

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



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

One of the largest public transit authorities in the United States, serving almost 6 million people with nearly 5000 employees, has a very large legacy network with sporadic documentation that the new IT Security Manager needed to get under control so that he could modernize their cybersecurity protections. He chose QualysGuard to obtain the visibility needed to rapidly reach his goals. But he quickly discovered that despite how easy Qualys is to manage and maintain, his team didn't have the required skills to get Qualys deployed on time and in the most optimal configuration for his needs. They had accomplished a partial deployment but weren't using Qualys to its full potential.

CHALLENGES

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

- They didn't have the information needed from the networking team to scan all available IPs
- Vulnerability scans weren't properly scheduled, with a standardized Option Profile
- Reports and metrics weren't standardized, and they were using individual scan results rather than the powerful "Host Based" database
- Authentication wasn't enabled, so the vulnerability scan results were limited and they weren't taking advantage of QualysGuard's built-in "Agent-less Host Tracking" features
- They were struggling with assigning vulnerabilities to individuals and teams for remediation
- Lack of defined metrics and KPIs to track progress
- Lack of effective communication between the network, IT, and security teams



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 Analysis** – Reviewed subnet information provided by the networking team to determine the optimal scanning coverage and schedule
3. **Continuous Vulnerability Management** – Designed and implemented a comprehensive solution around Qualys where scans, ticketing, and reports were optimized and automated
4. **Vulnerability Prioritization and Metrics** – Identified usable and understandable metrics that were the most important to the customer and automated them, for the security and remediation teams to have continuously updated action items
5. **GRC** - Drafted Vulnerability Management and Remediation policies and procedures
6. **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 3,000,000 internal IPs, answering the question: **“Am I scanning everything with Qualys?”**
- Obtain a continuously updated asset and software inventory of all 7000 networked devices, answering the question: **“What do I need to protect?”**
- Focus on the most important 150 assets out of the 72,000 “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