DARKTRACE

DARKTRACE FRAMEWORK MAPPING:

NIST SP800-160 Vol 2

CONTENTS

Summary

This whitepaper examines the core ideas developed in the National Institute of Standard and Technology (NIST) regulations for developing cyber-resilient systems and connects them to the observed threat landscape for OT, as well as Darktrace's technical philosophy and solutions.

NIST and Cyber Resilience

The formalization of resilience by the National Institute of Standards and Technology (NIST) is a welcome development in government guidance for OT cyber security. The previous decade demonstrated repeatedly that most organizations, using the legacy security technologies that were widespread at the time, could not defend themselves against novel and fast-moving attacks or against Advanced Persistent Threats (APTs). This holds in both Enterprise (IT, SaaS, cloud, email) as well as Industrial (OT) environments. To this day, organizations across all industry verticals are still repeatedly falling victim to sophisticated cyber-attacks.

Cyber resilience begins with the understanding that not all threats can be prevented from entering an organization, and, moreover, that attacks might not be easily recognizable. While NIST primarily addresses slower-moving APT type threat scenarios, it also mentions practical requirements to extend protection to faster moving threats as well as outright prevention of threats.

For these purposes, the use of AI is a practical necessity: while simple methods of automation can streamline traditionally human-enacted workflows and make them faster, they cannot fundamentally add anything new.

How Darktrace helps with NIST compliance

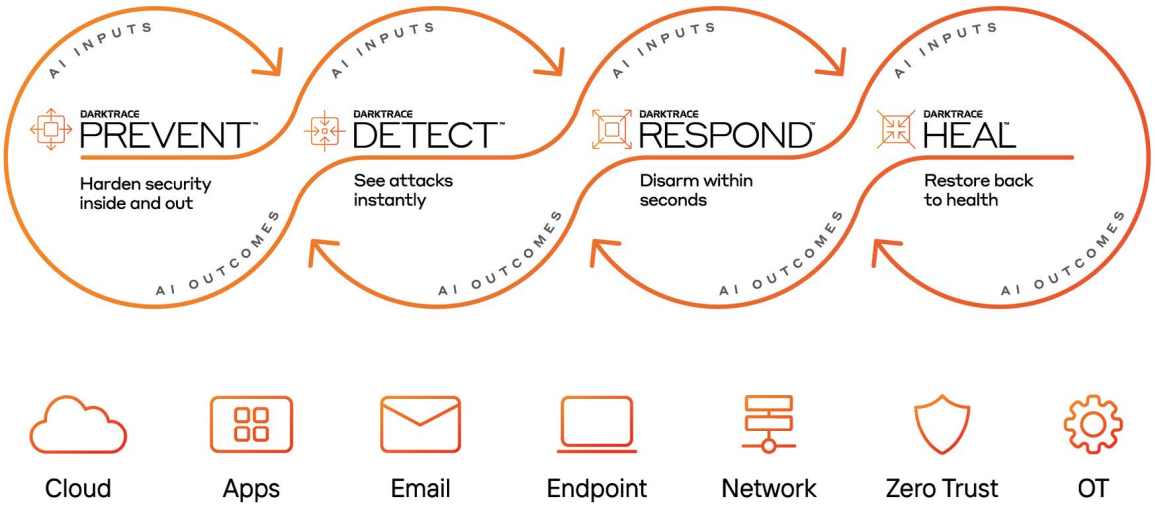
Darktrace's Self-Learning AI, the core technology of the Cyber AI Loop, learns an organization of any size – public or private – from the inside out. It is powered by four AI-powered engines – PREVENT, DETECT, RESPOND, and HEAL – that operate wherever you need them across the entire digital ecosystem - whether on external data, internally in cloud infrastructure or applications, email systems, endpoints, the corporate network, or industrial systems.

Within the Cyber AI Loop are Darktrace DETECT and RESPOND, which action autonomous detection and response capabilities to identify and stop to known and unknown threats.

Specifically for IT/OT environments, Darktrace looks at contextualized factors like metadata to catch threats wherever they occur, bringing top-down visualization of OT environments and passive and active asset identification.

