exabeam

TUCANA CYBER SECURITY SOLUTIONS

White Paper

How Exabeam Solves 7 Use Cases for Compromised Insiders

Summary

Compromised insiders are one of the most difficult security risks for an enterprise to manage. A compromised insider is a legitimate user on the network whose account or asset has been commandeered by an attacker without the legitimate user's knowledge. The attacker can then masquerade as the trusted insider and execute attacks with impunity. The impact of these attacks can be massive if the compromised insider is an executive or other employee with access to sensitive information or assets – or if the attacker is able to escalate privilege to obtain system administrator rights to access privileged information and assets on the network.

This white paper describes how Exabeam can identify and mitigate the potential risk of seven common compromised insider use cases:

1. **Compromised Credentials**
2. **Lateral Movement**
3. **Privilege Escalation**
4. **Privileged Activity**
5. **Evasion**
6. **Account Manipulation**
7. **Data Exfiltration**

Defining the compromised insiders risk

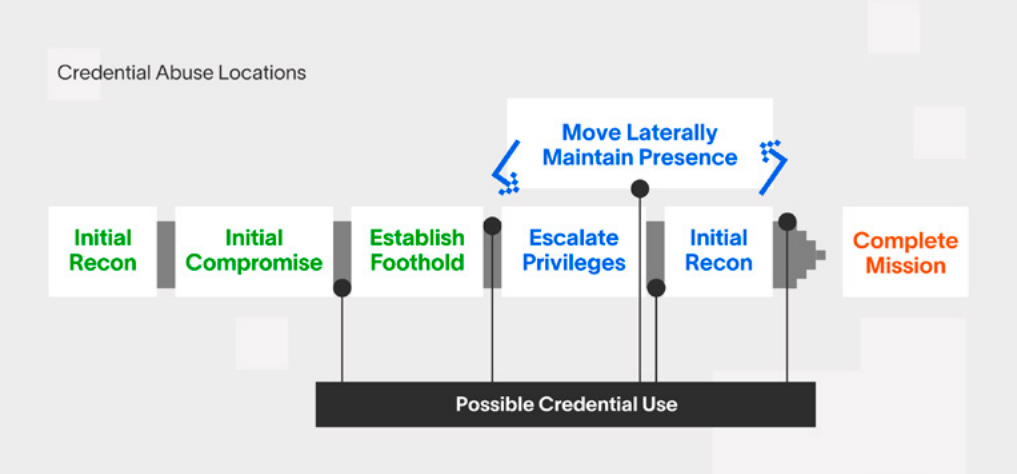
There are two components of risk associated with a compromised insider. The first is about protection: how secure are the accounts and assets with regard to security controls and processes? These are the systematic security measures an enterprise should have in place for every user. The other component of risk is about threat detection, investigation, and response: how can the organization know when they have a compromised insider, what is the intruder doing, and how to respond to the attack before damage occurs? With legacy rules-based approaches, it is impossible to distinguish between the legitimate actions of an authorized user and unauthorized use of that same person's accounts or access to resources.

This white paper is about understanding seven compromised insider use cases and how Exabeam Advanced Analytics in Exabeam Fusion XDR and Exabeam Fusion SIEM can help the organization detect, investigate, and respond to these threats.

1 Compromised Credentials

Definition

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



Problem

Some types of attacks, and the methods used to carry out and obtain credentials are:

- **Phishing and spear-phishing**
  Sending a message to a user with a malicious link that tricks a user into entering their valid password.
- **Password spraying**
  Attempting to authenticate with a known username and commonly used, unsafe passwords.
- **Credential stuffing**
  Using username and password combinations stolen from other databases in the hopes that the pair will be repeated.
- **Keyloggers**
  Putting a piece of malicious software that logs keystrokes and passes the keystrokes to an attacker to recreate a username and password.
- **Brute force**
  Attempting to authenticate by iterating through a list of potential passwords, such as all words in a dictionary, or all words in a dictionary in a hashed value, in hopes that it will match.
- **Social engineering**
  Using trickery to lure an individual into believing there is a legitimate need to pass their network credentials to the person with whom they are communicating.

Solution

Advanced Analytics in Fusion XDR and Fusion SIEM mitigates threats posed by compromised credentials by establishing a behavioral baseline for all users and assets in the network. It assigns risk scores to anomalous events and highlights deviations from that baseline.

The combined scores from these modeled, anomaly-based rule triggers, along with prepackaged correlation rules, are aggregated and summed into a total session risk score that, if high enough, becomes a notable session displayed on the homepage.

The result is better coverage and less alert fatigue than using sets of static correlation rules sent as alerts to analysts.

2 Lateral Movement

Definition

Lateral movement is when an attacker compromises or gains control of one asset within a network and then moves internally within a network ("east-to-west") from that device to others. It is generally the next move an attacker makes after they compromise credentials. While lateral movement is not always necessary for an attacker to achieve their objectives, usually compromises of additional assets are required to reach systems and privileges that allow them to get what they are after.

Problem

Some types of attacks, and the methods used to carry out lateral movement by an attacker are:

- **Port scans**
  Attackers use port scan tools such as Nmap to find vulnerable ports by which they can expand their footprint, move laterally, or find other accounts to compromise.
- **Remote desktop access**
  With a set of valid credentials and the legitimate user away from their computer, a hacker can gain full access to the graphical user interface of the exploited computer. With this access, the attacker can move around with impunity.
- **Windows attacks**
  Windows Server Message Block is a protocol that allows users to access other parts of the network without continuously entering their credentials. This pass-through authentication is helpful to allow users to access other locations on the network. Attackers use the protocol's commands to move around the network such as PsExec and scheduled tasks.
- **Pass the hash**
  Attackers use a hashed, or algorithmically hidden password for authentication if they can catch it in transit or gain access to password hash repositories such as the Security Account Manager (SAM), the Local Security Authority Subsystem Service (LSASS), or the Active Directory database.
- **Golden ticket**
  A Kerberos exploit where an attacker has access to a client's username and hashed password. This allows the attacker to gain access to a ticket-generating ticket ("Golden Ticket") and log into any account that they please on the domain.
- **Pass the ticket**
  Like "Golden Ticket." Compromise does not require a user password, but the level of privilege will be lower.

Solution

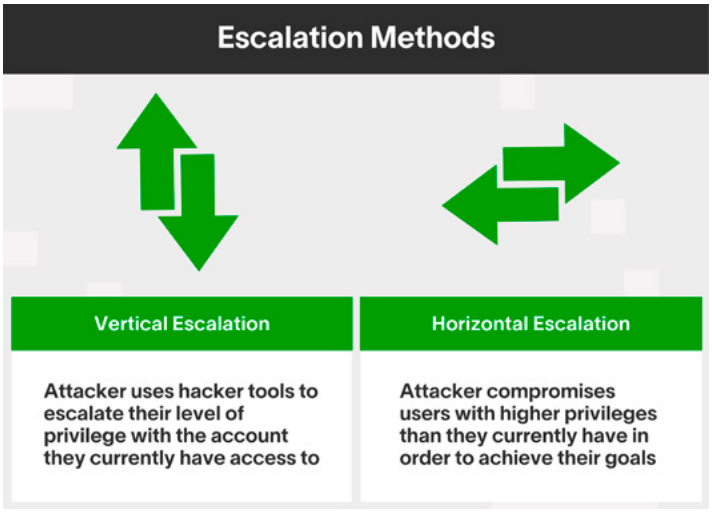
Advanced Analytics in Fusion XDR and Fusion SIEM have prepackaged rules to highlight activities such as port scanning, remote desktop access, event codes indicating possible Windows attacks, pass the hash, golden ticket, and pass the ticket.

The rules improve operational efficiency with pre-assembled timelines, risk scores for prioritization, watchlists of highest risk users, and lists of compromised assets. Rules improve analysts' efficiency in performing investigations that take minutes instead of hours to resolve lateral movement incidents faster. And the rules improve security posture by reducing the risk of lateral movement on your network.

3 Privilege Escalation

Definition

Privilege escalation refers to a technique where the attacker gains higher-level permissions or unauthorized access to achieve goals that require these permissions. The attacker might use an enumeration tool to find a valid account to compromise, switch to an account with greater access privileges, or increase permissions on a compromised user or system to elevate their access. It occurs during the post-exploitation phase of an attacker's work.



Problem

Some types of attacks, and the methods used to carry out privilege escalation by an attacker are:

- **Horizontal escalation**
  Attackers use compromised credentials to move around in the network until they compromise credentials with the requisite permissions that allow the attackers to carry out their objectives. Many times, the ultimate target is domain administrator privileges.
- **Discovery**
  Account switches are sometimes indications of privilege escalation. Excessive and abnormal account switching is a very good indicator of horizontal and vertical escalation by an attacker. The password retrieval associated with these account switches is also a good indication of vertical escalation.
- **Credential dumping**
  Attackers may manage to dump a Windows Security Accounts Manager (SAM) database on a domain controller, providing the LM or NTLM hashes of all users on that domain. These hashes are then used in hash passing attacks to escalate the attacker's privilege to any member's privilege on the domain.
- **Vertical escalation**
  Attacker gains access to an account and bypasses the account controls that are intended to limit permissions, typically performed with post-exploitation hacker tools. Techniques include modification of the domain group policy, exploiting weak service permissions, deploying executable files in Metasploit, and bypassing user account control security settings.
- **Weak security**
  An attacker will attempt to find configuration files with weak permissions to modify and escalate privileges for certain tasks. This works the same way for assigned permissions on executable binary files.

Solution

Privilege escalation is highlighted to analysts when an account or entity displays abnormal behavior or triggers a fact-based rule. Advanced Analytics in Fusion XDR and Fusion SIEM create a baseline of what systems a user typically accesses and account parameters that, when manipulated, show as anomalies. A compromised account being used to escalate privileges and run amok in your network will trigger preconfigured rules based on the modeled data for a particular user.

4 Privileged Activity

Definition

Privileged activity is any activity on a network that represents a heightened risk should the user account or asset become compromised by an attacker. Privileged accounts are those that have greater access compared to standard users and grant both extensive control over and access to sensitive data and IT systems. Their elevated access rights make privileged accounts the most sought-after target by bad actors. Compromising and abusing privileged accounts are often among the first targets of an attack; they provide the external party with an opportunity to bypass security controls and monitoring, maneuver in the network with administrator privileges, disrupt corporate operations, or exfiltrate large amounts of sensitive data. For this reason, a best practice is to apply a level of monitoring commensurate to the level of privilege.

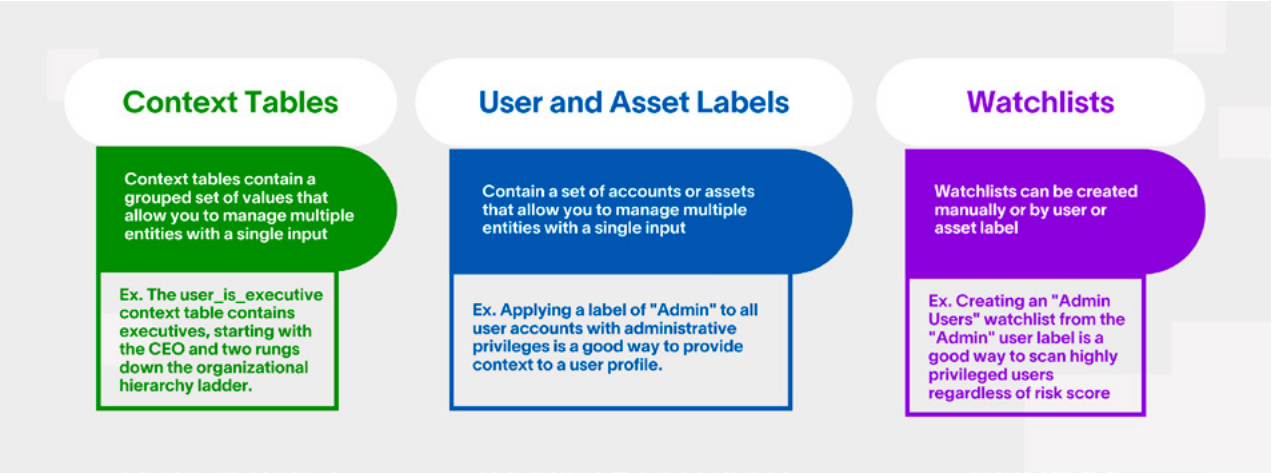
Problem

Some types of attacks, and the methods used to exploit privileged activity by an attacker are:

- **Privileged users**
  Attacks target credentials of unique and specific privileged users who have or have access to sensitive information or privileged processes. Executives and system administrators are prime targets.
- **Privileged accounts**
  Service accounts are a prime example of the privileged target. A service account is a user account that belongs to an application rather than an end user and interacts with a particular piece of software. Because service accounts are often used by more than one person and don't require interval-based password resets, they merit a higher level of scrutiny.
- **Privileged assets**
  Typically, privileged assets are servers that handle sensitive data. Other privileged assets may contain customer information, sensitive corporate intellectual property, personally identifiable information, or data that might be damaging to a corporate reputation.
- **Domain controllers**
  Domain controllers also are privileged assets, but they are exceedingly difficult to monitor with legacy security tools due to the deluge of audit logs they produce. Monitoring access to them with Advanced Analytics is a best security practice.

Solution

Advanced Analytics in Fusion XDR and Fusion SIEM provide the foundational tools for defining and managing privileged entities and processes, which are shown in the infographic below.



5 Evasion

Definition

Evasion refers to an attacker's attempts to maintain persistence on a network while avoiding detection. After a breach of the system, an attacker needs to circumvent security controls on the network to maintain stealth while continuing the exploit. While evasion is often very difficult for security practitioners to detect, it remains one of the most important aspects of cybersecurity for detection. Today, it takes on average 280[1] days to identify and contain a data breach. The longer a bad actor is allowed to remain on your network, the greater the risk for more financial and reputational damage. Evasion also exponentially complicates the incident response and remediation following detection.

Problem

Some types of attacks, and the methods used to exploit evasion by an attacker are:

- **Create processes with PowerShell**
  Use PowerShell-based processes to delete, suppress, or modify audit logging.
- **Pass encrypted or encoded commands**
  Attackers can bypass controls in certain circumstances by passing their command arguments in an encoded format. Users can pass Base64 encoded commands to mask their arguments. They also can ping IPs in a hexadecimal encoded format to avoid revealing their intent to security controls.
- **Delete files**
  To mask their presence on the network, attackers sometimes need to delete files that would contain evidence of their presence.
- **Use TOR**
  The Onion Router is a method of IP traceroute obfuscation used by hackers and others who are trying to hide the location of their access. TOR uses a series of proxies that do not have static routes to add layers of obscurity to their location.
- **Manipulate processes**
  To navigate without detection, attackers may unload Sysmon with command line scripts; use Windows Management Instrumentation script consumers to disable native Windows logging; disable the Event Tracking for Windows event trace log; manipulate svchost processes to make themalicious file appear benign; or create task manager processes and renaming them to look legitimate.
- **User hacker toolkits**
  Attackers use tools developed by black and gray hat actors to evade detection. These tools are often used to manipulate trusted processes for nefarious purposes.

Solution

Advanced Analytics in Fusion XDR and Fusion SIEM detect evasion attempts by leveraging fact-based rules indicating evasion along with behavior analytics for users, assets, and processes.

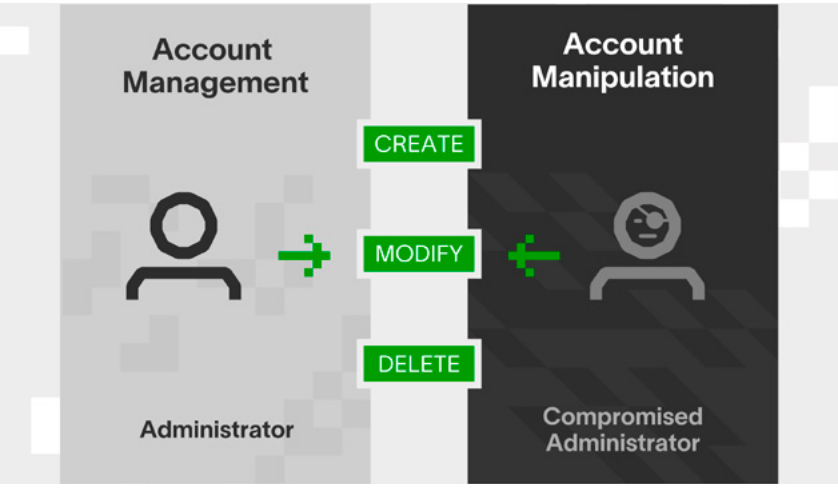
When the attacker takes an action, Advanced Analytics does too. It uses the baseline established for the compromised user to point out anomalous activity being conducted by the attacker as well as indications of compromise via specific system processes.

[1] Verizon, Cost of a Data Breach Report 2020

6 Account Manipulation

Definition

Account manipulation entails attackers leveraging unauthorized use of account controls to escalate privilege, move laterally, compromise further credentials, and potentially gain privileges that allow them to do major damage to your organization's network, finances, and reputation. Attackers do this by changing permissions and rights on accounts to achieve their goals.



Problem

Account manipulation is closely tied to other attack vectors used for a Compromised Insider campaign. These include compromised credentials, lateral movement, privilege escalation, and evasion. The most common technique is exploiting vulnerabilities in operating systems that allow for injection of code into processes, modifying scheduled tasks to enable escalated privilege, dumping credentials or a number of toolkits such as Metasploit.

- **Directory services**
  Directory services manage users and their granted privileges, including rights to network resources such as printers, applications, network devices, and authorizations and authentication on the network. Attackers leverage directory services information to grant themselves access to sensitive resources.
- **Account creation / deletion**
  Creating accounts and exploiting vulnerabilities in processes to highly provision a new account allows an attacker to escalate privileges and move laterally through the network.
- **Membership / permission**
  Attackers escalate privileges and assign themselves permissions to execute their nefarious purposes that otherwise would be impossible without granting such explicit rights. Once granted, such activity by attackers will appear legitimate without behavior analytics.

Solution

Behavior analytics is the backbone of how Fusion XDR and Fusion SIEM detect account manipulation. Prepackaged scenarios include abnormal account management activity; abnormal directory services activity; account creation activity; account deletion activity; membership and permissions modifications; and system account activity. These scenarios have rules mapped to them that contain prepackaged content designed to detect account manipulation activity in your environment. Over 85% of the rules mapped to the account manipulation use case are model-based rules that leverage behavior analytics.

7 Data Exfiltration

Definition

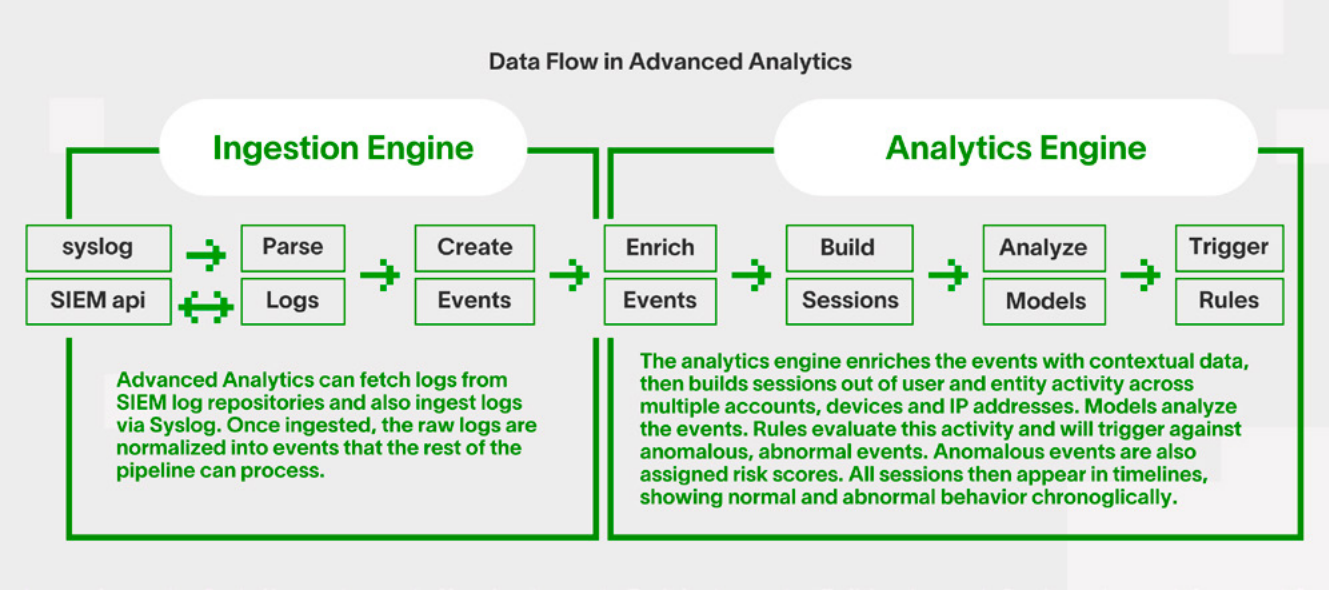
The Data Exfiltration use case entails a compromised user being exploited by an attacker to surreptitiously remove data from a network. It represents several techniques by which an attacker attempts to covertly exfiltrate data while evading detection by traditional data loss protection solutions. Due to their technical nature, data exfiltration, as defined in the Exabeam Data Exfiltration Use Case, is likely to be carried out by a savvy intruder.

Problem

Attackers know that most of the typical data pathways will have monitoring and alerting in place, so they avoid sending data out via email, print jobs, removable media, and other data transmission methods which can be detected. What they are seeking is a means out of the network that is unlikely to set off alarms. For this reason, most hackers will resort to creative means of getting data out. For example, a bad actor encodes the data they are after, divides it up into tiny pieces, sends the data out in DNS request packets, and then reassembles the data once it has been moved out of the network. Or, they might set up an SSH server to use port forwarding to exfiltrate data to which they have found access. In both scenarios, detection using a traditional SIEM would be difficult.

Solution

As with other compromised insiders use cases, detecting data exfiltration uses Exabeam's advanced analytics capability, for which data flow is shown below. When abnormal activity occurs, the modeled baseline data for the user or asset(s) triggers alerts of suspect behavior. Likewise, fact-based rules alert on processes and utilities known to be used by attackers attempting to exfiltrate data. Things like network sniffing, data encoding, web shells, and tunneling are activities that likely don't have a business purpose and need to be seen. Exabeam uses signatures to highlight this type of activity.



Conclusion

Achieving swift and accurate detection, investigation, and response to a compromised insider is not possible with legacy correlation rules–based approaches to security. It is time-consuming to manually collate sessions chronologically with aggregated security vendor logs and anomaly detection and carries risks of missing critical clues.

The ability for security teams to distinguish between legitimate user activity and unauthorized use of the same person's account or access to resources requires a modern approach using Advanced Analytics. This capability is provided in Fusion XDR and Fusion SIEM as prepackaged use cases that detect threats missed by other tools.

Modern analytic capability also helps to enhance the productivity of security teams and reduce response times with automation.

To learn more about how modern analytics with Exabeam can help, please visit https://www.exabeam.com/product/solutions/compromised-insiders/ .

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. The leader in next-gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. Exabeam offers a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. We design and build products to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives and best protect their organizations. For more information, visit www.exabeam.com

For more information, visit

exabeam

TUCANA
CYBER SECURITY SOLUTIONS
www.tucana.com info@tucana.com