SpyCloud

CYBERCRIME ANALYTICS CHECKLIST

How to automate remediation of compromised digital identities and protect against next-gen threats

WHY YOU NEED BETTER DATA TO PREVENT NEXT-GEN ATTACKS

Faced with a **laundry list of challenges**, SOC teams need a better way to tackle threats to employee digital identities and corporate data. To unlock automated workflows that maximize SOC resources and improve security outcomes, teams have to have better, more actionable exposure data.

SpyCloud's approach – **Cybercrime Analytics** – turns raw, unstructured darknet data into actionable insights, giving you the ability to quickly identify and respond to exact-match exposures of compromised passwords, cookies, and identity data, all so you can better protect your business from targeted cyberattacks.

BUILD THE FOUNDATION FOR ACTIONABLE DATA ▼

To reap the benefits of automation, you first need reliable data from sources you trust. High-fidelity alerts lead to confident decisions – so make sure you're sourcing clean data that's not just scraped from surface-level forums or repackaged into combolists.

FACTORS TO CONSIDER:

- [ ] **Is the data curated to remove noise?**

  It should be parsed, normalized, and de-duped to transform raw datasets into machine-readable information.

- [ ] **Is the data made available fast enough to take action before criminals can use it?**

  Request a data speed test from your shortlist of vendors to compare how fast they collect and publish darknet data from the criminal underground.

- [ ] **Has the data been enriched for insights?**

  Your data should include key details like the breach source and description, or the malware infection path, with IP address and target URLs. Most importantly, make sure your records include plaintext passwords so you can run exact matches to look for any exposures.

- [ ] **Has the data been correlated to understand the full scope of exposures?**

  Look for the full picture of exposed employee identities, which means credentials that can be connected across multiple breach and malware records. Make sure you can triage alerts accordingly to focus on the high-priority exposures first.

- [ ] **Does the data account for evolving criminal tactics?**

  The cybersecurity landscape is always evolving, and sidestepping authentication is the newest preferred currency for criminals – so make sure your data accounts for stolen session cookies, API keys, webhooks, and other increasingly targeted assets.

- [ ] **Does your data detect exposures across your leadership accounts, third-party vendors, and supply chain?**

  You should be able to see compromised credentials for the personal accounts of executives, board members, and anyone with systems access – including your entire supply chain.

LAYER ACTIONABLE DATA INTO AUTOMATED IAM, SIEM, AND SOAR WORKFLOWS

SOC teams can respond faster and more effectively to digital identity threats with automation. Integrate your data sources with key IAM, SIEM, and SOAR vendors to power your response to next-gen threats.

- [ ] **Are you running automated scans for exposed credentials?**

  Run daily scans within your directory service (on-prem, hybrid or cloud) to check for any exposed credentials in use by active employees. Scanning against plaintext passwords removes the chance of false positives, so you don't waste unnecessary time.

- [ ] **Are you automatically forcing password resets?**

  If a match is found, you can automate remediation by forcing a password reset or even disable accounts to prevent targeted account takeover.

- [ ] **Are you automating analysis with high-fidelity alerts in your SIEM?**

  Drive productive investigations and shorten the attack window by continuously feeding breach and malware records into your SIEM.

- [ ] **Are you automatically creating workflows within your SOAR?**

  Create new incidents in your SOAR that can automate actions like resetting exposed application credentials or closing low-severity incidents. Go one step further building additional workflow steps by retrieving additional enriched and analyzed recaptured identity data into your playbooks.

Protecting against next-gen threats requires connecting the dots across cybercrime data.

Understanding the full breadth of identity exposure – so you can prevent full-blown targeted attacks – means leveling up your data and automation game with these foundational components.

"I know if I get a SpyCloud alert, it's actionable. We consider SpyCloud as a trusted resource for any type of incident that may impact our consumers or employees."

ANTHONY BRUNSON | SECURITY OPERATIONS MANAGER
LendingTree

LendingTree:

- Reduces alert fatigue with high-fidelity notifications
- Saves 60% of SOC team's time and resources with actionable data & automation

ABOUT SPYCLOUD

SpyCloud transforms recaptured breach and malware data so businesses can proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime.

Get exposed data insights at spycloud.com.