opentext™ | Cybersecurity

eBook

Zeroing in on Zero Trust

Why federal agencies must take a threat-informed defense approach

Content

Move beyond traditional security controls

Traditional security controls are insufficient in protecting against major security breaches. Why? They tend to be reactive, static, noncontextualized and are often rooted in compliance requirements and IT practices.

Given the evolving threat landscape, organizations must supplement these traditional controls with forward-leaning approaches that leverage global adversary analytics, threat intelligence, automation, and machine-aided models. It is the only way to respond to shifts in threat actor tactics and behaviors.

Threat actors are evolving and adapting

Threat actors research and study widely adopted security standards to circumvent security controls. They leverage and weaponize machine learning and other forms of artificial intelligence to attack the blind spots in security controls that become stale and obsolete in a relatively short period of time. Weaponizing machine learning as part of an attack arsenal gives threat actors a tremendous advantage against many government organizations that rely on traditional security standards and frameworks, which are often forced upon them from compliance mandates.

Threat actors have been known to shift their tactics and behaviors based on information shared in public forums (ex. Virus Total, Joe Sandbox, House Call by TrendMicro) and in the news to continue stealth operations. For example, threat actors have made changes to their infrastructures, such as adding new domains, new IP addresses, new firmware, changes to their code and filenames to remain undetectable.

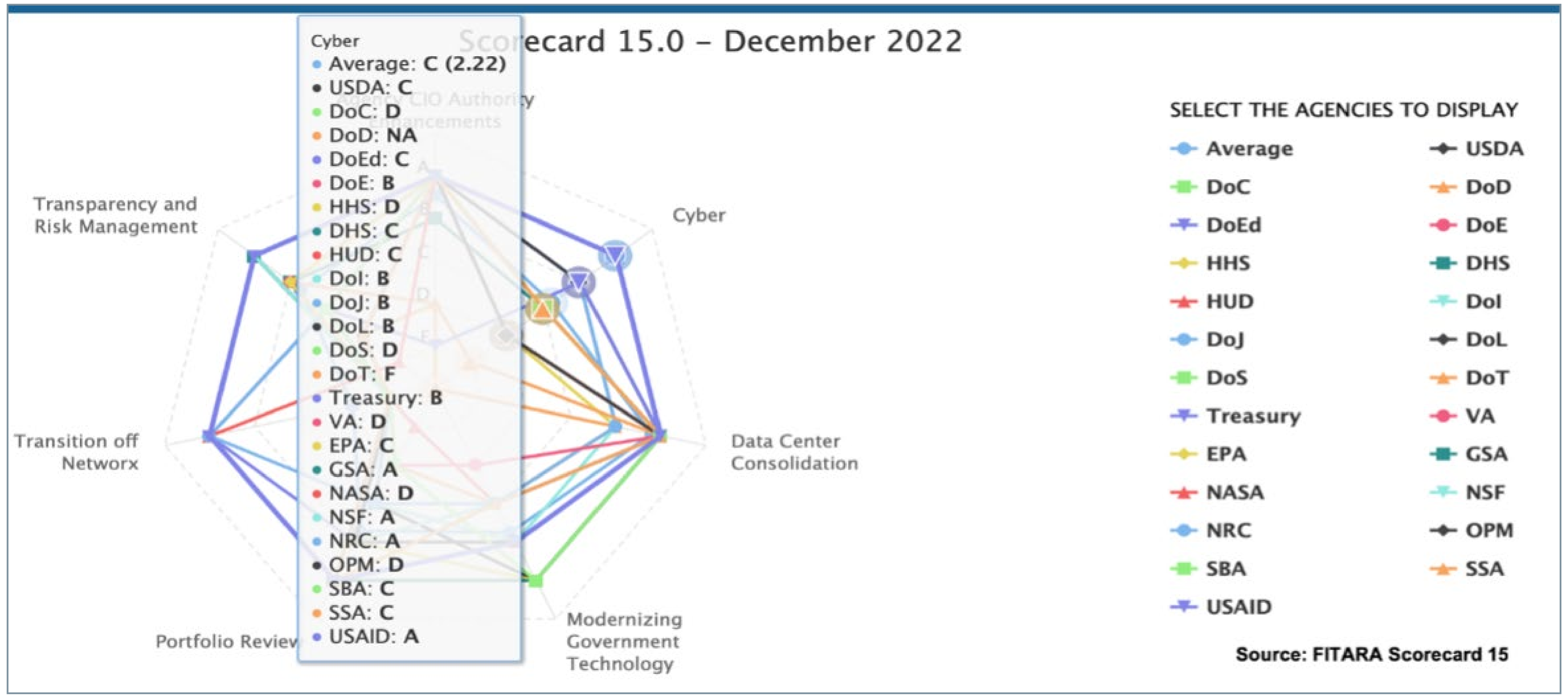
Traditional security controls are not robust enough

While many security standards like NIST SP (Special Publication) 800-53 provide foundational guidance for implementing security controls, they lack the context and awareness to adapt to the shifts in threat actors' tactics and behaviors. Consequently, over time these security controls become stale and are not able to prevent security breaches. Even with the emergence of continuous monitoring activities, organizations still operate behind the power curve with many blind spots in their security control coverage because they do not clearly and fully understand how they are being attacked. As indicated in NIST SP 800-137, ***"The focus of a continuous monitoring strategy is to provide adequate information about security control effectiveness and organizational security status allowing organizational officials to make informed, timely security risk management decisions."*** It should be noted that security control effectiveness considers organizational risk tolerance and is defined in NIST SP 800-53 by whether the security control is implemented correctly, operating as intended and producing the desired outcome for meeting the security requirements of the system that is defined in the organization's system security plan (SSP). While the security controls may satisfy specified requirements from NIST SP 800-53, the advancement in threat actors' tactics and behaviors can make these security controls obsolete and ineffective in preventing security breaches.

In a cybersecurity presentation by researchers from Indiana University Center for Applied Cybersecurity Research titled, “Beyond the Beltway: The Problems with NIST’s Approaches to Cybersecurity and Alternatives for NSF Science,” the researchers identify several problems with the Risk Management Framework (RMF) that are consistent with the fact that traditional security controls are failing us. The researchers point to several problems with the efficiency and effectiveness of the RMF process, with respect to security controls in particular:

- A massive security control list and documentation become a barrier to implementing good security practices.
- Security controls are not prioritized based on risks.
- Security controls are all treated equally, making it tough to prioritize which controls may have a greater impact or significance.
- The vagueness of security guidance makes it difficult to test for adherence.
- RMF promotes quantitative or semiquantitative risk assessment that is time-consuming, based on guesswork and rooted in many assumptions.
- Compliance does not produce a state of security commensurate with reducing risks.

The process is more system focused than mission focused. There is also growing evidence that security controls do not improve an organization’s security posture, as shown here in the FITARA (Federal Information Technology Acquisition Reform Act) Scorecard 15.



Source: FITARA Scorecard 15

Figure-1 FITARA Scorecard 15

Not all security controls are created equally

In the latest release of security controls in NIST 800-53, revision 5, there are 1007 security controls and enhancements, of which 66 are new base security controls, 202 are new enhancements, and 131 are new parameters to existing security controls. The design of these controls is to help organizations focus and prioritize resources toward detecting and mitigating threats and issues that most often lead to security breaches. This leads us to an underlying question about traditional security controls: What security controls are most effective and efficient? Oftentimes, it is difficult to strike the right balance between security and compliance, given one can be compliant and not secure, as seen with security incidents and breach activity. Compliance (a snapshot in time) does not mean security, and security does not mean compliance. They should complement each other to help determine if security controls are commensurate in addressing potential threats and risks.

