All devices	Mar 17, 2021	Indicator of type IpAddress
185.184.25.235		Alert and block	Informational	All devices	Mar 17, 2021	Indicator of type IpAddress
45.93.201.167		Alert and block	Informational	All devices	Mar 17, 2021	Indicator of type IpAddress
61.85.7.243		Alert and block	Informational	All devices	Mar 17, 2021	Indicator of type IpAddress
78.89.177.83		Alert and block	Informational	All devices	Mar 17, 2021	Indicator of type IpAddress
120.136.24.164		Alert and block	Informational	All devices	Mar 17, 2021	Indicator of type IpAddress
211.38.186.45		Alert and block	Informational	All devices	Mar 17, 2021	Indicator of type IpAddress

Alert and Block function within MS Defender for Endpoint EDR

Threat Description / Scenario

Assets utilized away from the corporate network may be subject to insecure networks such as public wifi or home networks. This can lead to infections that would otherwise have been blocked or mitigated by controls on a traditional perimeter network. As the assets are offline, the infection may take hold and sit dormant waiting for the asset to rejoin a domain.

Procedure

- Integration Setup:** Integrate Recorded Future with Microsoft Defender for Endpoint.
- Indicator Identification:** Identify the IOCs to ingest into Defender. These can be malicious URLs, IP addresses, hashes. Specific risk lists can be used to align with the security operations priorities.
- Proactive Blocking:** Configure Microsoft Defender for Endpoint to block access from these malicious IOCs, thereby preventing any potential infections.
- Alert Configuration:** Set up alerts within Microsoft Defender for Endpoint for any suspicious activities or attempts to access blocked IOCs.

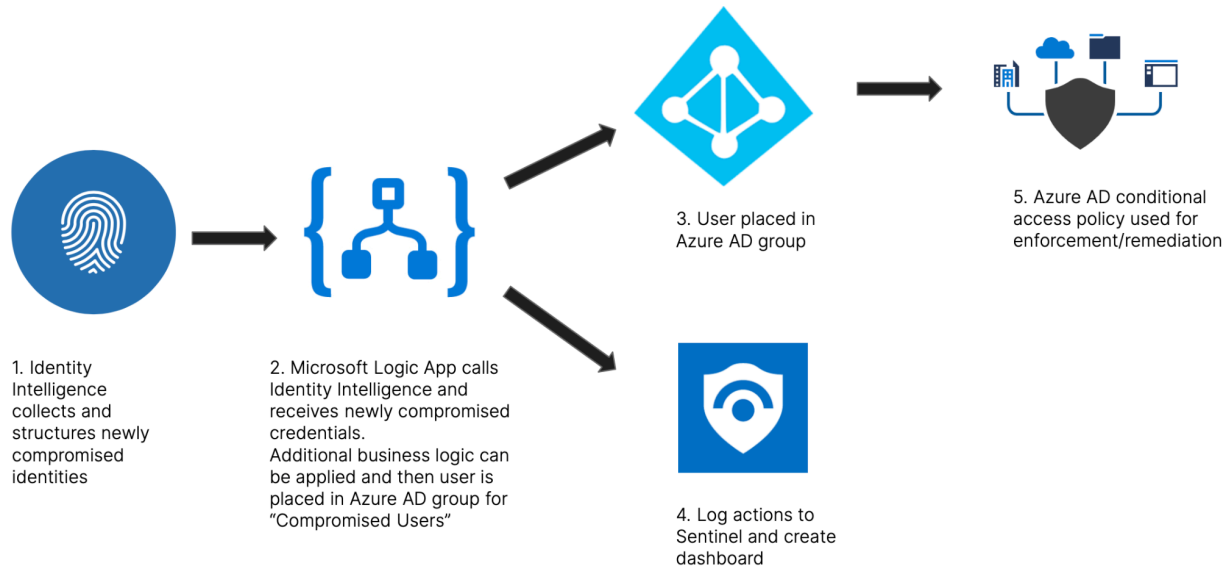
Benefits

- **Asset Protection:** Proactively safeguard assets by blocking access from identified malicious IOCs.
- **Efficient Threat Identification:** Rapidly identify and analyze suspicious events, facilitating swift response and remediation actions.
- **Enhanced Security Posture:** Increase the overall security posture of the organization by proactively protecting assets and efficiently dealing with threats.

