PROJECT DESCRIPTION

IMPLEMENTING A ZERO TRUST ARCHITECTURE

Alper Kerman
Oliver Borchert
Scott Rose

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Eileen Division
Allen Tan

The MITRE Corporation

DRAFT

March 2020

zta-nccoe@nist.gov

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://www.nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a Community of Interest, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

Abstract

The proliferation of cloud computing, mobile device use, and the Internet of Things has dissolved traditional network boundaries. Enterprises must evolve to provide secure user access to company resources from any location and device, protect interactions with business partners, and shield client-server as well as interserver communications.

A zero trust cybersecurity approach removes the assumption of trust from users and networks. It focuses on accessing resources in a secure manner regardless of network location, user, and device, enforcing rigorous access controls and continually inspecting, monitoring, and logging network traffic. This requires data-level protections, a robust identity architecture, and strategic micro-segmentation to create granular trust zones around an organization's digital resources. Zero trust evaluates access requests and network traffic behaviors in real time over the length of open connections while continually and consistently recalibrating access to the organization's resources. Designing for zero trust enables enterprises to securely accommodate the complexity of a diverse set of business cases by informing virtually all access decisions and interactions between systems.

This NCCoE project will demonstrate a standards-based implementation of a zero trust architecture. Publication of this project description begins a process that will further identify project requirements and scope, as well as the hardware and software components for use in a laboratory environment. In the laboratory, the NCCoE will build a modular, end-to-end example zero trust architecture(s) that will address a set of cybersecurity challenges aligned to the NIST Cybersecurity Framework. This project will result in a freely available NIST Cybersecurity Practice Guide.

Keywords

cybersecurity; enterprise; network security; zero trust; zero trust architecture

Disclaimer

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

Comments on NCCoE Documents

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov/.

Comments on this publication may be submitted to zta-nccoe@nist.gov

Public comment period: April 14, 2020

TABLE OF CONTENTS

1 Executive Summary

Purpose

Traditional network security has focused on perimeter defenses—once inside the network perimeter, users are often given broad access to a number of corporate resources. This means malicious actors can also come from inside or outside the network. Moreover, the growth in cloud computing and the number of remote workers raises the complexity of protecting an organization's digital resources because more points of entry, exit, and data access exist than ever before.

Organizations are being forced to rethink the traditional network security perimeter. A zero trust architecture (ZTA) addresses this trend by focusing on protecting resources, not network perimeters, as the network location is no longer viewed as the prime component to the security posture of the resource.

Zero trust is a set of cybersecurity principles used to create a strategy that focuses on moving network defenses from wide, static network perimeters to focusing more narrowly on users, systems, and individual or small groups of resources. A ZTA uses zero trust principles to plan and protect an enterprise infrastructure and workflows. By design, a ZTA environment embraces the notion of no implicit trust toward systems and users regardless of their physical or network locations (i.e., local area networks versus the internet). Hence, a ZTA never grants access to resources until a user and device are thoroughly verified by reliable authentication and authorization.

This document defines a National Cybersecurity Center of Excellence (NCCoE) project to help organizations design for zero trust. This project will produce an example implementation of a ZTA that is designed and deployed according to the concepts and tenets documented in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, *Zero Trust Architecture* [1]. More specifically, the primary objective of this project is to demonstrate a proposed network topology that brings into play different enterprise resources (e.g., data sources, computing services, and Internet of Things [IoT] devices) that are spread across on-premises and cloud environments and that inherit the following ZTA solution characteristics:

- All network traffic is encrypted regardless of network location within the topology.
- Access to each enterprise resource is authorized on a per-connection basis, and an authorized connection will not automatically permit access to different enterprise resources.
- Access to enterprise resources is determined dynamically based on the following information captured within the environment:
    - organizational policies that apply to:
        - user
        - network location
        - enterprise device characteristics
        - time/date of access request
        - enterprise resource characteristics
    - observable state of:
        - device identity requesting access
        - enterprise asset requesting access
    - previously observed behavior surrounding the user/device identity and access request

- Enterprise assets, devices, and resources are identified and continually reassessed and monitored to maintain them in their most secure states possible.
- User and device interaction are continually monitored with possible reauthentication and reauthorization by using multifactor authentication.
- Information about the current state of the network and communications is logged and leveraged later for better policy alignment to increase the enterprise's overall security posture.