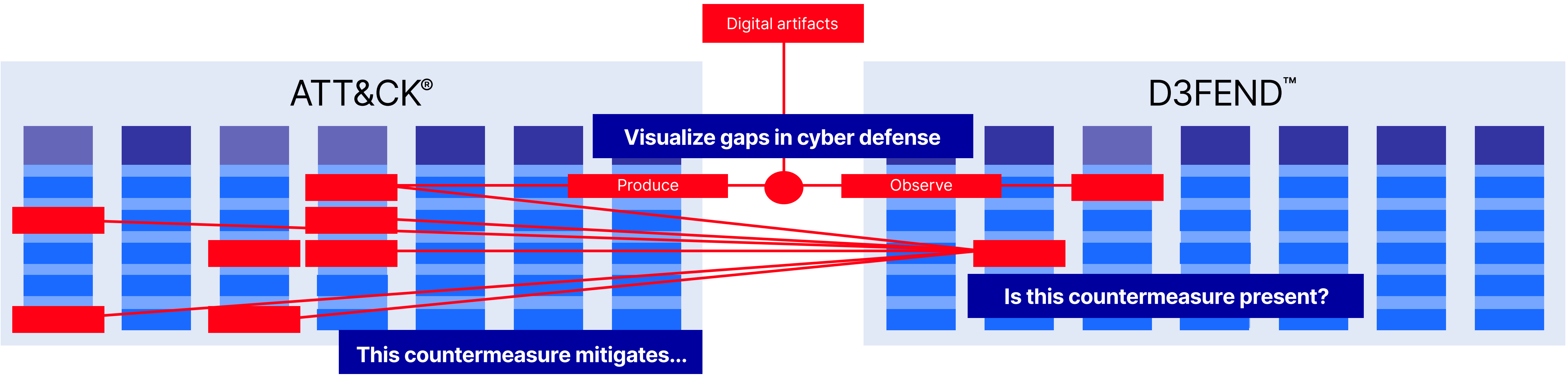

Digital artifacts
ATT&CK®
D3FEND™
Visualize gaps in cyber defense
Produce
Observe
Is this countermeasure present?
This countermeasure mitigates...

Figure-2 MITE ATT&CK and D3FEND Relationship

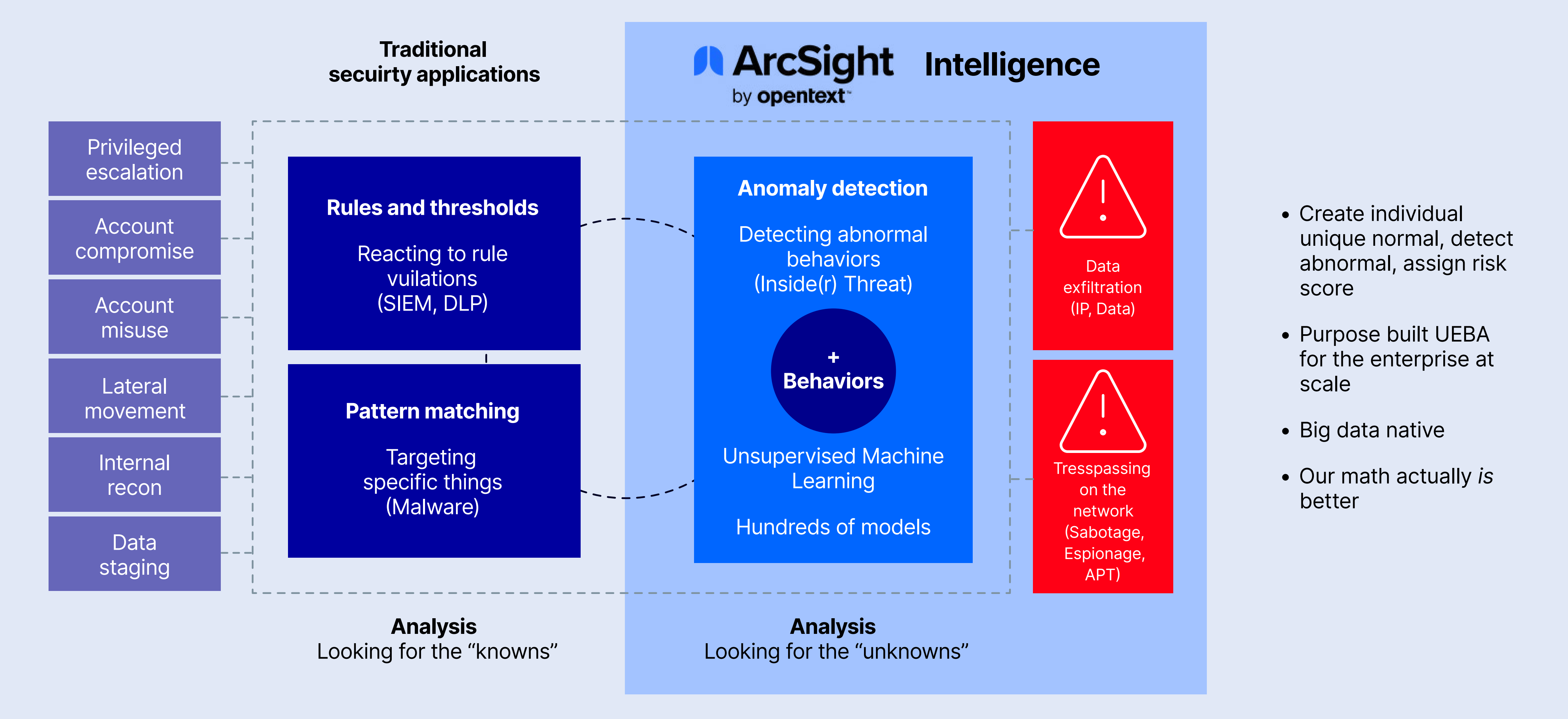
There is a subset of security controls that can be attributed to most security breaches over the last decade or so. The Center for Internet Security (CIS) has its Top 20, the Australian Signals Directorate has its Essential Eight, and MITRE has the ATT&CK mitigations and mappings to NIST 800-53, as well as the D3FEND knowledge base. In terms of the coverage in the D3FEND knowledge base, there are at least 200 prescribed countermeasures, of which 97 are access controls and four are identity related. D3FEND represents countermeasures for ATT&CK techniques and sub-techniques (as shown in Figure-2). However, it does not represent full coverage for threat activity defined in ATT&CK.

Using ATT&CK and D3FEND to prioritize which security controls are most important based on curated threat intelligence is a helpful resource for government organizations to improve cyber defense. The crosswalk between ATT&CK and D3FEND is a great way to visualize potential gaps in cyber defense, which security controls or countermeasures mitigate specific threats, and which security control and countermeasures are most prevalent in mitigating threat actors and can be used to communicate security risk and deficiencies in security posture.

Moving to unconventional security controls

In the book Borderless Behavior Analytics, former Chief Information Security Officer (CISO) of Aetna and Mass Mutual, Jim Routh, talks about implementing what he considers unconventional security controls to keep pace with threat actors. He defines conventional security controls as well-known controls driven by regulatory and compliance mandates, whereas unconventional controls are derived and driven by automation and machine learning to amplify their effectiveness. In essence, it uses risk and threat telemetry to build situational awareness to anticipate, adapt and evolve cyber defenses to counter threat actor behavior and activity. This approach deviates from the norm, where security controls are static and reactive. Its aim is to shift from reactive to proactive cyber defense capabilities by infusing a threat-informed defense approach, which can intelligently implement and apply context-based security controls that fill gaps in cyber defense capabilities.

OpenText™ ArcSight™ Intelligence extracts and pinpoints unknown threats in a sea of Extended Detection and Response (XDR) and Endpoint Detection and Response (EDR) telemetry associated with user entities and behaviors. ArcSight Intelligence is 100% unsupervised machine learning that leverages a plethora of algorithms to establish unique normal behavior baselines to detect the riskiest users and account for anomalies with continuous learning and assessments, as shown in Figure-3.



Traditional securty applications

ArcSight by opentext™ Intelligence

Privileged escalation

Account compromise

Account misuse

Lateral movement

Internal recon

Data staging

Rules and thresholds

Reacting to rule vuilations (SIEM, DLP)

Pattern matching

Targeting specific things (Malware)

Anomaly detection

Detecting abnormal behaviors (Inside(r) Threat)

+ Behaviors

Unsupervised Machine Learning

Hundreds of models

Data exfiltration (IP, Data)

Tresspassing on the network (Sabotage, Espionage, APT)

Analysis
Looking for the "knowns"

Analysis
Looking for the "unknowns"

- Create individual unique normal, detect abnormal, assign risk score
- Purpose built UEBA for the enterprise at scale
- Big data native
- Our math actually *is* better

Figure-3 ArcSight Intelligence Overview

Identifying anomalies and risky behavior associated with users allows departments and agencies to implement conditional access, adaptive authentication, and step-up activities to secure and re-establish the trust of users, devices, and access to sensitive data.

Threat-informed cyber defense

Using a threat context to inform and improve cyber defense is almost non-negotiable in today's cyber battlefield. Applying what is called Threat-Informed Defense, as coined by MITRE, to communicate the benefits of ATT&CK threat intelligence in preventing security breaches is important. Threat-Informed Defense is described by MITRE in the following way:

"Threat-Informed Defense refers to the use of cyber threat intelligence to gain an understanding of our adversaries and then apply that knowledge to cyber defense activities in your security program."

