Recorded Future®

Palo Alto Cortex XSOAR

Use Case & Capabilities Overview

Created by: Recorded Future Professional Services Architecture Team
Published: February, 2024
Updated: November, 2025
Version: 1.3

Summary

This reference architecture aims to give the reader an understanding of the use cases and capabilities achievable with the Recorded Future integration into Cortex XSOAR. This document also outlines useful commands and their outputs within the 'Technical References - Commands and Outputs' section. This document will also highlight the different content packs available in the Cortex XSOAR Marketplace.

Integration Overview

Security teams overwhelmed by manual work and high alert volumes often rely only on internal data, missing broader threat insights. They need a platform that centralizes real-time intelligence and drives automated action. Recorded Future delivers this by combining its comprehensive threat intelligence with Cortex XSOAR's orchestration and automation to enhance visibility and accelerate response.

- **Threat Triage**:
  With the Recorded Future and Cortex XSOAR integration, analysts can quickly identify high-priority alerts using real-time risk scores backed by clear evidence. An enrichment playbook automates alert prioritization, filters out false positives, highlights major threats, triggers immediate actions, and supports deeper analysis by submitting files and URLs to the Sandbox.

- **Threat Detection**:
  The surge in indicators makes threat detection increasingly difficult for strained security teams. Recorded Future correlates intelligence from a wide range of multilingual sources, providing the context Cortex XSOAR needs to automatically analyze and identify IOCs tied to phishing, malware, and command-and-control activity. This enables automated responses and reduces organizational risk.

- **Threat Hunting:**
  With proprietary, evidence-based insights, organizations can automatically identify and block high-risk IPs, URLs, hashes, and domains, reduce false positives, streamline incident response, and strengthen overall security posture.

- **Vulnerability Prioritization:**
  Recorded Future delivers real-time, relevant context on disclosed vulnerabilities based on an organization's technologies and industry. With direct access to evidence on new and exploited CVEs in Cortex XSOAR, teams can perform deeper analysis and prioritize vulnerabilities more quickly.

- **Real-Time Alert Ingestion:**
  Acting on the context provided in Recorded Future alerts is essential for staying ahead of emerging threats. Pulling this context into Cortex XSOAR enables automated tasks, analyst notifications, and historical reference. Analysts can seamlessly incorporate the added insight into existing workflows, saving time and resources.

- **Identity Exposure:**
  Quickly ingest identity breach alerts to prevent threat actors from exploiting newly compromised credentials. Validate credentials by comparing full and partial hash data, then take immediate action to protect the affected identity.

Content Packs

There are multiple content packs empowering many use cases when implementing Recorded Future Intelligence for orchestration and automation. These packs can be found within the Cortex XSOAR Marketplace.

Content Packs Available:

- ***Recorded Future Intelligence Pack***
    - *The Recorded Future Intelligence Pack brings together several automation use cases within XSOAR. It streamlines reputation lookups, on-demand enrichment for IOCs, and automated list management, helping analysts quickly access high-confidence intelligence during investigations.*
- ***Recorded Future Alerts***
    - *The Recorded Future Alerts pack significantly enhances the UI and overall investigation experience for Recorded Future alerts. Classic and Playbook Alerts are now routed through a classifier and mapper, transforming them into more analyst-friendly alerts optimized for efficient triage.*
- ***Hatching Triage (Recorded Future Sandbox)***
    - *The Hatching Triage integration allows you to submit large volumes of files or URLs to the Recorded Future sandbox. It automatically executes samples, retrieves detailed analysis reports, and supports deeper investigation through dynamic behavioral insights.*
- ***Recorded Future Feed***
    - *The Recorded Future Feed delivers curated risk lists and fusion files directly into XSOAR. These actionable intelligence sources enable teams to proactively identify, alert on, and block malicious IOCs across the environment.*
- ***Recorded Future Identity***
    - *The Recorded Future Identity module helps uncover exposed identities that match an organization's requirements. It provides contextual data for each identity or exposure, supporting faster assessment and response to credential-related threats.*
- ***Recorded Future Attack Surface Intelligence***
    - *The Attack Surface Intelligence integration with XSOAR provides visibility into external assets, exposures, and risks. It helps security teams understand and monitor their attack surface to prioritize remediation and reduce external threat exposure.*

Use Cases

Recorded Future owns and maintains a library of template playbooks available for download on our support site.

Utilizing Recorded Future Intelligence within a SOAR environment is extremely flexible. The following Use Cases are neither exhaustive nor extensive in scope and are designed to portray common Use Cases and provide a quick overview of the capabilities of Cortex XSOAR combined with Recorded Future to gain immediate value from the content packs.

Associated with these Use Cases are Recorded Future's Template Playbooks which can be found within each content pack. By utilizing playbooks, clients can chain together and pass data from one action to another.

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 Cortex XSOAR Use Case development, assistance with creation of custom Use Cases and implementation, please contact your sales rep and arrange a conversation with Professional Services at Recorded Future to see how we can help.

Artifact Enrichment

Use Case Summary

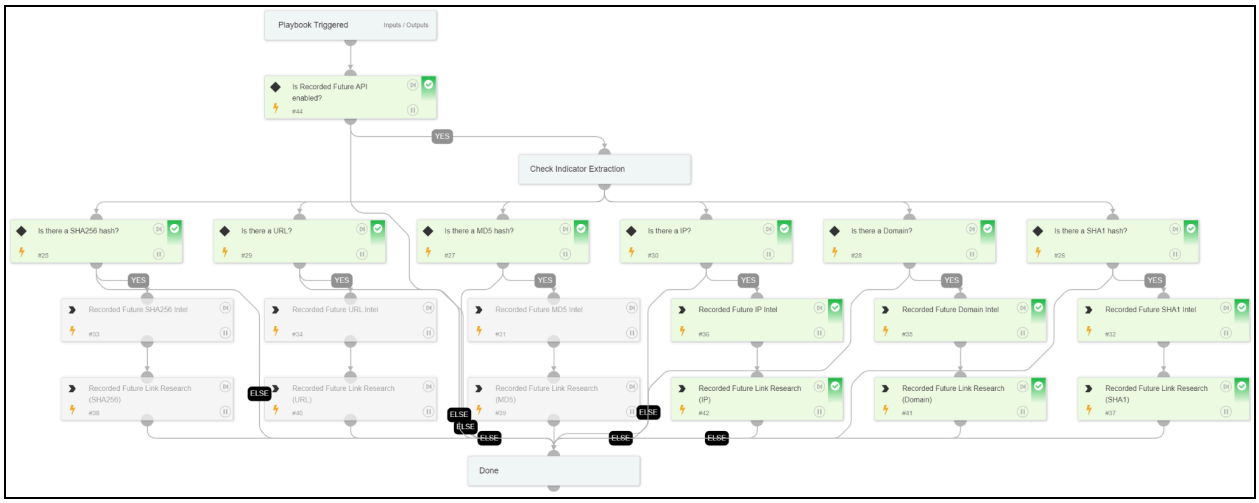
Enrichment capabilities include gathering Technical links and the associated risk scores and risk rules attached to those to understand the potential impact or attribution of a threat. These additional indicators and attributions can aid in understanding the threat.

