HOPF
PARTNER | SOLUTIONS | COMPONENTS

THE CIS CRITICAL SECURITY CONTROLS AND TRIPWIRE SOLUTIONS

◆ Tripwire solutions capture activity data from monitored assets in order to meet foundational security controls—regardless of your preferred framework. No matter if you rely on physical, virtual or cloud-based IT infrastructure, Tripwire provides centrally-managed controls and information you need to protect your sensitive data and evaluate risk. ◆

Many organizations face the challenging threat environment by strategically choosing a security controls framework as a reference for initiating, implementing, measuring, and evaluating their security posture, as well as managing risk. While many frameworks are available, three of the most notable and commonly used are

- CIS Critical Security Controls (The Controls, 20 CSC)
- NIST Special Publication (SP) 800-53
- ISO/IEC 27002

These well-known frameworks all share the common goal of offering combined knowledge and proven guidance for protecting confidentiality, integrity, and availability of critical assets, infrastructure, and information. Security controls themselves are technical safeguards and operational procedures that strengthen defenses against threats. They typically involve the triad of technology, people, and process and when implemented and automated.

One of the main reasons organizations put off choosing a security controls framework is the fear that it may be too large an undertaking and won't get completed. However, security is a job that's never done, and getting started is essential. If you're serious about improving your organization's security, you should have a strategic plan, a framework and a set of security controls against which you can measure and evaluate your progress.

Tripwire provides solutions that align with each of the following (and additional) security control frameworks. Tripwire can accelerate your organization's efforts to evaluate risk, improve security, and achieve immediate short-term wins and long-term confidence.

THREE IMPORTANT SECURITY CONTROL FRAMEWORKS

The following are the most prominent and workable security control frameworks. They have natural overlap with some of the specified controls, and closely align to each other. They are considered living documents and are regularly updated by their parent organizations as threats, technology, best practices and attack scenarios evolve.

CIS CONTROLS OVERVIEW

The CIS Critical Security Controls (CIS Controls) reflect the combined knowledge of actual attacks and effective defenses as well as exclusive and deep knowledge about current threats by a broad range of industry experts. The Controls are a foundational reference and starting point for any organization.

BACKGROUND

- A prioritized, agreed-upon set of "most critical controls," heavily imformed/drawn from by NIST SP 800-53
- Developed by a consortium of information security experts
- Customizable and applicable regardless of organization size, type (government or commercial), maturity level, likely threat vectors, or technologies in use
- Recommended for use by Verizon's Data Breach Investigations Report to address the majority of breaches they investigated
- Provides detailed guidance to prioritize implementation and customize your security controls as well as sequence, test, and achieve continuous automation

NIST SP 800-53 OVERVIEW

The National Institute of Standards and Technology (NIST), is a measurements and standards laboratory. It functions as a unit of the the Department of U.S. Commerce, its 27000-series guidelines relate to internet security and legislative requirements. The Federal Information Security Management Act of 2002 (FISMA) works with NIST to set standards and requirements for federal information systems, enforceable by the Secretary of Commerce.

BACKGROUND

- Guideline minimums, and legislative requirements for information security in federal organizations, though usable by the private sector
- Researched by NIST's Information Technology Laboratory (ITL) and findings collaborated upon by broad range of industry experts
- Federal Information Processing Standards (FIPS) testing and compliance are also granted by NIST/ITL
- Compliance with NIST guidelines are set and enforced by the Office of Measures and Budget (OMB)

ISO/IEC 27002 OVERVIEW

The ISO/IEC 27002 standard is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The 27000-series standards are dedicated to best practice recommendations for helping organizations preserve the confidentiality, integrity, and availability of information security management systems and processes.

BACKGROUND

- A guide for information security management systems (ISMS) processes, and controls, not a granular specification for detailed implementation
- International participation and acceptance with national equivalents in over 23 countries worldwide
- Includes 11 areas, with specifying controls, objectives, implementation guidance, and other information
- Security controls align and map reasonably with both the CIS Controls and NIST SP 800-53

Regardless of your starting point, or which framework may be suited to your organization's security challenges, there's a lot of implementation flexibility. Tripwire solutions enable faster adoption of your chosen security framework as they meet key criteria, multiple controls, continuous monitoring automation, and the evolving threat environment.

> ***"If I had to pick one, it would be Critical Control 3, configuration management. If you have a secure configuration in hardening and locking down services and ports and software, you're really going to get the best payoff."***
>
> **ERIC COLE, FOUNDER AND CHIEF SCIENTIST, SECURE ANCHOR**

ACCELERATE SECURITY MANAGEMENT WITH THE CIS CRITICAL SECURITY CONTROLS

Security control frameworks give freely researched and broadly validated guidelines for protecting confidentiality, integrity, and availability of critical assets, infrastructure, and information.

Tripwire knows that some of the biggest security gains against the most common threat vectors can be simply and inexpensively achieved by starting with the foundational controls, as documented in the CIS Controls framework. Implementing Controls 1 through 4 assures that you know your network assets and what's on them (e.g. hardware, software, configurations, locations, etc), and that their configurations are in a secure, hardened state regularly scanned for vulnerabilities, policy compliance and other weaknesses. And finally, that as they are discovered, issues are remediated. Getting started is the most important step, and the CIS Controls apply to nearly any enterprise.

