Forescout Reduces SOC Workload by 75%

316 DETECTIONS
from 10 billion logs/month

17 ESCALATIONS
from 254 cases/month

0.5 FTE
for response to true threats

Forescout Technologies
www.forescout.com

INDUSTRY

Cybersecurity

ENVIRONMENT

- Over 5,000 globally interconnected devices
- 1,000+ employees
- 3,000+ customers globally

CHALLENGE

- Excessive SIEM-related costs, nuisance alerts and false positives
- Limited specialized SIEM skillset

Overview

Forescout, a global cybersecurity leader, continuously identifies, protects and helps ensure the compliance of all managed and unmanaged cyber assets – IT, IoT, IoMT and OT. For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide vendor-agnostic, automated cybersecurity at scale. Led by Director of Information Security Joe Cardamone, CISSP, Forescout's nine-person Information Security and Compliance team supports over 1,000 employee users and secures more than 5,000 connected assets globally.

By the time the Forescout InfoSec team went looking for a threat detection and response solution, it was fed up with its third-party SIEM that was "almost completely unusable." It generated 100 to 300 alerts per day but little actionable information. The Cysiv extended detection and response (XDR) solution prevailed in a competitive POV process that emphasized easy onboarding of data sources, clean alerts of true threats and easy rule tuning. Within six months of implementing the new XDR, the InfoSec team was able to turn off the SIEM completely.

The product made such a difference that Forescout took the extraordinary step of buying the company in July 2022, renaming the solution Forescout® XDR and integrating it with the Forescout® Platform.

Business Challenge

Throughout Forescout's evolution, the company has used its own products to provide continuous, automated asset management and network access control across its environment, and to orchestrate asset remediation and incident response among its multi-vendor security products.

SOLUTION

Forescout XDR

USE CASES

- Threat detection and response
- Regulatory compliance

RESULTS

- 10 billion logs/month reduced to 17 actionable incidents
- 75% reduction in SOC workload

> "We selected [Forescout XDR] because it triages alerts and provides a clean picture of actual problems vs. noise. We were wowed by the sheer simplicity of setting it up, onboarding all our data sources and getting it functioning as a security product, not just a log aggregator."
>
> *— Joe Cardamone, Director of Information Security*

Until recently, however, the threat detection and response process had been largely manual – and fraught with issues. The SIEM system that the team had been using for almost two years was adequate for log storage, but getting actionable information out was almost impossible.

The SIEM product generated too much noise, which made it hard for team members to focus on actual incidents coming out of it. The team received 100 to 300 alerts per day that had to be reviewed, tuned and responded to. Moreover, the tool required its own specialized skillset in order to build queries, alerts and reports.

The third-party SIEM was almost completely unusable. Cardamone had to dedicate nearly two FTEs to its care and feeding, not just for incident response but also for configuration, management and maintenance – without getting much value out of it. And, the InfoSec team had to keep hiring the vendor's engineers to address even a small number of things they needed to get out of it.

In 2021, the InfoSec team began looking at alternatives.

Business Drivers and Success Criteria

The selection process was guided by compliance and operational requirements. On the compliance side, the team needed to have all logs in one central location, indexed and analyzed for threats, with the ability to set up alerts and other types of notifications to ensure compliance with various regulations. On the operations side, they needed clean alerts that were easy to tune and that could be triaged along with incidents found in the logs.

After a competitive POV process, Forescout selected the Cysiv XDR solution, based on three success criteria.

1. An easy onboarding experience.

The InfoSec team needed to be able to onboard the solution quickly and cleanly. After nearly two years, the incumbent SIEM still wasn't fully onboarded. The team struggled to get data into the platform, and if a data stream failed it would take weeks to be fixed and normalized, with the added expense of vendor engineers.

The InfoSec team started onboarding the Forescout XDR product (formerly Cysiv) in July 2021, and it was fully loaded with all data sources by the end of September. The team worked with a dedicated individual who knew how to interconnect the systems, overcome challenges in the Forescout environment and ensure all the logs got ingested and normalized properly. If a data set ingestion failed for any reason, she was able to write a custom connector and tweak it until it worked properly.

2. Operationalization in the Forescout environment.

The InfoSec team manages its workload through its ticketing system, so integration was essential. When a case is created in Forescout XDR (it could be an event, alert or incident that needs human attention), it is automatically entered into the ticketing system. As expected, for the first few months the cases coming out of the XDR product needed tuning to reduce false positives. The InfoSec team worked with the security operations center (SOC) team to tune the rules, an easy process that drastically reduced the noise. Today, cases in XDR are almost entirely actionable incidents with high fidelity, and detailed contextual data that streamlines the follow-up process. They are first triaged by the SOC, which cuts down on even more noise.

3. Log access, reporting and dashboards.

For compliance and investigations, Forescout retains all logs for 13 months. The team needed to be able to access the historical logs, pull reports and build dashboards. The Forescout XDR user interface features many dropdowns and field selections to guide reporting and configuration.

