SecureWorks

DATA SHEET

Security Device & Application Assessments

Security Design & Architecture

The Challenge

Assurance that IT/security devices and applications are resistant to vulnerabilities and operating to their fullest potential can be the difference in detecting and stopping a potential breach. With security devices and applications deployed in critical locations, pinpointing areas of opportunity to enhance configurations, processes, integrity and availability and remediate discovered issues is an opportunity to mitigate risk and maximize investments.

The Solution

SecureWorks Security Device and Application Assessments are a collection of services focused on individual security controls and tools designed to help you identify, enhance and remediate areas of opportunity that may compromise security and performance for better alignment to security objectives and maximize technology investment.

SecureWorks Security Design & Architecture Continuum

Focused on Individual Security Control/Tools	Focused on Enhanced Security Control/Tool Connectivity	Focused on New Optimal Security Control Connectivity Design
Security Device & Application Assessments	**Security Design Assessments**	**Security Design Creation**
• Server, Device & Application Hardening • Health Check/Assessment • Advanced Health Check/Assessment	• Architecture Assessments • Cloud Security Architecture Assessment • Compliance Architecture Assessment (PCI, HIPAA, SCADA, NIST CSF, DSI, NIST 800, o-ESA, SABSA, TOGAF) • Defense in Depth Assessment • Infrastructure Assessment • Web Application Firewall Configuration and Architecture Assessment • Zero Trust Assessment	• Datacenter Re-Build or Migration Design • Growth Architecture Design • Merger & Acquisition Integration Design • Network Segmentation • Secure Remote Access • Vulnerability Scanning Architecture Design

*Not an all-inclusive list

What does it help you answer?	• Are devices and application configurations outdated? • Are device and applications configured to mitigate security risk and enhance performance? • Is the network properly segmented to mitigate risk? • Are the right features turned on, can I get rid of unnecessary features to enhance performance and decrease vulnerabilities? • How do we create an upgrade plan of the device or application that doesn't leave us vulnerable? • How do we seamlessly migrate to another device instead of this one? • Is my logging correct? • How do we trace an attack across this device or application? • How do we optimize this device or application to protect certain assets? • How do we mitigate vulnerabilities that cannot be remediated?
Benefits	• Review and remediation of key security components and applications • Identify and correct device configuration and application issues compromising security and performance • Develops best practice recommendations for solving discovered issues • Brings you up to date with the latest security policies and patches • Devices and applications configured to optimize and enable SIEM/MSS investments

Solutions

Server, Device and Application Hardening

Hardens the configuration of devices, server OSs, and other applications by reducing the risk surface. A checklist of up to 500 items are reviewed against the system or application for security optimization. Many of the assessments align to CIS Benchmarks.

Time: 1 week to complete

Deliverable: A report that shows all the hardening checkpoints that require configuration changes and ranks the findings by severity as well as the effort required to resolve each.

Health Check/Assessment

Reviews a subset of the hardening assessment checklist. The health check contains up to 50 items and is more focused on access control. Detailed reviews of Policies, ACLs, Signatures, VLANs etc. are a major portion of the assessment focus.

Time: 2 days to complete

Deliverable: A report that shows the findings and gives recommendations by rank and severity and the effort required to resolve each.

Advanced Health Check/Assessment

Reviews a subset of the hardening assessment checklist. The advanced health check contains up to 200 items that are reviewed to ensure device or application security optimization. Detailed reviews of Policies, ACLs, Signatures, VLANs etc. are combined with business context to constitute the main focus of this assessment. These assessments align best practices for cyber security combined with extensive industry experience.

Time: 1 week to complete

Deliverable: A report that shows all the hardening checkpoints that require configuration changes and ranks the findings by severity as well as the effort required to resolve each.

Why SecureWorks:

Our Security Consultants

SecureWorks hires only the best and brightest. From our in-depth technical hiring process to our continued investment in our consultants through generous training programs, we seek to find and cultivate security design excellence. Our consultants can be found speaking at industry conferences and releasing cutting-edge security research that becomes industry standard best practices.

SecureWorks Global Threat Intelligence

Threat intelligence is the fuel that powers the engine of the security solutions we provide. With more than 65 of the world's most highly regarded security researchers, SecureWorks' distinguished Counter Threat Platform™ (CTU) research team is what sets us apart. Our researchers analyze threat data across our global client base and actively monitor the cyber threat landscape to provide a globalized view of emerging threats, which provides a basis for the design and architecture decisions we provide.

Proven Methodology

SecureWorks has performed thousands of consulting engagements for a wide array of companies from small business to Fortune 500. Our methodology is based on a combination of our experts' advice and years of experience, SecureWorks' industry leading experience in Global Information Security Services, and grounded in the ISO 27000 standards, the current SANS TOP 20 Critical Security Controls, and a collection of NIST 800 standards. Our methodology is updated on a regular basis to match current industry and attack trends.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com