"Threat-Informed Defense applies a deep understanding of adversary tradecraft and technology to protect, detect and mitigate cyberattacks."

Using threat-informed context to guide unconventional controls—and to a larger extent, how Zero Trust (ZT) strategies are to be developed—is an important approach to bolstering cyber defense and mature Zero Trust capabilities. For instance, the Sightings Ecosystem: A Data-driven Analysis of ATT&CK in the Wild, is a way to ensure coverage for the most prevalent threat actor activity and gives a picture of which techniques adversaries use, how their use changes over time and how adversaries sequence techniques.

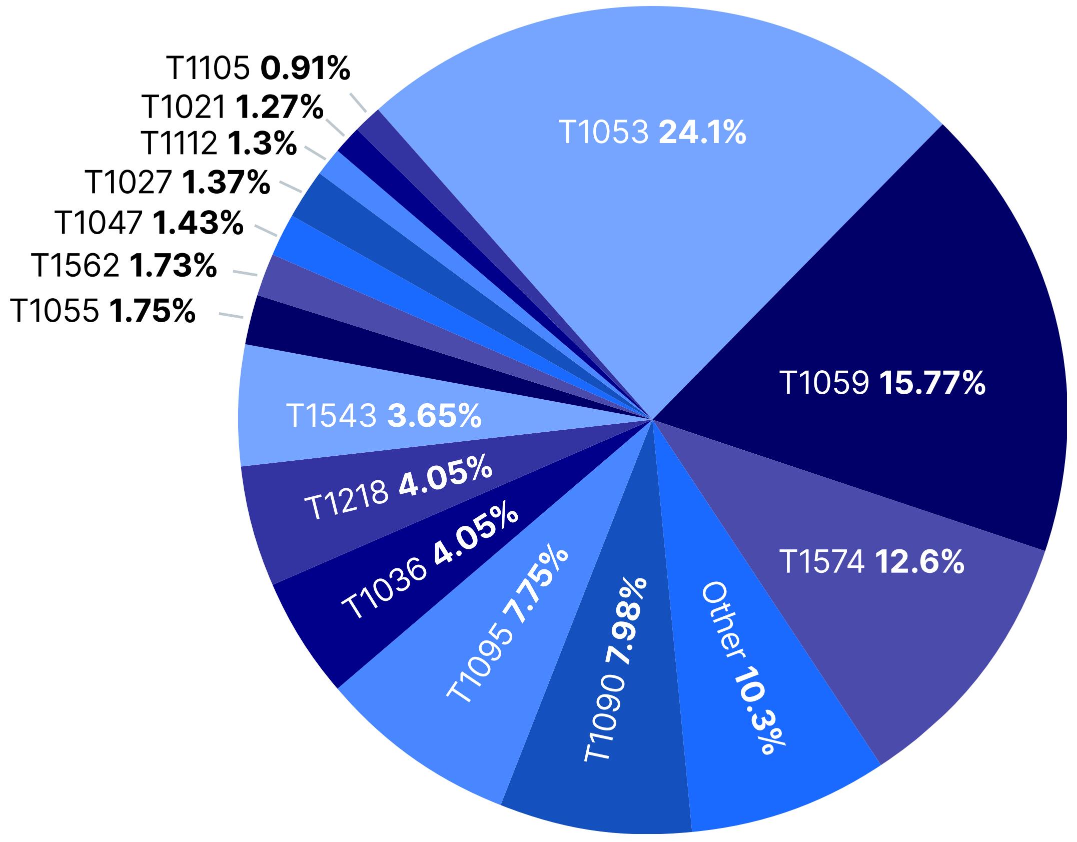
As federal agencies start their Zero Trust journey, at a minimum, their overall Zero Trust strategy should address the Sightings Ecosystem. This means having commensurate D3FEND countermeasures to mitigate associated techniques and sub-techniques, or a plan to address these gaps in cyber defense with other compensating means. Figure-4 addresses the most prevalent ATT&CK sighting, Scheduled Task/Job (T1053), and shows how D3FEND can mitigate threat actor techniques.

This allows federal agencies to do the following:

- D3FEND mappings to NIST 800-53 allow federal agencies to **prioritize security controls** most likely associated with ***adversary behavior.***
- Threat-informed approach helps select, design, and implement security controls to bolster cyber defense capabilities.
- **Mature zero trust strategy** with security analytics and threat intelligence.

The Top 15 Techniques:

1. Scheduled Task/Job [T1053]
2. Command and Scripting Interpreter [T1059]
3. Hijack Execution Flow [T1574]
4. Proxy [T1090]
5. Masquerading [T1036]
6. Signed Binary/Proxy Execution [T1218]
7. Create or Modify System Process [T1543]
8. Process Injection [T1055]
9. Impair Defenses [T1562]
10. Obfuscated Files or Information [T1027]
11. RemoteServices[T1021]
12. Non-Application Layer Protocol [T1095]
13. WindowsManagementInstrumentation[T1047]
14. Modify Registry [T1112]
15. IngressToolTransfer[T1105]



Source: Sightings Ecosystem: A Data-driven Analysis of ATT&CK in the Wild

Maps to

Counters to consider in your ZT strategy

Conutermeasures for T1053 - Scheduled Tesk/Job

off rel	Off artifact	D3FEND Tactic	D3FEND Technique	def rel	def artifact
invokes	Create Process	Detect	System Call Analysis	analyzes	System Call
invokes	Create Process	Detect	Process Spawn Analysis	analyzes	Create Process
creates	Property List File	Deceive	Decoy File	spoofs	File
creates	Property List File	Harden	Local File Presmissions	restricts	File
creates	Property List File	Harden	File Encryption	encrypts	File
invokes	Create Process	Isolate	Executable Allowlisting	restricts	Create Process
invokes	Create Process	Isolate	Executable Denylisting	restricts	Create Process
invokes	Create Process	Isolate	Hardware-based Process Isolation	restricts	Create Process
invokes	Create Process	Model	Asset Vunerability Enumeration	evaluates	Digital Artifact
creates	Property List File	Evict	File Removal	deletes	File
modifies	Task Schedule	Detect	Scheduled Job Analysis	analyzes	Task Schedule
creates	Property List File	Detect	File Analysis	analyzes	File
invokes	Create Process	Isolate	System Call Filtering	filters	System Call
invokes	Create Process	Isolate	Mandatory Access Control	restricts	Create Process

Figure-4 ATT&CK Coverage and D3FEND

Evolving to responsive cyber defense

Cyber defense has always been guided and influenced by threat intelligence to help construct threat profiles around threats that have, will or are currently targeting the mission. Threat intelligence's purpose is to inform and help prepare, prevent, and identify threat actors who are targeting critical mission assets. As threat actors continue to evolve their capabilities, the frequency of activity continues to intensify, requiring the need for tailored or curated threat intelligence to at least keep pace and be more timely and less reactive. Unfortunately, tailored, and curated threat intelligence still does not address the responsive nature required to gain visibility and insight to mitigate threat actors early in the attack life cycle.

Building **situational awareness** around threats to your mission is essential in understanding the *effectiveness* in your cyber defense capabilities.

