Six Ways to Combat Credential Attacks in State and Local Government Agencies

Introduction

Compromised credentials are involved in the majority of cyberattacks, and have become a persistent problem for state and local government agencies due to phishing, data breaches, social engineering, and other risks. In many cases, attackers use these credentials to infiltrate internal networks and escalate their access privileges. Most of these attacks have a narrow focus: to access private data or high-value assets for exploitation.

Although many agencies or organizations have traditional security point solutions, log management, and security information and event management (SIEM) solutions in place, these legacy systems and tools struggle to provide a comprehensive view of threats, making the detection of compromised credentials even more challenging. Security teams face increasing pressure due to limited resources and the vast number of systems and applications they manage on a daily basis.

Legacy solutions rely on static correlation rules that generate a large volume of alert noise, fail to detect advanced or zero-day threats, and are difficult to maintain. Additionally, these outdated solutions demand extensive resources from security teams to consolidate and interpret information from disparate tools.

The following are six key aspects to consider when evaluating solutions to detect compromised insiders:

1. User and entity behavior analytics (UEBA)

Modern solutions for detecting compromised credentials utilize advanced analytics, unlike the static correlation rules used by legacy solutions. These static rules produce many irrelevant alerts and cannot detect new or sophisticated threats that don't match the specific, constrained rules. Security teams often have to create hundreds of custom rules, resulting in significant maintenance overhead and alert fatigue.

User and entity behavior analytics (UEBA) involves tracking, collecting, and analyzing user and machine data to detect threats such as compromised credentials within an organization. UEBA uses analytical techniques to distinguish anomalous behavior from normal activity. This is usually achieved by collecting data over time to establish a baseline of normal user behavior and alerting to deviations from this pattern. UEBA can also identify signs of compromised credentials without relying on static correlation rules, then risk scoring is used to identify notable users and events so security teams can prioritize investigations.

The Exabeam Security Operations Platform, built for security people by security people, helps agencies identify behavior that might appear normal but deviates from established patterns.

2. Comprehensive, automatically compiled user timelines from various solutions

Security analysts typically need to gather evidence from multiple security tools and from their SIEM to assemble a user or entity timeline when alerted to a potential incident. This process is time-consuming, tedious, and error-prone, and often results in an incomplete picture of an incident. An effective solution for detecting compromised credentials should automatically stitch together events, incidents, and alerts from all security tools and systems, presenting a user's activity in a single timeline without requiring analysts to switch between and query multiple tools.

Smart Timelines™ automatically reconstruct security events, accelerating time to resolution. These automated, machine-generated timelines enable faster, more thorough investigations, requiring less time and technical expertise from analysts. This helps reduce time to resolution and increase investigation accuracy, allowing for greater efficiency and focus on higher-priority tasks.

3. Lateral movement detection

After compromising a user's credentials, attackers can move undetected throughout the organization, gaining increased access and targeting high-value assets. Tracking lateral movement is inherently challenging, as activity is spread across multiple users and entities.

By combining UEBA capabilities with automated user timelines, lateral movement can be detected using machine intelligence, eliminating the need for analysts to manually connect the dots across legacy SIEM and security point solutions.

4. User-centric information summaries

Although SIEM solutions collect information from various sources, they present data without the context that ties everything together. This issue is exacerbated by the decentralized infrastructure commonly found in state and local government agencies. As a result, security teams face increased workloads as they must sift through a barrage of siloed, disjointed information without proper context. While capturing and analyzing data is important, without focus and context, it can create security noise pollution.

This lack of context and effective data presentation highlights the need for UEBA to associate related data with users or entities, analyzing events and alerts from a user-centric perspective rather than focusing on data silos. Populating a list of the most notable users helps prioritize a security analyst's time and presents security information in a way that is easily understood without additional investigative effort. An effective solution features user-centric summaries and security incident dashboards that prioritize:

- User behavior data, such as downloads and accessed apps
- Organization data including users, contact information, reporting structure, and cohorts
- Fact-based data from systems such as FireEye, Palo Alto (Wildfire), and Sourcefire, offering a network perspective of behaviors that can be linked to users
- Threat intelligence data feeds to relate discovered malicious behaviors at other organizations

5. Risk-based security alert framework

Given the overwhelming volume of alerts that security teams have to triage and respond to, there is often a lack of focus and prioritization for risk investigations. Solutions should emphasize alerts and investigations on high-risk activities. This approach requires all user and entity activities to be quantitatively scored within a risk framework. Higher scores automatically prioritize a security analyst's efforts, ensuring their focus remains on activities more likely to indicate breaches.

6. Ability to augment existing tools

Security leaders in state and local government agencies are responsible for building world-class programs capable of defending against current and future threats, all while operating with limited resources. Traditional SIEM solutions like Splunk, ArcSight, and QRadar offer powerful data centralization capabilities but often require knowledge of complex query languages, extensive customization and maintenance, and exhaustive analyst cycles for triage and investigation.

Conclusion

Public sector organizations can address these challenges by augmenting legacy SIEM and log management solutions with behavioral analytics, enabling security teams to maximize their existing investments. Security leaders should consider UEBA solutions that can be deployed alongside and ingest data from existing SIEM solutions, providing joint customers with improved threat detection, enhanced cloud service visibility, and reduced incident response times without requiring architectural changes to their existing deployment.

Compromised credentials will remain a preferred attack vector for malicious actors. Therefore, it's important to choose security tools that can automate and consolidate information, enabling security teams to effectively identify and combat this threat.

This automation also improves visibility into existing coverage. Exabeam offers a unique solution through Outcomes Navigator, which displays how well an environment is configured to protect against specific use cases and provides recommendations for improving security coverage. These features boost analyst productivity, reduce response times, and ensure consistent, highly repeatable results.

For more information on detecting, investigating, and responding to threats, we invite you to **read our solution brief** for state and local governments.

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more about Exabeam today

Get a Demo Now →