Issue

Typically identifying technically related indicators following an incident takes time and effort by the Forensic analysis team. The time taken to identify additional indicators can give the attackers time to spread wider or achieve objectives before the incident is fully investigated and mitigated.

Solution

Utilizing Recorded Futures technical links can provide associated threat actors, vulnerabilities, malware and IOCs for the analyst to attribute to previous Incidents (Campaigns & Actors) or perform manual hunting activities on the EDR and / or SIEM to determine if any of the associated indicators are present to extend the detection of the active threat. *Template Playbook*



Threat Map Hunting

Use Case Summary

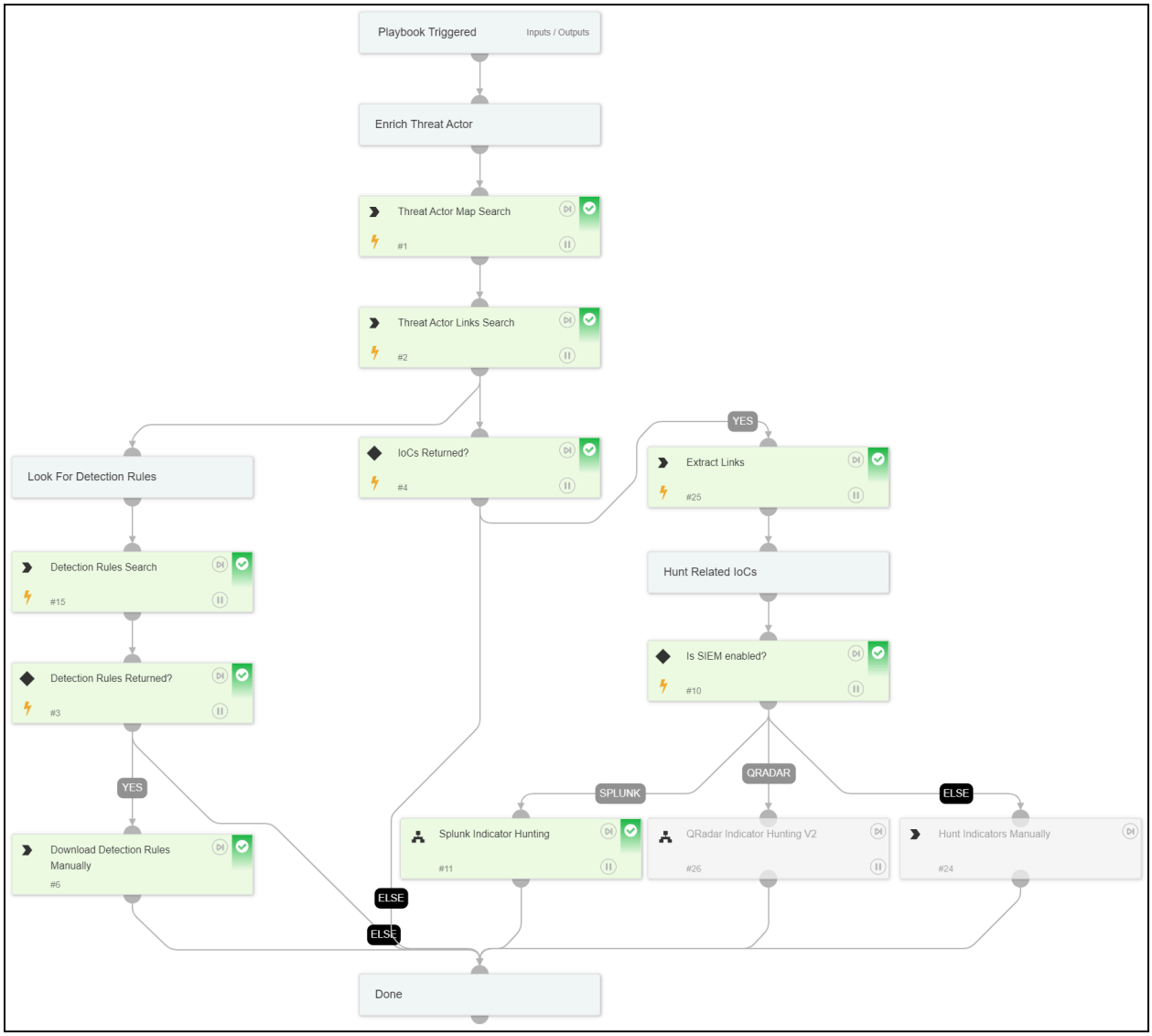
Recorded Future can assist with Threat Hunting utilizing Intelligence led Threat Maps, Threat Actor Indicators and Technical Links to identify new threats previously not detected by SIEM correlation rules.

Issue

Detections are governed by strict syntax and are prone to generate noise and unwanted alerts. Tuning is time consuming and detection can be problematic. Threat Hunting provides a more robust detection method however it is time consuming and doesn't provide timely detection.

