Comtrade Three-Sixty

CASE STUDY

Cyber-attack protection and data security

Industry

IT Infrastructure Products and Cyber Security Solutions

Technology

Palo Alto Networks Next Generation Firewall
Cortex XDR and Panorama
Tenable Nessus Professional™
SecurityScorecard
IBM Security® QRadar® SIEM
ESET Antivirus
Burp Suite

At a glance

When a client working in the field of Cloud Backup and Recovery needed to improve their product's feature development, architecture and design, our team stepped in and upped the game. Effectively overseeing the complete software development lifecycle, we worked on R&D, QA and test automation, DevOps, technical writing, as well as L3 support, releasing high-quality product versions spot-on and on time.

Client

Our client was a large multinational enterprise company, who hired us as an independent third-party security service provider to help them supervise their digital environment and control their critical assets. Our goal was to establish swift security incident response that can execute real-time incident analysis and provide a solution in close cooperation with their IT team.

The client showed us their workflow including the security and compliance measures implemented at the time. Their IT team gave us full support from the start, as well as complete access to their main company's infrastructure, their security logs and tools.

Project goal

We were hired to do a professional assessment of Cyber Security resilience. Initial service of Cyber security vulnerability identification using ethical hacking approach and pen test tools successfully evolved into fulltime engagement of our Cyber Security experts. We now do a real-time monitoring of the whole IT infrastructure, perform investigations of security events/incidents and manage ongoing risk analysis process in order to further improve our business partner's cyber security resilience.

Firstly, we assessed the security status, then analyzed and prioritized security risks and then improved security controls together with their inhouse IT team experts and vendors. Additionally, the company started to route all new security issues to us, providing us with required access for an expert real-time issue analysis which gave them much-needed confidence and full control over the security of their environment. This cooperation provided a win-win results for both entities and opened important channels for implementing the latest and best Cyber Security practices, detecting exploitable vulnerabilities and developing and ongoing pool of ideas for security improvements.

About Comtrade 360

Comtrade 360, a member of the Comtrade Group, helps businesses stay ahead in an ever-evolving digital world. For more than 30 years, we have accelerated innovation and growth by providing solutions to key technology partners.

Our clients, leading enterprise infrastructure and system software vendors across the globe, know what we're about: delivering a comprehensive range of top-notch software development services and solutions for your IT challenge.

Challenge

One of the security tools detected that the personal credentials of a third-party accounting administrator supporting the finance department, which is a smaller subsidiary, were stolen and used to establish an RDP connection. The cyber attacker then used the vulnerability of the Windows RDP protocol to impersonate an IT Manager, granting himself access to confidential information via that account. As a result, both accounts were immediately locked to prevent further activities.

To have a fruitful and productive cooperation, honest and trustful communication about the infrastructure, potential issues, strengths and weaknesses was crucial from the start. This also required a part of IT access rights to be shared and opened to a trustworthy business partner.
Since team members were from different locations, with their own responsibilities for different parts of integrated infrastructure and security, we needed to open dedicated real-time communication channel where all findings, issues and security related task statuses were communicated right away to all involved. This resulted in full transparency about open/critical security issues, working as active security and IT knowledge sharing portal, providing real-time feedback and explaining guidelines to all stakeholders.

Solution

The solution development started on Windows Server, allowing Remote Desktop Connections that were initially used by the cyber attacker as the entry point. We performed a sequence of internal and external testing, vulnerability assessment, wireless and physical security assessment, and final security review. During the assessments, we evaluated their password policy and the usage of their MFA method. Previously, to avoid attacks, the client used an account lockout policy, which did not help in preventing cyberattacks or data loss. If an attacker already got the credentials and was able to successfully log in, he could impersonate another domain user, create new admin accounts, or even move from computer to computer within the organization. To resolve this problem, we provided them with a solution on how to quickly respond to critical security incidents and prevent further damage to their business. We performed follow-up reviews of their infrastructure for remote desktops and re-evaluated their security risks based on the last security incident.

Based on our input and the solution we provided; our client changed their remote access policy and removed all published desktops and apps that were available to users. This limited access to only specific domain users who could not use other methods to access the company's apps and resources. Additionally, the client decided to render the remote desktop functionality obsolete in the following year. This way, we helped our valued business partner minimize critical security risks and improve their cyber security status.

Result

The Comtrade 360 team brought its proven track record and long-lasting expertise in the area of data and cybersecurity.

Our client was able to focus on its primary role and operating activities once again, while having a 24/7 backup system with the support of our cyber security team. Our experts can investigate and resolve around 70% of the incoming security events and incidents on their own.

The impact on the IT team is kept on the minimum. All issues which require intervention follow adapted security risk analysis and simple review-and-approve improvement implementation process from both sides. They are also provided with constant objective feedback on the security posture they are aiming for.

Our business partner's Security ScoreCard improved from 68% to 97% in one-year time due to high involvement of both business partners. Our cooperation and quick implementation of best practices into operations has had a great impact on improving the company's Cyber Security Resilience.

Comtrade
Three-Sixty

info@comtrade360.com
+38681605200
comtrade360.com