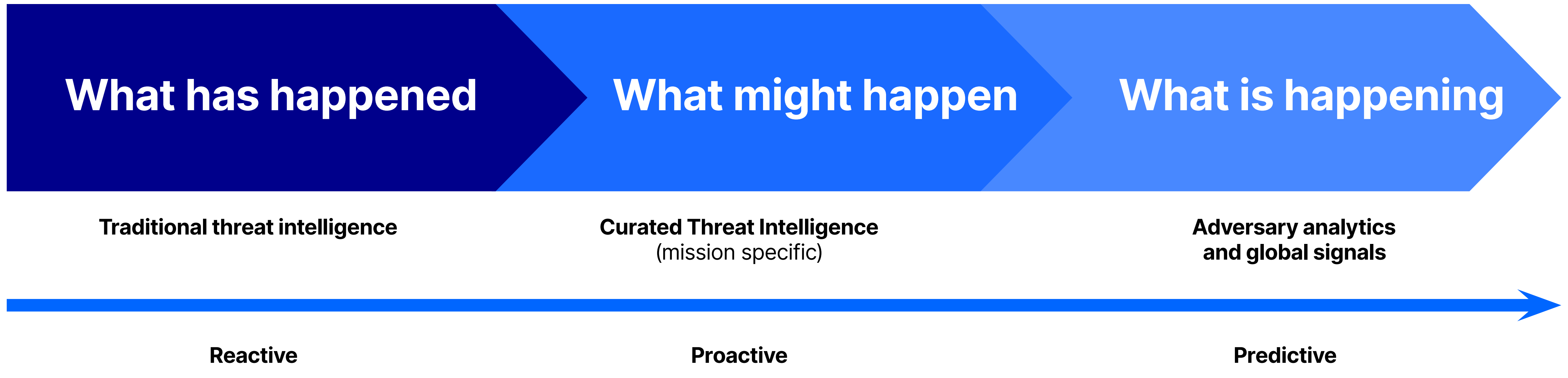


Figure-5 Threat Intelligence Approaches

Understanding what has happened and what might happen (based on what has already happened) is not enough to be responsive to threat actors in today's cyber battlefield. Adding a new dimension as shown in Figure-5 is incredibly important to formalize and gain insights, not only on what may happen, but also on what is happening in near-time, using what is considered "Adversary Analytics and Global Signals." This new perspective allows government organizations to be more proactive in defending against imminent attacks.

Adversary Analytics and Global Signals are designed to tell you what is happening based on adversary signals coming in and out of your "covered space" in near-real time. A covered space is the IP address footprint (your Classless Inter-Domain Routing [CIDR] and Autonomous System Numbers [ASN]) assigned to or used by an organization. This is a shift from traditional threat intelligence, which in most instances only highlights the indicators of compromise (IOCs) that agencies can codify into their daily security operations activities. Global signals around adversary analytics are pre-IOCs and are considered early warnings of an imminent attack. Building situational awareness around threats to your mission is essential in understanding the effectiveness of cyber defense capabilities, which can be used by federal agencies to enhance their Zero Trust strategies.

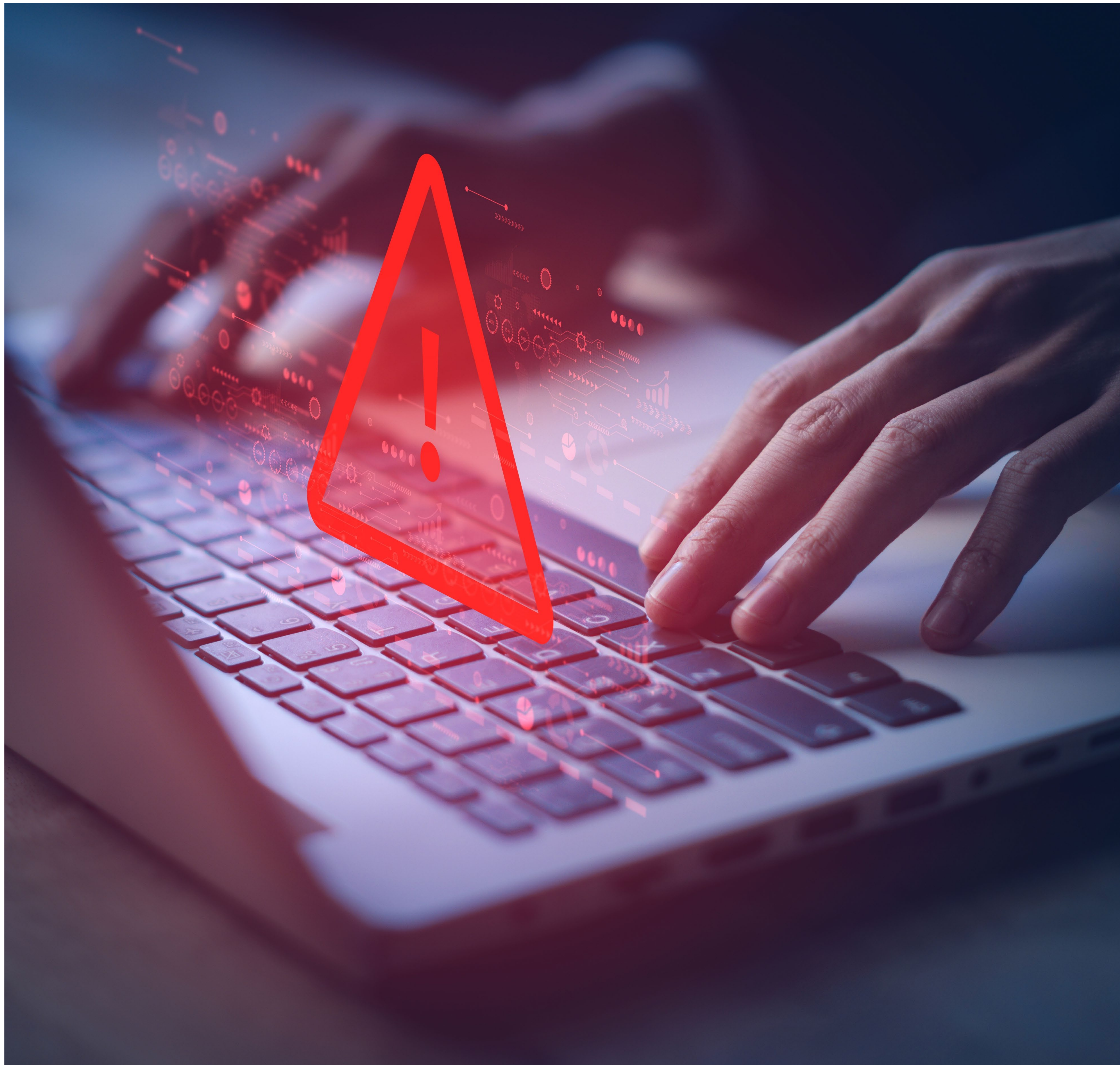
Indications and warnings

Defending and protecting mission capabilities in cyberspace requires early indications and warnings of imminent cyberattacks. Indications and Warnings have traditionally been used by the intelligence community since World War II to inform military strategies.

"Indications and warnings is an intelligence product upon which to base a notification of impending activities on the part of foreign powers, including hostilities, which may adversely affect military forces or security interests."[1]

"Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests."[2]

It is an assessment process that critically analyzes sources of threat intelligence to formulate judgments about the probability or likelihood of specific threats. While this has been primarily used in non-cyber domains, there are synergies in cyber where indications and warnings can identify impending cyberattacks and threats on the internet that are targeting critical mission assets.



(Watson, Watson and Hopple 1990, 594; Grabo 1987, 5).
(Department of Defense 2013, p. GL-12)
https://www.rand.org/pubs/external_publications/EP68144.html

The use of indications and warnings in the cyber domain can help government organizations build early warning capabilities to inform their cyber defense and Zero Trust strategies and achieve greater cyber resiliency against cyberattacks.

Using indications and warnings to “defend forward” helps departments and agencies align with the National Cyber Security Strategy, Pillar 2, Disrupt and Dismantle Threat Actors. This can be done by using global signals from adversary analytics to anticipate impending cyberattacks. From a MITRE ATT&CK perspective, this is before initial access, which is often associated with a critical mission asset being compromised.

The MITRE definition of Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. These techniques include targeted spear phishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited use due to changing passwords.

Indications and Warnings (I&W) Definitions

An analytical process focused on **collecting and analyzing** information from a broad array of sources to develop indicators which can facilitate the **prediction, early detection,** and **warning** of cyber incidents relative to one’s information environment.

Source: 2019 11th International Conference on Cyber Conflict

An **analytic process** where an anticipated scenario in cyberspace is decomposed into indicators that can be continuosly monitored to provide warning of the scenario coming to fruition.

Source: INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Figure-6 Indications and Warnings (Cyber domain)

Implementing early warning capabilities

To answer the question "what is happening" relative to threat intelligence requires early warning signals and telemetry about threat actor behaviors and activities directly from the internet backbone. One way to implement early warning capabilities is to use adversary analytics and global signals to develop the genealogy and ancestral relationships for threat actors using machine-aided models and probabilistic analysis. This is considered Far-Space telemetry because it relies on Layer-4 information directly from the internet backbone. The machine-aided models and probabilistic analysis are used to develop an inspection shield for signals in and out of a covered space. Specifically, it looks for global signals tied to an adversary, threat operations, and likely risky activity.

