INTEGRATION DATASHEET

SpyCloud

ENTERPRISE PROTECTION: CORTEX XSOAR BY PALO ALTO NETWORKS

BETTER-INFORMED, FASTER INCIDENT RESPONSE TO SAFEGUARD EMPLOYEE IDENTITIES

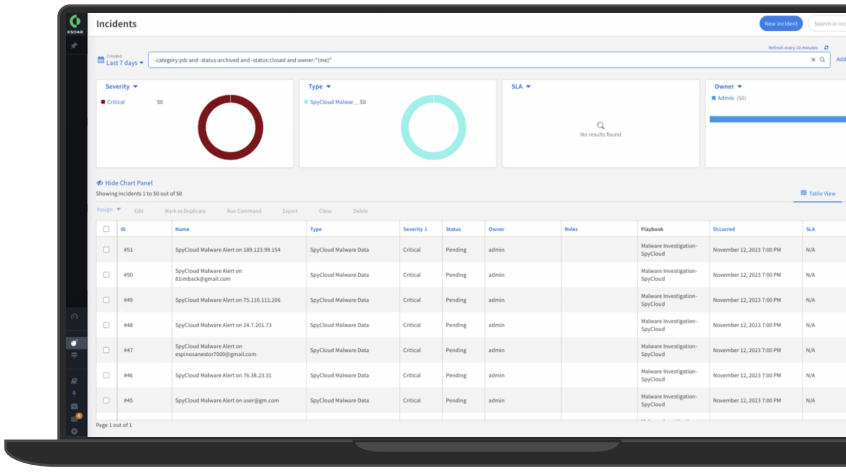
SpyCloud Enterprise Protection for Cortex XSOAR gives security teams the power to easily triage and remediate identity-related exposure incidents – shutting down threats to prevent targeted account takeover and cyberattacks. The integration takes breach and malware data from SpyCloud and ingests it into Cortex XSOAR as incidents and helps automate remediation.

Security teams can take advantage of pre-built incident response playbooks, or build out their own playbooks using enrichment commands to create automated steps for responding to breached credentials and malware exposures – calling SpyCloud's API directly to gather enriched data.

DECREASE MTTR WITH TIMELY, ACCURATE EXPOSURE INSIGHTS

Automate and analyze recaptured darknet data in your workflow, shortening the attack window for exposed employee credentials:

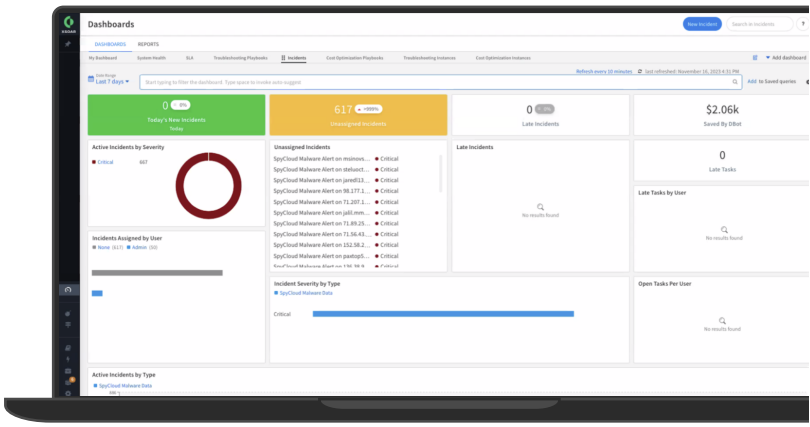
- Trigger remediation with a playbook for exposed credentials
- Streamline SOC workflows to accelerate remediation of compromised credentials and malware-infected devices, users, and applications
- Automatically create high-priority incidents for new breach or malware records, correlated with employee identities
- Expand visibility of malware exposures into all possible business applications



SpyCloud

HOW IT WORKS

PaloAlto Cortex XSOAR fetches the freshest, high-quality darknet data from SpyCloud – breach and malware insights that are curated, clean, normalized, and free of duplicates. SpyCloud's integration content pack also includes an enrichment integration which includes two built-in playbooks and several enrichment commands for remediation.



A view of the Cortex XSOAR Dashboard displays incidents generated by SpyCloud based on known exposures ▲

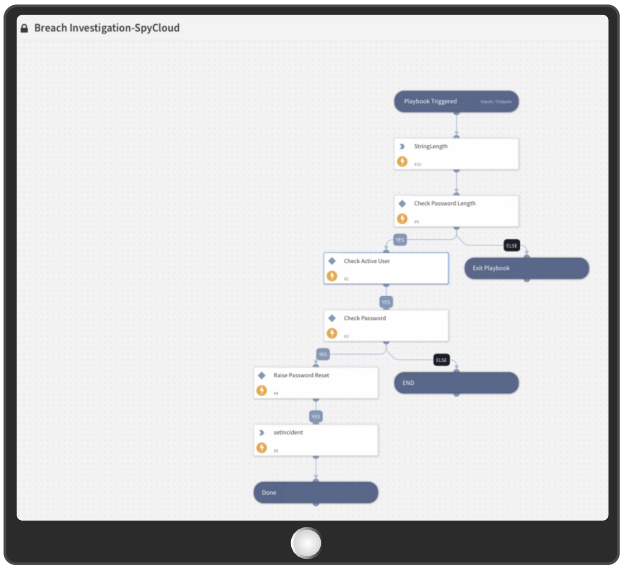
INCIDENT REMEDIATION

SpyCloud's integration with Cortex XSOAR generates high priority incidents when certain criteria are met for new records.

