MANAGED SERVICE BRIEF:

Secutor Signature Vulnerability Management

INTRODUCTION

The Secutor Signature Vulnerability Management (SSVM) service 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.

Over 10,000 companies use QualysGuard solutions to transform their asset and vulnerability data into answers that power their security programs. **Provided as a service managed by our top security experts**, SSVM is a comprehensive solution leveraging QualysGuard, Lumeta Spectre, RedSeal, Sentinel IPS, Digital Shadows, and Comodo to serve as a solid foundation upon which a successful cybersecurity program can be built.

CHALLENGES

Your network is expanding. Not only in the traditional sense, but also with the ever increasing role of endpoints, servers, and the Internet of Things. Each year the amount of data multiplies exponentially, the attacks become more sophisticated, and the challenge of minimizing risk while optimizing operations grows more challenging. It's a never-ending battle; and identifying, prioritizing, and managing vulnerabilities all the way thru remediation isn't simple… *but it doesn't have to be hard*.

SERVICE

You're strapped for time and resources, but need to prioritize risk. SSVM provides industry-leading scanning technologies, people, and processes that enable you to identify attacker's targets of opportunity and fix the vulnerabilities at the source. This combination equips you to focus on your broader security strategy without growing your organization. We manage your scan operations to provide actionable, tailored recommendations to prioritize risk mitigation within your environment. We help your team to digest the reports and plan next steps.

Secutor's team of IT and cybersecurity experts run your program for you, leveraging best practices from years of industry immersion and thousands of scans. They leverage threat intelligence from across various verticals to anticipate vulnerabilities even faster, to keep your environment safer.

> *"Secutor provided insight to the Security Architecture of our network which let me stay focused on providing great service to our users while improving our overall Security posture."* - **Richard Eaton, IT Support Manager, Botanical Research Institute of Texas**

ADDITIONAL SERVICES

SSVM is powered by Qualys technology, and includes additional techniques and services that allow you to identify weak points, prioritize what matters most, and improve your security posture. Our resident experts utilize threat intelligence to have the most up-to-date threat data, which helps them to better advise how to prioritize and remediate. This technology is the backbone of our Managed VM offering. We also offer other services which are fully integrated with Qualys to provide a cohesive solution.

- **Real-time Infrastructure Visibility and Network Change Monitoring** - Powered by Lumeta Spectre, Secutor identifies infrastructure blind spots; sees every network and endpoint add/drop or path change; uncovers unauthorized movement, segmentation violations, and leak paths; and detects unauthorized flows, command and control activity, and other attack vectors common to advanced attacks.

SECUTOR

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

ADDITIONAL SERVICES (continued)

- **Network Security Architecture Analysis** - Powered by RedSeal, Secutor analyzes all of your network devices to build a complete picture of all possible access vectors in to, out of, and within your network. We use this map to identify and prioritize all vulnerabilities that are exposed to a threat source, whether that's the internet, partner networks, or even your guest wireless.

- **Web Application Scanning** - On the internet or under development, SSVM's dynamic deep application scanning covers all of your apps, giving instant visibility of vulnerabilities like SQLi and XSS. With programmatic scanning of SOAP and REST API services, SSVM also tests IoT services and APIs used by mobile apps and modern mobile architectures. While scanning your websites, SSVM can identify and report infections, including zero-day threats via behavioral analysis.

- **Indicators of Activity and Compromise** - SSVM uses non-intrusive data collection and delta processing techniques to transparently capture endpoint activity information from assets on and off the network. Threat hunting and suspicious activity detection is performed on billions of active and past system events, coupled with threat intelligence data to identify malware infections and threat actor actions.

- **Asset Inventory** - SSVM identifies every live host on the network, providing a complete, multidimensional view of each asset to your CMDB to enable better ownership tracking and reporting.

- **Patch Management** - Keeping application software and Operating Systems up-to-date with the most recent security patches protects your company from malware and ransomware attacks. Patch and Configuration Management reduces the risk of having a security breach and all of the related problems that come with it, like data theft, data loss, PII and PHI violations, reputation issues, or even legal penalties. Secutor experts can help you eliminate the vulnerabilities that attackers use to exploit your users and work their way to your crucial data. We'll work together with your IT team and service owners to identify the most critical vulnerabilities, and develop and execute a remediation plan for you.

- **Intrusion Prevention System** - Powered by Sentinel IPS, Secutor provides management and monitoring with CINS active threat intelligence. IDS/IPS are very effective tools for identifying and mitigating a wide variety of attacks, from basic scans and probes to trojans and malware infections. But traditional IPS devices are difficult at best to manage and maintain: keeping up with the latest signature sets, updating software, monitoring devices, and managing false positives can be overwhelming. We manage all of that for you, 24/7. In the rare cases where it's an issue, we work with you to mitigate the false positives and make sure they don't happen again.

- **Cyber Threat Intelligence** - Powered by Digital Shadows, Secutor enables organizations to manage digital risk by identifying and eliminating threats to their business and brand. We monitor for digital risk across the broadest range of data sources within the open, deep, and dark web to deliver tailored threat intelligence, context, and actionable remediation options that enable security teams to be more effective and efficient. You can focus on growing your business knowing that you're protected if your data is exposed, employees or third parties put you at risk, or your brand is being misused.

About Secutor

Secutor Consulting is a trusted partner comprised of industry leading experts in the fields of Cybersecurity and 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.

Follow Us
Website: www.secutoris.com
LinkedIn: www.linkedin.com/company/secutor-consulting
Twitter: @Secutoris

SECUTOR