OpenText™ Cybersecurity can help government organizations develop and formalize early warning capabilities based on adversary analytics and global signals. This capability can be further explained using terminology consistent with threat intelligence. For example, using Warnings of Attack (WoA) and Warnings of Compromise (WoC) provides a clear and consistent way to describe how early warning capabilties can be leveraged from threat intelligence perspective.

WoAs are inbound global adversary signals that indicate in **near time** an adversary **attack or compromise** on critical mission assets and resources.

WoA is based on a high-fidelity machine analysis of far-space telemetry, such as covert operations, honeypots, Border Gateway Protocol (BGP) data and threat intelligence to provide **early warning detection** of an attack.

WoCs are outbound global adversary signals from assets and resources that indicate **suspicious communication** and demonstrate **compromised behaviors**. WoC is based on adaptive risk profiling and contextual analysis to identify and monitor communication pathways to **known infrastructure controlled** by adversaries or infrastructure supporting compromised assets and resources.

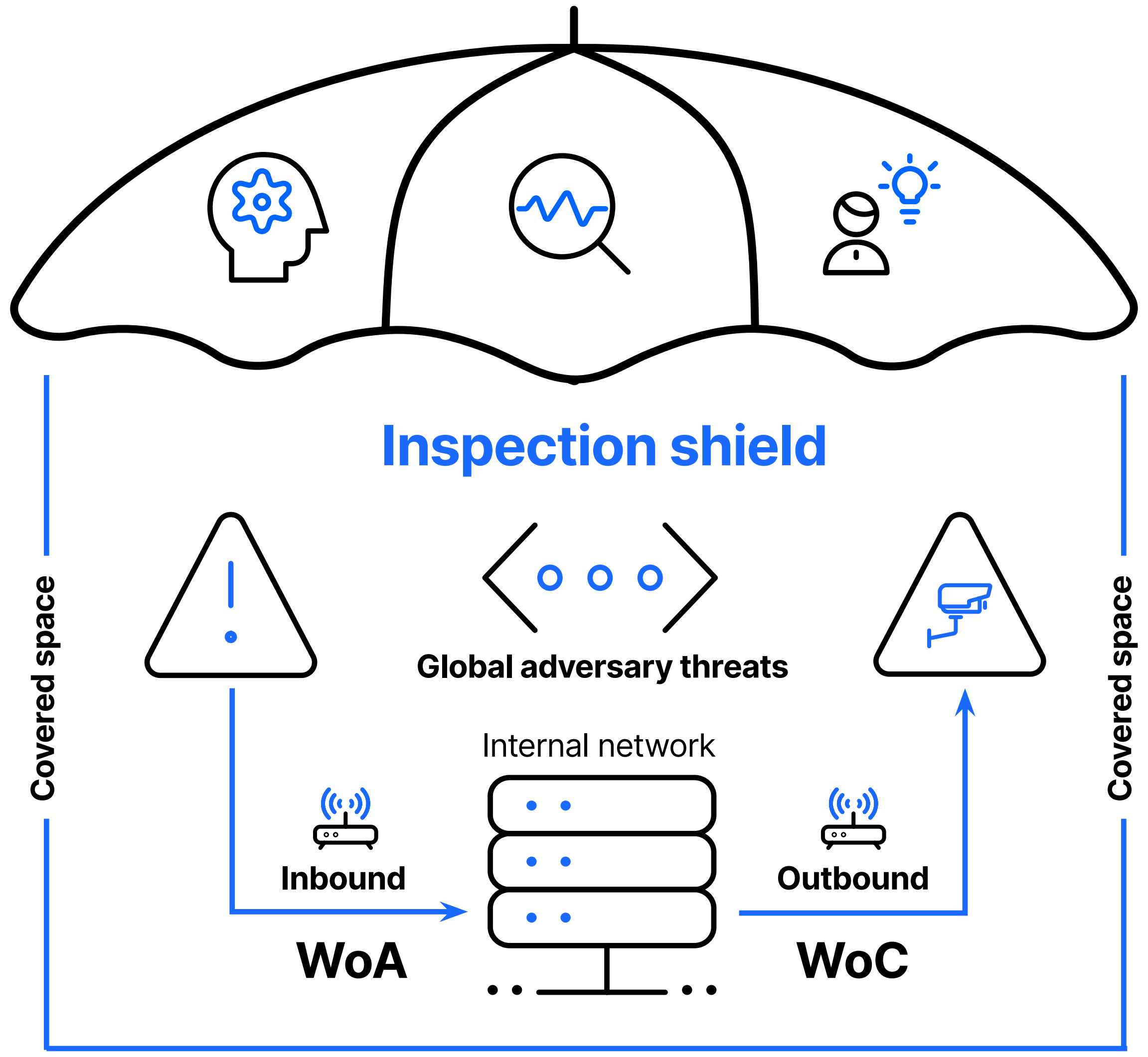
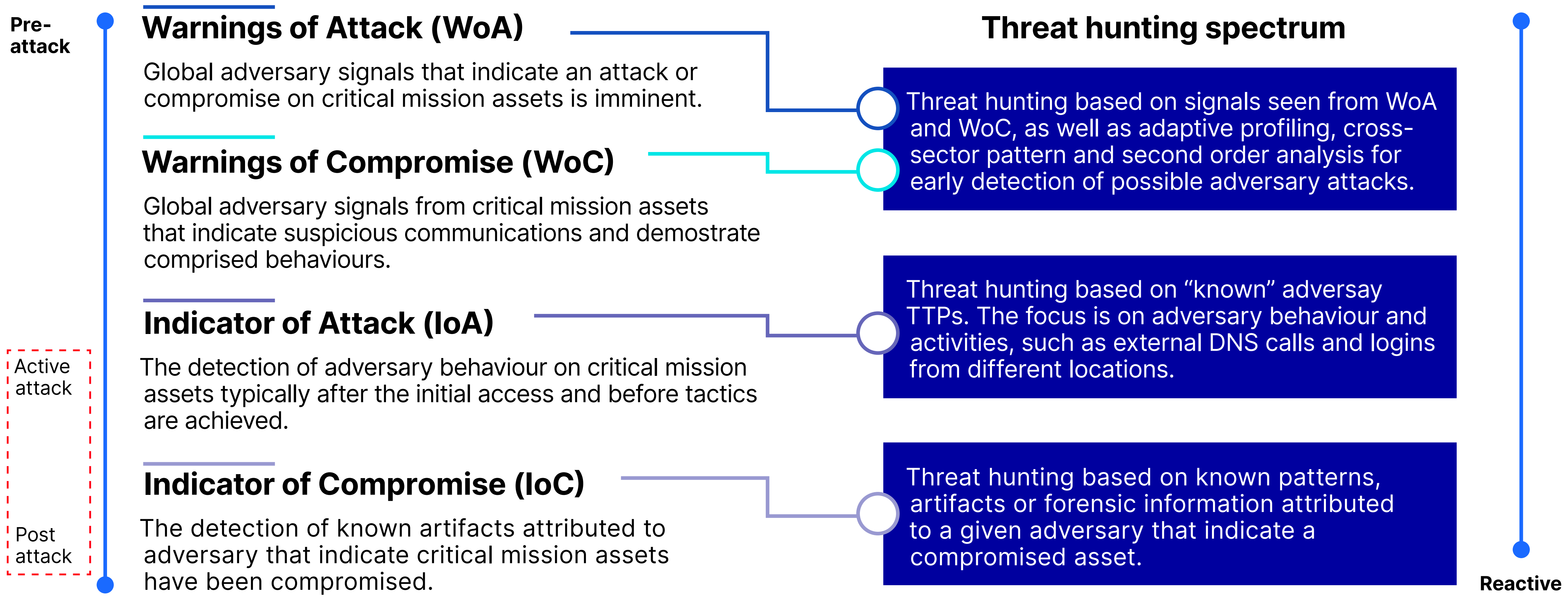


Figure-7 WoA and WoC

Once identified, WoA and WoC provide early warning capabilities to hunt for adversary signals proactively inside the internal network. Threat hunters and cyber defenders can use these signals to hunt for unknown threats hidden in XDR/EDR telemetry. This will allow departments and agencies to “defend forward” and disrupt threat actor behaviors and activities. Furthermore, telemetry data for IoA (Indicator of Attack) and IoC may not yet be available. Far Space signals are too early in the attack life cycle (as shown in Figure 8) and occur before initial access. Shifting to a more proactive approach with early warning capabilites allow you to hunt, rather than be hunted.



Warnings of Attack (WoA)

Global adversary signals that indicate an attack or compromise on critical mission assets is imminent.

