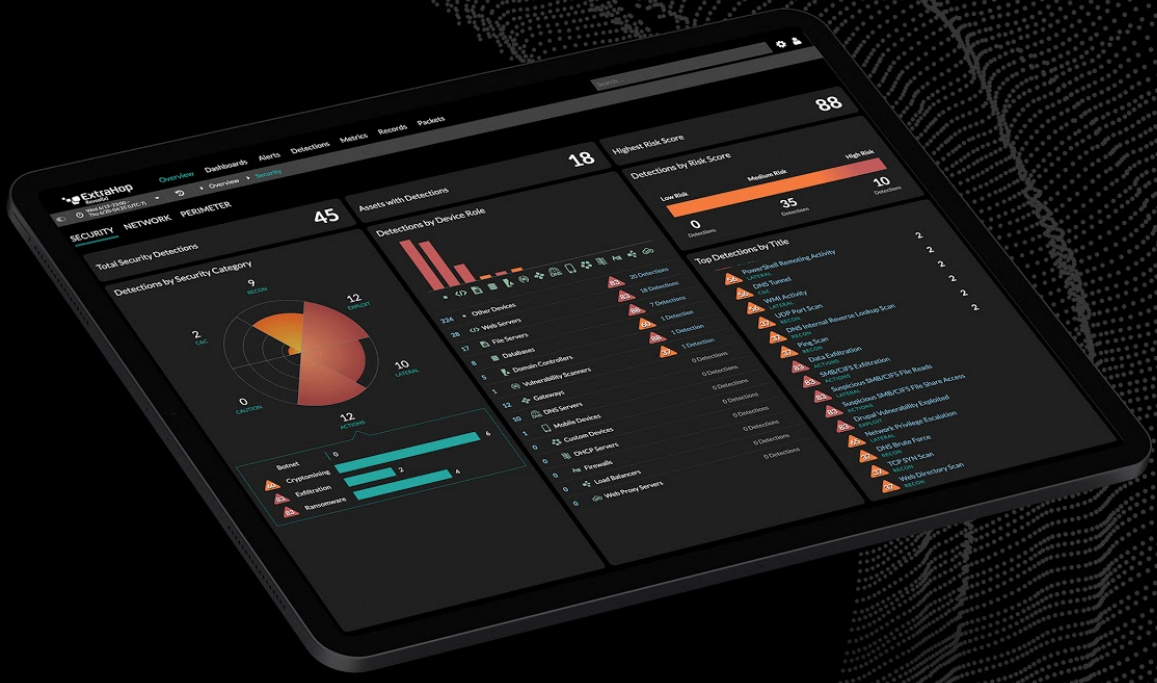
ExtraHop

TECHNICAL BRIEF



How Reveal(x) Supports the NIST Cybersecurity Framework and NIST Special Publication 800-53 Revision 4

Overview

The NIST Framework for Improving Critical Infrastructure Cybersecurity and NIST Special Publication 800-53 Revision 4 are documents detailing guidelines, controls, and best practices to manage cybersecurity-related risk. While initially created for federal organizations, these guidelines and controls are relevant, and widely used, by public and private organizations in a wide range of sectors. This document provides a brief overview of the content and structure of the NIST documents, and explains how ExtraHop Reveal(x) Network Detection & Response supports many key controls.

What are the NIST Cybersecurity Framework and NIST Special Publication 800-53 Rev. 4?

The *NIST Framework for Improving Critical Infrastructure Cybersecurity*, which for brevity we'll call the Cybersecurity Framework (or CSF), is a set of "standards, guidelines, and best practices to manage cybersecurity-related risk."[1] The guidelines in the Cybersecurity Framework are divided into five broad functions: Identify, Protect, Detect, Respond, and Recover. Each function is divided into categories and subcategories. For example, the Identify function has a category called Asset Management, denoted with the four-letter code ID.AM, followed by a number indicating which outcome category (e.g. "physical devices within the organization are inventoried.") is being discussed. The Asset Management category has subcategories for physical device management, software and applications, organizational data flows, and more. Each outcome subcategory includes informational references to the relevant controls from *NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*.

How Do Organizations Use NIST CSF and NIST SP 800-53 R4?

