Framework Mapping: Cisco Secure Network Analytics (SNA) + NIST CSF 2.0

Overview of the NIST Cybersecurity Framework 2.0

The National Institute of Standards (NIST) Cybersecurity Framework (CSF) 2.0 is a voluntary set of guidelines developed to help organizations manage and reduce cybersecurity risks. While voluntary, its adoption can significantly improve an organization's security posture by offering a structured approach to risk management.

In February 2024, NIST released the CSF 2.0, updating version 1.1 from April 2018. This update incorporates feedback from various industries and stakeholders, enhancing the framework's flexibility, applicability, and relevance. The NIST CSF 2.0 continues to serve as a voluntary, risk-based framework designed to help organizations of all sizes and sectors manage and reduce cybersecurity risks, foster resilience, and align with best practices.

Purpose of the Framework

The NIST Cybersecurity Framework provides a structured yet flexible approach to improving an organization's cybersecurity posture. It is used for:

Assessing Risks: Identifying, analyzing, and prioritizing cybersecurity risks.

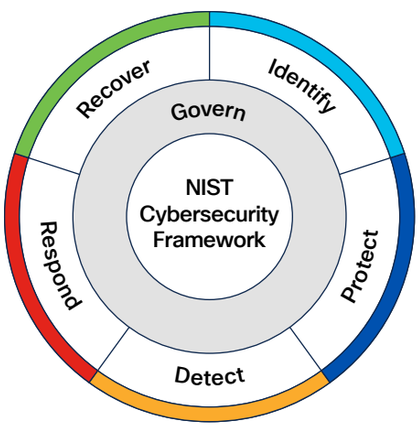
Guiding Cybersecurity Programs: Establishing or improving cybersecurity strategies in alignment with organizational goals.

Enhancing Communication: Facilitating clear communication about cybersecurity risks and strategies between technical teams, leadership, and external stakeholders.

The framework is particularly valuable for organizations that lack formalized cybersecurity programs or resources, though it is robust enough to benefit even the most mature organizations.

Key Components of the NIST Cybersecurity Framework 2.0

The NIST CSF 2.0 maintains the foundational structure of the original framework while introducing several enhancements. Its key components are:



Core Functions

The Framework Core outlines six **high-level functions** that provide a strategic view of cybersecurity risk management. These functions remain foundational in CSF 2.0 and are as follows:

GOVERN:

Establish and oversee policies, roles, processes, and accountability to align cybersecurity efforts with organizational objectives and regulatory requirements.

Examples: Risk management policies, executive accountability, cybersecurity governance framework

IDENTIFY:

Develop an understanding of cybersecurity risks to systems, assets, data, and capabilities. This involves identifying critical resources, threats, and vulnerabilities.

Examples: Asset management, governance, risk assessments

PROTECT:

Implement safeguards to ensure the delivery of critical services and mitigate risks.

Examples: Access control, data protection, training, and maintenance

DETECT:

Establish systems to identify cybersecurity events or anomalies in a timely manner.

Examples: Continuous monitoring, intrusion detection, and threat intelligence

RESPOND:

Develop and implement appropriate actions to mitigate the effects of a detected cybersecurity event.

Examples: Incident response planning, mitigation strategies, and communication

RECOVER:

Develop plans to restore operations and reduce the impact of cybersecurity incidents.

Examples: Disaster recovery, business continuity planning, and lessons learned

Implementation Tiers

The framework includes **Implementation Tiers** to help organizations evaluate their current cybersecurity practices and set goals for improvement. These tiers reflect the degree to which an organization's cybersecurity practices are informed by risk management processes, integrated with business needs, and adaptive to evolving risks:

Tier 1 (Partial): Limited awareness and ad hoc implementation of cybersecurity practices.

Tier 2 (Risk-Informed): Risk management practices are formally defined but not fully integrated.

Tier 3 (Repeatable): Cybersecurity practices are consistently applied and documented across the organization.

Tier 4 (Adaptive): Practices are continuously improved and proactively adapted to changing risks.

Profiles

The Framework Profiles allow organizations to align the framework to their specific goals, resources, and risk tolerance. A profile compares the current state of an organization's cybersecurity practices to its desired state, serving as a roadmap for improvement.

Why Use the NIST Cybersecurity Framework?

Organizations adopt the NIST CSF 2.0 for several reasons:

Flexibility: Its non-prescriptive nature allows organizations to tailor it to their unique needs.

Widely Recognized: The framework is globally acknowledged as a standard for cybersecurity best practices.