Similarly, Cyber AI Analyst for OT conducts autonomous investigations with specialized models of OT, unifying OT and IT specialists.

Cyber AI Loop



Cyber Resilience Techniques and Approaches

The following 14 techniques are part of the cyber resiliency engineering framework. Here is an overview of how Darktrace's solutions correspond with each technique; more detailed explanations of each correspondence can be provided upon request.

1. **Adaptive Response: Implement agile courses of action to manage risks.** Darktrace RESPOND can autonomously stop potentially known or unknown threats.

2. **Analytic Monitoring: Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way.** Darktrace/OT analysis is based on AI, meaning it is in real-time and can detect novel threats. Similarly, Cyber AI Analyst optimizes threat investigation by continuously examining every security threat that arises. It spotlights the highest priority threats and rapidly synthesizes all of the context around an attack into a natural language report.

3. **Contextual Awareness: Construct and maintain current representations of the posture of missions or business functions considering threat events and courses of action.** Darktrace's Threat Visualizer interface has multiple methods of enhancing awareness including but not limited to the following: asset inventory (passive and optional active); visualization of real-time network activity and user credentials; alert prioritization; and well-explained reports from Cyber AI Analyst.

4. **Coordinated Protection: Ensure that protection mechanisms operate in a coordinated and effective manner.** Darktrace can integrate with other tools in multiple ways, from delivering alerts and reports to a central SIEM, to comparing asset data with peer technologies, to ingesting logs or alerts from other security tools. Moreover, Darktrace components can drive firewalls as part of autonomous response to possible threats.

5. **Deception: Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary.** Monitoring of tainted assets or other deliberate security sinks can be performed by Darktrace/OT.

6. **Diversity: Use heterogeneity to minimize common mode failures, particularly threat events exploiting common vulnerabilities.** Darktrace/OT learns normal activity within a network and then continues to evolve its understanding as the network changes over time. Differences are not problematic for monitoring and consistent activity automatically understood and made use of by the AI.

7. **Dynamic Positioning: Distribute and dynamically relocate functionality or system resources.** Visibility of where resources currently exist and how they are interacted with can be achieved with the Threat Visualizer interface. Dynamic changes are automatically tracked, and the understanding of Darktrace/OT's AI also evolves along with them.

8. **Non-Persistence: Generate and retain resources as needed or for a limited time.** Darktrace/OT requires no user input to evolve its understanding alongside changes made to the network. This means that rapid changes and non-persistent existences do not impose extra workloads.

9. **Privilege Restriction: Restrict privileges based on attributes of users and system elements, as well as on environmental factors.** Darktrace/OT models the activities of users (via credentials) as well as devices and groups of devices that it learns are similar. Use of unintended privileges (or maliciously gained privileges) creates unusual activity that Darktrace actively monitors.

10. **Realignment: Structure systems and resource uses to align with mission or business function needs, reduce current and anticipated risks, and accommodate the evolution of technical, operational, and threat environments.** Darktrace/OT is not a past-signature or prior-intelligence based system; instead, it identifies risks based on its understanding of the business' unique environment and highlights what does not fit in, finding zero-day and novel attacks as they emerge.

11. **Redundancy: Provide multiple protected instances of critical resources.** Darktrace/OT detects unwanted changes regardless of whether they were caused by intentional threat.

12. **Segmentation: Define and separate system elements based on criticality and trustworthiness.** Darktrace/OT provides visualizations of network topology, including ways to automatically specify criticality or other characteristics of systems and view how these separate system elements interact with each other.

13. **Substantiated Integrity: Ascertain whether critical system elements have been corrupted.** Darktrace/OT's detection of unknown threats makes use of information about input interactions with critical systems as well as subsequent activities by those systems.

14. **Unpredictability: Make changes randomly or unpredictably.** While it cannot perform these actions itself, Darktrace/OT's visibility can be used to choose where to make changes that would most heavily impact an adversary. It also evolves along with changes to the environment it observes.