Warnings of Compromise (WoC)

Global adversary signals from critical mission assets that indicate suspicious communications and demostrate comprised behaviours.

Indicator of Attack (IoA)

The detection of adversary behaviour on critical mission assets typically after the initial access and before tactics are achieved.

Indicator of Compromise (IoC)

The detection of known artifacts attributed to adversary that indicate critical mission assets have been compromised.

Threat hunting spectrum

Threat hunting based on signals seen from WoA and WoC, as well as adaptive profiling, cross-sector pattern and second order analysis for early detection of possible adversary attacks.

Threat hunting based on “known” adversary TTPs. The focus is on adversary behaviour and activities, such as external DNS calls and logins from different locations.

Threat hunting based on known patterns, artifacts or forensic information attributed to a given adversary that indicate a compromised asset.

Figure-8 Threat Hunting Spectrum

Depending on how early the warning signals are, government organizations can pair adversary emulation (red and purple teams) with threat hunting to assess gaps in cyber defense capabilities before an imminent attack, which would allow federal agencies to evolve and adapt their cyber defenses.

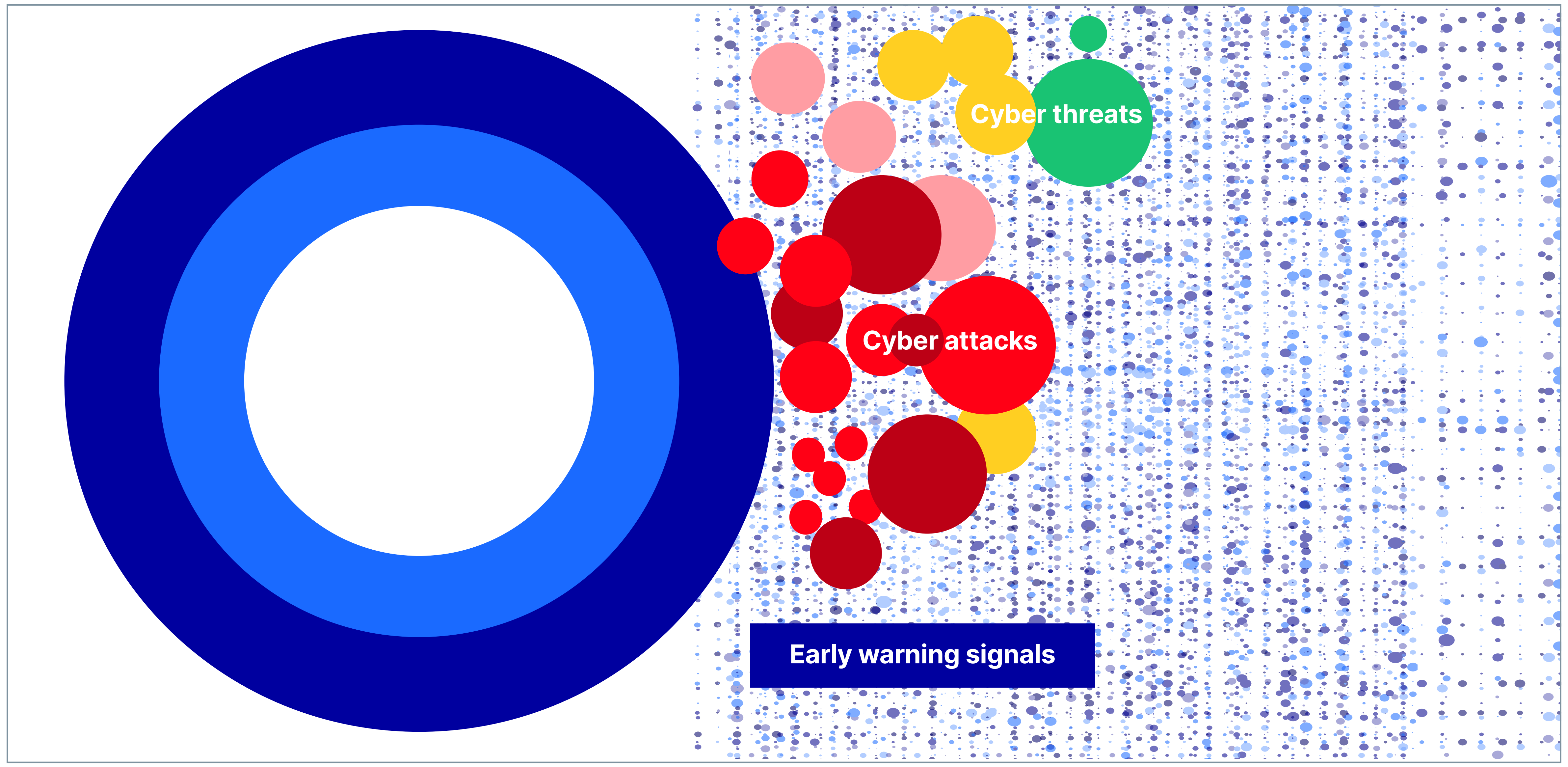


Figure-9 Early Warnings Signals

Early warning signals help organizations:

- Gain visibility into which adversaries are escalating their activity for an imminent attack. This threat information can then be codified into security operations.
- Identify reconnaissance activity and correlate against active adversary campaigns.
- Build situational awareness of threat profiles helps identify lurking cyberattacks.
- Review and assess Zero Trust architecture and strategy for coverage against emerging threats.
- Determine whether targeted exploits are running against other regions/sectors—are they going after a software target first?
- Leverage Security Orchestration, Automation & Response (SOAR) capabilities to scale and automate mitigation activities against adversary threats.
- Leverage threat intelligence and telemetry to enforce adaptive IdAM (Identity & Access Management) controls like conditional access and step-up authentication.
- Automated whitelisting of Tactics, Techniques and Procedures (TTPs) to disrupt threat actor capabilities and force them to modify their campaigns.

A good example of this approach is the APT 29 Spear-Phishing campaign that was supposedly crafted to disrupt the 2018 mid-term elections, as noted in a case study in the “Applying Indications and Warning Frameworks to Cyber Incidents” research conducted by RAND. This research looked at the targeted organization of this campaign and deconstructed how early warning signals and knowledge of threat actor tradecraft helped disrupt the targeted campaign. In preparing for an impending attack, the organization used Cobalt Strike, an adversary emulation platform to assess their cyber defense capabilities against this attack. This led to several counter moves, such as:

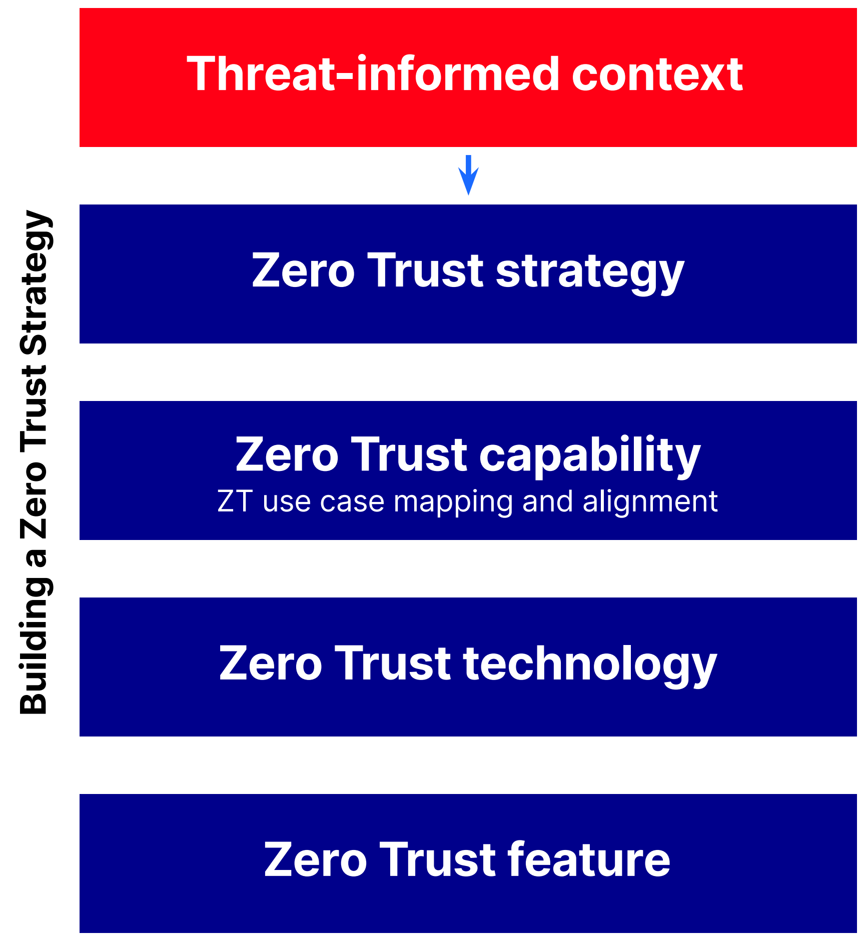
- Security Information and Event Management (SIEM) content was enriched by adversary emulation. SOAR and notification capacities were developed for this threat activity.
- The organization uploaded to Virus Total malware known and associated with threat actor tradecraft.
- Threat hunters became more proactive in hunting for TTPs, and other behavior associated with the threat actor.
- The day before the election (November 5), the Cyber National Mission Force, a unit subordinate to U.S. Cyber Command, posted its first malware sample to the website Virus Total.