Risk Management: It helps organizations prioritize risks and allocate resources effectively.

Compliance Alignment: While voluntary, the framework aligns with various regulatory requirements and standards, simplifying compliance efforts.

Mapping to other Frameworks

The NIST National Online Informative References (OLIR) Program provides a framework for organizations to map cybersecurity standards, guidelines, and frameworks. By leveraging OLIR, Cisco can cross-reference the NIST Cybersecurity Framework (CSF) 2.0 with other standards like NIST SP 800-53, simplifying compliance and security alignment. This approach eliminates the need for separate mappings, saving time and effort while ensuring traceability across frameworks.

For Cisco, this means that once its security solutions, such as Cisco Firewalls, are mapped to NIST CSF 2.0, these mappings can be extended through NIST OLIR to align with other frameworks. This capability is particularly beneficial for public sector and regulated industries, where compliance with multiple frameworks is often required. By using NIST CSF 2.0 as a common backbone, Cisco helps customers achieve compliance efficiently while demonstrating how its solutions align with best practices and regulatory mandates.

This cross-mapping capability strengthens Cisco's position as a strategic enabler of cybersecurity compliance, providing customers with a clear understanding of how its solutions fit into their broader compliance and risk management strategies.

Understanding Cisco Secure Network Analytics

As organizations' networks grow in scale and complexity, traditional monitoring tools may struggle to deliver the visibility and threat detection needed to protect critical assets. Cisco Secure Network Analytics (SNA) is designed to address these modern challenges by providing comprehensive, real-time network visibility and advanced threat detection. By leveraging continuous traffic analysis, behavioral modeling, and enriched security analytics, Cisco SNA empowers organizations to identify anomalies, detect suspicious activities, and respond to threats swiftly—all from a unified platform. This holistic approach enables organizations to strengthen security, support compliance, and maintain operational resilience across dynamic network environments.

What is SNA?

Cisco SNA is a comprehensive network visibility and threat detection solution that enables organizations to monitor, analyze, and secure traffic across on-premises, cloud, and hybrid environments. SNA goes beyond traditional monitoring tools by providing advanced features such as behavioral analytics, anomaly detection, encrypted traffic analytics, and integration with threat intelligence platforms.

Cisco SNA leverages automation, real-time analytics, and rich network telemetry to help organizations identify suspicious activities, detect threats, and accelerate incident response. As part of Cisco's security portfolio, SNA is designed to scale from small businesses to large enterprises, offering centralized management, flexible deployment options, and robust compliance support—all while maintaining network performance and operational efficiency.

Benefits of Cisco SNA

Cisco SNA offers several key advantages for organizations aiming to strengthen network security and gain actionable insights:

Comprehensive Network Visibility: SNA delivers extensive visibility into network traffic across on-premises, cloud, and hybrid environments, enabling organizations to continuously monitor all devices, users, and applications.

Advanced Threat Detection: By leveraging behavioral analytics, anomaly detection, and enriched network telemetry, SNA can rapidly identify suspicious activities, policy violations, and emerging threats—even in encrypted traffic.

Operational Efficiency: Automated threat alerts, intuitive dashboards, and centralized management streamline security operations, allowing IT and security teams to detect, investigate, and respond to incidents more efficiently.

Real-Time Analytics and Response: SNA provides real-time analytics and contextual insights, helping organizations quickly understand security events and accelerate incident response to reduce risk.

Scalable and Flexible Integration: Built to scale with organizational growth, Cisco SNA integrates seamlessly with Cisco's broader security portfolio and third-party solutions, supporting evolving security needs and compliance requirements. It also lets you make the most of your investments with an agentless solution, using rich telemetry generated by your existing network infrastructure.

No more blind spots: SNA is the only security analytics solution that can provide comprehensive visibility across the private network and into the public cloud without deploying sensors everywhere. It is also the first solution to detect malware in encrypted traffic without any decryption.

Focus on incidents, not noise: By using the power of behavioral modeling, multilayered machine learning, and global threat intelligence, SNA significantly reduces false positives and alarms on critical threats affecting your environment.

Cisco SNA Deployment Options

Cisco provides a range of deployment options and appliance types to help organizations achieve optimal visibility, scalability, and threat detection across their networks:

- **Physical Appliances:**
  Deploy dedicated Cisco SNA hardware for robust, high-performance, on-premises monitoring. Appliance types include:

  SNA Manager: Provides centralized administration, policy management, alerting, and reporting for the entire SNA deployment.