Cyber Resiliency Approaches

Adaptive Response
- Dynamic reconfiguration
- Dynamic resource allocation
- Adaptive management

Contextual Awareness
- Dynamic resource awareness
- Dynamic threat awareness
- Mission dependency and status visualization

Dynamic Positioning
- Functional relocation of sensors
- Functional relocation of cyber resources
- Asset mobility
- Fragmentation
- Distribution functionality

Realignment
- Purposing
- Offloading
- Restriction
- Replacement
- Specialization
- Evolvability

Substantiated integrity
- Integrity checks
- Provenance tracking
- Behavioral validation

Analytic Monitoring
- Monitoring and damage assessment
- Sensor fusion and analysis
- Forensic behavioral analysis

Deception
- Obfuscation
- Disinformation
- Misdirection
- Tainting

Non-Persistence
- Non-persistent information
- Non-persistent services
- Non-persistent connectivity

Redundancy
- Protected backup and storage
- Surplus capacity
- Replication

Unpredictability
- Temporal unpredictability
- Contextual unpredictability

Coordinated Protection
- Calibrated defense-in-depth
- Consistency analysis
- Orchestration
- Self-challenge

Diversity
- Architectural diversity
- Design diversity
- Synthetic diversity
- Information diversity
- Patin diversity
- Supply chain diversity

Privilege restriction
- Trust-based privilege management
- Attribute-based usage restriction
- Dynamic privileges

Segmentation
- Predefined segmentation
- Dynamic segmentation and isolation

Case Studies

To demonstrate the effectiveness of Darktrace/OT, two real examples from anonymized users of the platform are provided below.

The first focuses on how to recognize that threatening behavior is occurring, even when one does not have any prior knowledge of what the threat is and cannot name it. Zero-day ransomware is fast-moving, highly damaging, and usually makes heavy use of encrypted network connections that easily bypass or confuse simple security approaches.

However, this example also demonstrates that a security process reliant on human intervention cannot be left unattended as, despite all the early and accurate detections made by the AI, the threat made a lot of progress due to a lack of human attention.

The second example, by contrast, shows the scenario where Darktrace RESPOND's autonomous response technology is enabled. Here, the attack is brought swiftly to a halt. While in this case the attack was investigated afterwards, there was actually no need to ever know the details of what was blocked.

Example 1

Defending Critical Infrastructure from an Unknown Double-Extortion Ransomware Strain

Darktrace detected every step of an attack as it unfolded over the course of 12 hours against a North American company in the electric grid supply chain. Unfortunately, nobody was watching Darktrace, and autonomous response was not deployed in active mode. Consequently, no action was taken until the following morning when incident response and remediation began.

The attacker gained entry via an Internet-facing vulnerability and escalated their privileges to admin. Darktrace detection: New Admin Credential on Client. The attacker then used encrypted connections to download, install, and initiate a common remote management tool. Darktrace detection: Remote Management Tool on Server.

After this, the attacker exploited the Windows file sharing protocol, SMB, to download GBs of sensitive data and exfiltrate it to a public cloud sharing platform, pcloud, using encrypted HTTPS. Darktrace detection: Uncommon 1 GB Outbound.

The attacker then deployed and executed an unknown ransomware strain using administrative Windows tools and encrypted 1000's files including back-ups. Darktrace detection: Sustained MIME Type Conversion.

In total Darktrace produced 23 alerts for the device in question, or 48% of all the alerts produced in the corresponding 24-hour period.

Evidently, the incident stuck out like a sore thumb. If the customer had been using RESPOND, the activityy would have been neutralized before significant volumes of data were exfiltrated or encrypted.

The customer, however, was able to use the Darktrace Ask the Expert (ATE) service for incident response to mitigate the impact of the attack and aid with disaster recovery.

