

CASE STUDY: Secutor's Signature Vulnerability Management system - Gold



INTRODUCTION

Secutor's Signature Vulnerability Management (SSVM) system is a holistic, risk-based approach to Vulnerability Management that places emphasis on using network security architecture in combination with the award-winning QualysGuard platform to identify critical attack vectors and prioritize vulnerability remediation. We help our clients find the "needle in a haystack": the risks and vulnerabilities that offer malicious entities the path of least resistance into their secured network.

In combination with GRC for Risk Analysis, Compliance Assessment, and Incident Management, SSVM is a comprehensive solution that serves as a solid foundation upon which a successful cybersecurity can be built.

SITUATION

A leading provider of enterprise-scale robotic process automation with development teams and customers around the globe has cybersecurity as a top concern for the executive management.

They were nearing the completion of two massive projects, a migration into the Azure cloud and HITRUST certification, and their CTO wanted an independent review of their network security architecture and to have their QualysGuard deployment optimized.

CHALLENGES

Secutor reviewed and rapidly identified their most pressing challenges, which included:

- QualysGuard, which was setup many years ago was not providing full product value or the information to protect their company and customers
- Reports and metrics had not been standardized, and they were using individual scan results rather than the more powerful "Host Based" database
- Authentication was not enabled, so the vulnerability scan results were limited and they were not taking advantage of QualysGuard's built-in "Agent-less Host Tracking" features
- They were critically short-handed on staff with the time and knowledge to implement a Vulnerability Management program
- Only the most critical systems were being scanned thus leaving out significant elements of the network where malicious activity could take hold for further invasion into the enterprise's infrastructure
- Lack of metrics and KPIs to track progress



Secutor Consulting LLC
Email: info@secutoris.com
Phone: 682-312-3990

SERVICES PROVIDED

Secutor Cybersecurity experts collaborated with the customer's Security team to provide the following services:

1. **Gap Analysis** – Reviewed the existing security policies and procedures to identify areas for improvement or refinement
2. **Network Security Architecture Audit** – Analyzed all layer 3 network devices to build a complete picture of all possible access vectors in to, out of, and within the network
3. **Continuous Vulnerability Management** – Designed and implemented a comprehensive solution around Qualys where scans, ticketing, and reports were optimized and automated
4. **Vulnerability Prioritization** – Merged the network security architecture audit with Qualys scans to identify the highest priority vulnerabilities: those that are exposed to threat sources
5. **Metrics** – Identified usable and understandable metrics that were the most important to the customer and automated them, for the CTO and his team to have continuously updated action items
6. **GRC** - Drafted Vulnerability Management and Remediation policies and procedures
7. **Training** - Provided knowledge transfer to ensure a smooth transition of the new systems and processes to the customer's staff

Follow Us

Website: www.secutoris.com

LinkedIn: www.linkedin.com/company/secutor-consulting

Twitter: [@Secutoris](https://twitter.com/Secutoris)



SUMMARY

Secutor helped this customer:

- Identify all 5,000 internal IPs, answering the question: **“Am I scanning everything with Qualys?”**
- Obtain a continuously updated asset and software inventory of all 250 networked devices, answering the question: **“What do I need to protect?”**
- Focus on the most dangerous 10 vulnerabilities out of the 2,000 “high priority” vulnerabilities that Qualys identified, answering the question: **“What do I need to fix first?”**
- Track improvements in security, answering the question: **“Is everyone rowing in the same direction?”**

About Secutor

Secutor Consulting is a trusted partner comprised of industry leading experts in the fields of Cybersecurity, Governance, Risk and Compliance. We partner with our clients to deliver on-demand solutions tailored to expertly navigate the regulatory demands of their specific industries.

Our proven track record of successfully exceeding client expectations is achieved through the combination of our methodical approach, advanced technologies, subject matter experts, and synergy with client team members.

Secutor is your team of world-class problem solvers with vast expertise and experience delivering complete solutions keeping your organization protected, audit-ready, and running smoothly.

Secutor Consulting LLC

Email: info@secutoris.com

Phone: 682-312-3990