exabeam

Solution Brief

Compromised Credentials

Detect, Investigate and Respond to Indicators of Compromised Credentials

Compromised credentials - when a legitimate user's credentials have been unknowingly obtained by a malicious actor and used to access the corporate assets.

Hackers Don't Break In - They Log In

Stolen credentials are a persistent problem, and organizations have yet to effectively solve that problem.

Attackers are stealing valid user credentials and carrying out attacks masquerading as legitimate employees going about their normal business. Operating under the covers of valid credentials attackers are hard to detect. Their under-the-radar activities often take weeks or months to be discovered, resulting in more severe data breaches or remediation costs. Tellingly, in 2019 over 80% of publicly disclosed breaches utilized compromised credentials.[1]

Investigating credential-based attacks with traditional tools is a complex, error-prone, and time-consuming process. Expert analysts must run dozens of manual search queries to trace the activities of attackers in order to understand the footprint and magnitude of the breach.

> The machine learning feature can help us identify users with anomalous behavior that could pose a risk.
>
> **Secure Soft Corporation**

[1]Verison Data Breach, "Investigations Report," 2020

Exabeam and Compromised Credentials

Exabeam helps security teams outsmart adversaries using compromised credentials with the support of automation and use case content across the full analyst workflow, from collection to response.

Leveraging machine learning and user behavior analysis to baseline normal behavior for every user, device and peer group, Exabeam automatically detects the anomalous behaviors that are indicative of a compromised account, regardless of the attacker's techniques. Detection models work out of the box and do not require security engineers to create complex correlation rules.

Analysts are provided with lists of compromised systems and accounts as well as user and device activity timelines, known as Exabeam Smart Timelines, to support their investigations. Smart Timelines are automatically created for every user and device in the environment, along with the lists of accounts and systems accessed by these entities. These preassembled timelines save hours of security analyst work. Analysts can then focus on reviewing activities and making decisions instead of creating complex search queries to assemble the data.

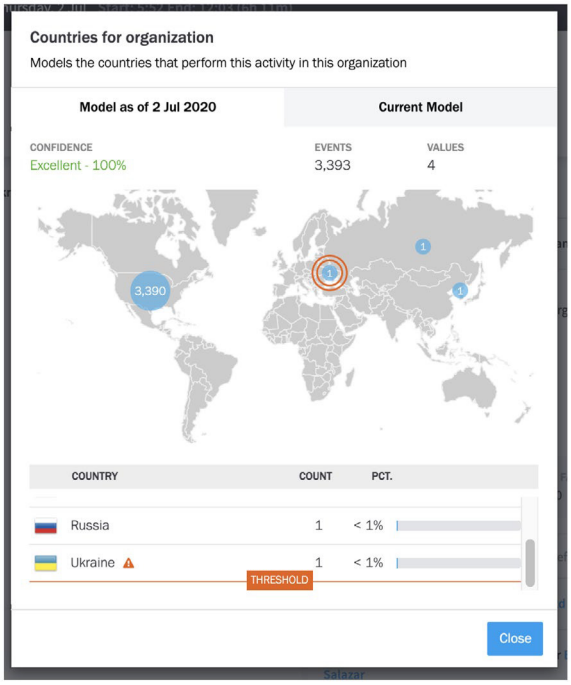
Key Capabilities

Challenge 1: Collection and Detection

Traditional security tools are not able to detect attacks involving compromised credentials.

Solution

Exabeam leverages machine learning and user behavior analysis to automatically detect compromised accounts regardless of the attacker's techniques. By learning and understanding the normal behavior for each user and their peer group, Exabeam can distinguish any anomalous behavior. Additional details about anomalies are provided in Data Insights Models.



