SecureWorks

GLOBAL BANKING GIANT STREAMLINES AND STRENGTHENS CYBERSECURITY

Bank fortifies its security capabilities with unmatched expertise from SecureWorks®

Industry: Banking & Finance | **Country:** Europe | **Employees:** Thousands

BUSINESS NEED

Even with a highly trained, in-house CERT team, the bank needed to strategically improve its security operations and maturity, its regulatory compliance, and its security escalation processes.

SOLUTION

Utilizing SecureWorks Security & Risk Consulting services, the bank was able to do a full maturity scoping to make strategic incremental improvements to its security program and governance. This engagement included sourced SecureWorks residency services to build a level-one SecureWorks Cyber Threat Operations Center that utilized the SecureWorks Counter Threat Platform® for enrichment to its security escalation processes.

BENEFITS

- Hundreds of locations worldwide and 13,500 endpoints now securely monitored
- 70 billion events monthly cut to 20–40 needing attention
- Enhanced regulatory compliance worldwide

SecureWorks Advanced Endpoint Threat Detection–Red Cloak | SecureWorks Counter Threat Platform | SecureWorks Security Residency and Implementation

FOR HACKERS AND OTHER THREAT ACTORS, THIS GLOBAL BANKING GIANT IS A WHALE OF A TARGET: THOUSANDS OF EMPLOYEES, WITH MANY WORKING REMOTELY; HUNDREDS OF LOCATIONS WORLDWIDE; MULTIPLE DATA CENTERS; AND MORE THAN 1,000 MISSION-CRITICAL APPLICATIONS.

For banking regulators around the world, cybersecurity is an ongoing and primary concern, especially given the growing number and sophistication of attacks across the industry. In 2015, the reported heist of up to $1 billion over two years from more than 100 banks only intensified that concern. And that's not to mention the $81 million cyber theft in 2016 from Bangladesh's central bank using the Swift interbank exchange system.

Until a few years ago, the bank had augmented the cybersecurity expertise of its internal Computer Emergency Response Team (CERT) team with outsourced monitoring of its firewalls, intrusion detection, vulnerability management and log retention. But the process by which security alerts were handled was deficient. It involved a third party, which would dispatch an alert to a regional data officer. This person would assign the alert to an asset owner, who often lacked the security expertise needed to properly address the intrusion or security issue. These handoffs took time and could involve miscommunications, leaving potentially disruptive matters to do more damage.

In 2013, an outside consultant to the bank carefully analyzed its security requirements and found the internal security team to be insufficient in size for the global scope of its operations. In response to this report, the bank issued a tender for engaging a qualified cybersecurity provider able to provide managed services globally. The winning candidate would also have to field a team of security experts who could work from inside the bank's organization — as a SecureWorks Cyber Threat Operations Center (CTOC) — in close collaboration with its CERT team.

IMPLEMENTING A COMPREHENSIVE, GLOBAL CYBERSECURITY PROGRAM

SecureWorks won the bid with a strategic proposal developed by the SecureWorks Security & Risk Consulting team.

SecureWorks team recommended an onsite Security Residency and Implementation operations model. SecureWorks showed how it could collaborate with the bank to provide a strategic approach through a carefully constructed maturity framework that would improve its operations and monitoring incrementally over time, while decreasing risk.

The SecureWorks Security Residency and Implementation provided the bank with a staff of senior security experts who effectively operate an in-house, level-one security operations center. To help them do their jobs, they tap into the security intelligence of the SecureWorks Counter Threat Platform (CTP), which closely monitors known and emerging threat actors and their many billions of activities across the entirety of the SecureWorks global client ecosystem — more than 4,300 clients in 59 nations. The CTP enables them to detect the bank's adversaries, not just their malware, and respond much faster to incidents, if not prevent them altogether.

Should this in-house CTOC staffed by SecureWorks need backup for any especially insidious threat actor at any time, they can turn to their colleagues at the SecureWorks Counter Threat Unit® (CTU) research team. The CTU team consists of scores of the world's most highly regarded security experts. Regularly called upon by government agencies, law enforcement, and private industry, CTU experts are often the first to identify developing threats and provides actionable intelligence on those threats to the bank's SecureWorks team as it does to SecureWorks clients around the world.

STREAMLINING ESCALATIONS TO ACCELERATE RESPONSE

Today, three years later, the SecureWorks CTOC team has developed a close working relationship with the bank's CERT team. With weekly meetings and frequent interim communications, they have improved security processes, procedures and governance across the bank's global enterprise, fine-tuning them in each meeting.

Operationally, they have worked together to dramatically streamline the escalation of imminent and potentially disruptive security threats — "true positives" — by improving the screening of 70 billion potential security events a month. From that number, they alert the CERT team to 20–40 threats a month and what actions were taken to contain those threats.

The SecureWorks CTOC team also handles an average of three to four phishing campaigns a day that find their way into employees' email inboxes. Although email filtering, IDS/IPS and EndPoint control keep most phishing attempts out, some do get past the email controls. SecureWorks staff then work quickly to identify malicious code, who clicked on it and how far it has spread. They then respond appropriately to contain and eliminate it.

PROTECTING MORE THAN 13,500 USER ENDPOINTS

SecureWorks provides 24x7 threat protection to more than 13,500 user endpoints, both desktops and laptops, via the SecureWorks Advanced Endpoint Threat Detection (AETD)–Red Cloak™ service.

AETD Red Cloak service works by downloading lightweight sensors to a client's user endpoints. These impose little CPU burden while they search for forensic evidence of malicious activity and continuously collect information about what is happening on the device, such as what programs are running, what commands are being executed, network connections, thread injection, memory inspection and more.

The sensors send the collected data to the SecureWorks Red Cloak Analytics system, hosted off-premises, where it is analyzed using intelligence from the SecureWorks CTU research team to spot attacker behavioral patterns and other threat indicators.

If found, an alert is generated with a rating on severity, confidence and event classification. An expert analyst in one of SecureWorks Counter Threat Operations Centers also assesses the threat. Any high-severity, targeted event is escalated to SecureWorks senior intrusion analysts, who will deconstruct the event and send the bank's SOC team actionable guidance to contain and remediate the threat.

PASSING REGULATORY CYBERSECURITY AUDITS CONSISTENTLY

The bank's improved security posture has helped it in its interactions with its regulatory auditors across the U.S., Europe and Asia. They are charged with checking its cyber safeguards periodically to ensure regional and national compliance with increasingly strict standards. Auditors look for clear signs of increasingly mature cybersecurity processes, procedures and governance across the bank. Given that the bank consistently passes ever-more stringent compliance assessments, regulators are finding just that.

As a result of the bank's comprehensive SecureWorks engagement, coupled with a close collaboration with the bank's CSIRT team, the bank continues to pass these increasingly stringent compliance assessments. Together, they have demonstrated continuous security control and spread across the bank's global enterprise, thanks to regular tuning calls to improve processes and governance.

Few examples of such a large-scale cybersecurity program exist in the world's financial services industry. This one can certainly provide a model for other banks to note. Today, the bank's cybersecurity is stronger than ever, with greater threat visibility due to the utilization of SecureWorks threat intelligence, which helps identify who is attacking them and for what purpose. More secure endpoints and intrusion protection help, too.

The bank's improved security posture has decreased the overall business risk associated with cyberthreats. Going forward, SecureWorks will continue to help it meet the increasing number and sophistication of threats head-on.