LOOKINGGLASS

CASE STUDY

LOOKINGGLASS HELPS GLOBAL FINANCIAL SERVICES ENTERPRISE REDUCE THIRD-PARTY AND SUPPLY CHAIN CYBER RISK

"LookingGlass is essential to our third-party risk management program. We use LookingGlass's scoutPRIME® as the main tool for monitoring our third-parties' Internet-facing assets and identifying threats and vulnerabilities, which are then communicated to the appropriate parties for remediation. This non-invasive, continuous monitoring capability complements our organization's point-in-time, questionnaire-based assessment process, giving us a holistic view of our suppliers' overall information and cybersecurity posture."

BACKGROUND

This global organization ("Company B") provides comprehensive financial services, from traditional banking to loans and capital markets access, to consumers and businesses, with a mission focused on economic growth and safeguarding customers' financial assets. It operates in more than 100 countries and has more than 200,000 employees. To enable its mission and ensure trust with its customer, cybersecurity is a critical support function. Approximately 3,000 team members make up the global information security (InfoSec) team.

Visual representation of Company B's interconnected third-party network.

THE CHALLENGE

Company B has long leveraged outside vendors to support its business. Thus, third-party risk management (3PRM) was not a new concept to the InfoSec team. To manage this risk, the InfoSec team required each supplier to complete a point-in-time self-assessment, which was reviewed and re-completed on a frequency based upon the risk associated with the vendor.

About a decade ago, with technological innovations such as software-as-a-service (SaaS) becoming mainstream and enabling significant efficiencies and cost-savings, this financial services company, like many of its peers, implemented digital transformation initiatives that led to a rise in the purchase and use of technologies and services owned and managed by third-parties or suppliers. And financial regulators began to look closely at the risk management strategies and mitigations around suppliers and third-parties.

The potential impact to Company B, should a vendor or supplier fall victim to a cybersecurity attack, could be devastating. Regulators noted that Company B should strongly consider adding a more continuous approach to 3PRM, such as assessing and monitoring the security of its supply chain on a daily basis. Though penetration testing (pen testing) is often used to test the security of an organization, continuous pen testing for networks and systems outside of Company B's ownership was not feasible.

In addition to needing to continuously monitor and assess its third-party vendors and suppliers, the risk assessments team was already fully tasked. Company B would need to stand up a new team within the 3PRM unit to manage, coordinate, and help mitigate any findings from the continuous assessments. The 3PRM team needed a tool to continuously monitor networks they didn't own with non-invasive methods that could uncover any potential cybersecurity risks. This tool would also need to provide the details necessary to help vendors and suppliers mitigate any issues.

THE SOLUTION

In September 2014, Company B's CISO engaged with LookingGlass to leverage LookingGlass's scoutPRIME® to help solve these challenges. The always-on, "outside-in" approach delivered by scoutPRIME meant that risk management strategies for continuously monitoring suppliers and third-parties could be easily implemented.

LookingGlass's scoutPRIME offers contextualized, correlated threat intelligence overlaid on a dynamic map of the world's internet infrastructure to provide an analysis and visualization – a footprint – of logical (IP routing), physical (geo-location) and transit medium (fiber, satellite) information.

By utilizing scoutPRIME®, Company B is able to continuously monitor their third-party vendors and suppliers without intrusively scanning those networks. This process complements their organization's point-in-time, questionnaire-based assessment process, giving a holistic view of their third-party suppliers' overall information and cybersecurity posture. They can detect a vulnerability immediately and can push it to the vendor for remediation. "Other products report once a week. LookingGlass's scoutPRIME® reports in real-time, whenever it sees something new, making it essential to our third-party risk management practice," said Company B's Regional 3PRM Manager.

Furthermore, the flexibility and extensibility of LookingGlass means organizations can use it as a foundational platform to serve a full spectrum of cybersecurity missions and operations. At Company B, LookingGlass's scoutPRIME supports the global information security team and can be utilized across multiple groups (e.g., Security Operations Center, Network Operations Center, Legal, Threat Intel, etc.) via the company's internal fusion center. With scoutPRIME's large-scale data collection, normalization, and correlation, the global information security group can access contextualized and actionable threat intelligence, helping to meet multiple cybersecurity missions and operations.

MEETING MISSION OUTCOMES

With LookingGlass, Company B not only met regulator recommendations, but more importantly, improved their security effectiveness by monitoring thousands of third-party vendors and suppliers globally to proactively identify and mitigate cyber risk and impact to the business. In one instance, Company B's 3PRM team was monitoring a third-party vendor through scoutPRIME and discovered an entire Classless Inter-Domain Routing (CIDR) block that was associated with the vendor, unbeknownst to that third-party. After further investigation, Company B discovered malware present within that CIDR block and was able to identify that it was running on a Windows XP (WinXP) machine. When presenting the evidence to the vendor, they claimed it was not possible, as none of their business machines ran WinXP. With scoutPRIME, Company B was able to pinpoint the IP address and geolocation of the infected machine and turned this data over to the vendor. With this more detailed intelligence, the vendor was able to find the machine, which belonged to an employee whom was running WinXP on an unauthorized virtual machine on their business computer. The vendor resolved the issue, ultimately strengthening Company B's cybersecurity posture and reducing its supply chain risk.

By utilizing scoutPRIME's expansive capabilities, Company B was able to move beyond simple vendor security ratings to get a deeper, more actionable view of cyber risk across their supply chain by monitoring the attack surface and layering on threat intelligence seamlessly. This enables the information security team to meet its mission and support the business quickly and thoroughly.

ABOUT LOOKINGGLASS

LookingGlass is a global cybersecurity leader that provides public and private sector clients with a comprehensive view of their attack surfaces layered with tailored, actionable threat intelligence. For more than a decade, the most advanced organizations in the world have trusted LookingGlass to help them protect their financial, economic, and national security interests.

Find out how we can help your organization at **www.LookingGlassCyber.com**