rubrik

Accelerate Incident Response with AI-Assisted Cyber Recovery

Rubrik Security Cloud Integration for Microsoft Sentinel

Microsoft Sentinel users can accelerate and enrich threat investigations with data risk insights and speed up recovery time with automated responses.

CHALLENGE

Security Operations teams (SecOps) have leveraged SIEM/SOAR tools, like Microsoft Sentinel, to aggregate and normalize their security events, alert on threat detection, and most importantly, orchestrate threat responses through various automated playbooks. However, recovering from ransomware threats requires tight collaboration between SecOps and IT Operations (ITOps) to answer important questions including:

- What is the blast radius of the attack? What applications, files, and folders have been compromised?
- Has any sensitive information been affected and where is it located?
- When did the first occurrence of malware enter the environment? What is the last known clean copy of data?
- Can we safely restore applications without the risk of reinfecting the environment?

Unfortunately, due to the siloed nature of many organizations, answering these questions today adds to the threat response time and increases the organizations' downtime. But what if we could bring insights from both the SecOps and IT Ops departments together in a centralized location to improve collaboration and automate recoveries?

SOLUTION

With the Rubrik Security Cloud integration into Microsoft Sentinel, Rubrik delivers data risk insights into Microsoft Sentinel. Leveraging these insights, Security and IT Operations teams can provide more efficient incident response, automate recoveries, and decrease business downtime. Strengthen your data security strategy by incorporating key intelligence from Rubrik, such as:

- **Anomaly Detection** – Rubrik uses a two-stage machine learning algorithm to detect file entropy and signs of encryption or malware. These insights are sent to Sentinel to provide visibility of the blast radius of an encryption attack.
- **Sensitive Data Monitoring** – Rubrik identifies sensitive data such as PII or PCI-DSS by using pre-built or custom analyzers. Sensitive data discovered is then sent and is available within Microsoft Sentinel to aid in the threat response.

CUSTOMER BENEFITS

Together, Microsoft and Rubrik integrate to strengthen your data protection and data security strategy. Microsoft provides security tooling such as SIEM/SOAR capabilities, while Rubrik ensures accelerated ransomware recovery across hundreds or even thousands of users.

The integration between Microsoft Sentinel and Rubrik Security Cloud provides capabilities that can help mitigate business risks, such as the mean time to respond, and the mean time to resolve a security incident.

Insights and Alerts in the Sentinel Dashboard:

Conduct deeper and faster investigations to help understand the scope and root cause of an attack.

Prevent Malware Reinfection:

Easily identify the last known "clean copy" and prevent malware reinfection.

Rapid and Granular Recovery:

Fast recovery, right from Sentinel, with prebuilt workflows and blueprints providing better IT/SecOps collaboration.

- **Threat Hunting** – Rubrik uses malware-specific YARA rules to investigate a time-series history of data, pinpoint the initial infection, and then sends a list of both clean and infected snapshots to Sentinel to aid in recovery efforts.
- **Automated, mass, or surgical recovery** – Rubrik provides the ability to surgically recover only what is needed or to pursue mass image-level recovery of applications. The different recovery methods provided by Rubrik can be executed directly from within Microsoft Sentinel.

By bringing data risk insights from both SecOps and ITOps together, organizations are able to determine the scope of the attack more efficiently, automate recoveries, and save valuable time.

ACCELERATE INCIDENT RESPONSE WITH AI ASSISTED CYBER RECOVERIES (Coming Soon)

During a cyber event, time is of the essence and knowing exactly what to do next is crucial to responding quickly to cyber incidents. Leveraging the Azure OpenAI service, the Rubrik Security Cloud integration for Microsoft Sentinel generates customized recommendations and suggested next steps, attaching them to the newly created incident as tasks. Incident responders can take advantage of AI-generated tasks in order to:

- Identify the scope of the potential attack.
- Identify and quarantine traces of malware within their backups.
- Perform deeper investigations with AI generated Kusto Query Language (KQL) syntax directly within Sentinel.

