SecureOps
Case Study

CoPilot™ Vulnerability Management, Analysis and Response

Developing a Risk-Based Vulnerability Management Program Leveraging a Tailored Service Methodology

Custom Security Solutions Empower Organizations to Create Robust, Efficient Vulnerability Management Programs

Introduction

Vulnerability management exists for the purpose of identifying and remediating vulnerabilities in systems quickly before they are exploited. Vulnerabilities are essentially weaknesses within software that can leave a system or network exposed to attacks. These vulnerabilities must be identified, assessed, and patched regularly to ensure ongoing security. In order to create and maintain a strong security posture, business owners and security officers must be keenly aware of the vulnerabilities on their systems, as well as the process by which they can be prioritized and remediated. If vulnerabilities are not kept under control, companies leave themselves open to preventable attacks.

The remediation gap between when organizations first detect vulnerabilities and when those issues are ultimately resolved is often longer than needed, which gives hackers the opportunity to breach systems and organizations. An Adaptiva survey found that companies overwhelmingly do not have adequate staff to manage the number of vulnerabilities. Leveraging current vulnerability management tools and their integration with other cybersecurity and IT management applications is a significant cybersecurity challenge. Further, in a study by the Ponemon Institute, 57% of cyberattack victims stated that applying a patch would have prevented the attack and 34% say they knew about the vulnerability before the attack.

Canada
Address: 1550 Metcalfe Street, Suite 502
Montréal, Québec, Canada H3A 1X6
Tel: 1.888.982.0678
Fax: 1.514.982.0362

Czech Republic
Address: Meteor Office Park, Sokolovská 100/94, 186 00 Praha 8, Czech Republic
Tel: 1.888.982.0678
Fax: 1.514.982.0362

The Challenge

Our client needed security engineers and other security staff to upgrade their vulnerability management program. The state of the program was leaving the client exposed to attacks and had fallen significantly behind industry standards. However, finding a cost-effective solution by either leveraging local expertise or traditional managed service solutions were not viable options due to the organization's need for diverse security expertise, internal control and visibility to the program and partner flexibility.

The Majority of Security Solution Providers Lack the Flexibility and Staff to Provide the Right Experts at the Right Time

The Evolution of a Best Practice Vulnerability Management Program

A vulnerability management process consists of four phases:

- Identification
- Scanning
- Analysis
- Remediation

Our client was struggling with a lack of security resources, a fragmented scanning and remediation strategy and an inefficient reporting and compliance processes. Their staff was overwhelmed and had lost faith in the process, tools and the asset owners who failed to remediate the vulnerabilities that were uncovered. In addition, the organization:

- Scanned less than 50% of the assets each quarter
- Had to manage a high false positive rate of vulnerabilities due to poor scanner configuration
- Had to conduct ad-hoc scans in order to plug security gaps between quarterly scans
- Had to manually prepare reports resulting in time-consuming data collection
- Had to manage a scan exclusion and exception list that was large and growing
- Could only scan 30,000 IP addresses monthly leaving many assets with critical vulnerabilities

Tailored security solutions like CoPilot™ is a means to enable employees, partners, and suppliers to work productively, seamlessly, and securely together

Canada
Address: 1550 Metcalfe Street, Suite 502
Montréal, Québec, Canada H3A 1X6
Tel: 1.888.982.0678
Fax: 1.514.982.0362

