DATA SHEET

Security Design Assessments

Security Design & Architecture

The Challenge

Security architecture is a cohesive design that addresses the potential risks involved in a certain scenario or environment that threat actors are likely to exploit. Whether motivated by the evolving threat landscape or meeting compliance mandates, identifying gaps in your security infrastructure policies, architecture and controls that put your organization's critical assets at risk is essential. However, having the resources and expertise to objectively assess and prioritize opportunities for improvement is a challenge for most organizations.

The Solution

SecureWorks Security Design Assessments are a collection of services that focus on evaluating the effectiveness of different areas of network infrastructure controls and tools connectivity to protect critical assets. SecureWorks consulting experts utilize industry standard best practices to discover and prioritize opportunities to remediate weaknesses and gaps in technical and operational controls, architecture and configurations that threat actors are likely to exploit. The result is a detailed report identifying the risks associated with topology, protocols, processes and security controls to remediate and improve overall security posture.

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?	• Do I have core security services and controls in place to withstand threats? • How do I evaluate the security architecture of key applications and data? • Does my security architecture meet compliance or framework standards? • Is my Application Architecture optimized for my investments? • Is my WAF Architecture protecting all of my critical applications? • Is my WAS Architecture current to my applications? • Does my Vulnerability management program give me the right data? • Am I remediating findings from vulnerability management scans? • Am I consistently reviewing the data from my vulnerability management scans? • Is that data communicated across all my scanning and vulnerability investments? • Are my Cloud and/or Amazon services architecture secure? • How does my critical, compliance data flow across my network? Am I exposed?
Benefits	• Comprehensive analysis of security controls and architecture • Identifies and prioritizes security architecture risks and the subsequent controls and remediation opportunities • Gain a complete view of security posture, supporting controls and infrastructure • Identifies security architecture design flaws typically discovered after a security breach • Compiles comprehensive security architecture assessment, design guidance, recommendations and mitigation roadmap

Solutions

(not inclusive of all design assessments)

Architecture Assessments

Evaluation of security gaps, misconfigurations and vulnerabilities associated with the existing network and security controls and infrastructure according to industry best practices, security frameworks and compliance alignment.

Time: Depends on the scope and complexity of the environment, minimum of 2 weeks.

Deliverable: A detailed report provides recommendations, priorities, roadmaps and migration plans based on ranking of the findings by severity and effort required to resolve them.

Cloud Architecture Assessment

Determines how best to implement the most effective and appropriate safeguards to protect public, private and hybrid cloud architectures. Consultants will review and perform security controls assessments to ensure best practices are being followed to protect against security and privacy risks and reduce chances of a data breach.

Time: Depends on the scope and complexity of the environment, minimum of 2 weeks.

Deliverable: A detailed report showing assessment of systems, policies and vendors and the resulting recommendations based on ranking of the findings by severity and effort required to resolve them.

Compliance Architecture Assessment

(PCI, HIPAA, SCADA, NIST CSF, DSI, NIST 800, o-ESA, SABSA, TOGAF)

Evaluate, from a technical perspective, the maturity of various components of an enterprise's information security program against compliance requirements. Evaluation consists identification of common security gaps, misconfigurations and vulnerabilities associated with network design and configurations.

Time: Depends on the scope and complexity of the environment, minimum of 2 weeks.

Deliverable: A detailed report delivered shows what configuration and network design changes are recommended in order to help achieve compliance and ranks the findings and recommendations by severity as well as the by effort required to resolve them.

Defense in Depth Assessment

Reviews the layers of technical controls that are in place and providing redundant security measures in case of failure or vulnerability exploit. This assessment provides a holistic approach to the architecture, the security layers, redundancy, and awareness and correlation of the technical controls.

Time: Depends on the scope and complexity of the environment, minimum of 4 weeks.

Deliverable: A detailed report showing assessment of systems, design and policy and the resulting recommendations based on ranking of the findings by severity and effort required to resolve them.

Infrastructure Architecture Assessment

Reviews the business areas your security infrastructure is designed to protect and identifies additional risks and compliance requirements. The assessment conducts an asset inventory of your systems and policies across network and host security, physical security, identity management, data security, wireless and SEIM and provides detailed recommendations based on the findings.

Time: Depends on the scope and complexity of the environment, minimum of 3 weeks.

Deliverable: A detailed report showing assessment of systems, design and policy and the resulting recommendations based on ranking of the findings by severity and effort required to resolve them.

Web Application Firewall Configuration and Architecture Assessment

Reviews the configuration and placement of your WAF devices and the applications they protect. In a risk based approach, understanding the business purpose and criticality of each application is the first step and enhancements to the architecture will be based on the findings.

Time: Depends on the scope and complexity of the environment, minimum of 2 weeks.

Deliverable: A detailed report that shows what program and configuration changes are recommended and ranks the findings and recommendations by severity as well as the by effort required to resolve them.

Zero Trust Assessment

Review of the technical controls and configurations of the architecture to achieve this security strategy. A comprehensive review of security zones, encryption and authentication controls and other security controls against the principles of zero trust.

Time: Depends on the scope and complexity of the environment, minimum of 3 weeks.

Deliverable: A detailed report showing assessment of systems, design and policy and the resulting recommendations based on ranking of the findings by severity and effort required to resolve them.

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

SecureWorks®