Solution

Recorded Future can automate Threat Hunting utilizing Threat Map data derived from your curated watch lists, known threat actors targeting your industry or organization and Recorded Future Analyst driven data to proactively detect threats in your event logs via hunting from the SOAR to the SIEM based on Incident related technical links or automated search criteria utilizing Threat Actor Risk Lists or Threat Map data. *Template Playbook*



Sandbox Detonation

Use Case Summary

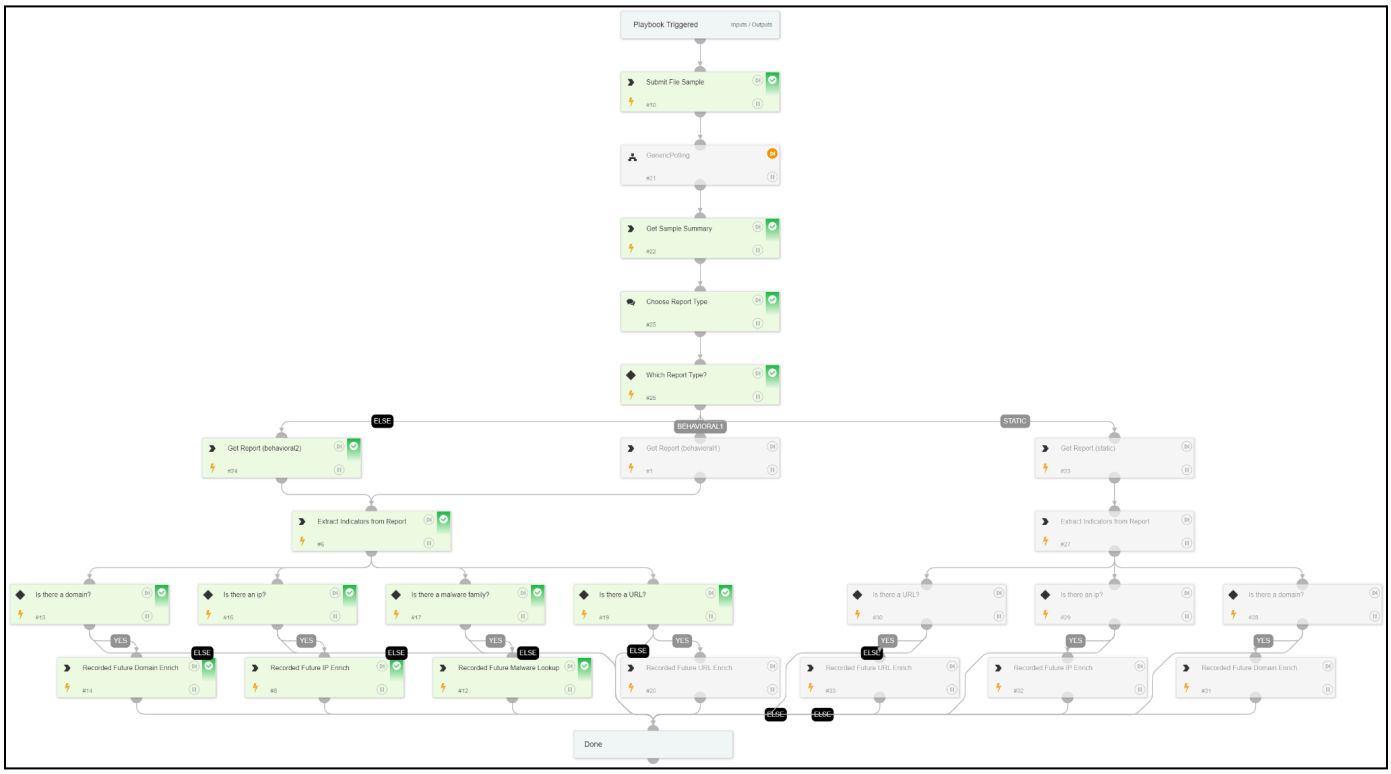
Sandbox analysis is designed to quickly triage a binary or URL to determine the threat based on active automated analysis. Recorded Future further enriches this process via matching Indicators from the sandbox analysis against available intelligence to determine an initial threat level based on risk score and risk rules.

Issue

Typically analysts are overwhelmed with alerts, events and incidents in a SOC and have a minimal amount of time (typically 15 minutes or less) to determine if an Incident is critical, invalid or a low priority. Performing manual analysis of Binaries and URLs can be a time consuming process involving multiple analysis engines, virtual environments and following complex processes.

Solution

Utilizing Recorded Future's Triage Sandbox, URLs and Binary payloads are detonated in a safe environment to determine known threats and further enriched with a risk scoring to determine a baseline threat level. This provides the Analyst team with a detailed analysis report along with a prioritized list of indicators to investigate. *Template Playbook*



Recorded Future Alert Management

Use Case Summary

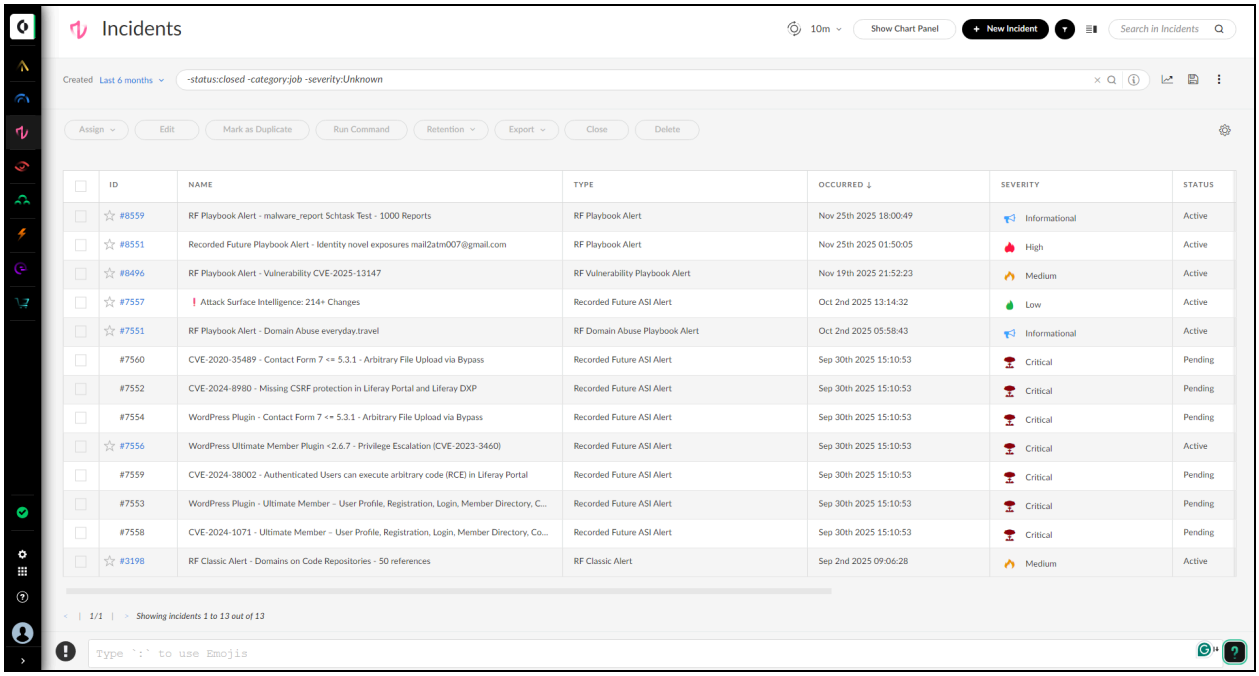
The new Recorded Future integration within XSOAR redesigns the existing integration and format of Recorded Future alerts. Utilising the Recorded Future Alerts package, users can now search & fetch alerts, update the alert status, & writeback to the Recorded Future platform. Screenshots, when present, can be fetched and attached with the accompanying alert.

