Cisco Security Portfolio, Splunk, and The NIST Cybersecurity Framework 2.0

Effective Cybersecurity Risk Management

From the largest federal agency to the smallest school district, every organization today is faced with managing cybersecurity risks efficiently and effectively. Can yours benefit from an innovative, best practices approach to Cybersecurity?

Cybersecurity can be overwhelming, and there's plenty of long to-do lists. The Center for Internet Security (CIS) has the Critical Security Controls, the International Organization for Standardization (ISO) has its 27000-serices publications, ISACA manages its COBIT 5 framework, and NIS 2 Directive strengthens cybersecurity requirements for entities that operate in the European Union. Layer all of these atop compliance mandates like Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) – and its often hard to know where to start.

That's why the National Institute of Standards and Technology (NIST) developed the Cybersecurity Framework (CSF) 2.0. It enables organizations of all sizes to discuss, address, and manage cybersecurity risk. And without reinventing the cybersecurity wheel, it references existing best practices through its core functions: Identify, Protect, Detect, Respond, Recover, and Govern.

The key points with NIST CSF 2.0 moving forward from NIST CSF 1.0 is it places a greater emphasis on cybersecurity governance, including clear roles, responsibilities, and decision-making processes. The new "Govern" function highlights the importance of managing cybersecurity risks within the organization's supply chain and the framework is designed to be adaptable to organizations of all sizes and sectors.

Let Cisco Help

Cisco's Security portfolio along with Splunk aligns with the NIST Cybersecurity Framework 2.0. In the following section, we will list each framework function and category, and then show how Cisco's products help organizations accomplish each specific framework goal.

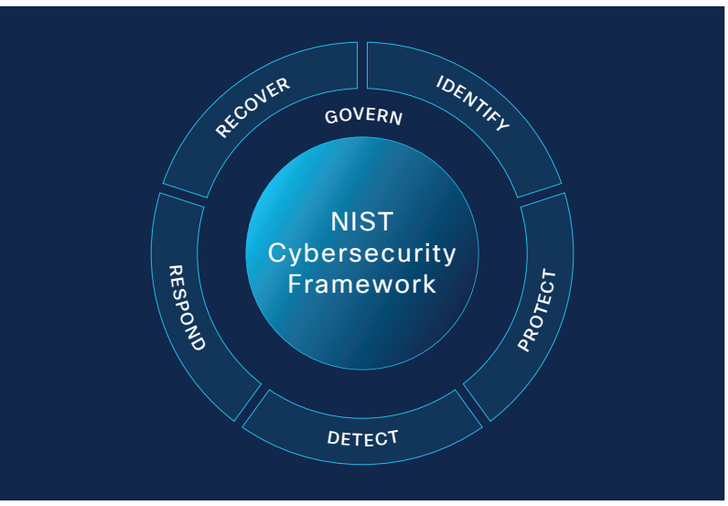
Our solutions are simple, open, and automated to interoperate at every level of the security stack. Not only across the Cisco portfolio but also with other vendors' products. Cisco solutions incorporate industry-leading, actionable TALOS threat intelligence directly into them. With Cisco Security, you can take a new approach to cybersecurity, adopt the NIST CSF 2.0, and bolster cyber defenses and readiness.

Cisco Security Portfolio and Splunk Support the NIST Cybersecurity Framework 2.0

Cisco's comprehensive cybersecurity products and services portfolio defends organizations throughout the world against today's advanced threats. Figure 1: Cisco Capability mapping to NIST CSF 2.0 shows how Cisco's Security portfolio along with Splunk map to the NIST Cybersecurity Framework 2.0.