A secondary objective of this project is to identify, and minimize where possible, the negative impacts on user experience as a result of employing a ZTA strategy with the solution characteristics described above. A successful ZTA solution should introduce as little friction to the user experience as practicable.

This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses the project objectives.

Scope

The current understanding of zero trust is focused on the enterprise. A generalized enterprise information technology (IT) infrastructure combines users (including employees, contractors, and guests), devices, and resources that are hosted on-premises, in the cloud, or some combination of the two. There may also be branch offices, remote workers, and bring-your-own-device usage that complicates formation and enforcement of access policies.

This project will focus primarily on access to enterprise resources. More specifically, the focus will be on behaviors of enterprise employees, contractors, and guests accessing enterprise resources while connected from the corporate (or enterprise HQ) network, a branch office, or the internet. Access requests can occur over both the enterprise-owned part of the infrastructure as well as the public/nonenterprise-owned part of the infrastructure. This requires that all access requests be secure, authorized, and verified before access is granted, regardless of where the request is initiated or where the resources are located.

Assumptions/Challenges

Many organizations are looking to build for zero trust, but challenges exist. Current challenges to implementing a ZTA include:

- maturity of vendor products to support a ZTA
- an organization's ability/willingness to migrate to a ZTA because of:
  - heavy investment in other (legacy) technologies
  - lack of ability and/or resources to develop a transition plan, pilot, or proof of concept
- security issues such as:
  - compromise of the zero trust control plane
  - ability to recognize attacks
- interoperability considerations of ZTA products/solutions with legacy technologies such as:
  - standard versus proprietary interfaces

    - ability to interact with enterprise and cloud services
- User experience. To date, there has been no detailed examination of how a ZTA would or could impact end-user experience and behavior. The goal of a ZTA should be to enhance security and provide a largely seamless user experience.

This practice guide aims to mitigate these challenges with the solutions and collaborators that will be selected for the demonstration project.

Background

Historically, the perimeter-based network security model has been the dominant model for information security. It assumes that users inside the corporate network perimeter are “trusted” and anyone on the outside is “untrusted.” For several decades, this view of trust has served as the basis for determining what resources a user/device can access.

Several high-profile cyber attacks in recent years, including the Office of Personnel Management breach in 2015, have undermined the case for the perimeter-based model. Moreover, the perimeter is becoming less relevant due to several factors including the growth of cloud computing, mobility, and changes in the modern workforce. It is with this backdrop that the Federal Chief Information Officer (CIO) Council engaged the NIST NCCoE in 2018 to help federal agencies coalesce around a definition for ZTA and understand the benefits and limitations of a zero trust architecture. The interagency collaboration resulted in publication of NIST SP 800-207, *Zero Trust Architecture*.

This NCCoE project description builds on the work with federal agencies and the Federal CIO Council as we seek to build and document an example ZTA using commercially available products and that aligns to the concepts and principles in NIST SP 800-207.

2 Scenarios

Responses from industry organizations that express interest in participating in this project will affect the potential scenario set in terms of the composition and number of scenarios demonstrated.

Scenario 1: Employee Access to Corporate Resources

An employee is looking for easy and secure access to corporate resources from any work location. This scenario will demonstrate a specific user experience where an employee attempts to access corporate services such as the corporate intranet, a time and attendance system, and other Human Resources systems by using an enterprise-managed device. The associated access request for that resource will be provisioned, dynamically and in real time, by a ZTA solution implemented in this project. The employee will be able to perform the following:

- Access on-premises corporate resources while connected from the corporate intranet.
- Access corporate resources in the cloud while connected directly from the corporate intranet.
- Access on-premises corporate resources while connected from a branch office.
- Access corporate resources in the cloud while connected from a branch office.
- Access on-premises corporate resources from the public internet.
- Access corporate resources in the cloud from the public internet.

Scenario 2: Employee Access to Internet Resources

An employee is attempting to access the public internet to accomplish some tasks. This scenario will demonstrate a specific user experience where an employee attempts to access a web-based service on the internet by using an enterprise-managed device. Although the web-based service is not owned and managed by the enterprise, the associated access request for that resource will still be provisioned, dynamically and in real time, by a ZTA solution implemented in this project. The solution will allow the employee access regardless of location, that is, the employee can access the internet while connected inside the corporate intranet, a branch office, or the public internet by using an enterprise-managed device.

If an employee is permitted by corporate policy to access nonenterprise-managed resources and services in the public internet by using enterprise-managed devices, the ZTA solution will allow the enterprise to determine the extent of this access.