  - Real-time, up to the minute data – Delivers data flow for monitoring traffic across hundreds of network segments simultaneously so that you can spot suspicious network behavior.
  - Capability to detect and prioritize security threats – Rapidly detects and prioritizes security threats, pinpoints network misuse and suboptimal performance, and manages even response across the enterprise.
  - Management of appliances – Configures, coordinates, and manages CSA appliances.
  - Use of multiple types of flow data – Consumes multiple types of flow data, including NetFlow, IPFIX, and sFlow.
  - Scalability – Supports the largest of networks demands. Performs well in extremely high-speed environments and can protect every part of the network that is IP reachable, regardless of size.
  - Audit trails for network transactions – Provides a complete list of audit trail of all network transactions for more effective forensics investigations.
  - Real-time, customizable relational flow maps – Provides graphical views of the current state of the organization's traffic. Administrators can easily construct maps of their network based on any criteria, such as location, function, or virtual environment. By creating a connection between two groups of hosts, analyzing the traffic between them can be done easily.

  Flow Collector (FC): Aggregates, processes, and stores network flow data from multiple sources for detailed traffic analysis and threat detection. It collects and stores enterprise telemetry (NetFlow, IPFIX, sFlow, NVM, and Syslog from the existing infrastructure such as routers, switches, firewalls, endpoints and other network devices. The telemetry data is analyzed to provide a complete picture of network activity. Months or years of data can be stored creating an audit trail than can be used for forensics investigations and compliance initiatives.

  - Threat detection – Ingests proxy records and associates them with flow records to deliver the user application and URL information for each flow to increase contextual awareness.
  - Flow traffic monitoring – Monitors flow traffic across hundreds of network segments simultaneously so that you can spot suspicious network behavior.
  - Extended data retention – Allows organizations and agencies to retain large amounts of data for long periods of time.
  - Scalability – Performs well in extremely high-speed environments and can protect every part of the network that is IP reachable, regardless of size.
  - Deduplication and stitching – The FC performs deduplication so that any flows that might have traversed more than one router are counted only once. It then stiches the flow information together for complete visibility of a network transaction.

  Data Store: Delivers scalable storage and high-performance retrieval of historical flow data, supporting compliance and long-term analysis. The Data Store cluster can be added between the SNA Manager and Flow Collectors. One or more FCs can infest and deduplicate the flow data, perform analyses, and then send the flow data and its results directly to the data store.

  - Increases data ingest capacity – Data stores can be combined to create a single cluster of data nodes capable of monitoring over 3 million Flows Per Second (FPS) to aid in relieving ingestion bandwidth challenges for organizations with high flow volumes.
  - Enterprise-class data resiliency – Telemetry data is stored redundantly across nodes to allow for seamless data availability during single node failures, helping ensure against the loss of telemetry data.
  - Single query and reporting response time improvements – The Data Store provides improved query performance and reporting response times that are at least 10x faster than those offered by other standard deployments. The Data Store can also perform an increased number of concurrent queries, whether through APIs or the SNA manager.
  - Storage scalability – The Data Store offers organizations with growing networks enhanced flexibility around data storage scalability through the ability to add additional database clusters.
  - Long-term data retention – Scalable and long term telemetry storage capabilities long-term flow retention of up to 1 to 2 years' worth of data with no need to add additional flow Collectors. This aids in satisfying regulatory requirements and reducing costs and complexity.

  Telemetry Broker: Collects, normalizes, and distributes telemetry data from a wide variety of network sources to analytics and security tools. It is capable of ingesting network telemetry from a variety of telemetry sources, transforming their data formats, and then forwarding that telemetry data to one or multiple destinations.

  - Ingest any of the following – On-premises network telemetry (e.g., NetFlow, Syslog, IPFIX) and Cloud-based telemetry sources (e.g., AWS CPC flow logs and Azure NSG flow logs).
  - Forward to the following destinations – Cisco SNA, Cisco XDR, Analytics platforms (e.g., Hadoop), Network Management and automation platforms (e.g., Cisco DNA Center and Cisco Nexus Dashboard Insights), Security Information and Event Management (SIEM) platforms, and Storage/smart capture (e.g., Cisco Security Analytics and Logging).
  - Brokering data – The ability to route and replicate telemetry data from a source location to multiple destination consumers to facilitate quick onboarding of new telemetry-based tools.
  - Filtering data – The ability to filter data that is being replicated to consumers for fine-grain control over what consumers can see and analyze.
  - Transforming data – The ability to transform data protocols from the exporter to the consumer's protocol of choice. This enables SNA and other tools to consume multiple and prior, noncompatible data formats.