Many believed that these counter moves may have delayed the inevitable, given that the actual campaign did not happen until eight days after the mid-term elections on November 14.

Zeroing in on Zero Trust

The National Cybersecurity Strategy endorses zero trust as fundamental in modernizing cyber defense capabilities. Many federal agencies are still trying to figure out how to make the right investments in Zero Trust and build a robust architecture and strategy. It is clear why federal agencies must take a threat-informed defense approach for Zero Trust given the shifts and advancements in threat actor capabilities. The answer is not more security controls, but the enhancements and application of proven controls. Formalizing this strategy across the federal government for Zero Trust is non-negotiable and should help agencies get started on their Zero Trust journey. Over time, a threat-informed defense approach will help mature Zero Trust capabilities and enhance cyber and mission resiliency for all government organizations.

At a minimum, Zero Trust must incorporate a data- and identity-centric approach that protects and secures access to sensitive data, but more importantly establishes clear lines of visibility to detect threats to sensitive data. Often, organizations fail to detect and identify when threat actors target and exfiltrate sensitive data. There have been countless data breaches over the last several years that confirm a lack of visibility and security controls to prevent data exfiltration. Understanding the threat profile and threat actors' tactics and goals should inform Zero Trust strategies.



Adversary targeting sensitive dara for exfiltration

Adversary behaviours and activities targets critical mission assets to gain elevated privileges to access sensitive data exfiltration.

What goals do you want to achieve?

To encrypt all sensitive data by default from creation to disposal. Ensure Business Data Owners have tools for visibility and to manage the "right to access" to sensitive data.

Cross-pillar capability (identify, intelligence, data security)

Implement Data Access Governance (DAG) that incorporates secure access, visibility, protection, automation and governance to bolster cyber resiliency against data breaches.

Aligning ZT capabilities and use cases to technology

Understanding what capabilities products cover that can be address use cases and capabilities associated with DAG - data discovery, classification, minimization, field level encryption and governance.

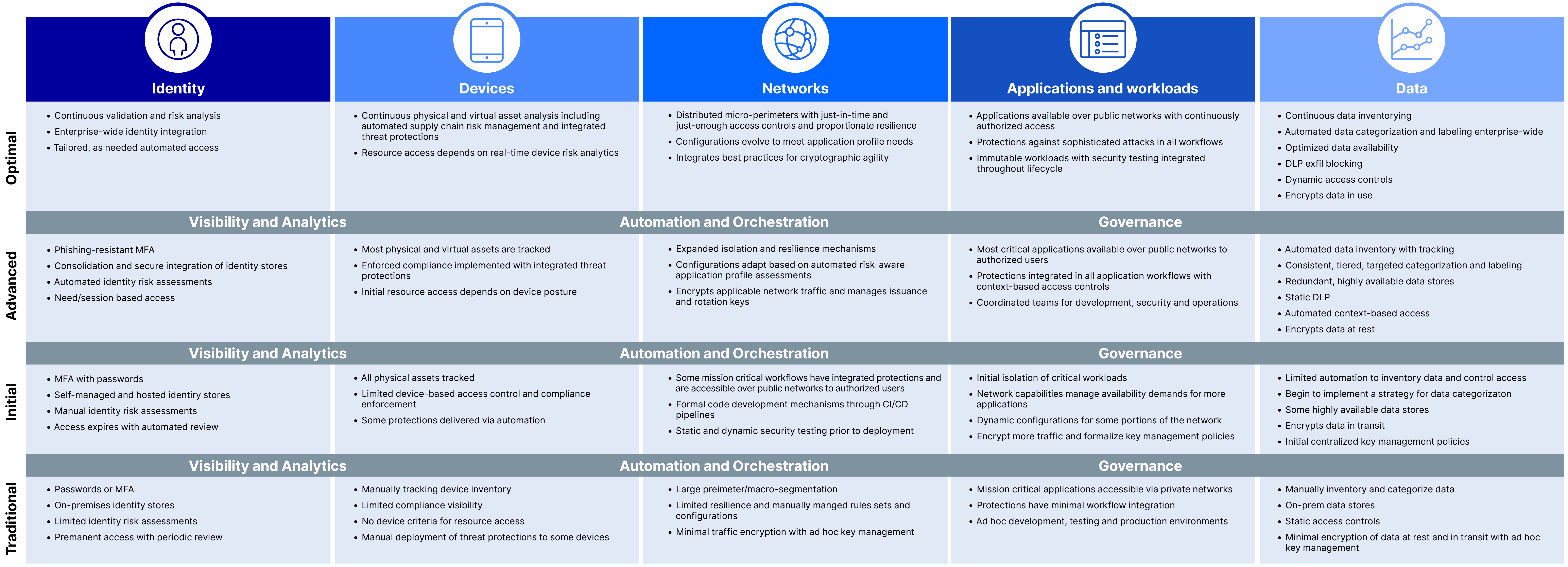
Feature set and coverage

Understanding how product features will enforce Zero Trust framework and principles. This will require mapping product features to Sero Trust capabilities and assess where gaps exists in feature set to augment and complement disparate technologies to extend coverage

Figure-10 Building a Zero Strategy

A threat-informed defense approach will guide federal agencies to make the right investments in capabilities to bolster cyber defense and resiliency. Using threat intelligence to inform Zero Trust is predicated on ensuring the right security controls are prioritized based on how they help mitigate threat actors' techniques and sub-techniques. The process outlined in Figure-10 is a notional way for government organizations to conceptualize how a threat-informed defense approach should influence how Zero Trust strategies, capabilities, technology and features must align to enforce Zero Trust principles.

This process highlights the need to incorporate cross-pillar capabilities to enforce Zero Trust strategies and satisfy use cases around protecting sensitive data. The Cybersecurity and Infrastructure Security Agency (CISA) Foundations of Zero Trust (inspired by the American Council for Technology and Industry Advisory Council) include five core pillar areas as depicted: **Identity, Device, Network, Application Workload and Data**, with supporting capabilities such as Visibility/Analytics, Automation/Orchestration, and Governance. Instantiating cross-pillar capabilities with Data and Identity will help federal agencies mature their Zero Trust strategies as highlighted in CISA Zero Trust Maturity Model 2.0 (as shown in Figure-11), where Initial, Advance, and Optimal maturity levels emphasize cross-pillar integration while leveraging support capabilities (i.e. visibility, automation, orchestration) to mature Zero Trust architecture.



	Identity	Devices	Networks	Applications and workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		Automation and Orchestration	Governance	
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation keys	• Most critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		Automation and Orchestration	Governance	
Initial	• MFA with passwords • Self-managed and hosted identiry stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code development mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorizaton • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		Automation and Orchestration	Governance	
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Premanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large preimeter/macro-segmentation • Limited resilience and manually manged rules sets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Figure-11 CISA High-Level Zero Trust Model 2.0

Optimal—fully automated, just-in-time lifecycles and assignments of attributes to assets and resources that self-report with dynamic policies based on automated/observed triggers; dynamic least privilege access (just-enough and within thresholds) for assets and their respective dependencies enterprise-wide; cross-pillar interoperability with continuous monitoring; and centralized visibility with comprehensive situational awareness.

Advanced—wherever applicable, automated controls for lifecycle and assignment of configurations and policies with cross-pillar coordination; centralized visibility and identity control; policy enforcement integrated across pillars; response to pre-defined mitigations; changes to least privilege based on risk and posture assessments; and building toward enterprise-wide awareness (including externally hosted resources).

Initial—starting automation of attribute assignment and configuration of lifecycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external systems; some responsive changes to least privilege after provisioning; and aggregated visibility for internal systems.

Traditional—manually configured lifecycles (i.e., from establishment to decommissioning) and assignments of attributes (security and logging); static security policies and solutions that address one pillar at a time with discrete dependencies on external systems; least privilege established only at provisioning; siloed pillars of policy enforcement; manual response and mitigation deployment; and limited correlation of dependencies, logs, and telemetry.

OpenText Cybersecurity has many cross-pillar use cases that can help government agencies formalize Zero Trust and create synergistic capabilities to the advanced and optimal maturity levels. Specifically for Building a Zero Trust Strategy (as shown in Figure-10), a cross-pillar workflow with OpenText™ NetIQ™ (Identity) and OpenText™ Voltage™ (Data Protection) can be leveraged to achieve the goal of the Zero Trust strategy while mitigating the adversary threat targeting and exfiltrating sensitive data. For instance, NetIQ can be used to provide identity and data governance, adaptive authentication, and risk scoring, as well as the ability to assign the "right" access while enforcing least privilege access. Voltage can be used to discover sensitive data (structured or unstructured), analyze, and classify sensitive data, and provide tools to control and protect sensitive data off the cloud or in the cloud.

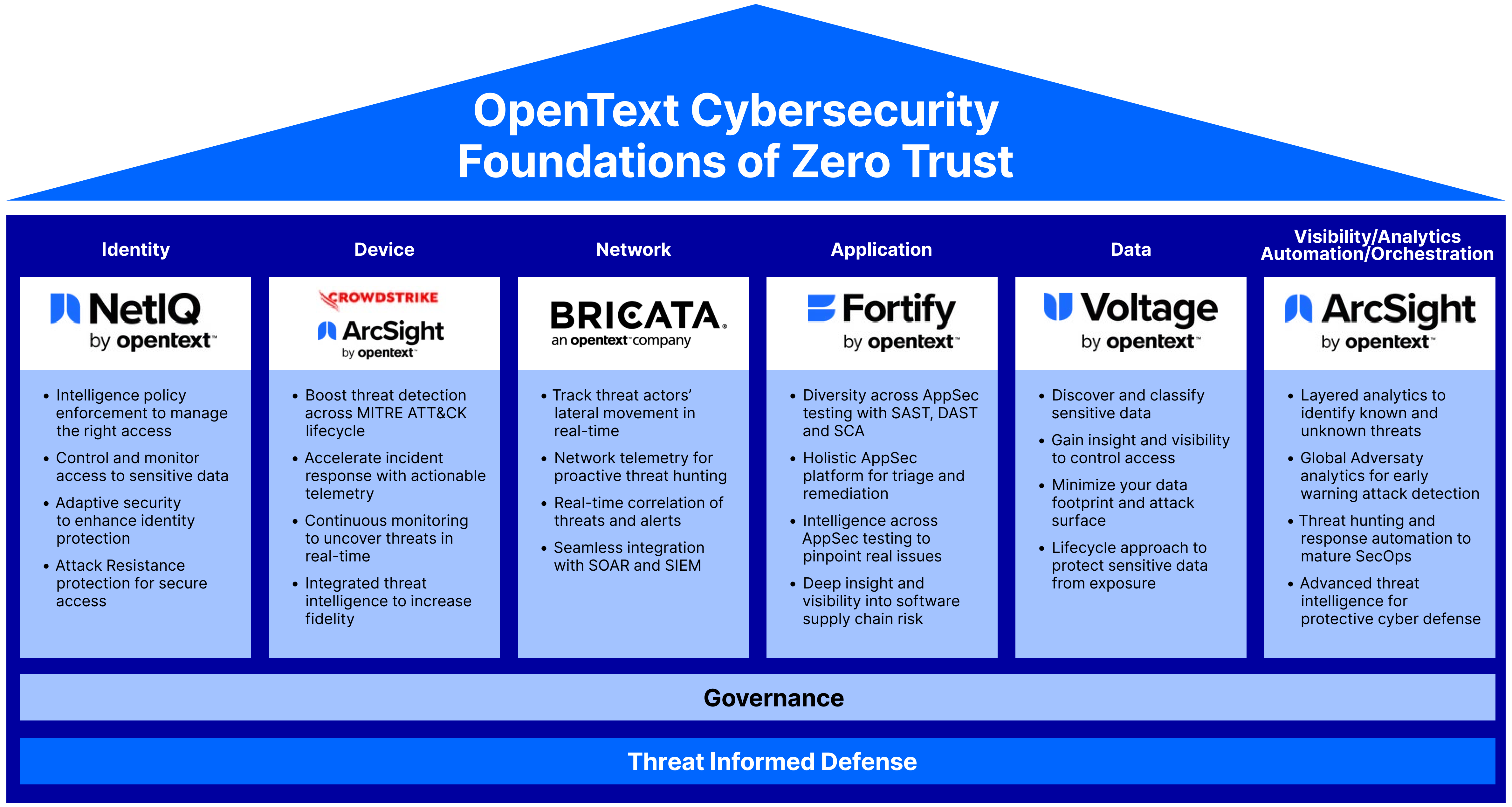
Voltage by opentext™

NetIQ by opentext™

OpenText Cybersecurity Zero Trust approach

OpenText Cybersecurity brings unique value to federal agencies formalizing Zero Trust. We have the breadth and depth (as shown in Figure-12) to establish data and identity-centric context as key components in enforcing Zero Trust principles with cross-pillar capabilities. OpenText Cybersecurity adds intelligence and deep analytics around user behaviors to identify known and unknown threats, as well as provide actionable threat intelligence and early warning capabilities about threat actors to identify gaps and mature Zero Trust strategies.

The use of SOAR and automated workflows provide intelligent responses to adapt to threat actor behavior and activities and evolve cyber defenses. This fortifies the enforcement of Zero Trust strategies to control and protect access to critical mission assets. OpenText's Cybersecurity diverse portfolio across Zero Trust provides departments and agencies the ability to mix and match capabilities for a broad range of use cases. In other words, situational awareness derived from imminent threats against the agency or mission can guide which capabilities to choose. OpenText can help all government organizations make the right investments to bolster cyber esilience while maturing their Zero Trust strategies.



OpenText Cybersecurity
Foundations of Zero Trust

Identity

- Intelligence policy enforcement to manage the right access
- Control and monitor access to sensitive data
- Adaptive security to enhance identity protection
- Attack Resistance protection for secure access

Device

- Boost threat detection across MITRE ATT&CK lifecycle
- Accelerate incident response with actionable telemetry
- Continuous monitoring to uncover threats in real-time
- Integrated threat intelligence to increase fidelity

Network

- Track threat actors' lateral movement in real-time
- Network telemetry for proactive threat hunting
- Real-time correlation of threats and alerts
- Seamless integration with SOAR and SIEM

Application

- Diversity across AppSec testing with SAST, DAST and SCA
- Holistic AppSec platform for triage and remediation
- Intelligence across AppSec testing to pinpoint real issues
- Deep insight and visibility into software supply chain risk

Data

- Discover and classify sensitive data
- Gain insight and visibility to control access
- Minimize your data footprint and attack surface
- Lifecycle approach to protect sensitive data from exposure

Visibility/Analytics
Automation/Orchestration

- Layered analytics to identify known and unknown threats
- Global Adversaty analytics for early warning attack detection
- Threat hunting and response automation to mature SecOps
- Advanced threat intelligence for protective cyber defense

Governance

Threat Informed Defense

Figure-12 OpenText Cybersecurity Alignment with CISA Zero Trust Model

The OpenText Cybersecurity Zero Trust approach is straightforward and fundamental, helping the public and private sector achieve greater cyber and mission resilience.

- **ENHANCE** cyber resilence to deliver mission and business value.
- **ANTICIPATE** disruption and minimize impact.
- Continuously **EVOLVE** cyber capabilities to keep pace with threat actors.
- **ADAPT** to new and emerging threats targeting the mission.

Given the current cyber battlefield with highly skilled and motivated threat actors, government organizations have no choice but to take a threat-informed defense approach to zero in on their Zero Trust priorities.

Resources

- Learn how to combat growing threats and cyberattacks
- The importance of empowering threat hunters with rich analytics
- Request a demo to see transformational threat hunting with intelligence

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market-leading information management solutions, on premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com.

opentext.com

Twitter | LinkedIn | CEO Blog