Examples of access restrictions in the above paragraph could include:

- Access to social media sites is not permitted.
- Access to an internet search engine is permitted, and the associated access request for this resource does not need to be provisioned in real time through the corporate network when an employee is working at a branch office or remotely (e.g., coffee shop or airport).
- Mission-critical services on the public internet (e.g., email, GitHub) can be accessed directly by the employee, but these services must be authorized using enterprise user credentials.

Scenario 3: Contractor Access to Corporate and Internet Resources

A contractor is attempting to access certain corporate resources and the internet. This scenario will demonstrate a specific user experience where a contractor hired to provide a specific service attempts to access certain corporate resources and the internet to perform the planned service for the organization. The corporate resources can be on premises or in the cloud, and the contractor will be able to access corporate resources while on premises or from the public internet. The associated network access requests for resources that the contractor attempts to access will be provisioned, dynamically and in real time, by a ZTA solution implemented in this project.

Scenario 4: Interserver Communication Within the Enterprise

Corporate services often have different servers communicating with each other. For example, a web server communicates with an application server. The application server communicates with a database to retrieve data back to the web server. This scenario will demonstrate examples of interserver interactions within the enterprise, which will include servers that are on premises, in the cloud, or between servers that are on premises and in the cloud. The associated network communications among designated servers that interact with one another will be provisioned, dynamically and in real time, by a ZTA solution implemented in this project.

Scenario 5: Cross-Enterprise Collaboration with Business Partners

Two enterprises may collaborate on a project where resources are shared. In this scenario, the ZTA solution implemented in this project will enable users from one enterprise to securely access specific resources from the other enterprise, and vice versa. For example, enterprise A users will be able to access a specific application from enterprise B, while enterprise B users will be able to access a specific database from enterprise A.

Scenario 6: Develop Confidence Level with Corporate Resources

Enterprises have monitoring systems, security information and event management (SIEM) systems, and other resources that can provide data to a policy engine to create a more granular confidence level for access to corporate resources and promote strict access based on the confidence level. In this scenario, a ZTA solution will integrate these monitoring and SIEM systems with the policy engine to produce more precise calculation of confidence levels.

Note: The scenarios above may be created and demonstrated in different phases throughout the project.

3 High-Level Architecture

Figure 1 illustrates a high-level representation of the logical components that may achieve the desired capabilities.

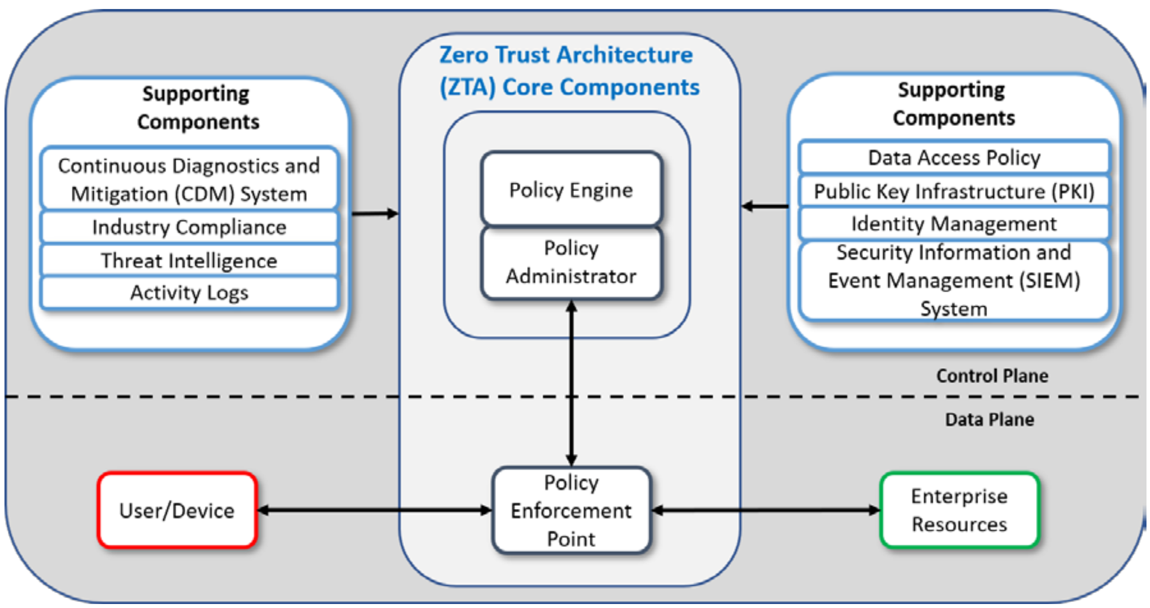

Figure 1: ZTA High-Level Architecture

Component List

The component definitions below come directly from the draft NIST SP 800-207, *Zero Trust Architecture.*