Issue

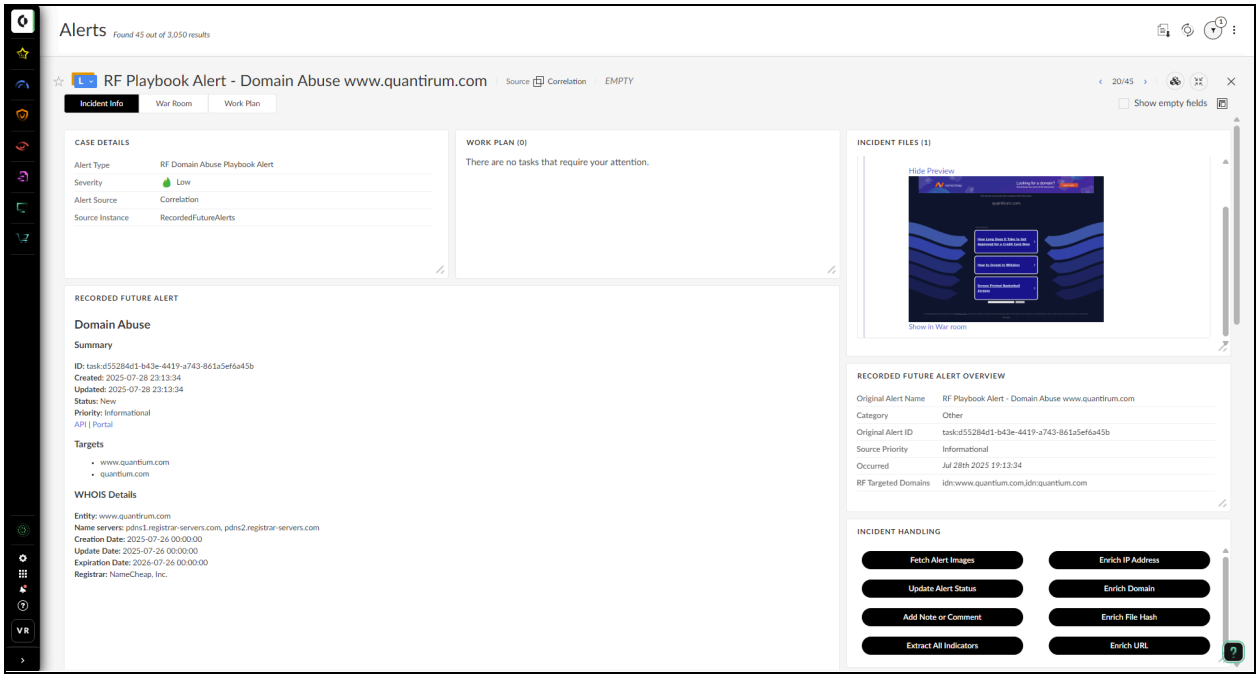
Not all analysts may have access to the Recorded Future portal and switching to platform to manage alerts may become time consuming and be managed on a batch basis as opposed to triaging and handling / closing the alerts in a timely manner as they are produced.

Solution

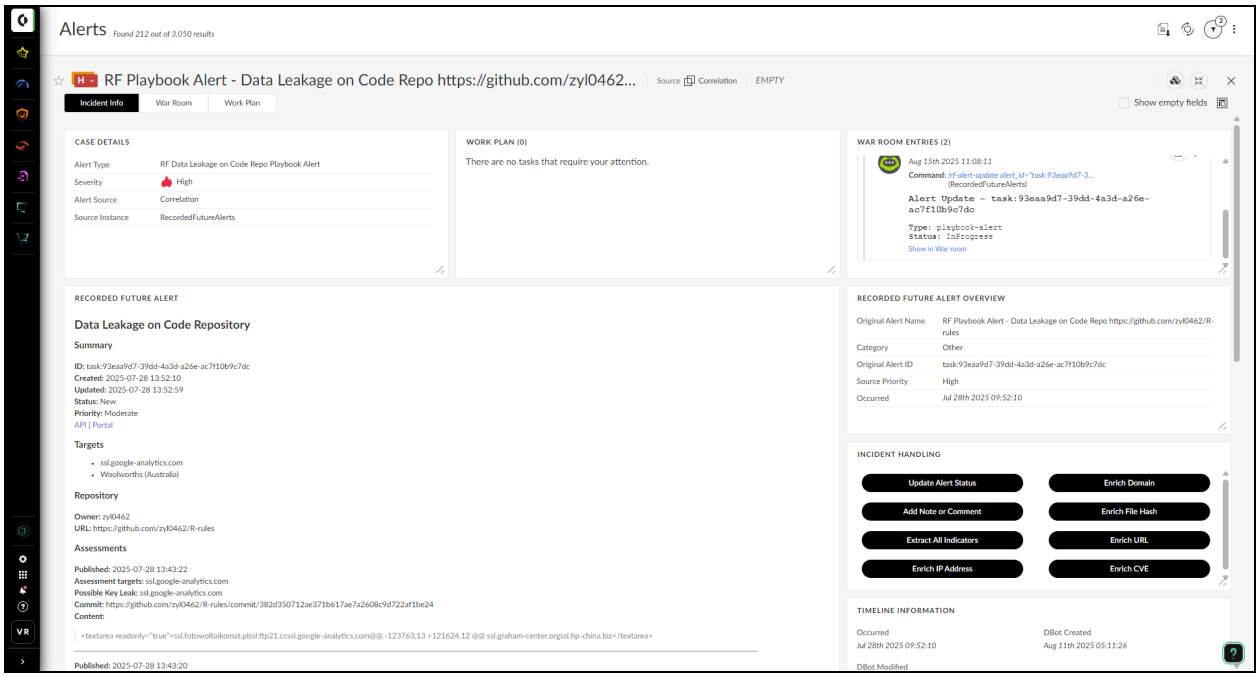
Ingesting Recorded Future Classic & Playbooks alerts into XSOAR provides an opportunity to automatically assign, triage, and close or escalate alerts without the need to manage them manually in the Recorded Future Platform. The integration now ingests alerts using a classifier that identifies the alert type, followed by a mapper that determines which JSON data should populate the incident fields for a more visual and user-friendly UI.



