ExtraHop Helps Leading Financial Institution Improve Banking Security with Real-Time User Behavior Analytics

Case Study: Global Financial Institution

The Beginning

Today, banking customers expect to access their accounts and manage their finances from any device, in any location, with the same level of consistent service and security. For IT and security operations teams, providing both of these things is no simple task.

For one global financial institution, finding the right balance between security and user experience came to a head when the security team wanted to incorporate real-time user behavior analytics into their authentication process. In order to do this, the security team needed to capture thousands of customer logins each minute, across dozens of banking applications, and stream this information into their Security Information and Event Management (SIEM) solution. While this measure would improve security and compliance, it also would have significantly impacted end-user experience over time. In order to align security priorities with IT operations requirements around system performance and user experience, the financial institution needed to find a better way to get the user behavior data into their SIEM.

The Transformation

For the security team, it turned out that the solution was right under their noses. The network team at the financial institution had long been using ExtraHop for performance management, giving them visibility from the infrastructure to the application and correlating it with end-user experience. ExtraHop's passive, out-of-band analytics not only provided the information the security team needed about user behavior, it did so without any performance impact on the banking applications.

The Benefits

Within four hours of deployment, ExtraHop was streaming user behavior data to the SIEM. Over the next several weeks, ExtraHop proved it could reliably capture, analyze, and stream the desired application information, alerting on activity as specific as users who had five failed login attempts in five minutes or less — behavior indicative of a possible hack attempt. By capturing this metric data on the wire, ExtraHop reduces the index volume and increases insight quality, alleviating data pipeline and ingest bottlenecks.

Faster Alerts

As a result of contextual analytics that provided more selective data capture and filtration, the security team significantly reduced ingest bottlenecks. The quality and reliability of the data also improved both the speed and accuracy of alerts on suspicious events related to user behavior. This allowed the team to react much faster, locking affected accounts or notifying information security personnel quicker than ever before.

Smarter Workflows

ExtraHop also improved the financial institution's threat investigation workflows. Rather than sifting through packets, the security team can now go from the initial threat alert to transaction-level details and corresponding packets in just three clicks. This on-demand root-cause analysis enables them to rapidly investigate attack patterns, helping mitigate the impact on customers and the business.

Challenge

This global financial institution sought to improve their security and compliance by incorporating real-time user behavior analytics into their authentication process without impacting the end-user experience.

Solution

To get the user behavior data they needed to stream into their SIEM, the security team looked to ExtraHop, a solution already being leveraged by the network team for performance management.

Benefits

- Alleviated data pipeline and reduced costs by only indexing actionable insights
- Improved speed and accuracy of alerts on suspicious events
- Faster investigations from threat alert to packet data in three clicks