Core Components:

- The policy engine is responsible for the ultimate decision to grant access to a resource for a given user/device. Confidence levels and ultimate access decisions are calculated by the policy engine.
- The policy administrator is responsible for establishing and maintaining the connection between a user/device and a resource.
- The policy enforcement point is responsible for enabling, monitoring, and eventually terminating connections between a user/device and an enterprise resource.

Supporting Components:

- The CDM system gathers information about the current state of enterprise assets and applies updates to configuration settings and software.
- The industry compliance system includes all the policy rules that an enterprise develops to ensure compliance with any regulatory regime it may fall under (e.g., healthcare or financial industry information security requirements).
- Threat intelligence feeds funnel information collected from internal and/or external sources about newly discovered attacks or vulnerabilities to the policy engine to help make access decisions.
- The network and access logging system is responsible for recording traffic metadata seen on the network and for access requests made to enterprise resources.
- Data access policies are the attributes, rules, and policies about access to enterprise resources. This set of rules could be encoded in or dynamically generated by the policy engine.
- The PKI system is responsible for generating and logging keys and/or certificates issued by the enterprise to resources, devices, and applications.
- The identity management system is responsible for creating, storing, and managing enterprise user accounts and identity records.
- The SIEM system collects security-centric information for later analysis. This information is used to refine policies and warn of possible attacks against enterprise resources.

Devices and Network Infrastructure Components:

- Devices include laptops, tablets, and other mobile or IoT devices that connect to the enterprise.
- Network infrastructure components encompass network resources that a medium or large enterprise typically deploys in its environment. Note: The network infrastructure is not depicted in Figure 1. It is assumed that the ZTA core and supporting components and devices are connected via the network infrastructure.

Desired Requirements

This project seeks to develop a reference design and implementation that meet the following requirements:

- represents a standards-based solution architecture that is an effective and secure approach to implementing a ZTA
- provides direct access to internet and corporate resources, on premises and in the cloud, without the use of third-party tools (e.g., virtual private network, trusted internet connection)
- demonstrates integration with cloud and enterprise on-premises resources
- shows integration with standard directory protocols and identity management services (e.g., Lightweight Directory Access Protocol [LDAP], Active Directory, OpenLDAP, Security Assertion Markup Language)
- demonstrates integration with legacy and current SIEM tools through standard application programming interfaces
- shows desired enterprise user device security requirements, including:
    - maintaining data protection at rest

- securing device vulnerabilities that could result in unauthorized access to data stored on or accessed by the device, and misuse of the device
- mitigating malware execution on the device that could result in unauthorized access to data stored on or accessed by the device, and misuse of the device
- mitigating the risk of data loss through accidental, deliberate, or malicious deletion or obfuscation of data stored on the device
- maintaining awareness of and responding to suspicious or malicious activities within and against the device to prevent or detect a compromise of the device, and remediating as quickly as possible

4 Relevant Standards and Guidance

The references, standards, and guidelines that are applicable to this project are listed below.

- NIST Cybersecurity Framework v.1.1, Framework for Improving Critical Infrastructure Cybersecurity https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments https://doi.org/10.6028/NIST.SP.800-30r1
- NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach For Security and Privacy https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-4/archive/2013-04-30/documents/sp800-53-rev4-ipd.pdf
- NIST SP 800-57 Part 1 Revision 4, Recommendation for Key Management: Part 1: General https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
- NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- NIST SP 800-63 Revision 3, Digital Identity Guidelines https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
- NIST SP 800-92, Guide to Computer Security Log Management http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf
- NIST SP 800-160 Vol. 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final
- NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

- NIST SP 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175b.pdf
- NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- NIST SP 800-205, Attribute Considerations for Access Control Systems https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-205.pdf
- NIST SP 800-207 (Second Draft), *Zero Trust Architecture* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf
- NIST SP 1800-3, *Attribute Based Access Control* https://www.nccoe.nist.gov/sites/default/files/library/sp1800/abac-nist-sp1800-3-draft-v2.pdf
- Cloud Security Alliance, Software Defined Perimeter Working Group, *SDP Specification 1.0* https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf
- ISO/IEC 27001, Information Technology–Security Techniques–Information Security Management Systems
- American Council for Technology-Industry Advisory Council, *Zero Trust Cybersecurity Current Trends* https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf
- Federal Information Processing Standards 140-3, *Security Requirements for Cryptographic Modules* https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

5 Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the *Framework for Improving Critical Infrastructure Cybersecurity,* and to other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices but does not imply that products with these characteristics will meet an industry's requirements for regulatory approval or accreditation.