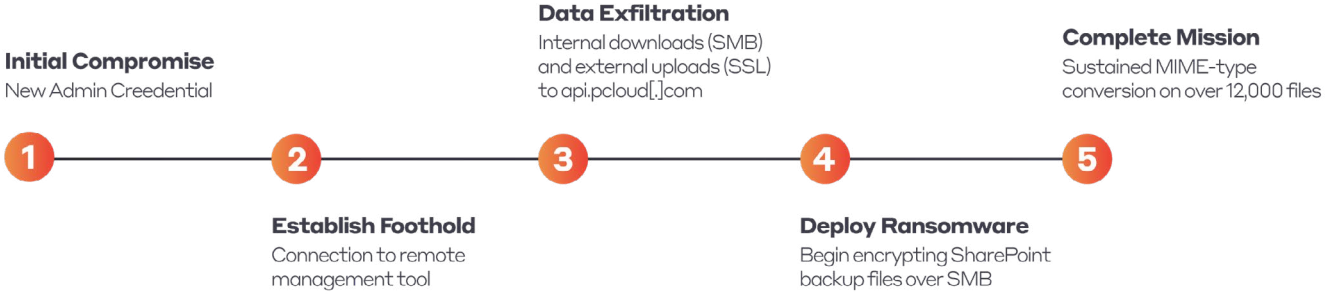
The insights provided by Darktrace helped minimize the damage caused by the attack.

Unaffected systems, including the OT production networks, remained online, while infected systems were isolated to prevent further spread of ransomware.

Lists of the files exfiltrated or encrypted were able to be audited and assessed for business risk, and the remote access backdoors used by the attackers were identified and removed to prevent a repeat of the attack.

The customer was able to return to full operations in a relatively short time, notably, without the level of disruption or reputational damage seen in the Colonial Pipeline and JBS ransomware events, which either directly or indirectly led to shutdown of OT systems.

Read the full blog here



Example 2

How Darktrace Neutralized Zero-Day Ransomware

Darktrace stopped a previously unknown 'zero-day' ransomware attack targeting an electronics manufacturer. This strain of ransomware was not associated with any publicly known indicators of compromise.

However, Darktrace was able to detect and autonomously respond to the threat, neutralizing it before it could do damage.

Darktrace DETECT was able to identify this never-before-seen attack based purely on its comprehensive understanding of the normal pattern of life for every device and user within the organization. Darktrace's AI identified a spike in the pattern of regular connections made by patient zero and a series of high-confidence alerts firing in quick succession.

These included:

Compromise / Ransomware / Suspicious SMB Activity — triggers when a device begins making unusual SMB connections across the organization

Antigena Ransomware Block — triggers Antigena to take an action when the behavior is significantly similar to ransomware

Device / Reverse DNS Sweep — triggers when a device makes unusual reverse DNS lookups, a tactic often used during reconnaissance

Darktrace RESPOND was in Active Mode, and so it enforced the usual pattern of life by blocking anomalous connections for five minutes, immediately stopping the encryption. This successfully neutralized the threat.

To contain the threat at point of impact, RESPOND then stopped the ransomware from spreading by quarantining patient zero for 24 hours, rendering the device unable to connect to the server or any other device on the network.

RESPOND successfully stopped encryption and prevented further lateral spread that could occur by scanning, using harvested admin credentials, or performing internal reconnaissance. The threat was contained while allowing normal business operations to continue as usual, effectively mitigating damage while maintaining business continuity.

Read the full blog here

Conclusion

APPENDIX C.2 DISTINGUISHING CHARACTERISTICS OF CYBER RESILIENCY

"Any discussion of cyber resiliency is distinguished by its focus and a priori threat assumptions. These are reflected in cyber resiliency constructs and engineering practices:

Focus on the mission or business functions.

Assume a changing environment.

Focus on the effects of the advanced persistent threat.

Assume the adversary will compromise or breach the system or organization. Assume the adversary will maintain a presence in the system or organization."

— NIST SP800-160 Volume 2

Deploying Darktrace's cyber security platform is a direct way to introduce cyber resiliency concepts into new or existing cyber security operations.

The solution has proven capable of detecting unknown novel threats as they emerge, and where its autonomous response components are active, it has been shown to defeat these threats without ever having to know what they were.

Organizations across all 16 critical infrastructure sectors rely on Darktrace's AI to achieve truly resilient cyber defense and safeguard their mission critical assets.

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,400 organizations globally from advanced cyber-threats.

Scan to LEARN MORE

DARKTRACE
Evolving threats call for evolved thinking™

North America: +1 (415) 229 9100
Europe: +44 (0) 1223 394 100
Asia-Pacific: +65 6804 5010
Latin America: +55 11 97242 2011
info@darktrace.com
darktrace.com