The NIST Cybersecurity Framework is essentially a subset of Special Publication 800-53 Revision 4 that is organized around the five essential functions listed above. This excerpt from the framework does an excellent job summarizing how organizations use it, and the outcomes they can expect:

"Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:
1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk[2]"

These frameworks were written for use by federal agencies managing critical infrastructure, but the guidelines and controls are highly relevant for any organization that wants to understand and improve upon its security posture.

How Does Reveal(x) Network Detection & Response Support Implementation of NIST CSF and NIST SP 800-53 R4?

ExtraHop Reveal(x) NDR uses stream processing to auto-discover and classify every transaction, session, device, and asset in your enterprise at up to 100Gbps, decoding over 70 enterprise protocols and

[1] Source: NIST Framework for Improving Critical Infrastructure Cybersecurity v 1.1
[2] Source: NIST Framework for Improving Critical Infrastructure Cybersecurity v 1.1

extracting over 4,800 features to fuel our cloud-scale machine learning. All this data is used to build predictive behavioral models for every device so that we can detect threats and let you know about suspicious behavior in time to prevent data loss.

Reveal(x) provides at least partial support in all five primary functions of the NIST CSF, and exceptionally strong support in the Identify and Detect functions. The rest of this document provides NIST's description of each of the five functions, along with a brief description of how Reveal(x) supports the listed subcategories.

Identify

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.[3]

NIST CSF Subcategory	Reveal(x) Support	Related Controls from NIST Special Publication 800-53 Revision 4
ID.AM-1: Physical devices and systems within the organization are inventoried	Reveal(x) automatically discovers and classifies every device communicating across the network.	CM-8, PM-5
ID.AM-2: Software platforms and applications within the organization are inventoried	Reveal(x) identifies the operating system and often the applications in use and role being fulfilled by each device communicating across the network.	CM-8, PM-5
ID.AM-3: Organizational communication and data flows are mapped	Reveal(x) automatically discovers and classifies all devices communicating across the network, and can identify the role each device plays, and the peer groups in which it participates. Reveal(x) also enables both automated and manual device grouping, which allows for fine-tuned monitoring of technical and organizational segments.	AC-4, CA-3, CA-9, PL-8

[3] Source: NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1

ID.AM-4: External information systems are catalogued	Reveal(x) automatically discovers and classifies all devices on observed networks, and offers a perimeter view for visibility into external systems communicating with internal systems.	AC-20, SA-9
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Reveal(x) automatically discovers and classifies all assets communicating on the network and uses advanced machine learning to infer criticality and conduct peer group behavior analysis. Reveal(x) also supports manual and automated device grouping for further precise prioritization.	CP-2, RA-2, SA-14, SC-6
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Reveal(x) automatically discovers all devices communicating on the network, identifies their roles, and conducts criticality analysis to identify critical assets that warrant more advanced monitoring and protection.	CP-8, PE-9, PE-11, PM-8, SA-14
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	Reveal(x) offers granular administrative controls, supporting role-based permissions for restricting and customizing access based on internal roles and access policies.	PS-7, PM-1, PM-2
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	Reveal(x) can ingest threat intelligence feeds from third parties in STIX format.	SI-5, PM-15, PM-16
ID.RA-3: Threats, both internal and external, are identified and documented	Reveal(x) can ingest documented threat intelligence in STIX format, and identify when devices or domains communicating with the network have previously been identified as threatening or risky.	RA-3, SI-5, PM-12, PM-16
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Reveal(x) conducts risk analysis on every detection and provides a risk score based on the likelihood, complexity, and business impact of the detected threat.	RA-2, RA-3, PM-16

ID.RA-6: Risk responses are identified and prioritized	Reveal(x) conducts risk analysis on every detection and provides contextual information about attack types, related devices, and potential response and mitigation steps to enable rapid prioritization of potential incidents.	PM-4, PM-9
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations	Reveal(x) observes and analyzes traffic generated by third-party vendors connecting to the network. This capability is often used to hold third-party partners and suppliers accountable for SLAs and policy compliance.	AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12

Protect

Develop and implement appropriate safeguards to ensure the delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.[4]

