Case Study

MULTINATIONAL TECHNOLOGY COMPANY

SOFTWARE AND TECHNOLOGY

SUMMARY

With Searchlight's ASM solution, this technology company successfully automated the discovery and prioritization of exposures in their systems through the eyes of a malicious actor. The security team can now preemptively tackle real threats without being overwhelmed by the noise they experienced with other tools - saving valuable analyst time while also delivering better security outcomes for the business.

CHALLENGES

- RAPIDLY EXPANDING EXTERNAL ATTACK SURFACE
- LACK OF VISIBILITY ACROSS ENTIRE ATTACK SURFACE
- ALERT FATIGUE

OUTCOMES

- COMPREHENSIVE ATTACK SURFACE VISIBILITY
- LACK HIGH-SIGNAL EXPOSURE PRIORITIZATION AND REDUCED NOISE
- UNCOVERED NEW SECURITY USE-CASES

SOLUTION

ATTACK SURFACE MANAGEMENT (ASM)

GAINING AN ADVANTAGE OVER THREAT ACTORS

This leading software provider faced the complex challenge of securing a continuously expanding external attack surface distributed across multiple subsidiaries, cloud providers, and geographical regions. Despite maintaining a mature security program, they lacked the holistic visibility required to fully validate the effectiveness of their controls or to stay ahead of rapid infrastructure changes.
The security team had evaluated numerous other tools to solve this problem, but found they consistently fell short. These alternatives failed to provide a comprehensive view of all the assets and systems that made up their attack surface, or the context needed to focus efforts across their many thousands of assets.

After hearing about Searchlight Cyber's Attack Surface Management (ASM) solution from industry peers, the company decided to see first-hand what the platform could do. The turning point occurred when, after providing only a few domains as initial seeds for demonstration, the Searchlight solution rapidly discovered the company's entire external attack surface - spanning on-premise assets, multiple cloud providers, and subsidiaries. Once the assets and systems were discovered, the platform started continuously monitoring the company's attack surface for high signal security exposures and immediately identified areas the security team could focus on, including use cases they hadn't yet considered.

SEEING ASSETS FROM A THREAT ACTOR'S POINT OF VIEW

The Searchlight ASM platform has become an indispensable part of the organization's security operations, with the SOC team viewing it as a critical dependency for their daily workflows.

Because the company's network and systems change constantly, the solution provides the necessary agility to keep up with these dynamic shifts. This ensures any new asset pushed to the internet is immediately discovered and assessed in context, giving the security team visibility into what's running and the ability to rapidly remediate exposures before they can be exploited.

SEARCHLIGHT. CYBER

"Today, networks are a living thing, they are changing every day. You spin up new assets, you shut some down, it's very dynamic. With Searchlight, they are the good guys that think like the bad guys, they look at our attack surface through the eyes of a malicious actor and will try to imitate similar techniques to find where we might have a problem." - Chief Information Security Officer

The security team can now validate the effectiveness of their existing controls by viewing their attack surface through the eyes of a malicious actor, with the platform rapidly creating new detections for critical exposures, ensuring the company stays ahead of emerging threats.

> Today, networks are a living thing, they are changing every day. You spin up new assets, you shut some down, it's very dynamic. With Searchlight, they are the good guys that think like the bad guys, they look at our attack surface through the eyes of a malicious actor and will try to imitate similar techniques to find where we might have a problem.
>
> **CHIEF INFORMATION SECURITY OFFICER**

UNDERSTAND AND PRIORITIZE THE REAL THREATS

The most significant value realized is a dramatic increase in operational efficiency. While other tools frequently inundated the team with thousands of alerts; forcing them to waste time deciphering what was real, the Searchlight solution cuts through the noise by alerting only on validated, exploitable exposures. This high-signal approach allows the security team to prioritize their efforts and respond rapidly to genuine threats.

"The platform allows my team to respond quickly and prioritize where they spend their time. As an example, other tools may send me 1,000 alerts, which my team needs to try and manage and understand what is real and what actually requires attention. Searchlight only alerts my team on real issues so they can cut through this noise and respond very quickly to alerts" - Chief Information Security Officer

The organization's use of ASM has already expanded to cover other use cases that were not initially considered. These include identifying whether any sensitive information is being leaked on third-party code sharing platforms, creating their own custom checks to run across their attack surface continuously, as well as gaining further insight into their public facing assets.

"I asked our SOC Team Leader earlier, how long could we be without Searchlight? Would it be for minutes, hours, days? The response: We couldn't. The Searchlight ASM solution is a key part of our security program, and we could not do without it," said the Chief Information Security Officer.

SEARCHLIGHT. CYBER

CONTACT US SALES@SLCYBER.IO // SLCYBER.IO

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
+44 (0)345 862 2925

USA HEADQUARTERS
Suite 213, 44 Merrimac St,
Newburyport,
MA, 01950
+1 (202) 684 7516