Identity Connector

Use Case Summary

Leverage the Recorded Future [Identity Intelligence Connector](#) to proactively detect and respond to employee and customer identity compromises. By automating the collection and analysis of identity intelligence, organizations can enhance their overall security posture and minimize the risk of unauthorized access or data breaches.



Threat Description & Scenario

In today's dynamic threat landscape, compromised employee credentials can lead to unauthorized access, data breaches, and reputational damage. Organizations must adopt a proactive approach to detect identity compromises and take appropriate action to minimize risk.

Procedure

1. **Periodic Monitoring:** Regularly search for newly exposed credentials of employees and customers using the Credential Search action.
2. **Automated Analysis:** When exposed credentials are detected, use the Credential Lookup action to obtain intelligence on the compromised account.
3. **Remediation (Azure Entra-IDy and Microsoft Sentinel):** Implement appropriate remediation steps based on the findings, such as password resets, user privilege revocation, multi-factor authentication setup, or user quarantining.

Benefits

- **Proactive Security:** Detects identity compromises early and takes action to mitigate risk and minimize potential damage.
- **Automation:** Streamline the process of collecting and analyzing identity intelligence data, and automating the triage process associated with prioritizing these incidents.
- **Enhanced Protection:** Implement additional security measures, such as multi-factor authentication, to strengthen overall security posture.

Sandbox Detonation

Detonation Template Playbooks:

- Outlook Attachment detonation [playbook](#)
- Blob storage file detonation [playbook](#)

Use Case Summary

Streamline malware analysis workflows by leveraging the Recorded Future [Sandbox Connector](#). This enables rapid, secure behavioral analysis of files and URLs, which expedites investigation and triage processes.

Threat Description & Scenario

Malware remains a persistent threat in cybersecurity. Rapid identification, understanding, and response to potential malware in files or URLs are crucial in minimizing its impact. By incorporating the Recorded Future Sandbox Connector, security teams can automate the process of submitting potential threats for analysis and retrieving reports for faster decision-making and response.

Procedure

1. **Detection (Microsoft Defender for Endpoint):** Detects potential threats in files or URLs within the network.
2. **Submission (Recorded Future Sandbox Connector):** Use the Sandbox Connector to submit the suspicious file or URL for analysis. This action returns an overview of the submission, including the sample ID.
3. **Analysis (Recorded Future Sandbox Connector):** Wait for the Sandbox to complete the analysis. Retrieve a short summary of the submission status and, once ready, the full report.
4. **Response (Microsoft Sentinel):** Based on the sandbox analysis report, orchestrate appropriate response actions via Microsoft Sentinel.

Benefits

- **Enhanced Speed:** Accelerate the malware analysis process with automated submission and report retrieval.
- **Improved Accuracy:** Gain in-depth insights into potential malware behavior, improving the precision of threat identification and mitigation.
- **Efficient Resource Use:** Free up security team resources by automating routine malware analysis tasks.
- **Holistic Threat Management:** Integrate the Sandbox Connector into existing security workflows for a comprehensive threat management approach.

Automated Phishing Triage

Use Case Summary

Automate the process of detecting, analyzing, and responding to phishing threats in an O365 environment using Azure's security tools and the Recorded Future V2 connector.

Description

This use case involves the use of Azure's security ecosystem, including Sentinel and Defender ATP, along with the Recorded Future V2 connector to create an automated workflow that detects potential phishing emails, enriches them with external threat intelligence data, and then takes action based on the enriched information.

Procedure

1. **Detection:** Utilize Office 365 Advanced Threat Protection (ATP) to detect and flag suspicious emails based on predefined policies or threat indicators.
2. **Alerting:** If a suspicious email is detected, an alert is generated in Microsoft Sentinel.
3. **Enrichment:** Once the alert is generated, an Azure Logic App playbook triggers the Recorded Future V2 connector to enrich the alert data. The connector pulls relevant threat intelligence related to the indicators (like IP, Domain, URL) found in the suspicious email.
4. **Analysis & Action:** After enrichment, the playbook analyzes the enriched data, including the Risk Score, Risk Rules, Intelligence Card Link, and High Confidence Evidence-Based Links provided by Recorded Future. Based on the analysis, the playbook can perform various actions. For instance, if the risk score is above a certain threshold, it might automatically move the email to the user's spam folder, block the sender, or even notify the security team for further investigation.