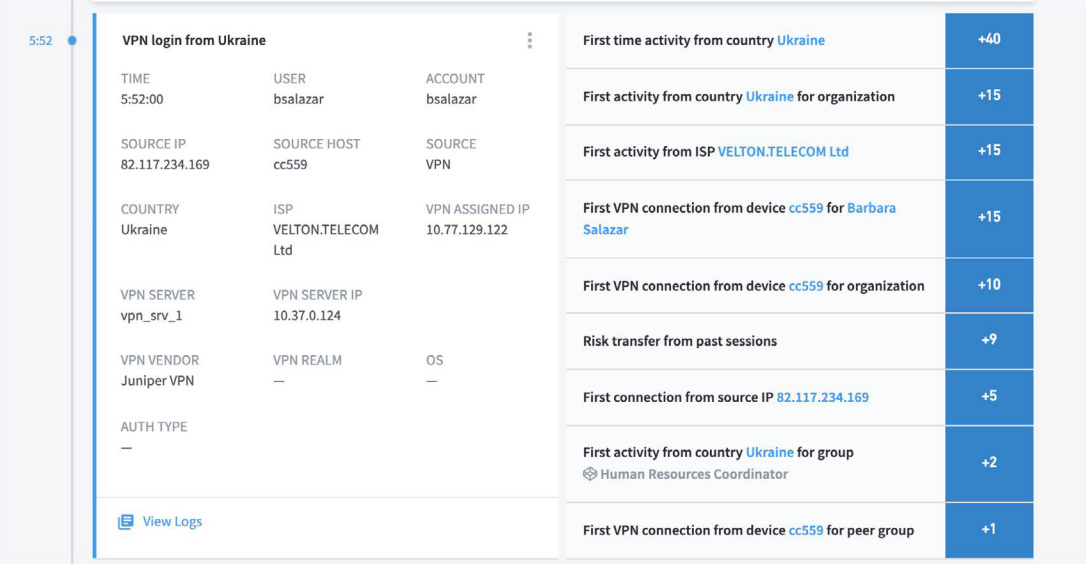
This smart timeline event shows an instance of a potentially compromised insider, with the employee's credentials seen accessing the network for the first time from ukraine. The timeline also flags access from ukraine as a first for the employee's peer group and for the organization

Benefit

Analysts can detect instances of abnormal behavior out of the box, eliminating the need for security engineers to create complex correlation rules.

Challenge 2: Visibility and Investigation

It is difficult to identify a compromised user. Moreover, piecing together evidence in a compromised credential investigation is a painstakingly manual process.



This smart timeline event shows an instance of a potentially compromised insider, with the employee's credentials seen accessing the network for the first time from the ukraine. The timeline also flags access from the ukraine as a first for the employee's peer group and for the organization

Solution

Exabeam accelerates the investigation process in two ways. First, Exabeam helps analysts identify potentially compromised credentials by distinguishing risky behavior from normal organizational changes, such as job role and department changes, or changes in user location. Second, Smart Timelines automatically assemble and present a user's session of activities, including the lists of accounts and systems accessed, thereby eliminating tedious point-click-and-pivot evidence gathering.

Benefit

by distinguishing risky behavior from normal organizational changes, such as job role and department changes, or changes in user location. Second, Smart Timelines automatically assemble and present a user's session of activities, including the lists of accounts and systems accessed, thereby eliminating tedious point-click-and-pivot evidence gathering.

Challenge 3: Response

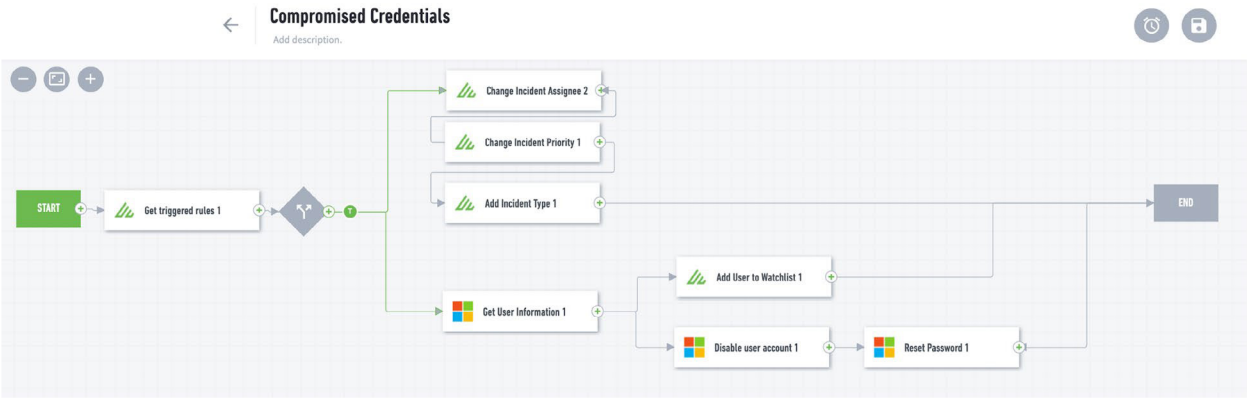
Processes and procedures related to incident response are often not tailored to the specific threat and largely entail manual processes.

Solution

Exabeam provides out-of-the-box checklists recommended remediation steps and response playbooks for incident response teams.

Benefit

Resolve compromised credential incidents faster.