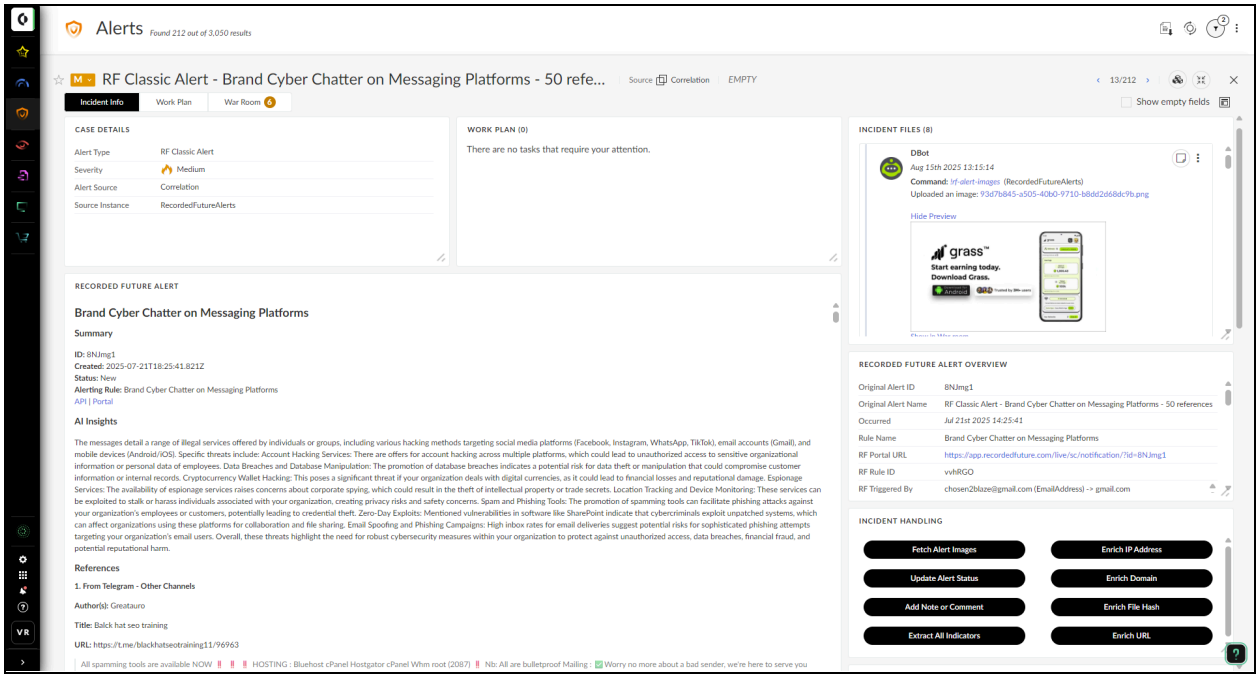
Recorded Future Incidents



Playbook Alert → Domain Abuse



Playbook Alert → Data Leakage on Code Repo



Classic Alert → Brand Cyber Chatter on Messaging Platforms

Vulnerability Alert Handling

Use Case Summary

Recorded Future provides vulnerability alerts against your organization's tech stack. Alerts include pre-NVD and vulnerabilities researched by the Recorded Future Insikt Group. These alerts will provide your organization with relevant vulnerability alerts for consideration of mitigation, patching, or monitoring to detect attempted exploits and protect against them.

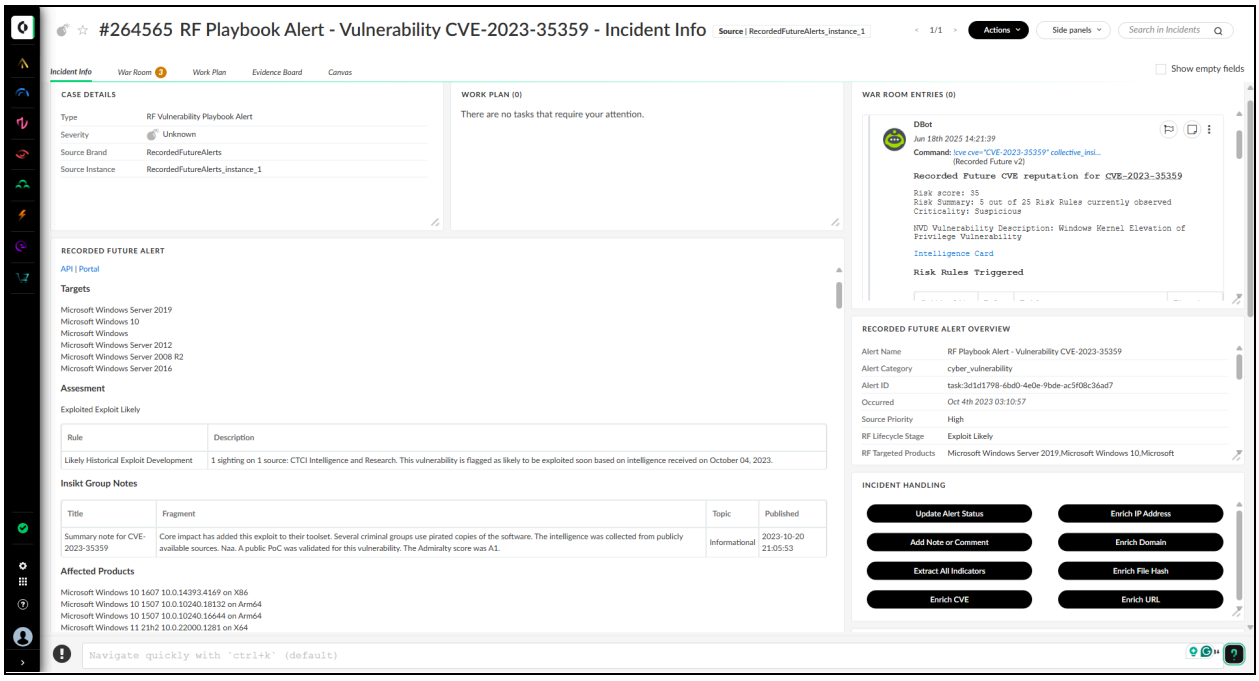
Issue

Vulnerability Management can be a timely and complex task to manage. Organizations typically have a disparate and varied technology stack which leads to difficulty in identifying, mitigating, and patching identified vulnerabilities.