BREACHES: In the event of a breach where a plaintext password was exposed, SpyCloud creates and flags the event as a high priority incident in XSOAR. SpyCloud offers several automation steps available through a built-in playbook to streamline the incident response process for exposed credentials and data breaches.

Examples include: Checking the password length to confirm it's a threat; confirming it's an active user and verifying their current passwords for a match; and then resetting the password and any additional steps.

MALWARE: For malware exposures, SpyCloud removes all blindspots across users, applications, and devices for comprehensive exposure remediation. All records associated with a specific malware infection are ingested into XSOAR so you can see the full breadth of an infection. SpyCloud Compass customers can view additional malware records outside their primary enterprise watchlist to gain visibility across all exposed applications and devices.

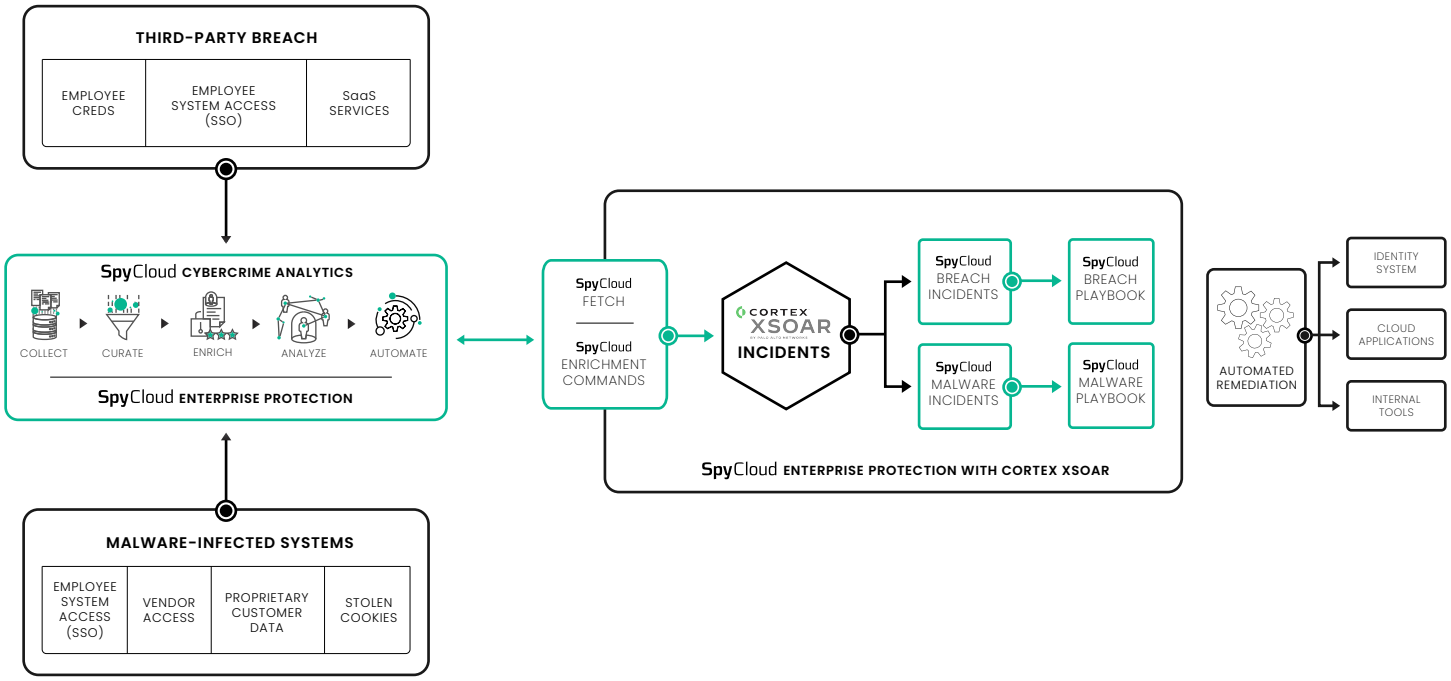


SpyCloud

ELEVATED INCIDENT RESPONSE

Enrich your incident response by using Cortex XSOAR's ML-powered bot, DBOT, to build out calls to SpyCloud's API, and leverage SpyCloud's extensive database of recaptured darknet data to quickly uncover hidden connections, identify potential threats, and gain a deeper understanding of related events surrounding each incident. Query by domain, email, IP, username, or passwords to ingest SpyCloud's user records of recaptured darknet data. Enrich your **Post-Infection Remediation** by searching for specific applications or subdomains to identify any exposed credentials.

SPYCLOUD INTEGRATION FOR CORTEX XSOAR | REFERENCE DIAGRAM



▲ *Streamline SOC workflows using SpyCloud's Enterprise Protection integration with Cortex XSOAR for enriched incident response and advanced remediation workflows*

SpyCloud

TECHNICAL REQUIREMENTS

- SpyCloud Enterprise Protection for Cortex XSOAR requires an active Cortex XSOAR License

- Analyzing SpyCloud breach or malware data requires a license for **SpyCloud Employee ATO Prevention**, and an additional **SpyCloud Compass** license is required to ingest malware records for applications outside the primary enterprise watchlist.

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to protect businesses from cyberattacks. Its products operationalize Cybercrime Analytics (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to make the internet safer with automated solutions that help organizations combat cybercrime.

To learn more and see insights on your company's exposed data, visit **spycloud.com**.