  Flow Sensor: Generates flow records from network traffic by monitoring network links, especially useful where native flow data is unavailable. It also provides visibility into the application layer. The Flow Sensor can also generate enhanced encrypted traffic analytics telemetry to be able to analyze encrypted traffic.

  - Layer 7 application visibility – Provides true Layer 7 application visibility by gathering application information.

- Packet-level performance and analysis – Provides true Layer 7 application visibility by gathering application information.
- Alerts on network anomalies – Additional telemetry from the Flow Sensor, such as URL information for web traffic and TCP flag detail, helps generate alarms with contextual intelligence so that security personal can take quick action and mitigate damage.

- **Virtual Appliances (VMware or KVM Hypervisor Environment):** SNA can deploy components as virtual machines within existing virtualization infrastructure. Virtual appliance types mirror their physical counterparts for flexible integration: **Flow Collector (Virtual) Manager (Virtual), Telemetry Broker (Virtual) and Flow Sensor (Virtual).**

- **Cloud and Hybrid Deployments:** Integrate SNA into cloud and hybrid environments for unified visibility and analytics across distributed networks:
  - Virtual appliances can be deployed in public or private clouds to extend monitoring and analytics.
  - Telemetry Broker and Flow Sensor components can help bridge on-premises and cloud environments, ensuring end-to-end coverage.

These options and appliance types allow organizations to tailor Cisco SNA deployments for scalability, performance, and comprehensive security analytics—no matter where their infrastructure resides.

Mapping Cisco SNA to NIST CSF 2.0

		NIST CSF 2.0 Mapping		NIST 800-53 Mapping	
Function	**Category**	**Yes**	**Supports**	**Yes**	**Supports**
Govern (GV)		Non-technical controls			
Identify (ID)	Asset Management (ID.AM)	ID.AM-01, ID.AM-03	ID.AM-02, ID.AM-08	CM-08, PM-05, AC-04, CA-03, CA-09, PL-02, PL-08, PM-07	AC-20, CM-08, PM-05, SA-05, SA-09, CM-09, Cm-13, MA-02, MA-06, PL-02, PM-22, PM-23, SA-03, SA-04, SA-08, SA-22, SI-12, SI-18, SR-05, SR-12
	Risk Assessment (ID.RA)	IR.RA-01, iD.RA-02		CA-02, CA-07, CA-08, RA-03, RA-05, SA-11(02), SA-15(07), SA-15(08), SI-04, SI-05, PM-15, PM-16	
	Improvement (ID.IM)	Non-technical controls			
Protect (PR)	Identity, Management, Authentication, and Access Control (PR.AA)		PR.AA-01, PR.AA-05		AC-01, AC-02, AC-14, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-07, IA-08, IA-09, IA-10, IA-11, AC-03, AC-05, AC-06, AC-10, AC-16, AC-17, AC-18, AC-19, AC-24, IA-13
	Awareness and Training (PR.AT)	Non-technical controls			
	Data Security (PR.DS)		PR.DS-01, PR.DS-02, PR.DS-10, PR.DS-11		CA-03, CP-09, MP-08, SC-04, SC-07, SC-12, SC-13, SC-28, SC-32, SC-39, SC-43, SI-03, SI-04, SI-07, AU-16, CA-03, SC-08, SC-11, SC-16, SC-40, SC-43, AC-02, AC-03, AC-04, AU-09, AU-13, CA-03, CP-09, SA-08, SC-04, SC-11, SC-24, SC-40, SI-10, SI-16, CP-06
	Platfrom Security (PR.PS)	PR.PS-01, PR.PS-04	PR.PS-05, PR.PS-06	CM-01, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-08, CM-09, CM-10, CM-11, AU-02, AU-03, AU-06, AU-07, AU-11, AU-12	CM-07(02), CM-07(04), CM-07(05), SC-34, SA-03, SA-08, SA-10, SA-11, SA-15, SA-17
	Technology Infrastructure Resilience (PR.IR)	PR.IR-04	PR.IR-01, PR.IR-03	CP-06, CP-07, CP-08, PM-03, PM-09	AC-03, AC-04, SC-04, SC-05, SC-07, CP, IR, SA-08, SC-06, SC-24, SC-36, SC-39, SI-13
Detect (DE)	Continuous Monitoring (DE.CM)	DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09		AC-02, AU-12, CA-07, CM-03, SC-05, SC-07, SI-04, AU-13, CA-07, CM-10, CM-11, CA-07, PS-07, SA-04, SA-09, SI-04, AC-04, CM-06, CM-10, CM-11, SC-34, SC-35, SI-07	
	Adverse Event Analysis (DE.AE)	DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-07, DE.AE-08, IR-04, PM-15, PM-16, RA-03, RA-10, IR-08		AU-06, CA-07, IR-04, SI-04, PM-16, IR-05, IR-08, PM-09, PM-11, PM-18, PM-28, PM-30	
Respond (RS)	Incident Management (RS.MA)	Non-technical controls			
	Incident Analysis (RS.AN)	RS.AN-03, RS.AN-07, RS.AN-08		AU-07, IR-04, AU-07, IR-06, IR-08, RA-03, RA-07	
	Incident Response Reporting and Communication (RS.CO)	Non-technical controls			
	Incident Mitigation (RS.MI)		RS.MI-01, RS.MI-02		IR-04
Recover (RC)	Incident Recovery Plan Execution (RC.RP)				
	Incident Recovery Communication (RC.CO)	Non-technical controls			

