WHITE PAPER

Nine Critical Questions to Prepare You for the CCRI Program

Advanced Threat Detection, Security and Compliance with Tripwire

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

The Command Cyber Readiness Inspection (CCRI) Program is a comprehensive, formal inspection of cyber readiness compliance led by The Defense Information Systems Agency (DISA). This program focuses primarily on network security policies and programs managed by the local network provider to provide cyber awareness to senior leaders.

The CCRI program holds senior mission Commanders at major Department of Defense headquarters, installations and facilities personally responsible for end-to-end cyber readiness. Because of this, these Commanders must be able to develop, maintain and update consistent and reliable cybersecurity situational awareness (SA) of the headquarter, installation or facility for which they are responsible (including policies, procedures, workspaces and user training), regardless of formal organizational affiliation or supporting network provider.

Tripwire helps Commanders anticipate and resolve network-related security issues prior to CCRI. Tripwire allows Commanders to repackage the same network metrics generated by network systems, applications and management tools used by the network manager into a mission-focused, technical cybersecurity common operational picture (COP). This facilitates metric-driven risk assessments geared to Commander-specified CCRI intelligence requirements. This white paper discusses the following nine critical CCRI preparedness questions:

1. What are my network hardware and application assets?
2. Who has access to my network?
3. Which systems are vulnerable?
4. Which systems are being attacked?
5. Which systems have been compromised?
6. Which systems should be fixed first?
7. Have these vulnerabilities been seen before?
8. When was my network last in a trusted state?
9. How can I keep this from happening again?

Tripwire delivers unprecedented risk visibility, operational context and security intelligence. Tripwire's trusted portfolio of high-priority security control solutions enables organizations and agencies to protect sensitive data from breaches, vulnerabilities and threats. The matrix in Figure 1 shows how Tripwire provides the responses to specified CCRI intelligence requirements.

Command Cyber Readiness Inspection (CCRI) Program Focus Areas

Key CCRI areas of interest for which headquarters, installation or facility senior mission commanders are accountable include policy, training, facilities and personnel considerations, as well as traditional network cybersecurity technical focus areas.

In general terms, CCRI inspections are packaged into the following categories:

Fixed networks: The physical information infrastructure, hardware and associated operating systems and facilities that make up the network systems architecture which support the headquarters, installation and facility users (including the hardware and software systems that support mobile users).

Mobile devices: This category includes all mobile user devices that connect directly to the supporting DoD network infrastructure and network services. It also includes mobile devices operated by headquarters, installation or facility tenants that use commercial network infrastructure to connect to DoD network services (including mobile

		Commanders CCRI Concerns								
CCRI FOCUS AREAS	Tripwire Capabilites	Where are my network assets?	Who has access to my network?	Which systems are vulnerable?	Which systems are being attacked?	Which sysems have been compromised?	Which sytems should be fixed first?	Have these vulnerabilitys been seen before?	When was my network last in a trusted state?	How can I keep this from happening again?
Auth & Access Mgmt	Limit & control network ports, protocols & services		X							
Auth & Access Mgmt	Control Administrative Privileges		X							
Auth & Access Mgmt	Need to Know Access		X							
Auth & Access Mgmt	Account Monitoring & Control		X	X	X	X		X	X	
Fixed Networks	Secure network engineering (secure coding)									
Fixed Networks	Inventory H/W Assets, Criticality & Location	X				X	X		X	X
Fixed Networks	Inventory S/W Assets, Criticality & Location	X					X		X	X
Mobile Networks	Wireless device control	X	X							
Network Security	Incident response			X	X	X	X	X		X
Network Security	Secure configured network	X								
Network Security	Vulnerability Assessment and Remediation			X	X	X				
Network Security	Malware Protection			X	X	X				
Network Security	Application security			X	X	X	X		X	
Network Security	Boundary defense			X	X	X	X	X		
Network Security	Maintain monitor and analyze audit logs		X		X	X		X	X	
Network Security	Secure Configuration Servers	X					X		X	X
Network Services	Data recovery								X	X
Network Services	Data loss prevention	X	X	X		X				X
User Security	Security skills assessment									
User Security	Preventative testing and red team exercises									X

Fig. 1 Commanders' CCRI concerns and Tripwire capabilities

tactical systems, special purpose sensor systems, emergency response mobile radios, commercial mobile telephones, data pads and more).

