Secureworks

DATA SHEET

Advanced Malware Protection and Detection

Managed Network Sandbox Detects and Rapidly Analyzes Evasive and Advanced Threats

Increasingly sophisticated malware and targeted attacks are designed to evade traditional signature-based protections and some next-generation security technologies. Even if you have skilled security resources who understand these advanced and emerging threats, your organization might be subject to elevated risk if you can't keep up with alerts from an increasing number of security tools.

Combatting Advanced and Emerging Threats

Security teams are increasingly aware of the risk posed by advanced threat actors bypassing existing security controls via phishing, fileless malware and constantly evolving ransomware variants. Targeted threats often evade your security by leveraging legitimate tools like PowerShell and Windows Management Instrumentation (WMI). Even the most advanced threat detection and prevention tools require skilled staff with the time to evaluate the output and determine which alerts require attention and which can be safely ignored. You can reduce the risk to your organization with a security strategy that includes an advanced network sandbox with 24x7 monitoring, so your security team can focus on more strategic business initiatives.

How Secureworks Helps

Advanced Malware Protection and Detection is a fully managed service that provides an elite layer of defense against evasive, targeted, and emerging threats designed to bypass your traditional security controls and compromise your organization. Our experienced security analysts combine Secureworks Threat Intelligence with Deep Content Inspection™ network sandbox technology to help you see, rapidly analyze and accurately diagnose advanced threats. Detonation of suspicious files and URLs clarifies the intent of the attack, while the Secureworks Senior Intrusion Analyst (SIA) team adds context and guidance to expedite your response and remediation efforts.

Client Benefits

- Accelerate time to protection and reduce TCO with a fully managed service
- Identify threats in email and web traffic not easily identified with other security tools
- Detonate suspicious content to understand the true intent of potential threats
- Thwart typical sandbox evasion techniques with Deep Content Inspection
- Focus on actionable events and reduce time spent investigating false positives
- Detect new and emerging threats faster and with more accuracy

Solution Features

- Automated collection and detonation of suspicious content
- Dynamic analysis in next-generation network sandbox shows exactly what the file would do on your endpoints
- Deep Content Inspection

How AMPD Works

- Lightweight appliances on your network inspect email and web traffic
- Appliances send suspicious traffic and files to Managers and Engines, in your network or in the cloud, for detonation and analysis
- Telemetry is processed by The Secureworks Counter Threat Platform™ (CTP) to identify more indicators of compromise
- Upon detection of compromise patterns, the system sends an immediate alert to the Secureworks Security Operations Center (SOC) containing details about the severity, scope, and impact of the compromise event
- The SIA team deconstructs the event detail and applies our Threat Intelligence to provide more context
- While all events are ticketed with details about severity and scope, critical events are escalated to you immediately with data about threat actor, intent of the attack, and likely target

Avoiding Sandbox Evasion

Advanced and emerging attacks, including fileless threats, can be a challenge to identify with traditional security tools. Advanced threat actors are well-versed in sandbox detection and often design attacks to evade this technology. Malware and targeted attacks may be crafted to look for indicators of a sandbox environment and then stop activity that could reveal malicious intent. To avoid being analyzed, malware can be designed to wait for a reboot or an end user action, or sleep timers can be inserted to trick the sandbox into stopping the investigation before malicious activity begins. Malware may also target specific systems to reduce the chance of detection and increase the chance of a compromise. For example, malware that targets point-of-sale (POS) systems may be smart enough to ignore non-POS systems.

AMPD's network sandbox technology was specifically designed to resemble a real endpoint to reduce the effectiveness of sandbox evasion techniques. Deep Content Inspection simulates the target environment at the physical hardware level, including CPU and memory, to convince the malware that it is running on a real endpoint. AMPD also interacts with malware so detonation is more successful in identifying the intended malicious behavior. As a result, this next-generation network sandbox is more accurate and more difficult to evade.

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that keeps organizations safe in a digitally connected world. We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist. **secureworks.com**

Secureworks®