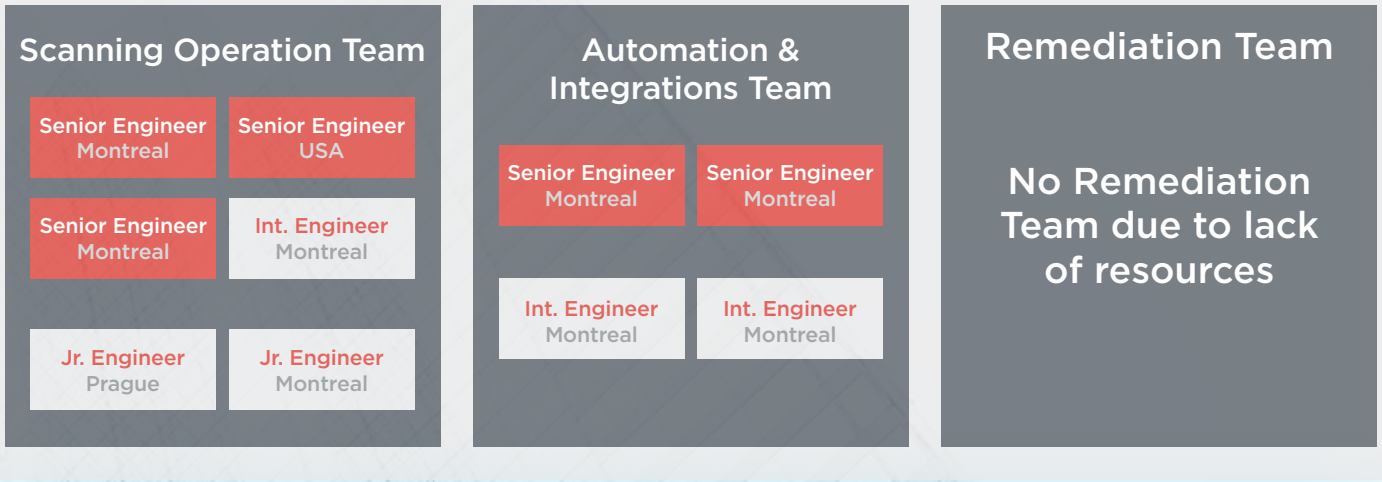
Czech Republic
Address: Meteor Office Park, Sokolovská
100/94, 186 00 Praha 8, Czech Republic
Tel: 1.888.982.0678
Fax: 1.514.982.0362

secure OPS

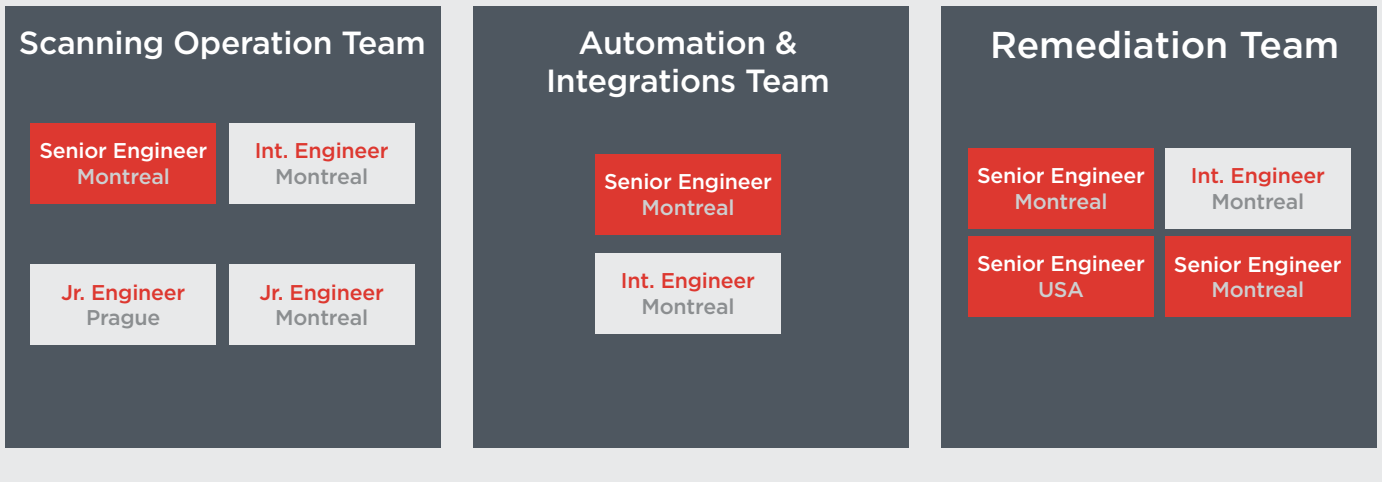
The Evolution of Vulnerability Management Processes

CoPilot™ Allows Organizations to Focus On Higher Level Vulnerability Management Processes

PHASE ONE



PHASE TWO



Key Learning

As organizations move up the security maturity curve, the number of hours they spend on vulnerability scanning, assessments, patching & management decreases. Rather than scanning and patching an entire environment with thousands of systems monthly, risk-based vulnerability management prioritizes high value systems with a higher level of focus and activity than lower value systems, thus fewer scans and patches.