Solution

Performing regular asset and vulnerability scans will provide your organization with up-to-date asset inventories. Ensuring these technologies are included in the Recorded Future Technology Stack Watch List will generate relevant alerts that help identify the most critical vulnerabilities and track their status along the exploitability timeline from proof of concept to exploitation in the wild.

This enables timely and accurate assessments of vulnerable assets and supports informed decisions on whether to implement mitigation, patching, isolation, or additional monitoring to protect the asset and its associated services.



Watch List Management

Use Case Summary

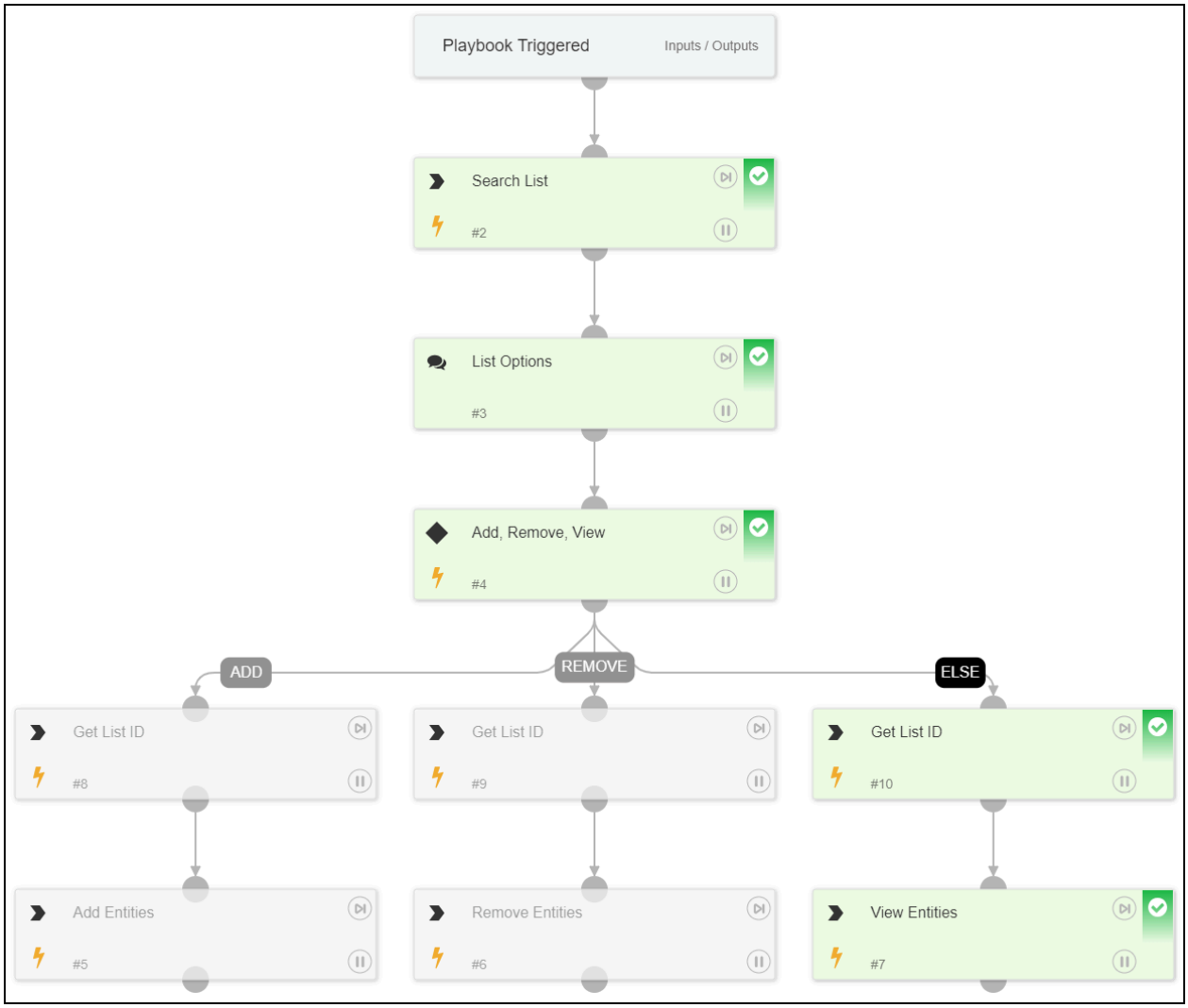
Recorded Future Watch lists help maintain relevance of Recorded Future alerts. The List API Provides a method to automatically maintain and manage these lists outside of the Recorded Future Portal.

Issue

Not all team members may have access to the Recorded Future portal and maintenance of watch lists may be considered a time consuming task which isn't highly prioritized which leads to the watch list data becoming stale and this in turn may generate more unwanted noisy alerts.

Solution

Managing the watch lists through the API allows the technology stacks to be maintained through asset scanners / vulnerability scanners ensuring the vulnerability alerts are always accurate and reflect potential threats to the organization. *Template Playbook*



Dynamic Blocking

Use Case Summary

Performing automated or analyst decision gated decision blocks against firewall and endpoint devices ensures accuracy and timely action is performed against known bad IOCs.