Network services: The applications, associated databases, and web services hosted on DoD controlled networks that provide network users access to mission-specific or day-to-day workplace information services such as voice, data, video and web services.

Authentication and access management: Policies, procedures, hardware, applications and user tokens (Common Access Cards, for example) that manage individual user identities and allow authorized users—based on unique user identity and functional or operational mission roles—to access networks and network services.

Network security: Policies, procedures, hardware and applications specifically designed to monitor and protect user identity, networks and network services.

End user security: Policies, procedures, facilities and training to ensure users properly operate, secure, protect and transport network user (endpoint) hardware, software and data.

CCRI places special emphasis on Commanders' responsibility and accountability to establish and enforce cybersecurity policies and procedures. With DoD's focus on joint, multinational and interagency operations, host tenants and organizations from other commands, services and federal agencies are not under their direct control.

The Tripwire solution for CCRI allows Commanders to bridge many of these organizational and functional mission cybersecurity gaps by using existing network metrics (generated by existing network hardware, software and security management tools). This creates a proactive Commanders' network cybersecurity common operational picture (COP) that spans the organizational and functional structure of headquarters, installations and facilities.

Tripwire's mission-focused CCRI intelligence will provide the cues and underlying data needed to answer key cybersecurity questions like, "What's in my network?" and "Where am I vulnerable?"

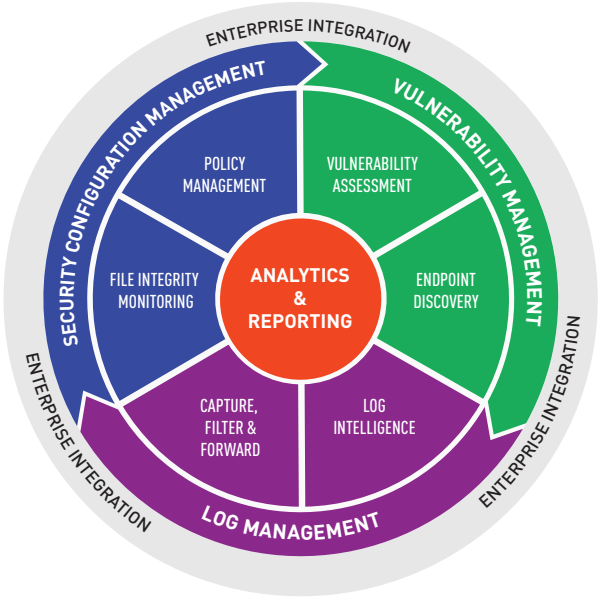

Fig. 2 Capabilities of the Tripwire solution for CCRI

> Use of data assurance and operating systems integrity products (for example, public key infrastructure (PKI), Tripwire, Internet protocol security (IPSec), transmission control protocol/internet protocol (TCP/IP) wrappers) will be included in product development and integrated into end-state production systems.
>
> — AR 25-2 INFORMATION SECURITY, PARAGRAPH 4–6. CONTROLS

The Tripwire Solution for CCRI

Tripwire provides vulnerability management, log intelligence and security configuration management that address many of the items audited in the CCRI while providing real time protection.

The Tripwire security suite can monitor over 125 operating systems and applications, including Windows, Mac, Linux, virtual infrastructures, databases and network devices, for change. This enables Tripwire to detect leading indicators of cyber activity, dynamically protect mission-critical systems and create a cybersecurity COP that is visible, measurable and actionable across three cybersecurity vectors:

» Network configuration

» Vulnerability management

» Network intelligence

Tripwire believes having relevant operational context is the only way to connect security efforts to what matters to mission and operational goals and to minimize risks. Tripwire automation applies intelligence to data and delivers more effective operations. The Tripwire CCRI COP includes vulnerability management, security configuration and

policy compliance, system integrity monitoring, and actionable network system log intelligence. It detects indicators of breach, compromise and vulnerability.

Tripwire is a widely-recognized DoD partner in network cyber defense. Army Regulation 25-2, Information Assurance, identifies Tripwire by name as a keystone cybersecurity capability that should be integrated into army network design from the start as indicated in Figure 3. Tripwire currently supports component services and federal agencies with over 700 deployments of the proven tools and processes needed to secure their networks.

Tripwire can arm Commanders with the specifics needed to review and revise cybersecurity and readiness policies, processes, procedures, resources, capabilities, personnel, training and cybersecurity management metrics. The Tripwire solution for CCRI bridges the enterprise cyberthreat gap for network and data security functions.