The vast majority of an organization's systems are often of lower value and are not the primary targets for attack yet without a risk-based vulnerability management program they consume the majority of the security team's time and effort.

The benefit of our model is fewer resources are required to execute the vulnerability management process. Further, they can focus on higher-level responsibilities like remediation, helping threat and incident response teams, assessing asset and vulnerability scoring, and evaluating the overall security and business risk level of the organization.

CoPilot's™ Collaborating Model Delivers Customized Expertise, Support and Personnel

SecureOps' CoPilot™ is a customer-driven solution providing a high-level, diverse, flexible team of experts at the right time with the right skills. Our goal was to provide our client the resources they needed to deploy reliable scanning technology, scan their entire environment, and automate their vulnerability management process by prioritizing assets, vulnerabilities, scanning and remediation.

Partnering with our client's IT security team, SecureOps' CoPilot™ empowered the organization to bolster their vulnerability management program by providing:

- A holistic review of their vulnerability management program, requirements, and objectives with recommendations.
- Implementation of a clear, concise vulnerability management strategy geared to bolster overall security maturity.
- The integration of the client's scanning tool's with CMDB platforms and ITSM standards.
- The handling of all scanning operations to ensure a smooth transition with no adverse effect or loss of current stable state service.
- A large "Discovery Scan" effort to identify areas of the network that had a large number of unmanaged assets, which resulted in improving the accuracy of data in the CMDB.
- Deployment of new scanners and agents into areas that were unreachable before or where the scans were causing network/firewall issues.
- Reconfiguration and breaking down of the large scheduled scans into multiple smaller scans to allow custom scanner selection, configuration, policies, frequency, and reporting requirements.
- Creation of a vulnerability remediation and rapid-response team.

Improving security maturity requires unique, high-level IT security skills delivered by a range of experts. Traditional staff augmentation does not address the evolving needs of our clients

Vulnerability Management Lifecycle

Delivering a Maximum Return on Investment and Improved Security with CoPilot™

The benefit of SecureOps' CoPilot™ to our client was the ability to transition from a fragmented, whack-a-mole vulnerability assessment and patching exercise to a comprehensive, prioritized, proactive strategy. The real value was improving the organization's overall security maturity by having a partner with the specialized experts to implement a best in class vulnerability management program.

SecureOps' CoPilot™ enhanced our client's vulnerability management program by providing measurable results including:

- Risk-based vulnerability management processes were implemented resulting in the evolution of the security program - the high number of resources that were tasked with running basic operations have evolved or been replaced to now perform higher value functions such as helping asset owners with remediation, supporting Threat and Incident Response teams, and performing additional automation and the optimization of processes.
- On-demand, costly, inefficient scans are no longer needed.
- The backlog of scans, patching and remediation was eliminated; vulnerability management is now conducted in near real-time.
- High criticality assets are typically scanned by priority on a daily or weekly basis rather than quarterly.
- Over 40 scheduled scan types are being run across more than 95% of the assets providing more information about system vulnerabilities sooner.
- Scoping and reporting are integrated with ITSM and CMDB, dashboards show a much clearer picture of the vulnerability landscape across the organization.
- Total number of IP scan/rescan monthly: 1,500,000.

Prioritizing systems, applications, vulnerabilities by CVSS score, testing patches, and consolidating software versions across an IT environment requires discipline strategies and processes

SecureOps CoPilot™
Our Collaborative Approach

Together, we will assess your staffing, coverage, and integration needs to accomplish your security goals. You will have a dedicated team whether they are full-time, or partial resources. The team will work inside your current workflows and tools and suggest changes that improve security, reduce costs and boost efficiency.

Canada
Address: 1550 Metcalfe Street, Suite 502
Montréal, Québec, Canada H3A 1X6
Tel: 1.888.982.0678
Fax: 1.514.982.0362

Czech Republic
Address: Meteor Office Park, Sokolovská
100/94, 186 00 Praha 8, Czech Republic
Tel: 1.888.982.0678
Fax: 1.514.982.0362

secure OPS