exabeam

Exabeam Use Case
SOC Efficiency & Advanced Analytics

How Behavior-Based Advanced Analytics Improves SOC Efficiency by Accelerating Attack Response Time

Speed is key in detecting, triaging, investigating, and ultimately remediating compromised credentials and detecting malicious users before more damage can be done. In this use case, you'll see how Exabeam immediately detected an alert that signaled a lateral movement attack.

The Problem

The customer's existing SIEM did not provide insights into user and entity activity. To gain more visibility and increase SOC efficiency, the customer added Exabeam Advanced Analytics on top of their SIEM.

Rapid Detection of Compromised Credentials

DAY 1

May 7 21:15
Initial Access
First Login from Singapore for User & Org

May 7 22:15
Lateral Movement
Attacker accesses many new assets for the first time

1 hr

exabeam

May 7 22:16
Exabeam generates a notable user alert 1 hr. into attack using only one Syslog feed to detect anomalous behavior

DAY 2

May 8 02:20
Lateral Movement
Attacker pivots off initial host and uses RDP for the first time to move to serverX

EDR

May 8 02:27
EDR alert to Powershell and Mimikatz on serverX

May 8 02:27–08:56
Lateral Movement
Attacker accesses 487 assets for the first time using 233 credentials for the first time dumped by Mimikatz

The Outcomes

Exabeam's out of the box content raised an alert for this incident 61 minutes into the attack. What would the customer have done without Exabeam? Reimaged serverX and moved on with the attacker still in the network.

1. Exabeam alerted the SOC 4 hours before EDR
2. Exabeam identified that 233 credentials were dumped from memory and compromised
3. Exabeam allowed the SOC to investigate this incident in a matter of hours, NOT days
4. The incumbent SIEM did not alert on the attack

Ready to take the next step? Contact us at **info@exabeam.com or 1.844.EXABEAM**

exabeam