Benefits

- **Reduced Response Time:** Automated detection, enrichment, and response reduce the time taken to react to potential phishing threats.
- **Improved Accuracy:** Context-rich intelligence from Recorded Future enhances the accuracy of phishing detection, reducing false positives.
- **Maximized Investments:** Leverages existing security tools in the Microsoft ecosystem, ensuring the best utilization of resources.
- **Proactive Threat Management:** Real-time intelligence helps to proactively manage threats, improving the overall security posture.

Sigma Rule Ingestion

Use Case Summary

Recorded Future Sigma Rules can be ingested into Sentinel utilizing a supplied Jupyter Notebook. The objective of this use case is to leverage Recorded Future's Sigma rules, convert them to KQL format and use them for querying Log Analytics workspace or generating Sentinel Analytic Rules for threat detection.

Description

This use case addresses the challenge of staying updated with the rapidly evolving threat landscape. In this scenario, we are utilizing Recorded Future's Sigma rules to improve threat detection capabilities. Sigma rules are a generic and open standard for expressing IDS rules, integrating them into Sentinel allows us to identify sophisticated cyber threats.

Procedure

Follow along the Jupyter Notebook found [here](#)

Benefits

- **Enhanced Threat Detection:** The use of Recorded Future's Sigma rules enhances Microsoft Sentinel's ability to detect sophisticated cyber threats.
- **Automated Updates:** The integration allows for semi-automated updates of Sigma rules, keeping the system's threat detection capabilities up-to-date.
- **Increased Efficiency:** The ability to convert Sigma rules into KQL reduces the need for manual rule writing, thereby increasing operational efficiency.

Integration Conclusion

Summary

Integrating Recorded Future into Microsoft Azure provides a host of benefits as detailed in this document. The flexibility of the platform along with the depth and breadth of Recorded Future's Intelligence introduced at the core of this integration provides additional opportunities over and above those summarized below:

Notably:

- Identification and comprehensive analysis of the Internal threat landscape.
- Automation capabilities to action IOCs with supporting evidence and risk scoring.
- Centralize technologies into a unified suite of solutions with intelligence at its core.

Requirements

- **SecOps Intelligence Module** for entity correlation and enrichment
 - **Risk Lists:** *IP, URL, Domain, Hash*
 - **On-Demand Enrichment:** *IP, URL, Domain, Hash*
- **Threat Intelligence Module** for entity correlation and enrichment and alert ingestion
 - **Risk Lists:** *IP, URL, Domain, Hash*
 - **On-Demand Enrichment:** *IP, URL, Domain, Hash*
 - **Alert data:** *Alert summary & Details*
 - **Intelligence Context:** *Analyst notes (Read & Write)*
- **Brand Intelligence Module** for Alert ingestion
 - **Alert data:** *Alert summary & Details*
 - **Intelligence Context:** *Analyst notes (Read & Write)*
- **GeoPol Intelligence Module** for Alert ingestion
 - **Alert data:** *Alert summary & Details*
 - **Intelligence Context:** *Analyst notes (Read & Write)*
- **Third Party Intelligence Module** for Alert ingestion
 - **Alert data:** *Alert summary & Details*
 - **Intelligence Context:** *Analyst notes (Read & Write)*
- **Vulnerability Intelligence Module** for Alert ingestion & correlation
 - **Risk List:** *Vulnerability*
 - **Alert data:** *Alert summary & Details*
 - **Intelligence Context:** *Analyst notes (Read & Write)*
- **Identity Intelligence Module** for identity lookups using the [Identity Connector](#)
- **Azure Integration License (Cat-A):**
 - [Recorded Future V2 Connector](#)
 - [Sandbox Connector](#)
 - Logic Apps to pull risklists into the TIindicators
 - Template playbooks & correlation dashboards
- **Defender for Endpoint Integration License (Cat-A):**
 - Import to Defender Logic App