NIST CSF Subcategory	Reveal(x) Support	Related Controls from NIST Special Publication 800-53 Revision 4
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Reveal(x) analyzes LDAP and Active Directory transactions in real time as they cross the wire, and can, therefore, provide visibility into misuse of credentials, unauthorized access, and the presence of disallowed devices and device types.	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
PR.AC-3: Remote access is managed	Reveal(x) detects and analyze the use of remote access mechanisms like SSH, PsExec, and PowerShell, and can alert on suspicious usage of those protocols.	AC-1, AC-17, AC-19, AC-20, SC-15

[4] Source: NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1

PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Reveal(x) observes and analyzes all traffic on the network and can monitor whether network segmentation is being employed effectively, especially in hybrid cloud environments where implementing and auditing network segmentation has additional challenges compared to on-premises environments.	AC-4, AC-10, SC-7
PR.DS-2: Data-in-transit is protected	Reveal(x) monitors data in motion and detects threats through behavioral analysis of the traffic. By detecting threats in real-time and either alerting or triggering automated response actions, Reveal(x) contributes to the protection of data-in-transit.	SC-8, SC-11, SC-12
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Reveal(x) automatically discovers and classifies all devices communicating across the network, and thereby maintains a current inventory of connected assets at all times. Reveal(x) can identify when assets and services continue to communicate on the network after they were supposed to have been removed, decommissioned, or disconnected.	CM-8, MP-6, PE-16
PR.DS-4: Adequate capacity to ensure availability is maintained	Reveal(x) offers application and network performance monitoring capabilities that enable the rapid diagnosis of issues that impact availability.	AU-4, CP-2, SC-5
PR.DS-5: Protections against data leaks are implemented	Reveal(x) can detect data exfiltration and alert against it, and can trigger automated protective responses by integrating with next-generation firewalls.	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Reveal(x) detects and parses administrative protocols (such as SSH) and remote access tools like PsExec, and can alert when unauthorized remote access occurs.	MA-4

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Reveal(x) continuously analyzes network traffic down to the transaction contents at layer 7, and enables ongoing, real-time auditing of events such as failed logons, administrative privilege usage, failed access attempts to information systems, and more.	AU Family
PR.PT-4: Communications and control networks are protected	Reveal(x) automatically discovers and classifies all of the devices and protocols being used on the network, and can see when weak ciphersuites are in use, or when certificates have expired or will soon. While Reveal(x) doesn't enforce protections, it provides a thorough, real-time way of monitoring for risky communications.	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43

Detect

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables the timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.[5]

NIST CSF Subcategory	Reveal(x) Support	Related Controls from NIST Special Publication 800-53 Revision 4
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Reveal(x) analyzes all traffic on the network, automatically discovers and classifies every device, and builds a continuously refined behavioral baseline driven by 100+ machine learning models for each entity being observed.	AC-4, CA-3, CM-2, SI-4
DE.AE-2: Detected events are analyzed to understand attack targets and methods	Reveal(x) detections include contextual information such as MITRE ATT&CK™ and CIS Top 20 controls references, attack descriptions, risk scoring, and guided investigation steps to allow even less-experienced analysts to rapidly understand targets and methods of a detected attack.	AU-6, CA-7, IR-4, SI-4

[5] Source: NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1

DE.AE-3: Event data are collected and correlated from multiple sources and sensors	Reveal(x) collects real-time wire data from multiple sensors on-premises, in the cloud, and at remote sites, and can ingest STIX-formatted threat intelligence.	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
DE.AE-4: Impact of events is determined	Reveal(x) enables risk assessment and the forensic investigation of incidents to determine the scope of impact.	CP-2, IR-4, RA-3, SI-4
DE.AE-5: Incident alert thresholds are established	Reveal(x) allows the user to set thresholds and other parameters for detections, as well as to build entirely custom detections with static or dynamic thresholds.	IR-4, IR-5, IR-8
DE.CM-1: The network is monitored to detect potential cybersecurity events	Reveal(x) monitors all network activity in real time to detect and respond to security incidents as they occur.	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Reveal(x) monitors all network activity in real time and can detect and alert upon internal security threats, including personnel activities that may constitute malicious or excessively risky activity leading to cybersecurity events.	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
DE.CM-4: Malicious code is detected	Reveal(x) can detect malicious code that crosses the wire, such as SQL commands transmitted from user input fields in a SQL injection attack, as well as many other examples.	SI-3, SI-8
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	Reveal(x) can monitor the connections that external service providers establish with the network, and is often used to detect security events and poor security hygiene, such as the use of deprecated encryption ciphersuites.	CA-7, PS-7, SA-4, SA-9, SI-4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Reveal(x) monitors all network activity and automatically discovers and classifies new devices, users, and operating systems that communicate across the network, allowing for real-time auditing of unauthorized activity.	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4

DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	Reveal(x) provides continuous monitoring and detection of threats in network traffic.	CA-2, CA-7, PM-14
DE.DP-2: Detection activities comply with all applicable requirements	Reveal(x) has both rules-based and behavioral detections. New detections can be built to meet the unique needs of a given environment, and existing detections can be customized with parameters to assure that they are only responding to relevant behavior within the monitored network.	AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
DE.DP-4: Event detection information is communicated	Reveal(x) displays detections within the product, and can also export detection data via REST API to other platforms. The product also has role-based access control, allowing for the granular definition of groups that may access detection information. Reveal(x) also integrates with various ticketing and chat platforms to communicate detection information in real time.	AU-6, CA-2, CA-7, RA-5, SI-4
DE.DP-5: Detection processes are continuously improved	Reveal(x) uses cloud-scale machine learning to build over 100 predictive behavioral models for every device it discovers on the network. These models are continuously updated and used as the basis for detecting threats on the network. New detections are added regularly.	CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Respond

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.[6]

NIST CSF Subcategory	Reveal(x) Support	Related Controls from NIST Special Publication 800-53 Revision 4

[6] Source: NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1

RS.CO-2: Incidents are reported consistent with established criteria	Reveal(x) performs continuous analysis of all traffic crossing the network, allowing for ongoing detection, audit, and reporting of incidents based on an organization's established criteria.	AU-6, IR-6, IR-8
RS.CO-3: Information is shared consistent with response plans	Reveal(x) offers fine-grained control of how event detection information is shared and allows this information to be shared through ticketing platforms. chat platforms, and REST APIs to fully automate responses, or streamline response workflows while keeping a human in the loop.	CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RS.AN-1: Notifications from detection systems are investigated	Reveal(x) detection notifications provide rich context, control framework references, and guided investigation steps with access to transaction records, packet captures, and session keys for decryption to enable the rapid validation and investigation of incidents.	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
RS.AN-2: The impact of the incident is understood	Reveal(x) detections include attack background information, visualizations, and contextual data to enable rapid understanding of the potential incident in progress.	CP-2, IR-4
RS.AN-3: Forensics are performed	Reveal(x) provides access to forensic-level data, including full packet captures and session keys for decryption.	AU-7, IR-4
RS.AN-4: Incidents are categorized consistent with response plans	Reveal(x) provides detection and analysis capabilities essential to timely and effective incident response, as well as forensic investigation capabilities necessary for confirmation that containment and eradication efforts have succeeded.	CP-2, IR-4, IR-5, IR-8
RS.MI-1: Incidents are contained	Reveal(x) provides confident, real-time threat detection and a robust set of integrations with firewall and orchestration (SOAR) products to enable security teams to rapidly scope and contain incidents.	IR-4

RS.MI-2: Incidents are mitigated	Reveal(x) provides an always up-to-date inventory of every device communicating across the network, as well as the protocols and ciphersuites they're using and the expiration status of their certificates. This enables security teams to reduce their attack surface and mitigate against known and unknown threats.	IR-4
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Reveal(x) can detect previously unseen threats, as well as ingest threat intelligence in STIX format from third parties to ensure that newly identified vulnerabilities are either mitigated or documented as accepted risks.	CA-7, RA-3, RA-5

Recover

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.[7]

NIST CSF Subcategory	Reveal(x) Support	Related Controls from NIST Special Publication 800-53 Revision 4
RC.CO-2: Reputation is repaired after an incident	Reveal(x) can provide precise, observed data about the scope of cybersecurity incidents, enabling organizations to understand and appropriately disclose, if needed, the scope of any incident.	None.
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	Reveal(x) provides visibility that enables clear, confident communication about the nature and scope of an incident, and the success of the response efforts.	CP-2, IR-4

[7] Source: NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1