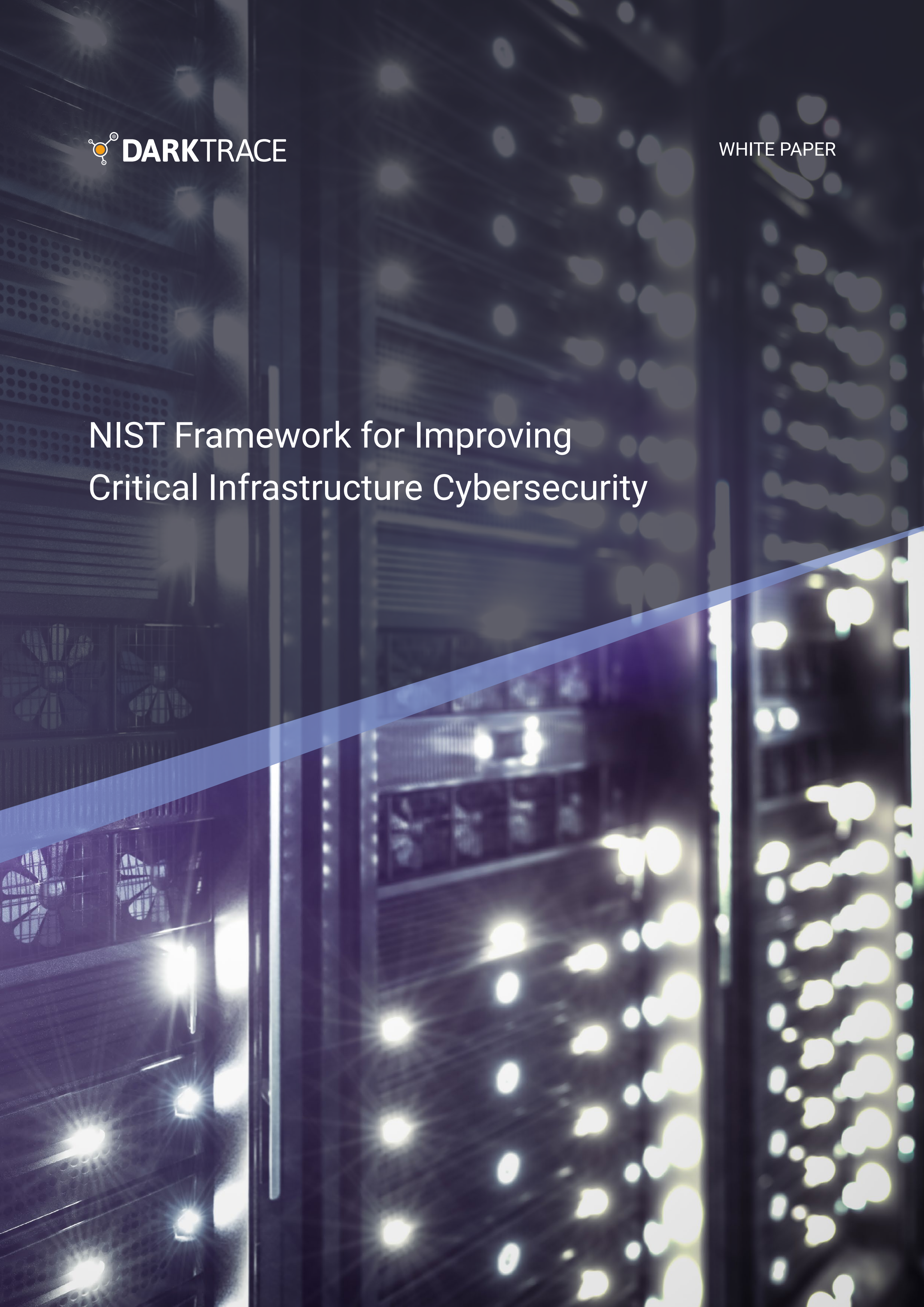
DARKTRACE

WHITE PAPER

# NIST Framework for Improving Critical Infrastructure Cybersecurity



# Executive Overview

The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity is a risk-based framework for analyzing an organization's cyber security across a core set of activities. The Framework assembles proven, industry-leading cyber security standards and practices, providing a coherent set of guidelines to enable organizations to align their approach to cyber security with their business requirements, risk tolerances, and resources.

While primarily aimed at organizations that own or operate critical infrastructure, the Framework can be advantageous for any organization that implements it, in any industry, as it provides concrete guidance on how to measure and improve an organization's cyber security.

The Framework is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles.