It also provides critical information and analytics to the Mission Commander as illustrated in Figure 1, in executing the CCRI responsibilities. The suite addresses many of the critical requirements found in the CCRI and can provide real-time, updated protection across the network, application and data spectrum.

How Tripwire Maps to the Nine Key CCRI Preparedness Questions

1. What are my network hardware and application assets?
You can't secure what you don't know you have. The Tripwire solution for CCRI allows commanders to identify all the hardware and software running in the network environment while continuously discovering new assets to deliver a complete network view. Commanders can also view network hardware and software assets through their unique mission lens by assigning tags that categorize assets based on notions such as risk, priority, geographic location, regulatory policies, priority, relevance and organizational alignment. This includes cloud-based web servers that host unit-specific mission applications and data. Because tags can be assigned to multiple assets simultaneously, it's quick and easy to onboard groups of similar assets.

2. Who has access to my network?
Your organization or agency's greatest asset can also be its greatest threat, as the people you trust to make your organization successful can also cause the most damage. Tripwire's solution for CCRI not only helps detect threats from outside your network, but also from within by identifying key risk indicators, thereby detecting malicious insiders before sensitive data is exfiltrated, thus containing potential damage. The solution can correlate data and events from both Tripwire and third-party products to identify suspicious patterns of use or malicious activity across multiple systems. The correlation function can be used to identify insider threats through patterns of behavior.

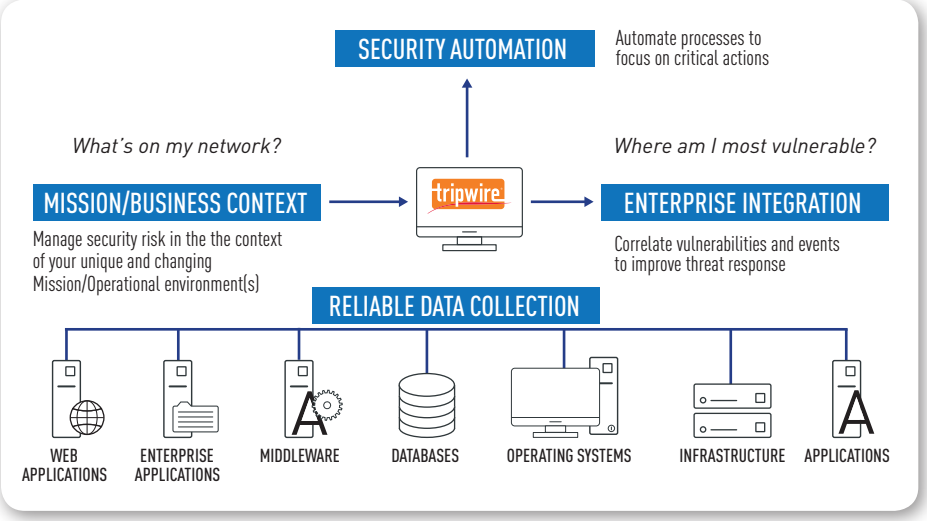

Fig. 3 Architecture of the Tripwire solution for CCRI

3. Which systems are vulnerable?
The vulnerability environment changes every day. Tripwire identifies and prioritizes vulnerabilities based on their level of risk to your organization so you can deploy your resources most effectively to reduce overall risk. With over 90 percent of unauthorized data access coming through compromised servers, continuous system hardening is critical to protect valuable IT assets. Tripwire knows your assets—file servers, databases, active directory, network devices and endpoints—and how they're configured to provide you a continuous view of both network security and compliance.

4. Which systems are being attacked?
Cyberthreats have become more sophisticated, sidestepping outdated detection methods and requiring quick discovery to contain damage and protect sensitive data. Tripwire reacts to changes in real time, identifying suspicious activities while securely collecting and archiving data. This gives you dynamic security analytics for rapid forensics, identification of historical indicators of risk and threat patterns, and then enables you to quickly restore systems to a known, trusted and operational state. This reduces the enterprise cyberthreat gap as illustrated in Figure 5.

