FEMSA CUTS DOWN ON INCIDENT RESPONSE TIME WITH EXABEAM

UEBA COMBINED WITH SIEM AND SOAR REDUCE RESPONSE TIME AND OVERHEADS.

FEMSA is a global leader in the beverage and retail industry with a broad portfolio of top brands, including Coca-Cola and Powerade. The corporation is also the largest franchise bottler of Coca-Cola beverages in the world.

FEMSA’s retail business is equally as impressive as its beverage business with 20,000 convenience stores across Mexico, Colombia, Chile, and Peru, including OXXO, the largest and fastest-growing chain of small-format stores in Latin America. FEMSA operates in 13 countries with over 300,000 employees, serving more than 360 million consumers.

BUSINESS CHALLENGE

To support FEMSA’s business growth and protect their corporate data centers and critical business units in Mexico, the FEMSA SOC team, led by Rhett Nieto, saw an opportunity to update their cybersecurity and incident response (IR) program.

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

RHETT NIETO, FEMSA IT SECURITY CHIEF

They were also tasked with creating an insider threat program to help identify bad user behavior, including fraud.

INDUSTRY

Food & Beverage, Retail

EXABEAM PRODUCTS

- Advanced Analytics
- Threat Hunter
- Data Lake
- Cloud Connectors
With these requirements, the FEMSA team realized they would need to do more than simply monitor their network. They also recognized that they had to change from viewing security incidents based on IP addresses to detecting events based on users. The complex environment FEMSA was operating in, however, made it impossible to identify unique users.

Legacy systems and applications presented unique challenges, making it difficult to connect to their existing network monitoring system; creating volumes of work for a relatively small SOC team. The team was also spending an excessive amount of time writing scripts to automate the creation of critical security reports.

**SUPERCHARGING THE SOC WITH UEBA AND MACHINE LEARNING**

Understanding the limitations of their SOC and threat monitoring systems, the FEMSA team embarked on a rigorous, multi-phase program to evaluate several SIEM vendors. The first phase consisted of testing each vendor’s solution in FEMSA’s lab environment. The second consisted of testing live data from their data center in Mexico. Exabeam was one of the vendors selected to participate in the evaluation and ultimately chosen as the preferred vendor.

“We knew we had to go beyond a traditional SIEM to UEBA, and we liked what we saw in Exabeam’s UEBA capabilities,” says Rhett Nieto, FEMSA IT Security Chief.

The team also chose Exabeam as the solution includes over 600 pre-loaded machine learning models. With the pre-loaded models, Rhett’s team don’t have to spend all their time configuring and tuning their threat monitoring and response system.

**CUTTING IR RESPONSE TIME TO 45MINS PER INCIDENT WITH SOAR**

The FEMSA SOC team is always under pressure to meet their internal clients’ incident response SLAs. Under the current SLA, the team must respond within 60 minutes. Meeting the SLA proved challenging, given the small size of the team and the lack of automation. The team was manually connecting multiple data sources, collecting information, and confirming possible incidents.
Before Exabeam, it usually took FEMSA’s SOC team 74 minutes to respond to each incident, which meant the team wasn’t always able to meet the 60-minute SLA. With Exabeam, the team was able to react in 45 mins. FEMSA’s internal clients were so impressed with the results that they asked the SOC team to make 45 mins the new SLA. Nieto and his team agreed and could do so easily after incorporating security orchestration, automation and response (SOAR). Once SOAR was deployed and by leveraging the information displayed in Exabeam’s single interface, the average time to detect and alert business units improved even more.

“We dreamt about having something like SOAR. Now that we have it, we can respond in 43 minutes,” says Nieto.

The FEMSA team uses the MITRE ATT&CK Framework to map and automate their security rules and, partnering with Exabeam, has been able to increase their coverage from 50 ATT&CK techniques to 120. As a result, the team has been working on collecting and connecting more data sources to increase detection rate.

DETECTING ZERO-DAY EXPLOITS WITHIN A DAY

FEMSA’s SOC team started to deploy Exabeam in March 2019. By April 2019, the team was able to move its entire operation to the Exabeam platform. In May 2019, they detected their first zero-day exploit. It usually took the team 2-3 days to detect a zero-day exploit, but they spotted this threat on the same day. In June 2019, the largest business unit joined the project one year ahead of schedule, tripling the number of users and resources the team had to support. By July 2019, the group decided it was time to begin automation and threat hunting. At this point, the team was able to completely automate their monitoring and response.

“When we were asked to move up our deadline one year ahead of schedule to support the largest business unit, you have to trust the tool to do that,” says Nieto.

FEMSA recently started using Exabeam’s automated report generation to monitor user behavior, reducing the hand-off times between shift changes. A team just starting their shift can use a report generated by the prior team to easily see security events that had taken place in the past hour, 6 hours, and 12 hours.

“Having just a SIEM solution can save some time. Having Exabeam saves even more time.”

Another benefit the FEMSA security team has seen, was where they would normally have had to generate a network traffic analysis report on an hourly basis by searching for anomalous traffic based on IP, port, source IPs, source port, destination IP, destination port, and the web service that triggered the event. The entire effort took 45 minutes to an hour and a half.

With Exabeam, the team was able to create the same report in 8 minutes.

“Reducing the time it takes us to generate a report from an hour and a half to eight minutes has saved FEMSA a lot of money.” The team also found cost savings with Exabeam as they now no longer have to create and change their security rules and models manually.
KEY BENEFITS

- Cost savings through automated creation of rules, reports, pre-loaded models
- Zero-day threat response improved from 2-3 days to same day
- Exceed internal SLA for threat response

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.