Issue

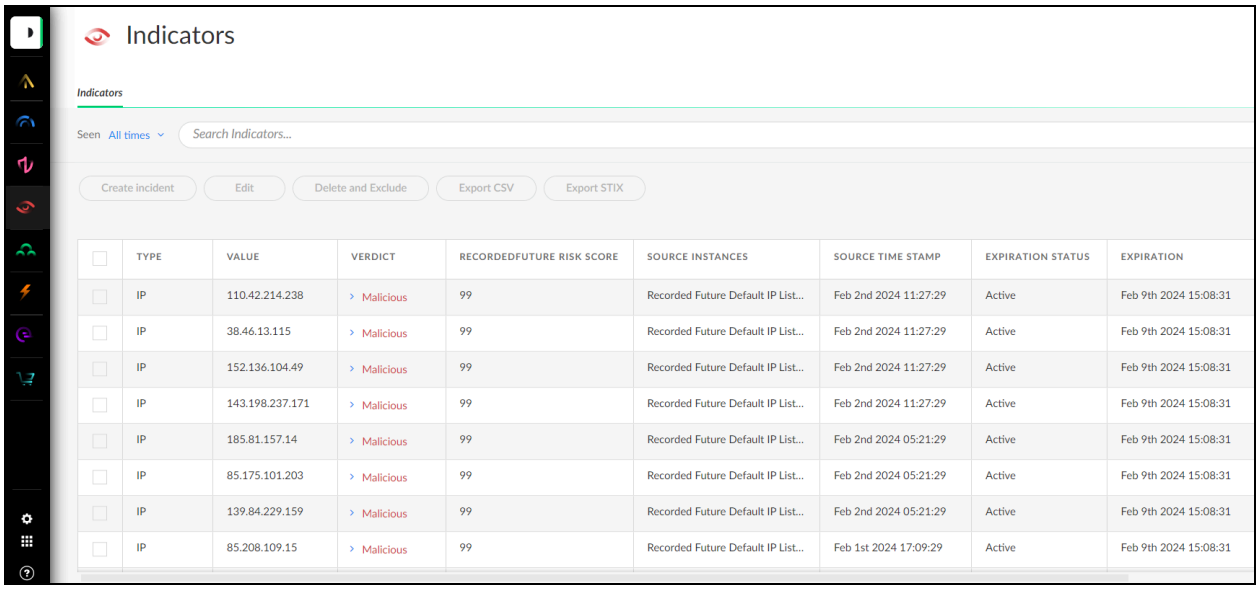
Determining whether to block an entity can be a time consuming task involving checking safe lists, critical asset lists and identifying whether the entity should be blocked based on triage information and intelligence. During this time, the entity may have been utilized by more victims or the threat actor to conduct objectives.

Solution

Automatically verify whether an entity with a high risk score is on a safe list, watchlist or no list and make appropriate decisions based on that data. For example if a high risk IP is not a safe list and the victim asset is on the critical assets list, it may be pertinent to Proactively block the IP and flag the Incident for priority triage / investigation to determine if the IP should remain blocked or be removed from the Block list. This will ensure critical assets are protected much faster and remediated quickly following automated threat mitigation.

Proactive blocking may also be utilized via pushing known high threat data to firewalls on a regular cadence. Recorded Future Security Control Feeds for example may be utilized to frequently update a known C2 Block list on a Firewall.

Batch enrichment could also be utilized to enrich large feed lists obtained from third parties with no previous context to determine a threat level and baseline to block high fidelity bad entities.



TYPE	VALUE	VERDICT	RECORDEDFUTURE RISK SCORE	SOURCE INSTANCES	SOURCE TIME STAMP	EXPIRATION STATUS	EXPIRATION
IP	110.42.214.238	Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 11:27:29	Active	Feb 9th 2024 15:08:31
IP	38.46.13.115	Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 11:27:29	Active	Feb 9th 2024 15:08:31
IP	152.136.104.49	Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 11:27:29	Active	Feb 9th 2024 15:08:31
IP	143.198.237.171	Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 11:27:29	Active	Feb 9th 2024 15:08:31
IP	185.81.157.14	Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 05:21:29	Active	Feb 9th 2024 15:08:31
IP	85.175.101.203	Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 05:21:29	Active	Feb 9th 2024 15:08:31
IP	139.84.229.159	Malicious	99	Recorded Future Default IP List...	Feb 2nd 2024 05:21:29	Active	Feb 9th 2024 15:08:31
IP	85.208.109.15	Malicious	99	Recorded Future Default IP List...	Feb 1st 2024 17:09:29	Active	Feb 9th 2024 15:08:31

Custom File Ingestion

Utilizing the Recorded Future Fusion API, security teams can create custom data outputs for SOAR Platforms, SIEMs, ticketing systems, endpoint security, and other analytic tools or security devices using internal client-sourced data enriched with Recorded Future's threat intelligence data. Or simply combine / augment the details available in the Recorded Future Graph API to a custom Recorded Future Risk List (for example combining multiple risk lists and reducing the fields to a simple block list).

Security Control Feed Ingestion

Security Control Feeds are precompiled Detect and Block grade Intelligence Feeds based on Recorded Future Data generated from internally verified sources & methods to create datasets for specific security use cases. The purpose of these feeds is for proactive blocking and high fidelity detection of threats. Unlike 'Recorded Future Risk Lists', Security Control Feeds do not contain 'Risk Scores', 'Risk Rules' or 'Evidence Details'.

The Security Control Feeds do in some instances generate risk rules against data contained in the Recorded Future Intelligence Graph; this data is on the "Recorded Future Risk Lists". As such not all Security Control Feed IOCs are contained in the Recorded Future Graph and some that are may have a low risk score; this does not detract from the fidelity of the IOC being high due to inclusion in the Security Control Feed.

Identity Exposure

Use Case Summary

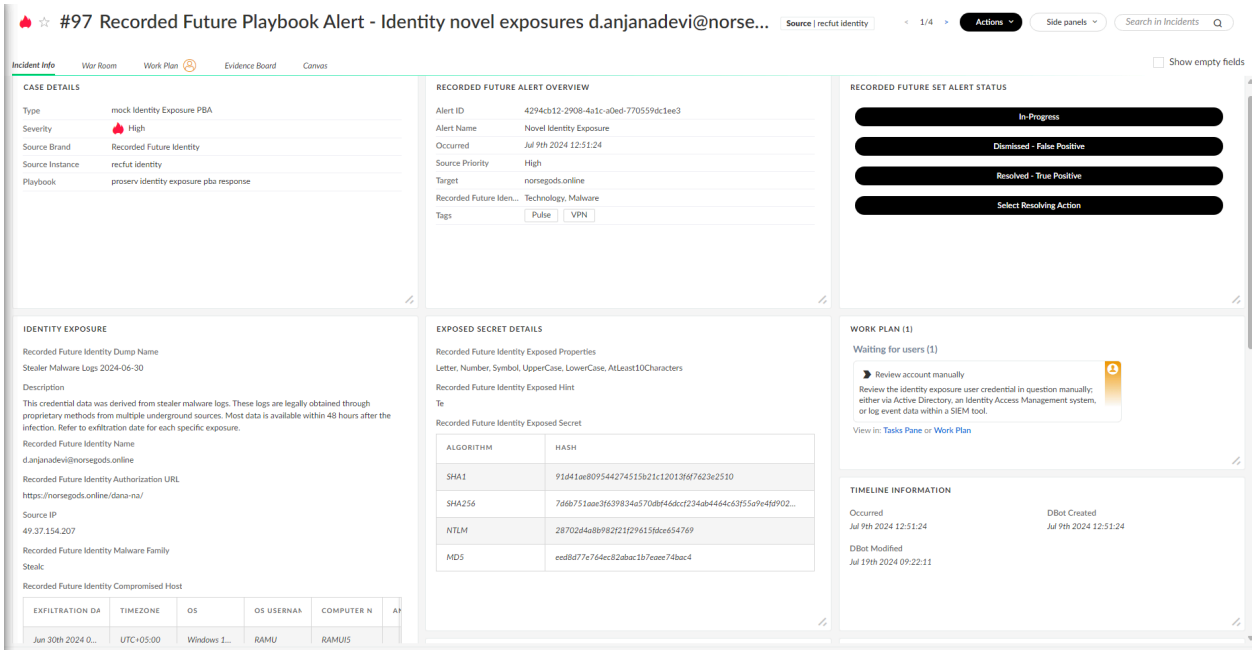
Credentials are commonly used to laterally move around a network undetected for long periods of time. Identifying leaked or stolen credentials early can assist with quick mitigation or identification of an asset breach.