XDR is the intelligence that makes raw log data actionable. The InfoSec team sees what they need to see plainly, easily and quickly, without Forescout having to spend over $500K on specialized skillsets and SIEM add-ons to get the same functionality. It works out of the box without the team having to beg it to do what they need it to do.

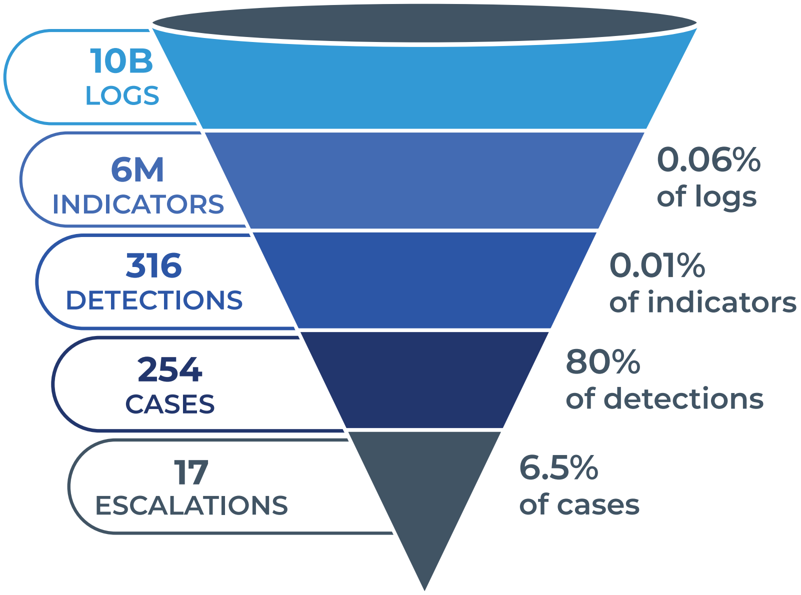
Business Impact

After migrating to Forescout XDR, the team was able to onboard many more data sources than the original SIEM could handle. As a result, the number of logs ingested more than doubled to almost 10 billion a month, which are automatically normalized and enriched to maximize their detection value. The two-stage threat engine then uses a blend of five techniques to weed out the vast majority of logs and generate about 6 million indicators – a mere .06% of ingested logs.

In Stage 2, the indicators are further refined into detections by correlating sequences, patterns or volumes of indicators. Of an average 316 detections a month – just .01% of indicators – 254 became cases and 17 were escalated for investigation by one of the analysts.

The important numbers are at the bottom of the funnel, namely, the fidelity of the alerts generated by opened cases. **For calendar year 2022, more than 80% of detections resulted in cases, and only 6.5% of cases required investigation by one of the analysts.**

2022 Average Monthly Data



> “We couldn’t do these proactive things before. We were so busy putting out fires we didn’t have time to make the fire department better.”
>
> *— Joe Cardamone, Director of Information Security*

Fewer, higher-fidelity alerts

Before XDR, the InfoSec team had to sift through 100 to 300 alerts a day coming out of the SIEM, about 95% of them unactionable (e.g., an alert for unusual access, but the user has permission). Now the team see fewer than 20 cases per month that require Level 2 support (escalations). And that number keeps dwindling as they further refine their rules to work out more noise.

Improved compliance

XDR enables the InfoSec team to see all the logs in one place and retain them for 13 months. It also tracks all the required compliance metrics for easy reporting: Time to detect, time to respond, time to resolve. This has taken a lot of manual work off of the team.

Risk reduction

Given the time to focus on what matters, the team has been able to remove items from their risk register instead of chasing ghosts in the SIEM and having to tune it, which improves their external security score. Previously, when the team’s headcount dropped that score dropped, because there was no one to address those problems. These numbers get reported to the board.

FTE redeployment

Before the team had XDR, there were two FTEs dedicated to SIEM maintenance. Now, they only need .5 FTEs for incident response when the SOC raises a case. Instead of spending so much time tweaking and tuning the SIEM (with limited success), the team can tweak and tune the InfoSec program overall. Things like adjusting endpoint settings to stop noisy alerts, evaluating the control policies on employees’ computers, integrating new security tools and tuning how they use the Forescout Platform itself. The team couldn’t do these proactive things before. They were so busy putting out fires they didn’t have time to make the fire department better.

Cost savings

FTE time savings translates directly into cost savings, not to mention retention of scarce resources. With the SIEM, to investigate an alert all the team had to go on was that, say, Bob, tried to access a restricted part of the network. Now all the data correlation they need to build fidelity is in one place: they know that Bob was on this machine at this time, trying to access that segment, and his machine is out of compliance. Instead of getting limited alerts in the SIEM, the InfoSec team gets a full case, including the data to make the right decision and shrink time to triage.

Forescout Technologies, Inc.

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com