Manufacturing
Protect Intellectual Property, Secure Smart Factory Initiatives and Overcome the Cybersecurity Skills Shortage

With manufacturing CEOs increasing their investment in smart factory initiatives and flagging operational risk as a key concern, security teams are the enablers of a successful smart factory transformation, tasked with laying the foundations for the businesses’ initiatives.

As a security leader, ensuring your team has visibility across employees, cloud and connected infrastructure is critical to success.

Facing adversaries with ready access to the compromised credentials needed to silently infiltrate networks, security teams are often burdened with legacy security tools to centralize and search security and network data, manually running time-consuming security investigations that regularly require specialist skills. The result is a lack of visibility into malicious activity, corresponding to delays in identifying and containing a breach, further exposing your organization in the event of an attack.

We knew we had to go beyond a traditional SIEM to UEBA, and we liked what we saw in Exabeam's UEBA capabilities.

FEMSA

¹ Manufacturers Alliance of Productivity and Innovation (MAPI), June 2020
Exabeam helps manufacturers address these cybersecurity challenges and lay the foundations for Smart factory initiatives.

Exabeam allows you to ingest log files from all relevant sources and then analyze the logs and apply behavioral analytics to detect early indicators of compromise and malicious insider threats, Exabeam’s automated workflows help you to mitigate your cybersecurity risks, secure smart factory initiatives, and operate efficiently even with limited security personnel and budgets.

**Exabeam Solution for Manufacturing**

**Mitigate Cyber Attacks**

Exabeam accurately detects high risk, anomalous user and entity activity across your network, through behavioral analytics.

By applying machine learning, Exabeam is able to analyze users’ day-to-day behavior in real-time for specific anomalies, detecting early warning signs of a potentially malicious employee or adversary techniques, and alerting your team so that they can thwart an attack before it succeeds.

Your security team would view this analysis in a machine-built incident timeline as shown in figure 1. Exabeam Smart Timelines provide all the information your analysts need to perform rapid investigations. They include every action a malicious user or an outside attacker who has compromised a user’s credentials took during a specific session, including access to data stores, so your team can see what preceded the security alert and what the adversary did from the time they logged on to the time they logged off. Each action is represented in the timeline with a risk score and additional context including mapping to the MITRE ATT&CK framework.

---

**Figure 1** – This Smart Timeline event shows an instance of a potentially compromised insider, with the employees credentials seen remotely accessing a part of the network for the first time, before moving laterally across the network to access payroll data.
Secure the Smart Factory

With Exabeam you can be assured that rules, alerts and searches are performed against the complete dataset, regardless of modern network evolution.

Exabeam monitors your IT, IoT and OT devices and cloud storage objects for anomalous behavior. Establishing baseline behavior using communication patterns, ports and protocols, and operating activity, Exabeam is then able to automatically identify irregular entity activities indicative of a security incident. Exabeam alerts your security team when the behavior patterns of a specific asset fall outside a normal range and warrant further investigation.

To ensure further efficiencies in your team, Exabeam performs IP association on current addresses and also all past DHCP IP addressing over time. So in the event an incident does occur, your security team isn't slowed down by having to match which assets correlate with the targeted addresses.

Address the Skills Shortage

SIEM solutions are renowned for being resource-intensive, requiring skilled analysts to run manual investigations that consume huge amounts of time, and are prone to human error. Your ability to source, train and retain proficient talent to run such solutions is expensive and hard to fulfill in a market that already suffers from a significant skills gap.
Key Points

- Enable smart factory initiatives
- Gain visibility into insider threats and indicators of compromise
- Monitor devices for unusual behavior
- Secure intellectual property
- Reduce time spent on security tasks by 51%

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are 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. The Exabeam Security Management platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and make security success the norm. For more information, visit www.exabeam.com.

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