rubrik

Get a Head Start in the Race against Ransomware

Rubrik Security Cloud Integration for Microsoft Sentinel

Microsoft Sentinel users can accelerate and enrich threat investigations with more 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, SecOps can't do this alone. Responding to a threat results in the need for some sort of recovery to take place, which in turn involves collaboration with IT Operations (ITOps) teams to answer important questions around ransomware recovery such as

- 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, retrieving the answers to these questions only adds to the threat response time and increases the organizations' downtime. But what if there was a better way? What if we could bring insights from both the SecOps and IT Ops departments together in a centralized location to foster collaboration and automate recoveries?

SOLUTION

With the Rubrik Security Cloud integration into Microsoft Sentinel, Security and IT Operations teams now have the ability to make data-driven decisions around threat response and automate recoveries directly from within Microsoft Sentinel. This new integration brings delivers key Rubrik data security insights and functionality front and center into Microsoft Sentinel such as:

- **Ransomware Investigation & Monitoring** – After each and every backup, Rubrik Security Cloud leverages a machine learning algorithm to detect the change rate between snapshots, resulting in a listing of files which have been created, modified and deleted. This listing is then sent through another machine-learning algorithm that looks for encryption and ransomware signs. This resulting blast radius is then sent to Microsoft Sentinel and attached to an incident to aid in the threat response

CUSTOMER BENEFITS

Together, Microsoft and Rubrik strengthen your defense in depth to give you complete data protection. Microsoft provides perimeter security while Rubrik accelerates ransomware recovery across hundreds or even thousands of users.

The integration between Microsoft Sentinel and Rubrik Security Cloud provides organizations with a better way to manage the risk of business disruption while minimizing the financial impact of ransomware

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

- **Sensitive Data Monitoring & Management** – Rubrik enables the ability to scan for sensitive data based on a number of prebuilt and custom analyzers mapped to common compliance regulations such as Personally Identifiable Information (PII) and PCI-DSS. Results from these scans are then sent to Microsoft Sentinel and attached to an incident to aid in the threat response.
- **Threat Monitoring and Hunting** – Using YARA rules targeting malware, Rubrik investigates a time-series history of data points to determine when the initial infection occurred. This listing of both infected and clean snapshots is sent to Microsoft 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 many recovery methods provided by Rubrik can be executed directly from within Microsoft Sentinel

By bringing data 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 and money.

HOW IT WORKS

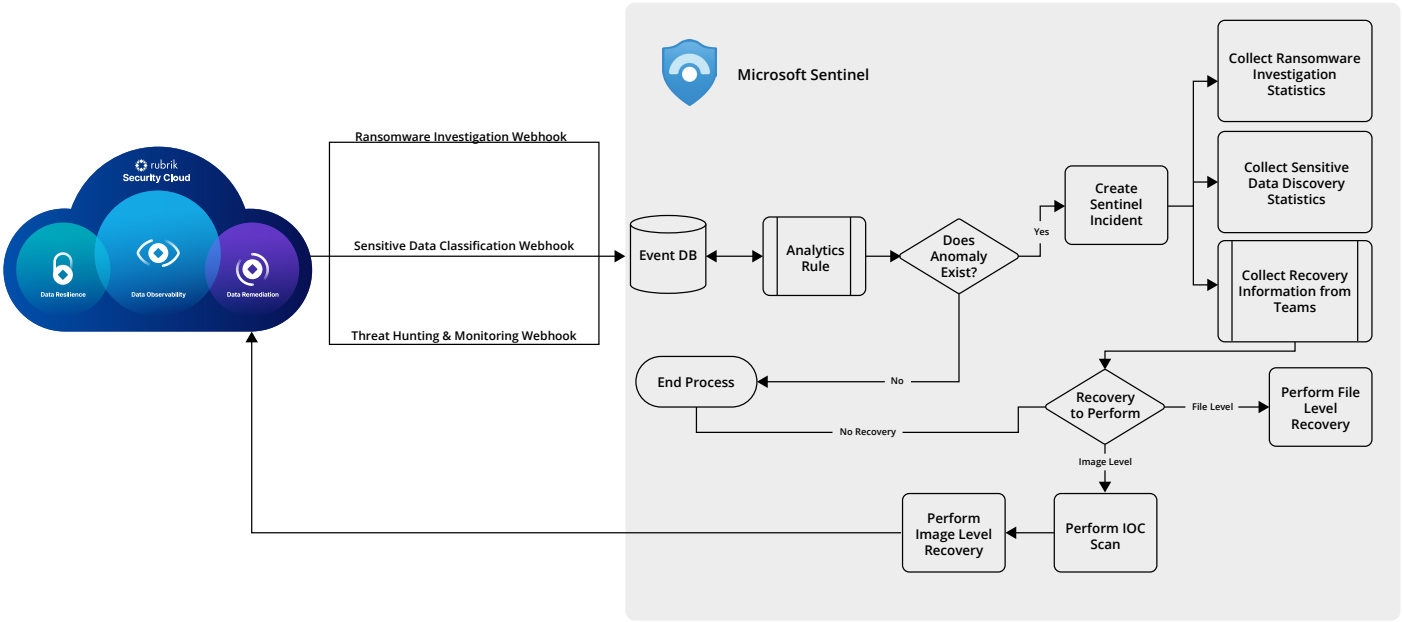
Installation of the Rubrik Sentinel integration is a breeze and can be accomplished in a few minutes. First, install the Rubrik Data Connector through the Sentinel Data Connectors gallery. From there, simply configure the webhooks functionality within Rubrik Security Cloud to send anomaly, sensitive data, and threat-hunting events to the newly deployed function URL.

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.



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 and Remediation service is also collected, allowing operators to easily see if any of their sensitive information such as PII or HIPAA has been compromised.

Once complete, an adaptive card is sent to a designated Microsoft Teams channel where both Security and IT Operations can collaborate on the issue and ultimately make a decision on whether or not to trigger 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.

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

brf-microsoft-sentinel / 20221103