INTELLIGENT, AUTOMATED PLAYBOOKS

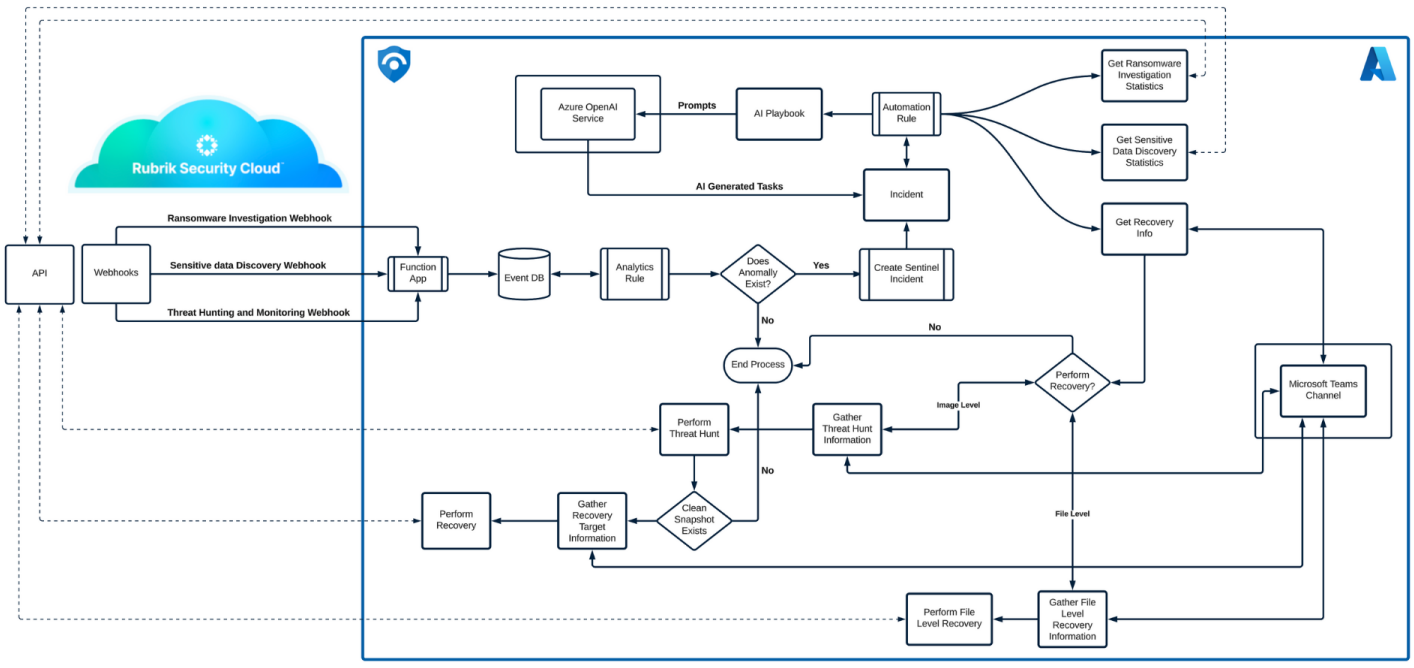
The Rubrik Security Cloud integration for Microsoft Sentinel includes a custom data connector along with 8 pre-built, intelligent playbooks that can be used to respond to security incidents, gather information about anomalies, determine if sensitive data has been exposed, execute threat hunts for indicators of compromise and perform both file and image level recoveries.

DEPLOY DIRECTLY FROM THE SENTINEL CONTENT HUB

The Rubrik Security Cloud integration for Microsoft Sentinel can be easily deployed into any Sentinel instance through the Sentinel Content Hub.

HOW IT WORKS

Through the Microsoft Sentinel Content Hub, the Rubrik Security Cloud integration can be easily discovered, installed and configured. Upon completion the Rubrik data connector and subsequent playbooks are ready to use. From there, simply configure the webhooks functionality within Rubrik Security Cloud to send anomaly, sensitive data, and threat-hunting events to the newly deployed data connector.



As anomalies are detected within Rubrik and sent to Microsoft Sentinel, a custom analytics rule is triggered which automates the creation of an incident. Simultaneous to the incident creation, a playbook is executed, gathering further information around the anomaly such as the number of files and folders which have been created, modified, and deleted, along with whether signs of encryption are present. Information from Rubrik Sensitive Data Monitoring service is also collected, allowing operators to easily see if sensitive information such as PII or HIPAA data has been compromised.

Once complete, Microsoft Teams is utilized to gather further information required in order to complete a recovery. If recovery is needed, information is passed through Microsoft Teams to Sentinel which initiates a Rubrik Threat Hunt to determine the last known clean copy of data based on user-specified YARA rules.

When Rubrik determines that last known clean backup, the recovery is automatically invoked—all without leaving the confines of Microsoft Sentinel.

SAFE HARBOR STATEMENT: Any unreleased services or features referenced in this document are not currently available and may not be made generally available on time or at all, as may be determined in our sole discretion. Any such referenced services or features do not represent promises to deliver, commitments, or obligations of Rubrik, Inc. and may not be incorporated into any contract. Customers should make their purchase decisions based upon services and features that are currently generally available.

ABOUT RUBRIK

Rubrik is a cybersecurity company, and our mission is to secure the world's data. We pioneered Zero Trust Data Security™ to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

PROUD MISA MEMBER

Member of
Microsoft Intelligent Security Association
Microsoft

The Microsoft Intelligent Security Association (MISA) is an ecosystem of independent software vendors and managed security service providers that have integrated their solutions to better defend against a world of increasingly sophisticated, fast-moving threats.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik is a cybersecurity company, and our mission is to secure the world's data. We pioneered Zero Trust Data Security™ to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, delivers data protection and cyber resilience in a single platform across enterprise, cloud, and SaaS applications. Our platform automates policy management of data and enforcement of data security through the entire data lifecycle. We help organizations uphold data integrity, deliver data availability, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.

ds-accelerate-incident-response-with-ai-assisted-cyber-recovery / 20230906