Meeting the Demand for Zero Trust Talent

Organizations are hurrying to implement zero trust architectures. Implementing a zero trust architecture creates a more adaptable security platform that is not designed around a static, perimeter-based network defense strategy, which can help further protect critical systems and data from attacks based on confidentiality, integrity and availability. Zero trust is unique because it maintains strict data control. It promotes persistent and secure data at all times, regardless of data being at rest, in transit or in use, agnostic to who or what is accessing them. Based on these benefits and the changing times, organizations are motivated to implement zero trust architectures. However, they do not seem to realize how important a tool the cybersecurity workforce is to successfully implementing zero trust.

As a specific security architecture approach within the cybersecurity domain, organizations must not only find cybersecurity talent, but they now need to find talent with specific zero trust architecture experience. It is important to find the right mix of zero trust talent to ensure that infrastructure changes do not introduce new misconfigurations or vulnerabilities that may occur when using untrained staff.

The ISACA® *State of Cybersecurity 2021* report does not paint an optimistic picture of the overall cybersecurity field:

- Sixty-one percent of respondents indicate that their cybersecurity teams are understaffed.
- Fifty-five percent of respondents say they have unfilled cybersecurity positions.
- Fifty percent of respondents say their cybersecurity applicants are not well qualified.
- Only thirty-one percent say their human resources department understands their cybersecurity hiring needs.[1]

Overall, the ability to train or reskill new cybersecurity professionals is far outpaced by the need. It has become more noticeable since the onset of the COVID-19 pandemic, made evident by the increase of cyberattacks on remote workers, phishing attacks on testing and vaccine communications, and other attacks used to encourage users to unknowingly share sensitive information. According to Cyberseek, there were 597,767 total cybersecurity job openings in the United States from October 2020 to September 2021.[2] To add further complexity, organizations are not only struggling to find general cybersecurity talent; they also need to find cybersecurity candidates with experience in zero trust architecture so they can ensure consistent and effective implementation. *Indeed.com*, an Internet platform for job posting, produced the following search results in February 2022:

- The search term "cybersecurity" produced 50,423 open job postings in the United States.
- The search term "zero trust" produced 7,457 open job postings in the United States.[3]

The *State of Cybersecurity 2021* report shows that hands-on experience remained the primary factor in determining whether a candidate is considered for

FORTUNE ONWUZURUIKE

Is an experienced cybersecurity professional. He is a security program manager at Microsoft and a doctoral student in the Doctorate of Science program at Marymount University (Arlington, Virginia, USA).

KENNETH MYERS

Is an identity and access management professional. He is the communications director for the ISACA® Greater Washington DC Chapter and a doctoral student in the Doctorate of Science program at Marymount University (Arlington, Virginia, USA).

a cybersecurity position.[4] Hiring managers already struggle to find candidates with a well-rounded body of work and hands-on experience in the cybersecurity field; zero trust experience is even more rare.

Zero Trust Principles

Some form of zero trust has been part of the security lexicon for the last 20 years. The US National Institute of Standards and Technology (NIST) defines zero trust as:

> *[A] collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.*[5]

A zero trust architecture is an organization's cybersecurity strategy focused around the seven principles of zero trust (**figure 1**), as defined in NIST Special Publication (SP) 800-207 *Zero Trust Architecture*.[6]

The US government has recognized the importance of zero trust and has made strides toward its implementation. The US federal government published two documents that direct US federal agencies to implement a zero trust architecture following the signing of US Executive Order 14028 on "Improving the Nation's Cybersecurity," which was created after the SolarWinds attack.[7] The US Office of Management and Budget published a federal zero trust strategy titled *Moving the US Government Toward Zero Trust Cybersecurity Principles*, which outlines broad security goals and includes a timeline for achieving them.[8]

The US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) published the *Zero Trust Maturity Model* as a draft companion to help federal agencies meet the intent of the *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*.[9] The maturity model outlines five pillars of zero trust:

1. **Identity**—The attributes that describe users and entities to ensure the right user or entity can access the right resources at the right time.
2. **Devices**—Any device, enterprise or other, that can connect to a network must be inventoried, secured and prevented from accessing unauthorized resources.
3. **Network and environment**—The internal and external communication medium for transferring data, which should be segmented, controlled and managed.

FIGURE 1
Comparing Traditional Security and Zero Trust Mentality

Common Security Mentality	NIST Zero Trust Principle	Zero Trust Mentality
Users are authenticated once to access multiple resources within a network.	Access to individual enterprise resources is granted on a per-session basis.	All resources are programmed to deny all access as a default setting.
Data do not need to be encrypted on the network.	All communication is secured regardless of network location.	All communication is encrypted in transit and data are encrypted at rest.
Only enterprise-owned devices are considered resources.	All data sources and computing sources are considered resources.	Any device can be a resource.
If someone has an enterprise credential, they are trusted.	Access to resources is determined by dynamic policy, including the observable state of client identity, application/service and requesting access, and may include other behavioral and environmental attributes.	In addition to a credential, an access decision may be made based on the device type, location and time of day.
Any managed device can access enterprise resources.	The enterprise monitors and measures the integrity and security posture of all owned and associated assets.	Only devices running the latest operating system can access enterprise resources.
A user is authenticated only once.	All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	Based on risk and data sensitivity, a user session is monitored for any changes such as device or location and then reauthenticated.
Only communication on an enterprise network is monitored.	The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.	All enterprise resources (on premises and in the cloud) are monitored for indicators of compromise and used to improve overall enterprise security.

