With Preempt's Insights and Analytics, FIBI was able to prioritize workload based on accurate risk scoring of users and incidents, giving them immediate value through real-time detection of any potential threats.

"All high severity incidents detected by Preempt were true positives. This helped prioritize incidents for our SOC team, reducing the overall noise and burden."

Eran Kalige, Cyber Defense Incident Management Domain Expert

FIBI FIRST INTERNATIONAL BANK OF ISRAEL

Company Overview

Headquartered in Tel Aviv, FIBI is one of the top five largest banks in Israel with over a billion-dollar in revenue. With a strong legacy dating back to 1972, FIBI aims to offer the best customer experience to their clients which includes implementing the best security solutions on the market that help protect customer data.

Challenges

FIBI has over 4,000 employees with the majority of its workforce coming into the office to perform their day-to-day operations. FIBI understands that sensitive personal and financial data is often the #1 target for attackers, so they take a hardened, conservative approach to data sharing. With a changing threat landscape where attackers use more and more advanced tools and techniques to breach an organization and to stay abreast of the evolving threats.

Benefits

- Preempt's insights and analytics gave FIBI unified visibility into their users and accounts, allowing them an easy, consumable way to understand Active Directory (AD) risks
- Preempt's automated capabilities helped FIBI streamline workload and focus investigative time on what matters
- Preempt gave FIBI the high confidence to accurately tackle any potential insider threats and also quickly detect different types of advanced attacks on AD

Where is the Insider Threat?

FIBI requires that the majority of their workforce log into their internal network before accessing sensitive information. Because most of the user activity is limited internally to various systems and applications, detecting any potential insider threat is mission-critical to their success. "Every morning I wake up and ask where the insider threat is," said Eran Kalige, "we need visibility into all user accounts and their access attempts to be able to spot a malicious insider."

"Preempt did exceptionally well on an internal pen test done for advanced attacks on Active Directory and we knew it was the solution for us"

Too Many Incidents, Too Much Noise

FIBI quickly realized that manual SOC investigation was not scalable to address the growing threat landscape. Security data was difficult to parse out and accurate and timely classification of incidents was difficult to achieve. Eran explains: "We already have a variety of security solutions feeding into our SIEM so reducing the noise and automating resolution is a big goal for us."

Solution

FIBI choose Preempt for the ability to spot potential insider threats, accurately detect other threats and risky activity, and automate alerts to help the SOC team prioritize their workload.

Faster Time-to-Value

Deployment was easy and simple: the management console was stood up in less than one day; risk scoring for all accounts (user or service)to understand normal vs. anomalous behavior was established in the next few days; machine learning to spot potential advanced threats happened in weeks. "Preempt was very easy to deploy. We had it running in one day and never seen a simpler solution that gives insight into our Active Directory traffic," said Eran. "After the first few weeks, we were amazed by the results from Preempt's risk engine. We could see valuable insights like shadow admins, improper or excessive privileges, advanced AD manipulation techniques, and misconfigurations from active users."

> "Preempt is led by some of the best AD experts in the industry and that is why we trust them over the competition."

Prioritized Incidents Means a More Productive SOC

"Preempt gave us one location for insider risk so we can place those users on a watch list and set alerts," said Eran. FIBI helped streamline the workload for their SOC team and laser focus their attention to the most critical incidents. In addition, the SOC team was able to quickly share this information with other teams like the HR and Fraud to take appropriate corporate remediation.

Machine Learning is Needed to Stop Advanced Threats

FIBI deployed various UEBA solutions internally but false positives were weighing down their security team. "Our SOC team uses [Preempt's] threat hunting for advanced forensics and preparation for the next attack," said Eran, "Rule-based alerts are old-fashioned. We need machine learning for anomaly detection to respond to advanced threats. This is a different and more accurate approach and we think it's the next generation of Active Directory alerts."

Conclusion

By being able to detect potential insider threat with threat hunting and prioritizing workload with risk scoring and automated responses, Preempt was always the obvious choice. Eran explains: "The team behind Preempt gave FIBI the level of technical and industry expertise that we were looking for. Preempt gives us high confidence and accuracy that we need for risk scoring of security events. All high severity incidents detected by Preempt were true positives. This helped prioritize incidents for our SOC team, reducing the overall noise and burden."