## Framework Core

The Framework Core provides a set of activities to achieve specific cyber security outcomes, and presents key outcomes identified by the industry as helpful in managing cyber security risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References.

The five Functions, which organize basic cyber security activities at their highest level, are: Identify, Protect, Detect, Respond, and Recover. The Categories are the subdivisions of a Function into groups of cyber security outcomes closely tied to programmatic needs and particular activities. The Subcategories further divide a Category into specific outcomes of technical and/or management activities.

## Framework Implementation Tiers

The Framework Implementation Tiers provide context on how an organization views cyber security risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4). They describe an increasing degree of rigor and sophistication in cyber security risk management practices, as well as the extent to which cyber security risk management is informed by business needs and is integrated into an organization's overall risk management practices.

These Tiers also reflect a progression from informal reactive responses, to approaches that are agile and risk-informed. Organizations determine their desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cyber security risk to critical assets and resources to levels acceptable to the organization.

Darktrace (Core) and Darktrace Antigena are appropriate for all organizations, up to and including those with Risk Management Processes at Tier 4:

> **"Through a process of continuous improvement […] the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner."**

## Framework Profiles

A Framework Profile is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. Framework Profiles can be used to describe the current state, or the desired target state, of specific cyber security activities. The Current Profile indicates the cyber security outcomes that are currently being achieved. A Target Profile indicates the outcomes needed to achieve the desired cyber security risk management goals. A comparison of these shows the gaps to be addressed to reach the objectives.

## Enterprise Immune System and Industrial Immune System

To learn more about Darktrace's innovative approach to cyber defense, download our white papers: 'Enterprise Immune System' and 'Cyber Security for Industrial Control Systems'.

## Darktrace and NIST

Presented below is a Framework Profile showing the activities and outcomes that can be achieved by implementing Darktrace's Enterprise Immune System or Industrial Immune System within an organization.

### IDENTIFY (ID)

| Category | Subcategory | Darktrace |
|---|---|---|
| **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. | **ID.AM-1:** Physical devices and systems within the organization are inventoried | While not a replacement for a formal asset register, Darktrace's visibility of the network provides a powerful visualization of all active devices for the last 7 days with the added ability to export this from the Darktrace user interface (the 'Threat Visualizer') in .xml format. Since Darktrace sits passively off a network tap or SPAN, it often detects devices that may be overlooked from an initial inventory (e.g. IoT devices). |
| | **ID.AM-2:** Software platforms and applications within the organization are inventoried | Software and applications with a network presence are visible to Darktrace, and can provide a view for comparison or compliance, without the burden of maintaining endpoint agents.<br>Darktrace Cloud Connectors provide added visibility for connections to cloud services. |
| | **ID.AM-3:** Organizational communication and data flows are mapped | Darktrace is ideal for viewing data flows on the network and verifying that they match the design e.g. checking that designated 'internal' servers are only communicating internally. |
| | **ID.AM-4:** External information systems are catalogued | Darktrace provides visibility of external information systems connected to and from the network, and crucially highlights unusual activity to these systems. |
| | **ID.AM-5:** Resources (e.g. hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | The Darktrace Threat Visualizer allows resources to be prioritized, and modeling to be specified based on the critical nature or heightened risk associated with a given device or user. |
| | **ID.AM-6:** Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | Darktrace supports a wide variety of roles with granular permissions limiting each user account. In addition to this, the Anonymization Mode gives users of the Threat Visualizer sufficient visibility to conduct initial triage and to identify incidents while protecting the privacy of employees and other users on a network. |
| **Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cyber security roles, responsibilities, and risk management decisions. | **ID.BE-1:** The organization's role in the supply chain is identified and communicated | |
| | **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | |
| | **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | |
| | **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established | |
| | **ID.BE-5:** Resilience requirements to support delivery of critical services are established | |

| | | |
|---|---|---|
| **Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber security risk. | **ID.GV-1:** Organizational information security policy is established | |
| | **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | |
| | **ID.GV-3:** Legal and regulatory requirements regarding cyber security, including privacy and civil liberties obligations, are understood and managed | |
| | **ID.GV-4:** Governance and risk management processes address cyber security risks | |
| | | |
| **Risk Assessment (ID.RA):** The organization understands the cyber security risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | **ID.RA-1:** Asset vulnerabilities are identified and documented | |
| | **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources | Where permitted, anonymized information from Darktrace deployments is shared across Darktrace's analyst team, who also draw intelligence from public sources.[1]<br>When actioned by the client, breaches can be output in STIX format to be shared with the wider community. |
| | **ID.RA-3:** Threats, both internal and external, are identified and documented | PCAPs, metadata, and logs are stored for a period of time, dependent on the amount of throughput and size of the appliance. The Threat Visualizer allows the review of the data, and relevant threats can be exported and compiled either via the report builder within the UI, or integrated with an existing threat collating platform. |
| | **ID.RA-4:** Potential business impacts and likelihoods are identified | Darktrace is often used to assess cyber security risk by continually monitoring networks for anomalies and compliance breaches. |
| | **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | Darktrace's full network visibility allows the continuous assessment and early mitigation of risks and vulnerabilities. This has proven useful to customers across all industries in their assessment of risk within their network. |
| | **ID.RA-6:** Risk responses are identified and prioritized | Darktrace Antigena is designed to take precise, targeted action with respect to the level of risk posed by a malicious action. Responses can be configured by the organization.[2] |
| | | |
| **Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders | |
| | **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | |
| | **ID.RM-3:** The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | |

## PROTECT (PR)

| Category | Subcategory | Darktrace |
|---|---|---|
| **Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. | **PR.AC-1:** Identities and credentials are managed for authorized devices and users | Darktrace provides full network visibility of unusual, and potentially unauthorized, use of user credentials in devices across the company. |
| | **PR.AC-2:** Physical access to assets is managed and protected | |
| | **PR.AC-3:** Remote access is managed | Darktrace highlights unusual activity over remote access connections and aids investigations. This is particularly powerful for identifying insider threats even when remote access itself is highly secure.<br>Darktrace Antigena can stop or slow unusual activity over remote access connections, buying the security team time to investigate and respond.[2] |
| | **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties | Darktrace highlights unusual access to resources, both where authorized access may be being misused and where unauthorized access is attempted or successful.<br>Additionally, the ability to replay events in history can provide insight into misuse after a human risk is identified. |
| | **PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate | Darktrace learns the normal 'pattern of life' of the network, and the limitations created by segregation forms a significant part of this. It is able to highlight when segregation is broken by unusual connections, and can also be used to investigate the real activity in the network for comparison with the design within the Threat Visualizer. |
| **Awareness and Training (PR.AT):** The organization's personnel and partners are provided cyber security awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. | **PR.AT-1:** All users are informed and trained | |
| | **PR.AT-2:** Privileged users understand roles & responsibilities | |
| | **PR.AT-3:** Third-party stakeholders (e.g. suppliers, customers, partners) understand roles & responsibilities | |
| | **PR.AT-4:** Senior executives understand roles & responsibilities | |
| | **PR.AT-5:** Physical and information security personnel understand roles & responsibilities | |

| | | |
|---|---|---|
| **Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. | **PR.DS-1:** Data-at-rest is protected | |
| | **PR.DS-2:** Data-in-transit is protected | Darktrace has visibility over the encryption state of data in transit. It can be used to compare this with the design, and can also highlight unusual use or lack of encryption. |
| | **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition | |
| | **PR.DS-4:** Adequate capacity to ensure availability is maintained | |
| | **PR.DS-5:** Protections against data leaks are implemented | Darktrace highlights potential data leaks and precursors, such as those resulting from unusual access to resources and associated actions.<br>Where Darktrace identifies a potential data leak in progress, Darktrace Antigena can quarantine or take targeted action to enforce a 'pattern of life', to allow security teams time to investigate.[2] |
| | **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity | |
| | **PR.DS-7:** The development and testing environment(s) are separate from the production environment | Darktrace highlights and shows unusual or unexpected connectivity between development, testing and production environments.<br>Darktrace Antigena can actively block or slow unusual connectivity between the development, test and production environments.[2] |
| | | |
| **Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. | **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained | Darktrace can be used to highlight or check compliance with baseline configurations, where these have effects on network activity. |
| | **PR.IP-2:** A System Development Life Cycle to manage systems is implemented | |
| | **PR.IP-3:** Configuration change control processes are in place | |
| | **PR.IP-4:** Backups of information are conducted, maintained, and tested periodically | |
| | **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met | |
| | **PR.IP-6:** Data is destroyed according to policy | |
| | **PR.IP-7:** Protection processes are continuously improved | Darktrace's core capabilities receive regular updates and improvements. Darktrace's unique application of unsupervised machine learning understands the 'pattern of life' of users, devices and the network as a whole and this understanding evolves with the organization as it changes. |

| | | |
|---|---|---|
| | **PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties | Deploying Darktrace is both a powerful defense capability and a strong statement of intent to relevant parties.<br>As part of Darktrace's service offering, periodic Threat Intelligence Reports collated by the in-house analysts can be used as an effective communication tool.[1]<br>Finally, Darktrace has the ability to export breaches, data and models to several formats to share information where appropriate. |
| | **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | |
| | **PR.IP-10:** Response and recovery plans are tested | |
| | **PR.IP-11:** Cyber security is included in human resources practices (e.g., deprovisioning, personnel screening) | |
| | **PR.IP-12:** A vulnerability management plan is developed and implemented | Darktrace learns the behavior of authorized vulnerability scanning activities and can highlight unusual sources and occurrences. |
| | | |
| **Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. | **PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | Darktrace's visibility and retention of data and metadata can be an additional source of log information. Unusual use of controlled tools can be highlighted for investigation. |
| | **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | Darktrace has visibility over remote maintenance activity and can highlight unusual occurrences. Custom models can be created to routinely highlight such occurrences within the Threat Visualizer. |
| | | |
| **Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. | **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | |
| | **PR.PT-2:** Removable media is protected and its use restricted according to policy | Darktrace can be used in conjunction with other tools that detect and log media use such as USB devices, and can also detect the use of advanced media that makes network connections. |
| | **PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality | Darktrace highlights unusual activity of systems and assets that may indicate unauthorized or unintended use. |
| | **PR.PT-4:** Communications and control networks are protected | Darktrace is a powerful defense of communications and networks.<br>Protection is increased when backed by Darktrace's analyst services, whether as a primary or secondary operating team.[1] |

# DETECT (DE)

| Category | Subcategory | Darktrace |
|---|---|---|
| **Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood. | **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed | Darktrace establishes a 'pattern of life' by leveraging its proprietary machine learning for network operations and data flows, an evolving baseline which incorporates authorized changes over time. |
| | **DE.AE-2:** Detected events are analyzed to understand attack targets and methods | Darktrace detects and highlights unusual events that may indicate cyber-threats. It also provides powerful investigation, historical data and analysis tools to an operator.<br>Darktrace can provide various levels of analysis as a service on some support packages.[1]<br>Additionally, training can be delivered by Darktrace's education specialists. |
| | **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | Darktrace receives a passive copy of all network traffic, data to and from multiple sources. Virtual sensors expand Darktrace's reach into virtualized environments, and Cloud Connectors also incorporate user activity in an organization's cloud services from any location. Log data can also be given to Darktrace so it can be monitored for unusual activity and included for context. |
| | **DE.AE-4:** Impact of events is determined | Darktrace assigns a Threat Score to all highlighted activity.<br>For customers using Darktrace with cyber analyst support services, Darktrace's Threat Intelligence Reports include observed and potential impacts.[1] |
| | **DE.AE-5:** Incident alert thresholds are established | Darktrace's threat score allows users to threshold and triage alerts. |
| **Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cyber security events and verify the effectiveness of protective measures. | **DE.CM-1**: The network is monitored to detect potential cyber security events | Darktrace continuously monitors the internal network and highlights potential cyber security threats. |
| | **DE.CM-2:** The physical environment is monitored to detect potential cyber security events. | Darktrace monitors and records the activity of personnel on the network, where they are identified by devices and user credentials |
| | **DE.CM-3:** Personnel activity is monitored to detect potential cyber security events | Darktrace monitors and records the activity of personnel on the network, where they are identified by devices and user credentials. |
| | **DE.CM-4:** Malicious code is detected | Darktrace does not pre-define what it expects a threat will look like, or what malicious code might attempt. It is therefore able to highlight unpredictable and completely novel threats, while also reacting to established malware activities such as command & control, lateral movement and ransomware. Darktrace is able to detect zero-day attacks, where no signature or rule is known. |
| | **DE.CM-5:** Unauthorized mobile code is detected | |

| | | |
|---|---|---|
| | **DE.CM-6:** External service provider activity is monitored to detect potential cyber security events | Darktrace monitors the whole network, including any interactions it has with other external networks. |
| | **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed | Darktrace highlights unusual and potentially unauthorized devices, connections, and software downloads. |
| | **DE.CM-8:** Vulnerability scans are performed | |
| **Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. | **DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability | Darktrace supports a wide variety of roles and responsibilities with granular permissions limiting each user account and an audit trail of user activity. |
| | **DE.DP-2:** Detection activities comply with all applicable requirements | Darktrace can fulfil the role of an IDS solution for cases where standards and regulations require this. |
| | **DE.DP-3:** Detection processes are tested | Darktrace can be used to defend against, oversee, record, and review Red Teaming activities and penetration tests. |
| | **DE.DP-4:** Event detection information is communicated to appropriate parties | Darktrace can be configured to send alerts through email and to SIEM systems and via the Darktrace Mobile App. Different levels of user access can be assigned appropriate to the user's role. |
| | **DE.DP-5:** Detection processes are continuously improved | Darktrace's core capabilities receive regular updates and improvements. Darktrace's understanding of the 'pattern of life' of users, devices, and networks adapts in real time, as the organization evolves. |

## RESPOND (RS)

| Category | Subcategory | Darktrace |
|---|---|---|
| **Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cyber security events. | **RS.RP-1:** Response plan is executed during or after an event | Darktrace can provide a 24/7 Security Operations Centre (SOC) service as part of some support packages. This expert service performs the early investigation and triage of cyber security incidents as part of a response plan.[1]<br>Darktrace Antigena can form part of a response plan, both as an autonomous, real-time response and as a tool manually activated by the security response team. This includes integration with the Darktrace Mobile App to allow remote interactions with response options.[2] |
| **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. | **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | |
| | **RS.CO-2:** Events are reported consistent with established criteria | |
| | **RS.CO-3:** Information is shared consistent with response plans | |
| | **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans | |
| | **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness | |
| **Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities. | **RS.AN-1:** Notifications from detection systems are investigated | Darktrace's Threat Visualizer is an interface for viewing, triaging, and investigating notifications. Alerts can also be sent to SIEM systems.<br>Darktrace can provide investigations and analysis as part of some support packages, via weekly Threat Intelligence Reports, and/or 24/7 as a Security Operations Centre (SOC).[1]<br>Darktrace can provide training to SOC teams to educate on best practices and system integration of the Enterprise Immune System technology. |
| | **RS.AN-2:** The impact of the incident is understood | Darktrace's analysis services include the communication of observed and potential impact of investigated incidents.[1] |
| | **RS.AN-3:** Forensics are performed | Darktrace is a powerful forensic tool, retaining metadata about the network's past activity and some raw data from past connections. In addition, the Threat Visualizer interface organizes and presents them effectively to an analyst.<br>Darktrace cyber analysts can provide forensic analysis as part of some support packages.[1] |
| | **RS.AN-4:** Incidents are categorized consistent with response plans | |

| | | |
|---|---|---|
| **Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. | **RS.MI-1:** Incidents are contained | Darktrace highlights developing cyber-threats in their early stages, allowing the security team to contain them.<br>Where included in the support package, Darktrace's cyber analysts can quickly communicate early signs of cyber-threats to the customer's security team.[1]<br>Darktrace Antigena can stop or slow a developing cyber-threat, helping to contain it and giving the security team time to catch up.[2] |
| | **RS.MI-2:** Incidents are mitigated | As with containment, Darktrace's early detection of cyber-threats allows security teams to mitigate them more effectively.<br>Darktrace Antigena directly neutralizes threats on its own in real time by blocking their actions, or slowing them down, buying the security team time to catch up.[2] |
| | **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks | |
| **Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | **RS.IM-1:** Response plans incorporate lessons learned | |
| | **RS.IM-2:** Response strategies are updated | |

## RECOVER (RS)

| Category | Subcategory | Darktrace |
|---|---|---|
| **Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cyber security events. | **RC.RP-1:** Recovery plan is executed during or after an event | Darktrace provides both visibility into the network during recovery, and highlighting of continued or newly unusual activity if the state has not been returned to normal. During normal operation, Darktrace's understanding of the network continuously learns and evolves to assist in the restoration after the given event. |
| **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | **RC.IM-1:** Recovery plans incorporate lessons learned | Darktrace's Threat Visualizer can be used as an analytical tool to examine past activity and timelines on the network and aid in learning about both remediation and recovery effectiveness. |
| | **RC.IM-2:** Recovery strategies are updated | |
| **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. | **RC.CO-1:** Public relations are managed | |
| | **RC.CO-2:** Reputation after an event is repaired | |
| | **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams | |

[1] These activities and outcomes are added when Darktrace also performs analysis activities as a service.

[2] These activities and outcomes are added when deploying Darktrace Antigena autonomous response modules alongside Darktrace (Core).

## About Darktrace

Darktrace is the world's leading cyber AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 3,000 organizations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 1000 employees and headquarters in San Francisco and Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.

## Contact Us

North America: +1 415 229 9100

Latin America: +55 11 97242 2011

Europe: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010

info@darktrace.com

darktrace.com