5. Which systems have been compromised?
Continuous monitoring is critical to both good security and compliance so there aren't gaps that attackers can find or that your auditors will question. Tripwire operates continuously and in real time to detect changes, risks and threats. Automatic change detection is the best early indicator for advanced threats. Tripwire is the gold standard in integrity

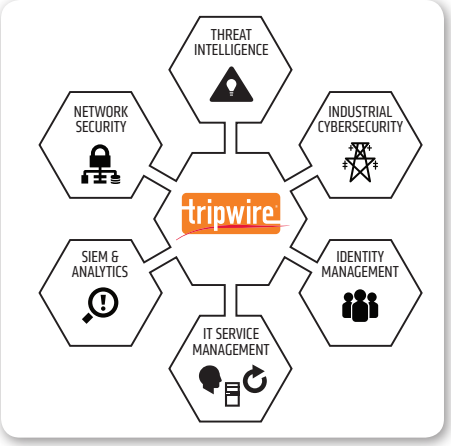

Fig. 4 Integration capabilities of the Tripwire solution for CCRI

monitoring, identifying changes to files and systems, and separates low- from high-risk change as part of real-time assessment, prioritization and reconciliation of detected change. Tripwire can also integrate with malware identification and sandboxing tools to dynamically validate files and executables against known malware signatures.

6. Which systems should be fixed first?
In addition to industry-standard CVSS vulnerability scores, Tripwire provides a unique prioritization metric that includes factors for depth of access, the skill required to exploit and the time elapsed since the vulnerability was published.

7. Have these vulnerabilities been seen before?
Tripwire provides trend reporting on vulnerabilities, which helps responsible parties assess progress in risk reduction. Tripwire also provides vulnerability aging reports that indicate how long vulnerabilities have been present in the environment. Once a vulnerability has been addressed, it should be validated against reoccurrence.

8. When was my network last in a trusted state?
Tripwire dramatically reduces the time and effort for CCRI preparation by providing continuous, comprehensive network infrastructure baselines along with real-time change detection and built-in intelligence to determine the impact of change. Through reporting on node variance, Tripwire identifies in deep detail the exact changes that pushed a system out of compliance and when they occured.

9. How can I keep this from happening again?
Organizations and agencies need to detect incidents and respond to threats—immediately. They also need to prove compliance with standards and regulations. Tripwire reliably and securely collects, analyzes and correlates log data from devices, servers, applications and automated security processes to improve security for analytics and forensics. Collected data is analyzed and filtered so only actionable and relevant events are presented. Network intelligence provided by Tripwire is a critical part of any threat protection deployment and includes both network and endpoint security information and analysis. Tripwire log intelligence can be deployed to local sites where expertise is greatest while simultaneously delivering events to another log collection system.

Summary

With the industry's best threat intelligence partner integrations, Tripwire helps customers detect, analyze and verify zero-day exploits and advanced persistent threats. Tripwire solutions are designed to support both on-premise and cloud-based threat intelligence platforms, giving you full flexibility that includes customization and open-source integration.

The Detection Gap

The amount of time it takes to discover a compromise and identify its nature. Reports show this often takes five to 18 months.

The Response Gap

The amount of time it takes to identify the full scope of the breach and limit its damage. Research indicates this typically takes over four months.

The Prevention Gap

The time it takes to implement measures to avoid a repeat (or similar) attack.

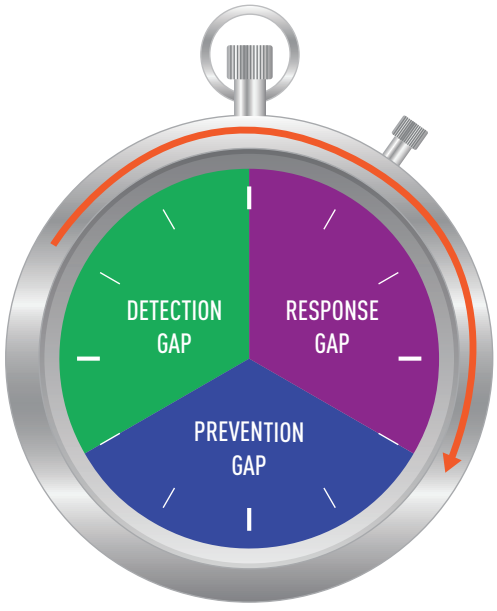

Fig. 5 The Enterprise Cyberthreat Gap

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**

***The State of Security*: Security News, Trends and Insights at tripwire.com/blog**
Follow us on Twitter @TripwireInc » Watch us at youtube.com/TripwireInc

WPCCRI2a 1807