SMX CyberHunter

Advanced, Rapid Response Solution for Next-Gen Threats

Overview

CyberHunter® is a managed hunting platform purpose built to detect cyber intrusion attempts with full-time Analysts and Investigators dedicated to pro-actively hunting for adversary activity in your environment 24x7x365. CyberHunter hunts for signs of attack and automatically alerts when it identifies malware or malicious activity. CyberHunter monitors for subtle signs of adversary actions, including those that reside only in memory, never being written to disk and eluding traditional end point malware protections.

Common Challenges in Today's Cyber World

The Game Changes Daily

Adversary offensive capabilities have far out-paced defender's capabilities, both in terms of depth-of-reach into compromised systems and breadth-of-systems targeted. Defenders have a significant gap between what the adversary is doing and what the defenders are able to detect or observe. This allows the adversary to hide in your environment, mimicking authorized traffic and blending in with benign activity.

This game changes daily, yet most defensive approaches and toolsets have stayed the same. Stealthy attacks (e.g., in memory malware) are not able to be seen using common analysis tools or traditional commercial security software. This makes it increasingly difficult for System Administrators and Security Analysts to determine if an instance has malware present or if it has been compromised. Performed manually, live system triage is very time consuming, requires specialty knowledge, and is prone to error. Common methods of triage look for known indicators of compromise, which by definition lag behind current threats and often miss the most concerning attacks.

The CyberHunter Solution

An Automated Hunt Capability with Seasoned Analysts

SMX developed CyberHunter as a multi-tenant rapid-scan capability for performing non-service impacting live system triage and compromise assessments. Our innovative detection techniques were developed based on our years of defending high-value environments from the most sophisticated threat actors. We merged our unique memory analysis methods and knowledge of other key points in system analysis to develop this intelligent platform that applies adversary behavior; machine/code learning; and proprietary, multi-faceted security analytics for the collection and triage of systems.

24x7x365

Proactively Hunting Adversary Activity in Your Environment

Our Partnerships

Google Cloud Partner

Gold Microsoft Partner

Azure Expert MSP

aws PARTNER Premier Tier Services

The CyberHunter Solution

A Hidden, Stealth-Like Capability

CyberHunter is designed to avoid detection with no obvious agent to disable, providing a hidden or stealth-like capability for our customers. Together, CyberHunter and our experienced Analysts provide customers the assurance that their environment is threat free of malicious code.

Highlights

- Triage with seasoned Analyst confirmation
- Advanced code injection detection
- Circumvention resistant
- Agentless with low visibility
- APIs for integration with your current processes and systems
- DevOps oriented with continuous improvement

Why a Managed Hunting Service is Essential

Improves Efficiency and Provides Critical Overwatch Support

Across the globe, seasoned security professionals are in high demand but very limited supply, so an advanced hunting service like CyberHunter is essential. Our experienced, proven hunters operate a custom-built platform that provides all the data needed to make analytical decisions using proven analytical processes. The CyberHunter Team maintains situational awareness on threat actor changes using several highly effective techniques. Many repetitive steps that are typically performed manually by today's defenders have been automated in CyberHunter with the results presented to experienced Analysts. This greatly improves an Analyst's efficiency, keeps them focused on doing the most difficult components of hunting, and provides critical 'overwatch' support that gives a higher level of assurance that bad actors are not attempting to operate in your environment.

Why SMX?

Cybersecurity, a Cornerstone of Our Capabilities

SMX has been providing top-level information technology, engineering, and cyber security for DoD, U.S. Government, and commercial customers for more than 25 years, placing our team at the leading edge of offensive and defensive cyber operations. Cyber security has been the cornerstone of our capabilities since we first began supporting one of our nation's most critical enterprise networks more than two decades ago. While defending these large-scale networks from adversary threats, we have gained valuable insight into the challenges of defensive operations.

This enables our CyberHunter Team to provide unique, innovative methods to counter adversary threats. When we observed the evolution of the adversary's methods and compare them to available defensive approaches, we became increasingly concerned at the growing gap between the attackers and defenders. This increased concern led SMX to create CyberHunter, a unique capability to help close the defensive gap on malicious intrusions.

For more information, please contact: solutions@smxtech.com

SMX harnesses the transformative power of technology to achieve mission success as a leader in digital and mission solutions, specializing in secure and advanced cloud, ISR, cyber, data analytics, engineering, space, and IT solutions. Operating in close proximity to our clients across the globe, the SMX team has a shared vision to deliver scalable and secure solutions to assure outcomes for the critical missions of our Government and commercial clients.

Learn more about our current contracting vehicles: www.smxtech.com/contracting-vehicles