TRIPWIRE SOLUTION SUPPORT FOR THE CIS CRITICAL SECURITY CONTROLS

	Critical Security Control	Overall Tripwire Solution Support	Tripwire Enterprise & Tripwire CCM	Tripwire IP360 & Tripwire PureCloud	Tripwire Log Center *Log data supports this control
Highest impact controls	**CSC1:** Inventory of Authorized and Unauthorized Devices	●	●	●	*
	CSC2: Inventory of Authorized and Unauthorized Software	●	●	●	*
	CSC3: Secure Configurations for Hardware and Software	●	●	◔	*
	CSC4: Continuous Vulnerability Assessment and Remediation	●	◕	●	◕
	CSC5: Controlled Use of Administrative Privileges	◕	◕		◑
	CSC6: Maintenance, Monitoring, and Analysis of Audit Logs	●	◔		●
	CSC7: Email and Web Browser Protections	◔	◔	◔	◔
	CSC8: Malware Defenses	◔	◔		◔
	CSC9: Limitation and Control of Network Ports	●	◑	◕	◔
	CSC10: Data Recovery Capability	◔			*
	CSC11: Secure Configurations for Network Devices	●	●	◔	*
	CSC12: Boundary Defense	◔			◔
	CSC13: Data Protection				*
	CSC14: Controlled Access Based on the Need to Know				*
	CSC15: Wireless Access Control	◔	◔	◔	*
	CSC16: Account Monitoring and Control	◑	◑		◑
	CSC17: Security Skills Assessment and Appropriate Training to Fill Gaps				*
	CSC18: Application Software Security	◑	◑	◑	*
	CSC19: Incident Response and Management				*
	CSC20: Penetration Tests and Red Team Exercises				

For detailed information on sub-controls, read the *Tripwire Solutions and the CIS CSC Detailed Mapping* brief

TRIPWIRE'S SOLUTIONS FOR ATTACK MITIGATION

ADVERSARY ACTIONS TO ATTACK A NETWORK

RECONNAISSANCE	GET IN	STAY IN	EXPLOIT
CSC1: Hardware Inventory	**CSC3:** Secure Hardware & Software Configs	**CSC5:** Administrative Privileges	**CSC10:** Data Recovery Capability
CSC2: Software Inventory	**CSC7:** Email and Web Browser Protections	**CSC6:** Audit Logs	**CSC13:** Data Protection
CSC4: Continuous Vulnerability Assessment and Remediation	**CSC8:** Malware Defenses	**CSC12:** Boundary Defense	**CSC17:** Security Skills Assessment and Appropriate Training to Fill Gaps
CSC20: Penetration Tests and Red Team Exercises	**CSC9:** Limitation and Control of Network Ports	**CSC14:** Controlled Access Based on the Need to Know	**CSC19:** Incident Response and Management
	CSC11: Secure Configurations for Network Devices	**CSC16:** Account Monitoring and Control	
	CSC15: Wireless Access Control	**CSC20:** Penetration Tests and Red Team Exercises	
	CSC18: Application Software Security		

STOP ATTACKS EARLY STOP MANY ATTACKS MITIGATE IMPACT OF ATTACKS

TRIPWIRE® ENTERPRISE

Tripwire Enterprise delivers best-in-class security, integrity monitoring, and configuration & compliance management with a plugable, extensible and high-performance endpoint data collection & communication platform—Tripwire Axon™. Tripwire customers benefit from unparalleled visibility and cyber-resilience while reducing operational burden and improving responsiveness.

TRIPWIRE® CCM

Tripwire Configuration Compliance Manager (CCM) delivers innovative agentless compliance and security audit that has proven to be light touch on most enterprise infrastructure and quickly provides value and insight through a risk-prioritized view of enterprise compliance and security posture.

TRIPWIRE® IP360

Tripwire® IP360™ is a vulnerability management solution that enables reduction of risk by focusing attention on the most critical threats and vulnerabilities. Tripwire IP360 provides complete network visibility including inventory of networked devices, applications and vulnerabilities. The solution includes the most comprehensive vulnerability scoring and endpoint intelligence integration for quick response to advanced threats.

TRIPWIRE® PURECLOUD

Unlike traditional vulnerability scanning products and services, Tripwire PureCloud requires neither software or hardware to deploy or manage, nor any changes to your firewalls. Tripwire PureCloud Enterprise provides an easy to deploy and cost effective solution that discovers and assesses hard-to-reach areas of any network.

TRIPWIRE® LOG CENTER

Tripwire Log Center® provides real-time intelligence to machine data, along with security analytics and forensics for rapid incident response. Tripwire Log Center provides integration with your existing infrastructure and includes a growing library of available correlation rules, empowering your team to monitor, detect and quickly respond to threats in your environment.

tripwire®

◆ Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. Learn more at tripwire.com. ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

SBCSC61b 201701