sumo logic

Automating insider threat monitoring

Results at a glance

- → Optimized insider threat monitoring program
- → Minimized people, tools and time required to monitor for insider threats
- → Gained speed and efficiency in identifying insider data exfiltration attempts
- → Reduced security risk of insider threats

netskope

SUMO LOGIC PRODUCTS

Cloud SIEM

USE CASE

Automating Insider Threat Monitoring

sumo

Challenge

Knowing that threat actors can come from external and internal sources, Netskope's security team wanted to implement a practice to monitor for insider threats.

Maintaining a strong security posture is essential for Netskope. Referencing 2022 research from the Ponemon Institute that insider threats cost organizations $15.38 million per incident, Sean Salomon, Information Security Analyst at Netskope, commented, "That's a lot of money companies aren't going to want to lose. It's just not good business and, as a security analyst, it's not a very pleasant thing to think about."

As Salomon mapped out an initial standard operating procedure (SOP) for Netskope's insider threat monitoring, he could see that a manual process would require too much time, effort and resources.

"A manual approach would have required at least five people, ten tools and a minimum of 90 minutes of human work time per investigation. That's a lot of resources for an SOP. Plus, what if a request comes in on a weekend or after business hours where there's less coverage?" Salomon noted.

As an important part of streamlining and automating its insider threat monitoring process, Netskope wanted to adopt a SIEM solution.

INDUSTRY

Cybersecurity

ABOUT

Founded in 2012, Netskope is a global cybersecurity leader, empowering its more than 2,000 customers to apply zero trust principles to protect data with its Secure Access Service Edge (SASE) platform.

Solution

For its insider threat monitoring program, Netskope needed rapid and accurate insights into user behaviors that can represent high-risk indicators of insider threats. And the company wanted to automate the process to alleviate resource constraints. This requires investing in real-time data analysis to gain visibility into Netskope's insider threat activity, and for that, Netskope chose Sumo Logic Cloud SIEM.

Results

Automated insider threat monitoring

Built natively in the cloud, Cloud SIEM makes it easy to gain deep security insights with pre-built applications, including out-of-the-box dashboards, queries, and rules. Cloud SIEM ingests data and brings together Netskope's many data sources, such as endpoint detection and response (EDR), cloud storage and marketing and sales tools, to provide central security monitoring and contextualized insights.

"Leveraging Sumo Logic Cloud SIEM, the entire standard operating procedure for our insider threat monitoring has been completely automated. It significantly cuts down our response time, reduces the chance of human error and ensures we can make efficient and effective decisions."

netskope

Sean Salomon
Information Security Analyst

Robust analysis for data exfiltration attempts

During an insider threat investigation, Sumo Logic enables Netskope to analyze historical data and monitor a user's current activity. "There's always the potential that a user will act against the organization's best interests when they're planning to offboard, and Cloud SIEM helps us alleviate this risk," said Salomon.

Netskope uses Cloud SIEM's content management API to detect when users initiate mass data downloads or attempt to share data externally with a personal or competitor's email address. Of course, there's also the possibility a user might attempt to copy data to an external USB, and Cloud SIEM monitors for this activity as well. Leveraging the solution's Search API, Salomon has set up a search job that checks every five seconds to detect if a user has transferred any data to an external USB drive.

This workflow can take 200-300 actions to automate gathering all the required information. The team no longer needs to connect and share credentials to a variety of API endpoints or a range of different tools.

"Cloud SIEM enables us to catch these insider data exfiltration attempts early so that we can address them as quickly as possible and limit the impact of a potential insider threat," said Salomon. "We get all that information automatically, relying on zero people, zero tabs and just one tool—Sumo Logic."

By the numbers

200+
actions

fully automated workflow

855 Main Street, Redwood City, CA 94603