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, malware, and successfully phished 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, malware and phishing 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

83	nt 7 days + 🖃	itegory job and -status archived and -status sized av	d swear "(rw)"						Arrest a	ere il m
	verity •	0	Type + If SeyChool Mathem, 30	C	)	SLA +	Q. No reposit for	al.	Ozener • • Advec (10)	
	de Chart Panel ng Incidents 1 to 10	Not of St.								
		Rans	Type	Security 1	Batter	Owner	Autor.	Playbook	Assessed	
	451	SpyCroud Mahaare Adent on 188,123,391 ISA	SpyCloud Malasset Data	Critical	Pandrag	admin		Malware Investigation- SpyCourd	November 14, 2023 7:00 PM	
	*16	SpyCloud Halvare Alert on REinsback/ggmail.com	SpyCloud Halware Data	Critical	runderg	adven		Halwark investigation RevCoord	November 12, 2023 7:00 PM	
		SpyCoud Malware Alert in 73.130.131.204	SpyCloud Molware Data	Critical	Parality	admin (		Halwary Investigation- SpyCood	November 13, 2023 7:00 PM	
	**1	SaryCould Malware Alart on 24 7,261.73	SpyCloud Meleore Data	Critical :	Fanding	adres :		Halware investigation- SpyCould	November 12, 2023 7:00 PM	16
	447	SpyCoul Malware.Nert on explosure.ster70000 gmail.com	SpyCloud Malware Data	Critical	Pending	admin		Malware Investigation SpyCloud	November 12, 2023 7:00 PM	
		SeleCloud Malware Alart on 76.38.23.31	SpyClouel Malware Date	Critical	resting	adren		Malwire Investigation- laryCloud	November 12, 2023 7:00 PM	
	**6									

#### HOW IT WORKS

PaloAlto Cortex XSOAR fetches the freshest, high-quality darknet data from SpyCloud – breach, malware, and phishing 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.

And the second state of th	ang Prakala <u>II kalalan</u> kacipangka Paginak Padalahatya k	n Hannahr 🦉 hat shadad tasanin (d. 2014) (the	
0 Today's New Incidents. Today	617 CON	0 COR	\$2.06k Barred By Dilot
Active tecklearts by Severity • Otent 647	Unanzigned twickents SpyClaud Malaum Alert on memory	Lata tricidents	0 Late Take
michant Auigeaf by User 19 Iown 612 - Alaren 101	StyClast Melsen Arts 18, 177.1 O'Dital StyClast Melsen Arts 18, 177.1 O'Dital StyClast Melsen Arts 19, and 19, O'Dital StyClast Melsen Arts 19, and 18, O'Dital StyClast Melsen Arts 19, and 18, O'Dital MyClast Melsen Arts 19, and 18, O'Dital StyClast Melsen Arts 19, and 19, O'Dital StyClast 19, O'Dital StyCla	Q Armuts boot	Late Tasks by User
0 = =	Incident Severity by Type  System Color Science Science  Officer	Open Tasks Per Uner	

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

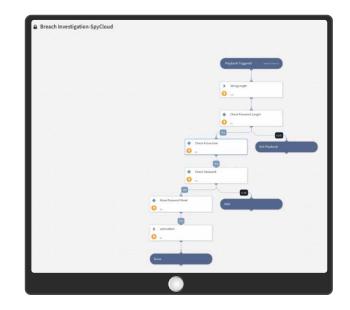
#### INCIDENT REMEDIATION

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.

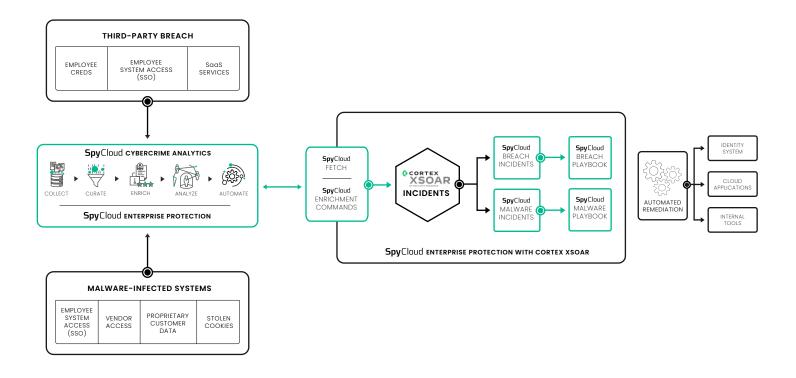
MALWARE: For malware exposures, SpyCloud removes all blindspots across users, applications, and devices for comprehensive exposure remediation. All records associated with a specific malware infection are ingested into XSOAR so you can see the full breadth of an infection. SpyCloud Compass customers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



## 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

### 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 disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics to proactively prevent ransomware and account takeover, safeguard employee and consumer accounts, and accelerate cybercrime investigations. SpyCloud's data from breaches, malware-infected devices, and successful phishes also powers many popular dark web monitoring and identity theft protection offerings. Customers include seven of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies worldwide. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.

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