Issue

Commonly, data breaches are detected before identity exposures. Infostealer malware may extract credentials for resale, or to be utilized in a later attack. It can be difficult to detect and attribute credential breaches to an attack after the breach has occurred without extensive forensic analysis.

Solution

Leverage the Recorded Future Identity Intelligence integration 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. *Template Playbook*



Detection Rules (Sigma, YARA, Snort)

Use Case Summary

Detection rules help identify malicious behavior across endpoints, files, and network traffic. Integrating Recorded Future detection content into XSOAR enables rapid operationalization of high-confidence intelligence, improving proactive threat detection.

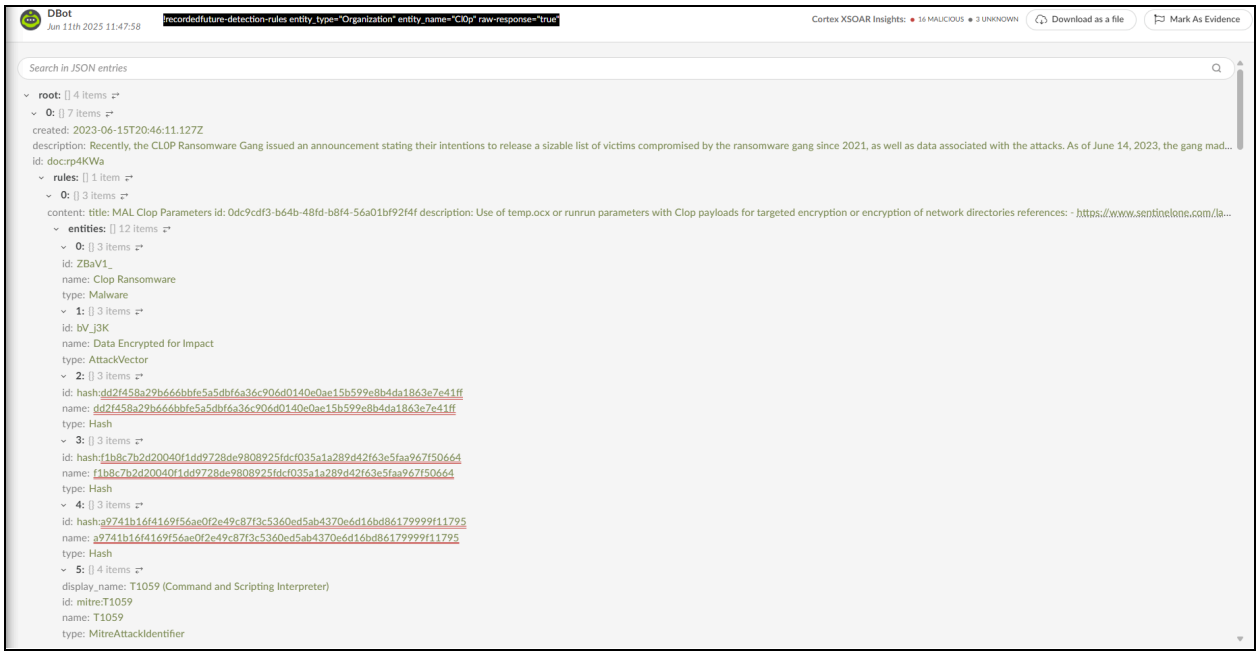
Issue

Manually searching for, validating, and updating detection rules is time-consuming and often inconsistent. Without automated context such as MITRE ATT&CK mappings, threat actor associations, or malware family relevance detections may be limited, outdated, or prone to false positives.

Solution

Use the Recorded Future integration with XSOAR to automatically query and ingest Sigma, YARA, and Snort rules. Searches can be filtered by rule type, entity, or Insikt Group analyst note title, ensuring only relevant detection content is returned.

XSOAR can then extract the rule title, description, and full detection logic, along with contextual tagging such as techniques, malware families, threat actors, and related vulnerabilities.



Collective Insights

Use Case Summary

Enriched security events serve as inputs into the Recorded Future platform, unveiling patterns and emerging trends across security tools employed by all clients. The fusion of Recorded Future Intelligence and Collective Insights from Cortex XSOAR delivers a comprehensive and holistic perspective, empowering organizations to effectively prioritize and address potential threats.

Issue

Effective detection of emerging threats faced by organizations require proactive insights from what is happening internally, externally, and to other organizations.

Solution

Customize insights based on internal telemetry with the new SecOps Intelligence dashboard, helping to proactively detect threats, and prioritize them based on risk factors. In addition, map detections against the MITRE ATT&CK framework to show what types of adversary TTPs are being used within the environment to prioritize mitigation techniques effectively. Collective Insights currently powers the Malware Threat Map within the Threat Intelligence module as well.

Opportunity *- A correlation between the malware's capabilities and an organization's vulnerabilities.*

Additional Reading

Find below additional information of the various Recorded Future products mentioned throughout this document.

[Recorded Future Sandbox FAQ]
[Recorded Future Vulnerability Intelligence Module]
[Recorded Future SecOps Module]
[Recorded Future Threat Intelligence Module]
[Recorded Future Brand Intelligence Module]
[Recorded Future List API]
[Recorded Future Entity Match API]
[Recorded Future Threat Map]

Professional Services Assistance

Recorded Future provides a custom service for Use Case Development 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 Cortex XSOAR use case development or assistance with creating custom use cases and implementation, please get in touch with your Sales or Intelligence Services representative and arrange a conversation with Professional Services at Recorded Future to see how.