COHESITY | CROWDSTRIKE

SOLUTION BRIEF

Ransomware Protection and Recovery

Security Incident and Event Management (SIEM)

Key Benefits

- Enhance visibility of defenses to eliminate blind spots.
- Automatic anomaly routing to launch incident response.
- Improve speed and reliability of ransomware recovery.

In the ever-changing landscape of cyber threats, organizations must automate the analysis and response to various risks, including those targeting their data security and management platform. This platform serves as a crucial safeguard by creating reliable backups of critical data. To ensure the platform's dependability and the integrity of recovery data in the face of destructive cyber events like ransomware, organizations need advanced measures.

Business Challenge

To combat the rising tide of ransomware attacks, collaboration between SecOps, ITOps, and NetOps organizations is crucial. However, traditional security measures and outdated data protection solutions present challenges, including:

1. **Complexity**: Investigating incidents across multiple consoles creates complexity, hindering the estimation of ransomware recovery service level agreements (SLAs) and increasing business risks.
2. **Siloed Visibility**: Limited visibility into data leads to longer dwell time during ransomware attacks, impairing quick response and containment.
3. **Slow Remediation**: Manual coordination among dispersed operational teams slows down the investigation and recovery process, resulting in disruptions and employee burnout.

Benefits of Automation

Implementing automation in security incident and event management offers several benefits, including:

1. **Enhanced Visibility:** Automation eliminates blind spots and provides improved visibility of defenses, ensuring comprehensive threat detection without any gaps.
2. **Automatic Anomaly Routing:** An automated system can efficiently route anomalies, enabling swift incident response and reducing manual intervention.
3. **Improved Ransomware Recovery:** Automation enhances the speed and reliability of ransomware recovery processes, minimizing downtime and data loss.

Modern Solutions for Effective Response

To address these challenges, organizations must adopt modern solutions that facilitate collaboration, streamline processes, and offer comprehensive visibility into data. These solutions provide organizations with AI enabled capabilities to withstand and recover from cyber incidents.

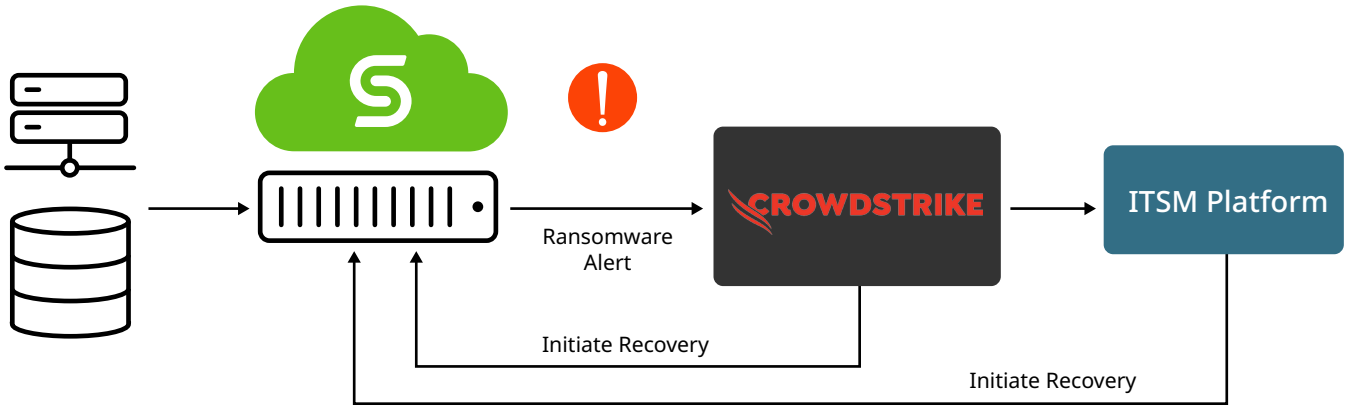

Figure 1: CrowdStrike Logscale and Cohesity Architecture

The integration of Cohesity and CrowdStrike significantly improves data protection, detection, response and recovery capabilities. It provides enhanced visibility and contextual insights into anomalies detected in production data by the data security and management platform. This integration empowers IT administrators and Security Operations Centers (SOCs) with simultaneous access to alerts, enabling swift response to ransomware attacks.

CrowdStrike consolidates valuable threat intelligence, enhancing security operations by providing comprehensive visibility into active ransomware threats. This enriched visibility enables quick correlation, triage, investigation, and response to ransomware incidents within a single location.

Through this integration, CrowdStrike plays a vital role in collecting and consolidating information, enabling security teams to investigate and take necessary actions from the CrowdStrike platform. These actions may include initiating workflows to restore compromised data or workloads to the last clean snapshot, facilitating a rapid recovery process.

To learn more, visit the Cohesity Marketplace

COHESITY