Technical Features

SNA delivers a robust suite of capabilities designed to provide deep network visibility, detect advanced threats, and streamline incident response across diverse environments. Key features include:

Comprehensive Network Visibility
SNA continuously monitors and analyzes all network traffic—across on-premises, cloud, and hybrid environments—delivering granular visibility into users, devices, applications, and data flows.

Behavioral and Anomaly Detection
By leveraging advanced analytics and machine learning, SNA establishes baselines for normal network behavior and automatically detects anomalies, potential insider threats, and policy violations.

Encrypted Traffic Analytics
SNA analyzes encrypted network traffic for threats and suspicious patterns without decrypting the data, helping organizations maintain privacy while ensuring robust security.

Automated Threat Detection and Response
SNA provides real-time alerts on suspicious activities, lateral movement, command-and-control traffic, and data exfiltration. It can also integrate with Cisco XDR and other security platforms for automated incident response.

Integration with Threat Intelligence and Security Ecosystem
Seamlessly integrates with Cisco and third-party security solutions, such as Cisco Secure Firewall, Cisco Identity Services Engine (ISE), and SIEM tools, to enrich analytics and orchestrate response actions.

Flexible Data Collection
SNA collects and analyzes telemetry from a wide range of sources, including NetFlow, sFlow, IPFIX, and cloud-native telemetry, enabling comprehensive monitoring even in complex, distributed networks.

Centralized Management and Reporting
Unified dashboards provide real-time monitoring, customizable reporting, and intuitive workflows, making it easy for security teams to investigate incidents, track compliance, and manage network security from a single interface.

Scalability and High Performance
Designed to scale from small deployments to large enterprise networks, SNA supports distributed architectures, high-throughput data collection, and robust data storage for long-term analysis.

Incident Investigation and Forensics
SNA maintains detailed historical records of network activity, enabling retrospective analysis, incident investigation, and compliance auditing.

Role-Based Access Control
Supports granular access policies for different users and teams, ensuring secure and appropriate access to analytics and management functions.

Conclusion

The NIST Cybersecurity Framework 2.0 is an essential guide for organizations aiming to manage cybersecurity risk, respond effectively to emerging threats, and build long-term operational resilience. Building on the strengths of the original framework, CSF 2.0 introduces updated guidance to address the complexities of today's digital landscape, including expanded focus areas for governance, supply chain risk management, and continuous improvement. Its flexible, scalable, and comprehensive structure is designed to be adaptable to organizations of all sizes and industries, helping them strengthen security postures, meet regulatory requirements, and ensure the continuity of critical operations.

Cisco SNA is a powerful solution that equips organizations with deep visibility into network activity, advanced threat detection, and streamlined incident response. By leveraging continuous traffic analysis, behavioral analytics, and integration with threat intelligence, SNA helps organizations identify suspicious behaviors, investigate incidents, and reduce dwell time for threats across complex environments.

Aligning SNA with the NIST CSF 2.0 enables organizations to enhance their ability to detect, analyze, and respond to cybersecurity risks, while supporting compliance and fostering collaboration between technical teams and leadership. With its scalability, centralized management, and seamless integration within Cisco's security ecosystem, SNA is a valuable asset for organizations implementing the NIST CSF 2.0—whether building foundational capabilities or optimizing a mature security program.

Resources

Cisco Secure Network Analytics + Splunk At-a-Glance
https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/secure-network-analytics-splunk-aag.html

Cisco Secure Network Analytics Data Sheet
https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/datasheet-c78-739398.html