SOLUTION BRIEF

Commvault Cloud integration with Palo Alto Networks XSOAR

Automate and orchestrate threat remediation and recovery actions

CHALLENGE

The relationship between IT and security teams can be challenging when trying to balance incident response and cyber recovery following a cyber incident. While the two teams use different systems and processes to accomplish their goals—investigate and remediate threats to the business and recover data quickly and cleanly—one is not possible without the other.

When an attack occurs, it's important to give security teams control of mechanisms to protect the last line of defense—backups. And they need to be able to do it without needing to learn a new tool.

Better collaboration
Enable security and IT teams to work better together by correlating security events and sharing data between Commvault and SecOps' tools, like XSOAR.

Faster incident response
Orchestrate actions that help security teams quickly respond to threats and protect their backup data by using the playbooks and tools they're familiar with.

Improved security
Respond and recover from cyber events faster and with confidence that the data protection environment is protected.

SOLUTION

Enabling security teams to perform actions on backup data and giving security teams visibility into data threats that may be detected using different detection technologies is a force multiplier when it comes to accomplishing their incident response and cyber recovery goals.

Commvault Cloud has built in threat detection capabilities that surface anomalies in file and backup behavior, as well as scan files to detect the presence of malware. If Commvault detects threats, those threats are surfaced in the Threat Indicator dashboard within Commvault and can also be automatically sent to SIEM/SOAR tools, like Palo Alto Networks XSOAR.

Pre-built Work Plans provide easy, out-of-the-box workflows that enable SecOps teams to respond to suspicious activity detected by Commvault or their other security tools. These workflows can also be customized to match an organizations' incident response plan.

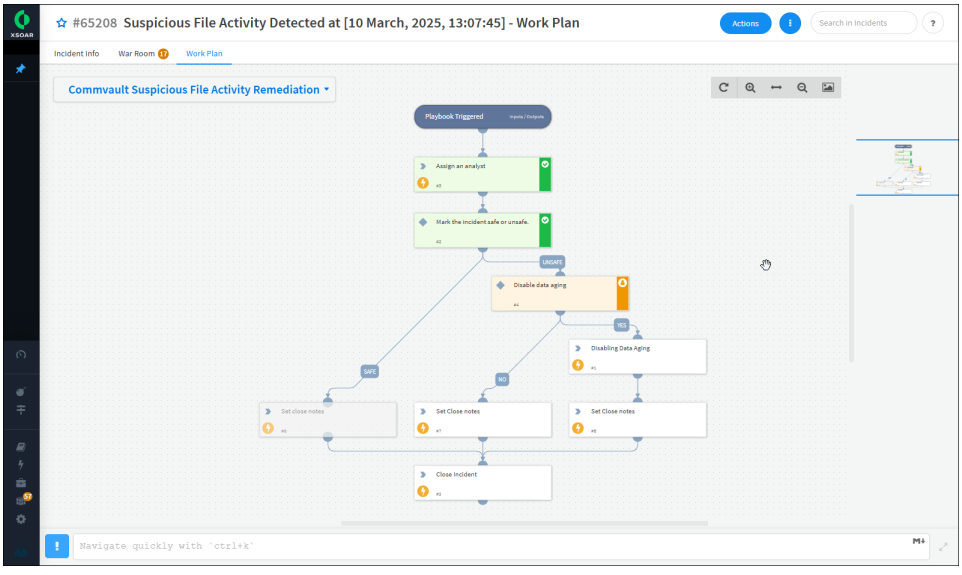

Fig. 1: XSOAR Work Plan that automatically executes when suspicious activity is detected.

The integration also allows security teams to monitor anomaly alerts from the Commvault Cloud data protection platform directly within Palo Alto Networks XSOAR so that they can respond with automated actions to help fortify their data protection and cyber resilience.

AUTOMATIONS

Automation is crucial in threat detection and response because it significantly enhances the speed and efficiency of identifying and mitigating cyber threats.

Data protection actions can be automated out-of-the box with the Palo Alto Networks XSOAR integration, including:

Action	Why it matters
Disable data aging	Many organizations set policies to only maintain a certain number of backup files before purging them to save space and money. By disabling data aging, you preserve previous copies of files, including both known-good (for clean recovery) and bad or compromised files (for forensic investigation).
Quarantine affected files and systems	By quarantining affected systems and files, you can prevent infected or compromised files from being restored following the cyberattack and preventing reinfection.
Disable compromised user	If a user account has been flagged as being compromised or behaving in a suspicious way, disabling that account from accessing the data protection platform can prevent malicious destruction of backups data, as well as data exfiltration from backup environments.
Disable identity provider	In the event of a full scale cyberattack, organizations can completely sever the connection between Commvault Cloud and the identity provider, enabling only 'break glass' accounts to access the backup environments to perform recovery actions.
Add resources to Cleanroom recovery groups	When resources show signs of compromise, you can automatically add those resources to Cleanroom recovery groups to begin automating the data validation and recovery process in an isolated, secure Cleanroom. Infected or compromised assets can also be added to a cleanroom to build a forensic environment for investigation.

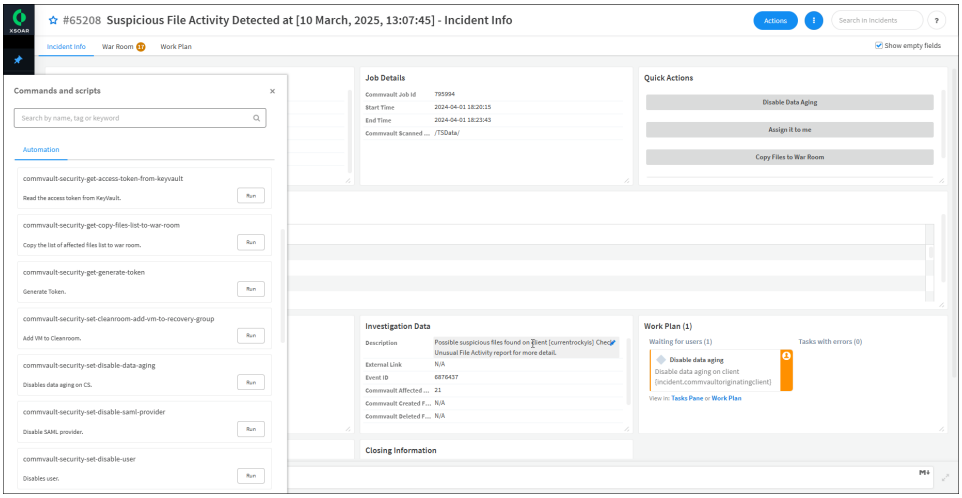

Fig. 2: Additional automations that can be run upon investigation in Palo Alto Networks XSOAR platform.

GET THE INTEGRATION

The Commvault Cloud integration with Palo Alto Networks XSOAR is available for free from the Palo Alto Networks marketplace.

Visit the Palo Alto Networks Marketplace to download the integration.

Visit Commvault Cloud Documentation to learn how to install and configure the integration.