FORESCOUT FRONTLINE

State Agency Accelerates Remediation And More With Forescout Threat Hunting Service

< 1 hour
to identify and isolate devices affected by Log4j

< 1½ days
to actionable intelligence to mitigate vulnerabilities

$0
cost for threat hunting service

INDUSTRY

Government

ENVIRONMENT

7,400 wired and wireless devices across 16 divisions and 220 sites; 4,200 employees

CHALLENGE

- Lack of IT staff resources to perform in-depth threat analysis and assess vulnerabilities such as Log4j
- Provide business continuity to deliver a wide variety of services to the public
- Safeguard PPI and other sensitive information
- Comply with state and federal regulations while reducing time spent on operational audits

Overview

To learn the full extent of the Log4j vulnerability in its environment, this State of Florida Agency engaged Forescout's threat defense team called Forescout Frontline. In less than a day and a half, this diverse U.S. state entity that supports several key Florida departments had in its hands not only the Log4j information it sought but actionable intelligence concerning embedded IoT vulnerabilities, insecure communications and other risks. Leveraging this free service shrunk time to mitigation and remediation of these security gaps and improved security posture.

Business Challenge

"We knew Log4j was a critical issue, but we lacked a full picture of the risk within our extended enterprise."

— *Information Security Manager, State of Florida Agency*

Like government organizations and companies across the globe, the State Agency's information security manager knew their organization needed to address Log4j, a zero-day vulnerability in a popular Java logging framework. They needed to know exactly where each instance of Log4j resided across the organization's 220 sites in 16 diverse divisions spread across the state. They knew they could benefit from someone with expertise and extensive experience conducting in-depth, proactive threat hunting and analysis.

SECURITY SOLUTION

- Forescout eyeSight
- Forescout eyeInspect
- Vedere Labs Threat Intelligence
- Forescout Frontline

USE CASES

- Threat and risk identification

RESULTS

- Obtained detailed information on scope of Log4j vulnerability as well as wide range of other security risks – in 12 hours of onsite engagement
- Discovered Log4j, PrintNightmare, NUCLEUS:13, RIPPLE20 and other vulnerabilities, including insecure communications and blacklisted credential usage
- Accelerated time to mitigation and remediation of security gaps, known and unknown
- Gained knowledge to enhance value of existing Forescout investment
- Made possible the identification and isolation of all managed devices vulnerable to Log4j in one hour

Why the Forescout Threat Hunting Service?

Consequently, the State of Florida Agency decided to take advantage of Forescout Frontline's new threat hunting service, currently available at no cost to Forescout customers as well as prospective customers as the service is being developed and fine-tuned with customer input. "We've been extremely pleased with Forescout support so far and the service was free, so we thought we would give it a try," explains information security manager. Shawn Taylor, head of Forescout Frontline's team, spent a day and a half on-site threat hunting using three key tools: the State of Florida Agency's existing Forescout's device visibility and control platform; Forescout eyeInspect, which passively analyzes network telemetry looking for vulnerabilities as well as such risks as use of blacklisted credentials, insecure communications methods and expired SSL certificates; and the Vedere Labs Threat Intelligence. (Forescout Frontline also uses other third-party and open-source tools when needed.)

Business Impact

"Shocking" Results and Actionable Intelligence within 12 Hours On-Site

After just a day and a half on site, Taylor produced a report with comprehensive threat hunting findings for the extended State of Florida Agency enterprise. "My initial reaction to the findings was shock," recalls the information security manager. "They were eye-opening. I reached out for one thing – visibility into our Log4j vulnerability – but received so much more. The findings gave us visibility into security gaps, some we already knew about and others we didn't…The report was way more thorough than I expected, with in-depth information and actionable intelligence. Not just on Log4j but on other critical vulnerabilities as well, and not just in general terms but exactly where they exist in our environment."

Shrinking Time to Mitigation and Remediation of Vulnerabilities

The detailed report also provided possible next steps for each type of vulnerability found. For instance, for the 37 devices with Log4j and the 2,500 devices with PrintNightmare, the recommended next step was to apply Microsoft's released patches and recommended configurations. For others, such as NUCLEUS:13 and RIPPLE20 vulnerabilities for which the vendor had not yet released a patch or upgrade, possible next steps

> "The [Forescout threat hunting] report was way more thorough than I expected, with in-depth information and actionable intelligence. Not just on Log4j but on other critical vulnerabilities as well, and not just in general terms but exactly where they exist in our environment."
>
> — *Information Security Manager, State of Florida Agency*

included monitoring traffic or isolating the devices to separate VLANs. Such detailed information helped – and continues to help – the State of Florida Agency mitigate risk and remediate much faster. For instance, they could isolate all 37 devices hosting Log4j vulnerabilities in less than an hour. Similarly, the instances of critical NUCLEUS:13 vulnerabilities embedded in their IoT devices could be isolated, or at a minimum, traffic to and from them could be monitored for anomalous activity.

Easy and Free Resource to Help Improve Security Posture

"The engagement was very easy on our end," notes the information security manager. "We basically made sure Shawn [Taylor] had visibility into network traffic – we just set up a SPAN (switched port analyzer) – and then Forescout took the ball from there. He did the drilling down for us… In addition, they walked us through a lot of things that will help us get more out of our Forescout investment."

"We developed Forescout Frontline because we believe cybersecurity is a shared responsibility," says Taylor. "At State of Florida Agency, we provided that incremental support and threat-hunting expertise to help organizations find those risks and threats they aren't necessarily able to find on their own. In a sense, we're helping them help themselves."

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