Figure 1: Cisco Capability mapping to NIST CSF 2.0

		Network Security					Device Security					User Security				Cloud Security			App Security		Analytics				Industrial Security			Other		Splunk Capabilities					
		Cisco Firewalls	Cisco Defense Orchestrator	Cisco Identity Services Engine	Cisco Multicloud Defense	Cisco XDR	Cisco Secure Client	Cisco Secure Endpoint	Cisco Security Connector	Cisco Meraki Systems Manager	Cisco Duo	Cisco Secure Email Threat Defense	Cisco Secure Access (SSE)	Cisco Secure Web Appliance	Cisco Attack Surface Management	Cisco Cloud Application Security	Cisco Umbrella	Cisco Secure Workload	Cisco Secure WAF	Secure Malware Analytics	Secure Network Analytics	Security Analytics and Logging	Cisco Telemetry Broker	Cisco Industrial Threat Defense	Cisco Cyber Vision	Secure Equipment Access	Cisco Secure DDoS Protection	Cisco Vulnerability Management	Splunk Core	Splunk Asset & Risk Intelligence	Splunk Enterprise Security	Splunk Attack Analyzer	Splunk User Behavior Analytics	Splunk SOAR
Function	Category																																		
GOVERN (GV)		Non-technical controls																																	
IDENTIFY (ID)	Asset Management (ID.AM)	●		●	●	●	●	●	●	●	●				●	●	●	●	●		●				●	●			●	●	●		●	●
	Risk Assessment (ID.RA)	●		●		●	●	●	●		●	●	●	●	●	●	●	●			●	●	●		●	●	●		●	●	●	●	●	●
	Improvement (ID.IM)	Non-technical controls																																	
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)	●	●	●	●		●	●	●	●	●		●	●			●	●	●	●	●	●			●	●	●	●		●	●	●	●	●	●
	Awareness and Training (PR.AT)	Non-technical controls																																	
	Data Security (PR.DS)	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●	●		●			●	●	●			●	●	●		●	●
	Platform Security (PR.PS)	●	●	●	●	●	●	●		●			●	●			●	●				●	●	●		●			●	●	●		●	●
	Technology Infrastructure Resilience (PR.IR)	●	●	●	●	●	●	●	●	●	●		●	●			●	●			●	●	●	●	●	●			●	●	●	●	●	●
DETECT (DE)	Continuous Monitoring (DE.CM)	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●
	Adverse Event Analysis (DE.AE)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
RESPOND (RS)	Incident Management (RS.MA)	Non-technical controls																																	
	Incident Analysis (RS.AN)	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●	●		●		●		●	●	●	●
	Incident Response Reporting and Communication (RS.CO)	Non-technical controls																																	
	Incident Mitigation (RS.MI)	●	●	●	●	●	●	●			●	●	●	●			●	●	●	●	●	●	●	●	●		●		●		●	●	●	●
RECOVER (RC)	Incident Recovery Plan Execution (RC.RP)		●		●	●		●		●		●					●		●			●							●	●	●	●	●	●
	Incident Recovery Communication (RC.CO)	Non-technical controls																																	



NIST CSF 2.0 Category Breakdown

GOVERN (GV)

The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. NIST defines this Function as “the organization’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.”

The Cisco Security portfolio and Splunk help streamline the governance process by offering comprehensive data analytics, reporting capabilities, and policy management features to ensure adherence to cybersecurity regulations and standards.

IDENTIFY (ID)

The purpose of the IDENTIFY function as defined by NIST is “the organization’s current cybersecurity risks are understood.” Understanding the organization’s assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under the GOVERN Function.

That’s why Cisco Security and Splunk deliver critical discovery capabilities; that is, identifying and categorizing systems, assets, and data on a continuous basis.

PROTECT (PR)

NIST defines the PROTECT Function as “Safeguards to manage the organization’s cybersecurity risks are used.” Once assets and risks are identified and prioritized, the PROTECT function supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities.

Cisco supports the PROTECT Function with the advanced capabilities that enforce and harden security controls before the inevitable cyberattack attack occurs.

DETECT (DE)

NIST defines the DETECT Function a “possible cybersecurity attacks and compromises are found and analyzed”. The DETECT Function enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. Many cybersecurity incidents go unnoticed for months, allowing hackers ample time to explore your network, locate sensitive information, and then slowly and carefully exfiltrate it. Cisco defines Time-To-Detection (TTD) for malware analysis as the window of time between the first observation of a file and the detection of an actual threat.

The Cisco Security portfolio and Splunk continually seeks to reduce the Time to Detect (TTD) so that our customers can detect cyber incidents faster than ever.

RESPOND (RS)

NIST defines the RESPOND Function as “Actions regarding a detected cybersecurity incident are taken.” The RESPOND Function supports the ability to contain the effects of cybersecurity incidents. The RESPOND Function is a bit like an insurance policy. No one ever wants to use it, but you have it for when disaster strikes. The likelihood of a cyberattack affecting your organization is extremely high.

Your organization might have already been breached, but simply have not discovered it yet. The RESPOND Function helps organizations develop and implement appropriate activities to act regarding a detected cybersecurity event.

Cisco has the capabilities and guidance you need to respond effectively to detected incidents.

RECOVER (RC)

NIST defines the RECOVER Function as “assets and operations affected by a cybersecurity incident are restored”. The Recover Function supports the timely restoration of normal operations to reduce he effects of cybersecurity incidents and enable appropriate communication during recovery efforts. The RECOVER Function also maintains plans for resilience and restores any capabilities or services that were impaired due to a cyber security event. It supports timely recovery to normal operations to reduce the impact from a cybersecurity event, and helps your organization build lessons learned back into your cybersecurity operations.

The Cisco Security portfolio and Splunk enable rapid incident recovery through automated threat detection, response capabilities, and comprehensive data analysis.

Cisco helps facilitate the execution of recovery plans by providing insights and tools necessary for restoring systems and services quickly and effectively after a cybersecurity incident.

Conclusion

Cisco provides one of the industry’s most comprehensive advanced threat protection portfolios of cybersecurity products and solutions. Our approach reduces complexity, while providing superior visibility, continuous control, and advanced threat protection across the extended network. Or mission is truly effective security, which is exactly in line with the NIST CSF 2.0.

Cisco will help you pull all the components together to establish your continuous security life cycle program. With Cisco, you can adopt the NIST CSF Framework, and bolster cybersecurity readiness and resiliency.

For more information on cisco Security, please visit: www.cisco.com/go/security

(1110R) 2221141413 01/25