This compromised credential playbook characterizes and escalates the incident, adds the compromised user to a watchlist while disabling their account, and resets their password.

Use Case Content

Key Data Sources

- Application activity
- Authentication and access management
- Cloud application activity
- Database activity monitoring (DAM)
- Endpoint security (EPP/EDR)
- File monitoring
- Operating system logs (e.g. UNIX/LINUX/OSX/WINDOWS)
- VPN/Zero trust network access
- Web security and monitoring

Key Detection Rule Types

- Deviations in a user's file, database, VPN or application access and interaction patterns
- A user authenticating from new or risky geographical locations
- A user accessing websites categorized as "malicious"
- Abnormal user or host executing a network sniffing tool
- Abnormal process activity indicating credential dumping
- 3rd party-alerts indicating compromised assets
- Compromised service accounts or assets
- Credential theft

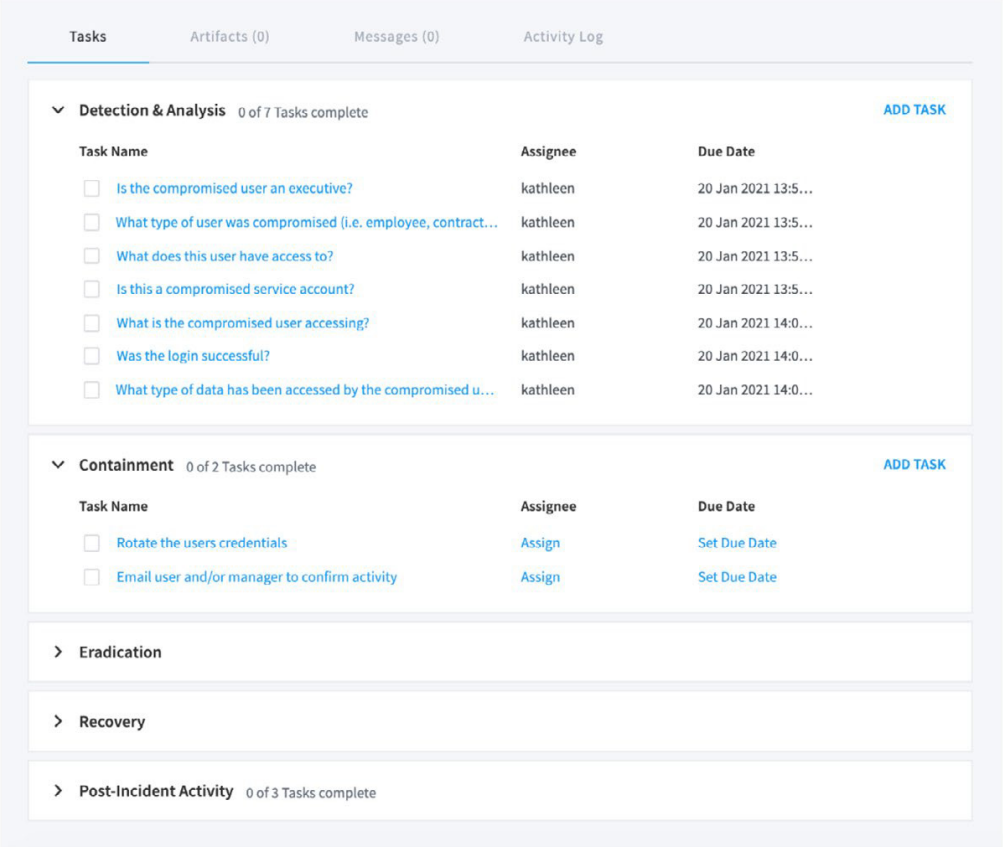
Mitre Technique Coverage

- T1213: Data from Information Repositories
- T1083: File and Directory Discovery
- T1133: External Remote Services
- T1071: Application Layer Protocol
- T1102: Web Service
- T1078: Valid Accounts
- T1040: Network Sniffing
- T1003: OS Credential Dumping
- T1027: Obfuscated Files or Information: Indicator Removal from Tools

Response Actions

- Contact a user/manager/HR department via email
- Add a user to a watchlist
- Rotate account credentials/reset passwords
- Block, suspend, or impose restrictions on users involved in the incident
- Prompt for re-authentication via 2-factor/multi-factor authentication
- Isolate systems

Incident Checklist



The compromised credential incident checklist prompts analysts to answer specific investigation questions and take containment actions

About Exabeam

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools – including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond. For more information, visit www.exabeam.com.

exabeam

To learn more about how Exabeam can help you visit exabeam.com today.