COMPLIANCE
BEST PRACTICES FOR CRITICAL INFRASTRUCTURE

INSIGHTS

In the past year, sophisticated cyber criminals infected the industrial control systems of hundreds of energy and public utility companies in the United States and Europe. Power and utilities users reported a six-fold increase of 7,391 reported incidents in the past year in PricewaterhouseCooper's (PwC) The Global State of Information Security Survey 2015.

Organizations require that their security environments operate according to established standards and security best practices. This isn't easy however, when often what needs to be checked is unknown, or the process is time-consuming and manual. With configuration and policy settings in a constant state of flux, IT departments must apply hundreds of changes each year.

As regulators around the world move to tighten compliance requirements for Critical Infrastructure organizations, improvements in security practices become increasingly essential to safeguard data. North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) presents clear security guidelines for network security managers, such as Electronic Security Perimeters (CIP-005) and System Security Requirements (CIP-007) among others. In addition, Configuration Change Management (CIP-010) requires firms "to prevent and detect unauthorized changes to systems by specifying configuration change management requirements.

SOLUTION

Our Compliance Software Blade automatically and continuously monitors the network environment with a library of over 300 security best practices, highlighting configuration errors and identifying security weaknesses.

By validating policy and configuration changes according to best practices and internal policies in real-time, the Compliance Software Blade enables security managers to identify issues before policies are implemented. In addition, it addresses NERC-CIP, ISA99, and NIST 800-82 requirements.

COMPLIANCE BLADE BEST PRACTICES ADDRESSES MANY NERC-CIP, ISA99, AND NIST 800-82 REQUIREMENTS

SECURITY BEST PRACTICES

Compliance Blade Best Practices reviews all Check Point management and enforcement points, comparing them to a library of over 300 security best practices. This provides a rich and extensive knowledgebase on how to configure your environment. Defined by engineers and security experts, each best practice ensures maximum utilization of our security deployments.

AUTOMATED ALERTS

With the network environment constantly in flux, security policy and configuration setting changes are frequent. Security best practices validate each saved configuration change. If it detects a violation that negatively affects the overall security status, it generates an automatic alert. All this happens before policy installation, reducing time associated with manual change management.

CONFIGURATION MANAGEMENT

NERC-CIP is clear on which security controls are needed and how they should be implemented. We address many of these requirements. The Compliance Blade's built-in NERC report highlights implemented and unimplemented controls.

Beyond the specific controls, NERC-CIP also requires businesses to implement a configuration change management process that prevents and detects unauthorized changes. In the context of our network security environment, our Compliance Blade Software Blade is the only way to go.

NERC-CIP COMPLIANCE & AUDIT

Compliance Blade best practices is a critical component of the Check Point Security Architecture for the Critical Infrastructure sector. Not only does it allow security policies audits in real time, but also ensures proper configuration and function of vital security controls such as Firewall, Antivirus, IPS and Data Loss Prevention.

NERC-CIP Compliance Requirements Mapping to Check Point Products		
CIP-005	Electronic Security Perimeter(s)	UserCheck, Identity Awareness, SmartLog
CIP-007	System Security Requirements	NGFW, Identity Awareness, Threat Prevention, SmartEvent,
CIP-008	Incident Reporting	SmartEvent
CIP-010	Configuration Change Management	Compliance Blade
CIP-011	Information Protection	Compliance Blade, DLP, Document Security

ASSESS YOUR COMPLIANCE STATUS TODAY

Save time and significantly reduce costs by leveraging your existing security infrastructure to automatically implement the Check Point Compliance Software Blade. Get started with a trial today, and learn more about the Compliance Software Blade.

Over 300 Best Practices

"THE CHECK POINT COMPLIANCE SOFTWARE BLADE HAS MADE ALL OF OUR AUDITS AN ORDER OF MAGNITUDE EASIER. IT NOT ONLY MAKES THE AUDITING PROCESS FASTER,

BUT INSTILLS CONFIDENCE IN OUR CLIENTS THAT WE TRULY KNOW WHAT WE ARE DOING.

IN THE COMPLIANCE WORLD,

CONFIDENCE IS EVERYTHING."

- Customer Testimonial

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com