REVERSINGLABS

WHITE PAPER

How To Map Your Cybersecurity Defenses To NIST

Key functions ReversingLabs covers with Advanced Malware Analysis

Executive Summary

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER

No matter the organization's size, cybersecurity can seem like a never-ending mission where success is challenging to define. Companies are moving beyond tribal knowledge and ad-hoc security stacks to a more systematic approach to address the relevant risks to operations. This is particularly true with malware analysis, where manual processes and open source tools hinder detection and response to the vast number of threats seen in the wild. As a result, organizations align their malware analysis and threat intelligence with the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) to create a unified infrastructure that can detect and respond to threats more effectively.

The NIST CSF has become the foundation on which cybersecurity practitioners have built the programs to define best practices and create a unified lexicon for understanding and managing the risks associated with the modern network. ReversingLabs alignment to the CSF creates a language that allows security teams to more freely discuss threats and share data in a way that easily plugs into existing governance processes. Furthermore, the CSF was designed to be flexible allowing application across industries and technologies and can be extended to include industry-specific mandates such as PCI-DSS, HIPAA, and GDPR. The flexibility enables organizations to address the cybersecurity impact on the physical world as well.

ReversingLabs helps organizations meet their security objectives by delivering advanced malware analysis and insights into destructive files and objects. The flexibility of the automated analysis and file reputation platform allows organizations to meet the needs of their security program no matter the industry or how security teams are applying the NIST-CSF Framework. We do this, in part, by delivering the fastest and most accurate insights into threats and supporting the most comprehensive number of file formats in the industry. The hybrid cloud delivery model provides connectors that integrate with EDR, Network Security, Email, SIEM, TIP, and Sandboxes which reduces cyber risk to the organization by providing a consolidated repository for threat analysis and intelligence.

It's important to note, this paper will focus on the areas where the **ReversingLabs Titanium Platform** addresses a specific security control. The open API's within the platform allow for integration that can enhance or improve other controls within the Framework which will not be covered to avoid confusion.

Unique Identifier	Function	Unique Identifier	Category	ReversingLabs Support
ID	Identify	ID.AM	Asset Management	Yes
		ID.BE	Business Management	
		ID.GV	Governance	
		ID.RA	Risk Assessment	Yes
		ID.RM	Risk Management Strategy	
		ID.SC	Supply Chain Risk Management	Yes
PR	Protect	PR.AC	Identity Management	
		PR.AT	Awareness and Training	
		PR.DS	Data Security	Yes
		PR.IP	Information Protection	
		PR.MA	Maintenance	
		PR.PT	Protection	
DE	Detect	DE.AE	Anomalies and Events	Yes
		DE.CM	Security Continuous Monitoring	Yes
		DE.DP	Detection Processes	
RS	Respond	RS.RP	Response Planning	
		RS.CO	Communications	
		RS.AN	Analysis	Yes
		RS.MI	Mitigation	
		RS.IM	Improvements	
RC	Recover	RC.RP	Recovery Planning	
		RC.IM	Improvements	

Controls to Improve Security

IDENTIFY PROTECT DETECT RESPOND RECOVER

The **Identify** function allows for the development of an understanding to manage cybersecurity risk to systems, people, software, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework and enables organizations to focus efforts and resources consistent with their business needs.

Within this function, ReversingLabs solutions improve the **Asset Management (ID.AM), Risk Assessment (ID.RA), and Supply Chain (ID.SC)** subcategories, increasing the understanding of cybersecurity risk and the impact on normal operations. The assessment requires an inventory of organization software and hardware assets, individuals, and workflows, and creates a map for how an organization operates.

	Category	ReversingLabs Titanium Platform
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	• Extends the inventory of physical devices brought into organizations by adding software inventory and image verification to the acceptance criteria before deployment.
	ID.RA-1: Asset vulnerabilities are identified and documented	• Detects advanced threats hidden in published software. • Detects unwanted and malicious functionality and behaviors through in depth analysis while confirming software integrity. • Avoids analysis limitations associated with file size, type and format while allowing users to ensure the software is free from tampering.
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	• Leverages the largest curated file intelligence repository in the industry and supports high speed file analysis capabilities to generate local threat intelligence. • Provides intelligence for Goodware as well as Malware for the most accurate verdicts and detailed classifications possible. • Combines reputation services, threat intelligence, and high-speed analysis that provides users visibility into global and local file threats.
	ID.RA-3: Threats, both internal and external, are identified and documented	• Supports flexible deployment options for the inspection of all files no matter the source. • Combines global threat intelligence with local analysis to provide security teams visibility into specific attack behaviors and threat actors.
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	• Generates risk scores to help security teams focus on the most pressing threats.

	Category	ReversingLabs Titanium Platform
Identify	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	• Verifies that malware or other vulnerabilities are not inserted into the software build and release processes. • Provides a bill of materials (BOM) for software installers and patches. • Supports the creation of a detailed software assessment and inventory that reduces the risk of malware or flaws being introduced to the production environment.
	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.	• Supports software assurance measures as part of vendor contracts to ensure cybersecurity risks are minimized through third-parties.

IDENTIFY PROTECT DETECT RESPOND RECOVER

The **Protect** function helps develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services. While the **Protect** function seems straightforward, organizations can be surprised by the breadth of services that require proper safeguards to support the ability to contain the impact of a potential breach.

Many of the subcategories within the Protect function focus on people and process controls and not technical controls. ReversingLabs supports the **Data Security (PR.DS)** controls, ensuring that both data-at-rest and data-in-transit are protected. Further, ReversingLabs provides capabilities to verify the software used in production has not been tampered with and create an isolated testing environment for malware analysis.

	Category	ReversingLabs Titanium Platform
Protect	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	• Inspects third-party software and firmware packages for known malware before deploying into the organization. • Detects advanced threats hidden in published software, including malware, malformed certificates and improperly signed packages, poorly implemented security mitigations, etc.
	PR.DS-7: The development and testing environment(s) are separate from the production environment	• Provides a unified threat analysis environment spanning automated static and dynamic analysis capabilities to support the full spectrum of software in use. • Adds in-depth analysis to the overall build and release testing procedures and optimizes file analysis to improve accuracy, efficiency, and automation. • Centralizes software analysis and streamlines escalation workflows by enabling secure services, or entities such as a “malware lab”, to analyze prospective software packages prior to release or deployment and sharing corresponding threat intelligence to reduce cyber risks.

The **Detect** function guides organizations to develop and implement appropriate activities to identify cybersecurity events. This function is the most tools-focused and enables timely discovery of cybersecurity events and breaches. The metrics used in this function focus on Mean Time To Detection (MTTD) and Mean Time To Response (MTTR).

ReversingLabs helps organizations reduce the Time To Detection by supporting the **Anomalies and Events (DE.AE) and Security Continuous Monitoring (DE.CM)** controls. These controls focus on automating the threat hunting process and correlating global and local threat intelligence allowing security teams to focus on critical threats. Having the most up-to-date threat intelligence will enable teams to speed the Time To Response, reducing the overall impact of a threat to the organization.

	Category	ReversingLabs Titanium Platform
Detect	DE.AE-2: Detected events are analyzed to understand attack targets and methods	• Provides flexibility to analyze files from multiple sources and provide transparent, context-aware diagnosis. • Automates manual threat research and generates results humans can interpret to take informed action on known and zero-day threats. • Provides high-speed file analysis, data extraction, and classification using advanced technologies like explainable machine learning to accelerate incident response and reduce the organizational impact of an attack.
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors	• Enables threat analysts, researchers, and hunters to work from a unified threat analysis workbench. • Includes indicator sources such as network (URI/URL, IP, Domain) and certificate trust chains. • Consumes files and data from multiple sources across the network allows security teams to have a holistic view of threats.
	DE.AE-4: Impact of events is determined	• Provides the ability to pivot and drill down on all file activities and metadata. • Combines automated static, dynamic, and machine learning analysis engines to provide a complete understanding of malware behavior and exposes malicious obfuscated files intent on evading traditional security detections. • Maps Indicators of Compromise (IOCs) to the MITRE ATT&CK framework automatically.
	DE.CM-4: Malicious code is detected	• Supports advanced hunting and investigations • Supports both global file reputation and data enrichment services by providing threat classifications and rich context on tens of billions of curated files, as well as local analysis and threat detection services across 4000+ file types with the option for private file and data retention if desired.
	DE.CM-5: Unauthorized mobile code is detected	• Instills trust in digital experiences, allowing security teams to scan mobile files and applications and look for complex, hidden attacks. • Enables businesses to function confidently in a digital ecosystem by assuring a chain of trust across repositories.

The **Respond** function helps develop and implement appropriate activities to take action when a cybersecurity incident occurs. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Proper response planning ensures team members know their roles and understand the appropriate actions to take for a specific security incident.

ReversingLabs provides comprehensive, automated static analysis on files entering an organization which improves the **Analysis (RS.AN)** control in part by generating a unique source of threat intelligence and consolidated metadata. This rich, highly relevant file intelligence enhances the correlation and visibility of malware and promotes more effective and efficient malware identification and response. The platform supports detailed forensics helping security teams understand how threats operate, where it originated, and what it may be after, which speeds remediation.

	Category	ReversingLabs Titanium Platform
Respond	RS.AN-1: Notifications from detection systems are investigated	• Enhances threat detection through continual analysis and can provide notifications when the disposition of files change. • Integrates with existing ticketing and response workflows, enriching data, optimizing decision support and enabling automation.
	RS.AN-2: The impact of the incident is understood	• Provides "explainable" threat intelligence in human readable form that advances threat classification beyond good/ bad convictions to better enable customization and automation of response workflows. • Maps IOCs to the MITRE ATT&CK framework which allows teams to understand the threat actors and gauge the level of threats.
	RS.AN-3: Forensics are performed	• Supports YARA rulesets by default. • Allows users to create and edit custom rulesets, as well as synchronize rulesets with other ReversingLabs products. • Supports YARA hunting and retro YARA hunting. • Transformed detailed metadata into human-readable formats to give a detailed understanding of threats.
	RS.AN-4: Incidents are categorized consistent with response plans	• Exposes reporting APIs to support the correlation of data for better visibility into the overall effectiveness of existing security controls and associated exposure risks. • Provides pre-built integrations to simplify workflows, enrich threat data, activate response plans and empower staff to automate playbooks.

The **Recover** function implements appropriate activities to maintain plans for resilience and to restore services that were impaired due to a cybersecurity incident and support the recovery to normal operations.

The Recover function maintains plans for resilience and restores any impaired capabilities or services due to a cybersecurity event. It supports timely recovery to normal operations to reduce the impact from a cybersecurity event and helps you build lessons learned back into your cybersecurity operations. While the recovery function is focused on people and procedural controls, it is vital for the technical tools to provide explainable information that will support post mortem analysis and enhance the improvement of security operations for the next event.
ReversingLabs Explainable Machine Learning supports the recovery function by providing human-readable indicators, with results that are always interpretable by a human analyst.
The underlying idea is simple. If the system makes a classification decision, it must be able to defend that decision with a description it provides for the malware it detects. This puts the human first and makes the machine its ultimate companion.

Conclusion

Building a comprehensive security program requires the merging of people, processes, and technology in ways that focus on continuous improvement while providing the best defenses possible. The NIST Cybersecurity Framework allows security teams to create risk management programs tailored to the needs of the organization while being flexible enough to adapt to the changes in the threat landscape.

ReversingLabs provides solutions that align with the Framework to provide unprecedented visibility into all files within an enterprise and expand use case coverage to include in-depth malware analysis, dynamically improved cyber defenses, local and explainable threat intelligence development and advanced malware detection. Automated static and dynamic analysis has the flexibility security teams need to utilize better shared global threat intelligence to find relevant threats earlier in the attack cycle. The platform's scalability allows room for growth, including quickly adopting new threat models and processes. Finally, Explainable threat intelligence gives organizations a way to mature their security programs and adopt new technologies and use them to deploy new detection, hunt, and response capabilities.

As the industry's most comprehensive threat analysis and intelligence platform, security teams who are looking to improve threat intelligence, application security, hunting, analysis, and rapid response capabilities should evaluate ReversingLabs Titanium Platform as a way to establish a unified malware analysis infrastructure within the NIST Framework.

For more information on the Framework, visit the NIST website with free resources and complete framework documentation.
www.nist.gov/cyberframework

REVERSINGLABS
+1.617.250.7518
sales@reversinglabs.com
www.reversinglabs.com