379 **Table 1: Security Control Map**

Cybersecurity Framework v1.1			Applicable Components
Function	**Category**	**Subcategory**	
Identify (ID)	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried.	SIEM User/Device Data Resources
		ID.AM-2: Software platforms and applications within the organization are inventoried.	SIEM
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	SIEM Policy Engine
	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented.	SIEM Threat Intelligence
		ID.RA-3: Threats, both internal and external, are identified and documented.	SIEM Threat Intelligence
Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	Identity Management System Policy Engine
		PR.AC-3 Remote access is managed.	Policy Engine Policy Administrator Policy Enforcement Point

Cybersecurity Framework v1.1			Applicable Components
Function	**Category**	**Subcategory**	
		PR.AC-4 Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	Policy Engine Policy Administrator Policy Enforcement Point
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	Policy Enforcement Point
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	Identity Management System PKI Policy Engine
		PR.AC-7 Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	Identity Management System PKI Policy Engine Policy Administrator

Cybersecurity Framework v1.1			Applicable Components
Function	**Category**	**Subcategory**	
Protect (PR)	Data Security (PR.DS)	PR.DS-2 Data in transit is protected.	Policy Engine Policy Administrator Policy Enforcement Point
		PR.DS-5 Protections against data leaks are implemented.	Policy Engine Policy Administrator Policy Enforcement Point
		PR.DS-6 Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	SIEM Policy Engine
		PR.DS-8 Integrity-checking mechanisms are used to verify hardware integrity.	SIEM Policy Engine
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).	SIEM
		PR.IP-3 Configuration change control processes are in place.	SIEM

Cybersecurity Framework v1.1			Applicable Components
Function	Category	Subcategory	
	Protective Technology (PR.PT)	PR.PT-3 The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	Policy Engine Policy Administrator Policy Enforcement Point
		PR.PT-4 Communications and control networks are protected.	Policy Engine Policy Administrator Policy Enforcement Point
		PR.PT-4 Communications and control networks are protected.	SIEM Threat Intelligence Policy Engine Policy Administrator Policy Enforcement Point

Cybersecurity Framework v1.1			Applicable Components
Function	**Category**	**Subcategory**	
DETECT	Anomalies and Events (DE.AE)	DE.AE-2: Detected events are analyzed to understand attack targets and methods.	SIEM Threat Intelligence Policy Engine Policy Administrator
		DE.AE-3 Event data are collected and correlated from multiple sources and sensors.	SIEM Threat Intelligence Policy Engine Policy Administrator
		DE.AE-5: Incident alert thresholds are established.	SIEM Threat Intelligence Policy Engine Policy Administrator
	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events.	SIEM Threat Intelligence
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	SIEM
		DE.CM-4 Malicious code is detected.	SIEM Threat Intelligence
		DE.CM-5 Unauthorized mobile code is detected.	SIEM Threat Intelligence

Cybersecurity Framework v1.1			Applicable Components
Function	**Category**	**Subcategory**	
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	
		DE.CM-7 Monitoring for unauthorized personnel, connections, devices, and software is performed.	SIEM Threat Intelligence
		DE.CM-8: Vulnerability scans are performed.	SIEM Threat Intelligence
	Detection Processes (DE.DP)	DE.DP-5 Detection processes are continuously improved.	SIEM Threat Intelligence
Respond	Mitigation (RS.MI)	RS.MI-1 Incidents are contained.	SIEM Threat Intelligence Policy Enforcement Point

Cybersecurity Framework v1.1			Applicable Components
Function	Category	Subcategory	
		RS.MI-2 Incidents are mitigated.	SIEM Threat Intelligence Policy Enforcement Point

Appendix A References

[1] S. Rose et al., *Zero Trust Architecture,* National Institute of Standards and Technology (NIST) Draft (2nd) Special Publication 800-207, Gaithersburg, Md., February 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf.