exabeam

Solution Brief

Lateral Movement

Detect, Investigate and Respond to Lateral Movement Incidents

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.

Security Teams Struggle to Detect Attacks Using Lateral Movement

Lateral movement is a growing problem, with nearly 60% of external attacks utilizing this stealthy tactic[1]. Adversaries using lateral movement move systematically through a network to find sensitive data or high value assets. After gaining initial access, attackers probe other assets for vulnerabilities to compromise other accounts, escalate privileges and ultimately exfiltrate data or deal other damage.

Traditional security tools are unable to distinguish between lateral movement activity associated with compromised accounts and normal user behavior. This allows adversaries to remain undetected and extend dwell time for weeks or months while expanding the attack.

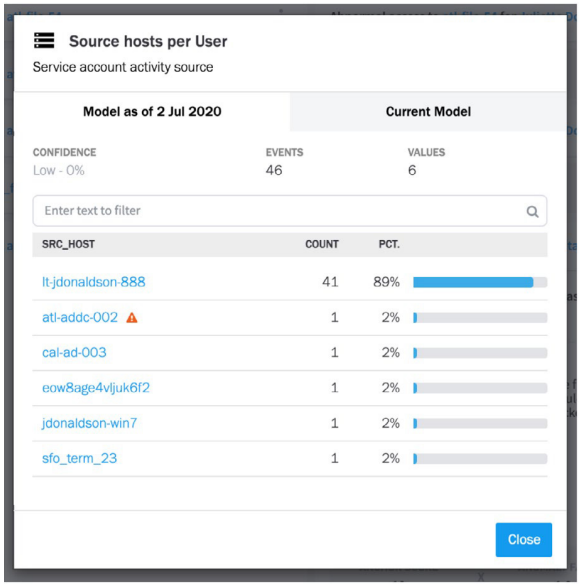
> With respect to lateral movement detection, Exabeam is always-on threat hunting.
>
> **ADP**

[1]Carbon Black Global, "Threat Report," 2019

Exabeam and Lateral Movement

Exabeam helps security teams outsmart adversaries using lateral movement with the support of automation and use case content across the full analyst workflow, from detection to response. First, we prescribe data sources to collect and analyze. Our user and entity behavior analytics (UEBA) then develops a baseline of normal activity for every user and device in an organization. As an adversary begins to move within a network, abnormal activity is identified using out of the box detection rules and models, including 7 MITRE techniques associated with lateral movement. This activity is flagged and added to the user or entity's risk score.

Risk scores and watchlists help security teams focus on the riskiest incidents, while Exabeam Smart Timelines automatically display the full attack chain to dramatically accelerate incident investigations. A guided investigation checklist and automated response playbooks enable analysts to quickly and effectively remediate incidents and reduce mean time to respond (MTTR).



This data insight model shows the source hosts accessed by a user. Exabeam alerts on anomalous access to a new host, in this case access to host atl-addc-002.

Benefit

Strengthen security posture by using behavior analytics to detect lateral movement, including techniques described in the MITRE ATT&CK framework.

Key Capabilities

Challenge 1: Collection and Detection

Legacy security tools cannot distinguish lateral movement by adversaries using valid credentials from normal user activity.

Solution

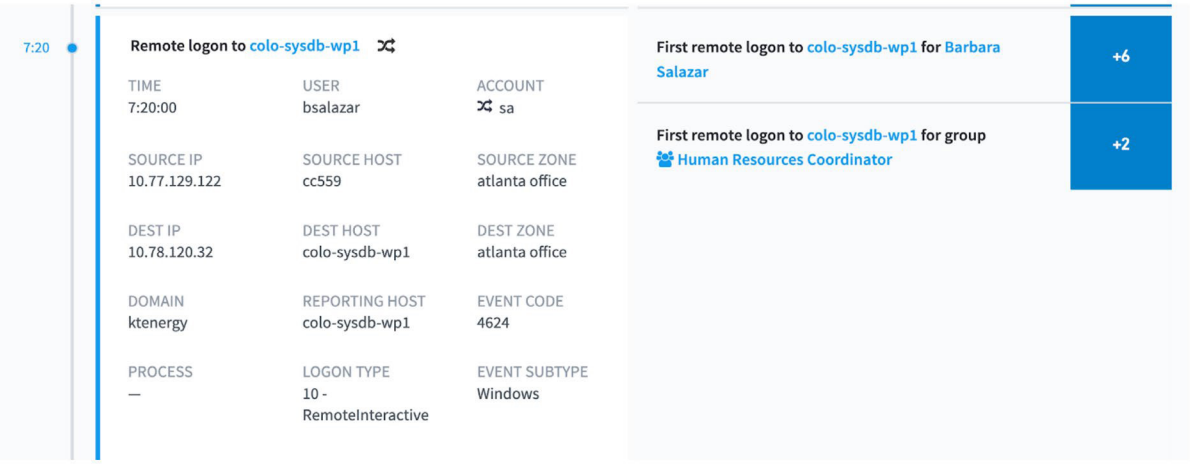
Exabeam ingests and analyzes key data sources to detect risky access and techniques like pass the hash, pass the ticket and more. Exabeam behavioral models put anomalous activity like first time or failed access to hosts and assets in the context of the historic behavior of that user, their peers and their organization to clearly identify adversary behavior from normal activity. Additional details are provided in Data Insights Models.

Challenge 2: Visibility and Investigation

Security teams are unable to answer key investigation questions and ensure they do not risk missing parts of a lateral movement attack.

Solution

Exabeam gives complete visibility into lateral movement attacks by providing a list of compromised users and assets. We create Smart Timelines for each user and asset using patented host-IP-user mapping to automatically assemble activity data into clear, readable events, all without an analyst needing to write a single query. Analysts can investigate further with Exabeam Threat Hunter to find other compromised users or assets, or drill down further in the timeline events to review the raw logs. Each step of the way, analysts can reference our lateral movement checklist to ensure their investigation is thorough and complete.



This Smart Timeline event shows compromised insider Barbara Salazar performing an anomalous remote login to the assets colo-sysdb-wp1.

Benefit

Improve investigation quality and speed by enabling analysts to quickly answer key questions like "Where is the user suspected of moving laterally?" or "Is this the first time they have accessed this asset?"

Challenge 3: Response

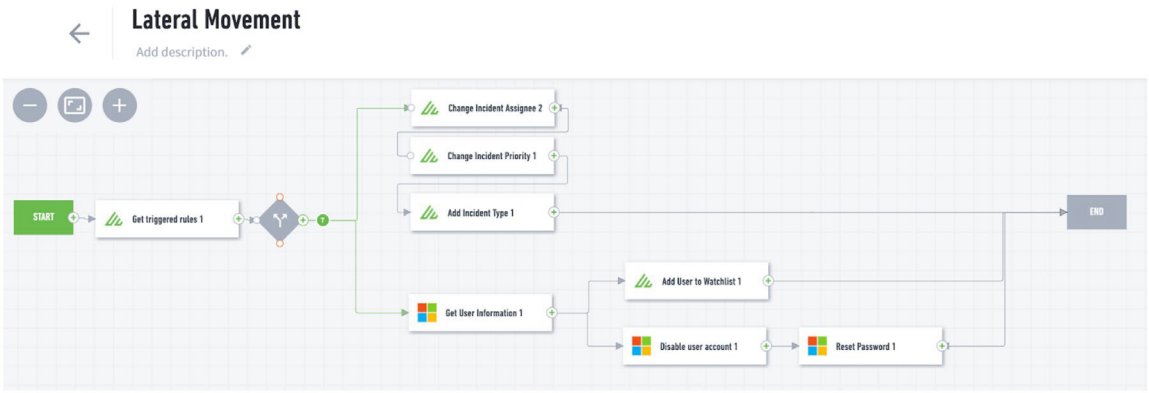
Security teams responding to lateral movements investigations spend hours or days coordinating a response across multiple security tools.

Solution

Exabeam playbooks orchestrate response to lateral movement incidents across your security stack. Out of the box integrations and customizable actions enable security teams to automate playbooks to respond to lateral movement incidents, such as suspending a user or resetting a password.

Benefit

Improve operational efficiency and decrease MTTR with security orchestration automation and response (SOAR) powered playbooks.



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

Use Case Content

To provide coverage for lateral movement, Exabeam identified key data sources and has built content for collection, detection, investigation and response.

Key Data Sources

- Asset logon and access
- Authentication and access management
- VPN and zero trust network access
- Network access, analysis and monitoring
- Endpoint security (EPP/EDR)
- Operating system logs (e.g. UNIX/LINUX/ OSX/Windows)

Key Detection Rule Types

- Pass the ticket
- Pass the hash
- Abnormal remote access and RDP activity
- Abnormal network connections and traffic

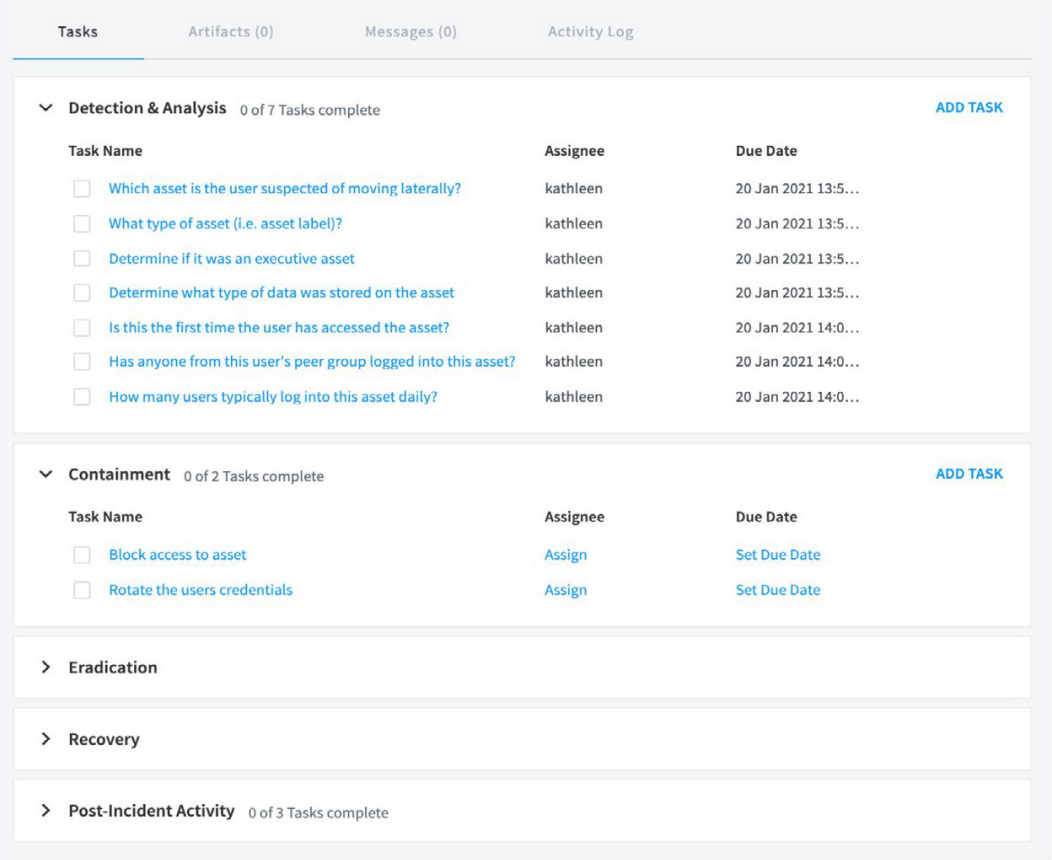
MITRE Technique Coverage

- T1090: Proxy
- T1205: Traffic signaling
- T1219: Remote access software
- T1071: Application layer protocol
- T1021: Remote services
- T1078: Valid accounts
- T1550: Use alternate authentication material

Response Actions

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

Incident Checklist



This lateral movement 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.