4. **Applications and workloads**—Services run on premises or on a cloud platform, including applications, containers and other workloads, should follow a secure development and delivery pipeline.
5. **Data**—Data should be protected on all devices and in all states, in transit and at rest.[10]

Although zero trust principles and architecture are not new, zero trust is unique because it expands the security focus by requiring specific competencies and work roles that are distinct from traditional security competencies. This may necessitate an overlay of existing work roles to align with a zero trust architecture. To overcome this obstacle, organizations need a tool competency model to identify cybersecurity professionals with zero trust competencies.

Cybersecurity Workforce Framework

A cybersecurity workforce framework is a method to categorize cybersecurity work roles and the knowledge, skills and abilities required of each work role. One common cybersecurity workforce framework is the NIST National Initiative for Cybersecurity Education (NICE) Special Publication (SP) 800-181 Revision 1, *Workforce Framework for Cybersecurity*, which offers insight into how to close the cybercompetency gap.[11] The framework is composed of knowledge domains, work roles, tasks, and knowledge, skills and ability (KSA) statements. Work roles map to one specialty area, but tasks and KSAs can map to multiple work roles. The framework contains the following data points:

- **Specialty areas (33)**—Concentration of work roles into a functional area
- **Work roles (53)**—Describes a grouping of KSAs and tasks
- **KSAs and tasks**
  - **Knowledge statements (634)**—Information applied to create performance
  - **Skill statements (377)**—Competencies
  - **Ability statements (178)**—For applying cybersecurity tools, frameworks, processes and controls
  - **Tasks (1,002)**—Defined pieces of work

The framework is a collaboration between the US government, academia and a private sector partnerships intended to identify standard cybersecurity workforce abilities. One of the main benefits of the framework is a common lexicon across all parties that can be used to define, categorize and describe cybersecurity work. This ensures a consistent approach for organizations when looking for talent in general, but it is also a benefit to professionals in identifying the KSAs and tasks necessary to self-identity any potential skill gaps. However, although the framework provides a consistent approach and standard cybersecurity roles and competencies, it is not granular enough to address specific community needs, such as how an organization can identify zero trust competencies or differentiate specific roles such as an identity system administrator vs. a device system administrator. To close this gap, communities or organizations should create cybersecurity workforce overlays.

"The addition of an overlay for zero trust could be a collaborative effort among the cybersecurity workforce community to align a zero trust architecture with the cybersecurity roles needed to implement it."

Cybersecurity Workforce Zero Trust Overlay

An overlay is a set of specific controls or guidance intended to complement and further enhance a set of baseline controls. In this context, a cybersecurity workforce is a set of specific roles and KSAs intended to help organizations identify the right talent needed to implement a zero trust architecture. For some industries, overlays already exist, such as the NIST Risk Management Framework Control Overlay Repository[12] or ISACA's *COBIT® for Small and Medium Enterprises Using COBIT® 2019*.[13] The addition of an overlay for zero trust could be a collaborative effort among the cybersecurity workforce community to align a zero trust architecture with the cybersecurity roles needed to implement it.

Although the NIST NICE Framework does not outline a method to create a workforce overlay, it does provide a building block approach to develop knowledge, skills and task statements (**figure 2**). An organization can use this building block approach to:

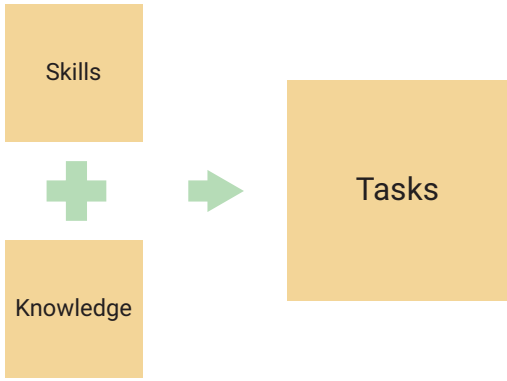
- Describe the cybersecurity work as it pertains to implementing a zero trust architecture.

LOOKING FOR MORE?

- Read *State of Cybersecurity 2022. www.isaca.org/go/state-of-cybersecurity-2022*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 2

NIST NICE Framework Building Block Approach



Source: Adapted from Petersen, R.; D. Santos; M. C. Smith; K. A. Wetzel; G. Witte; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181 Revision 1 *Workforce Framework for Cybersecurity (NICE Framework)*, USA, November 2020, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf*

- Document the tasks and task statements that describe the work.
- Document the knowledge and skill statements as they relate to the tasks.

The combination of tasks, knowledge and skills is what can be used to create a specific zero trust competency.

Conclusion

It is no secret that cyberthreats are growing exponentially, and organizations are struggling to find the right talent to address these threats. Layering new security paradigms such as zero trust complicates things even more. Cybersecurity is a science and an art in which cybersecurity professionals must continue to gain expertise over the years if they wish to become significant assets to any organization. As the world becomes more connected to technology than ever before, each and every organization must adapt to ensure that security is a top priority. NIST has adopted a cybersecurity workforce framework and a zero trust architecture to address these changes, but there is still a gap in identifying the right set of zero trust competencies needed to fully implement a zero trust architecture. NICE is used to guide the community to overcome cybersecurity workforce challenges and provide a standard for zero trust competencies and work roles. A proposed solution is creating a workforce overlay that uses the NIST NICE Framework work roles but tailors them to a zero trust architecture.

Endnotes

1 ISACA®, *State of Cybersecurity 2021, Part 2*, USA, 2021, *https://www.isaca.org/state-of-cybersecurity-2021*
2 CyberSeek, "Hack the Gap: Close the Cybersecurity Talent Gap With Interactive Tools and Data," *https://www.cyberseek.org/index.html#about*
3 *Ibid*.
4 ISACA, *State of Cybersecurity 2021, Part 1*, USA, 2021, *www.isaca.org/state-of-cybersecurity-2021*
5 Rose, S.; O. Borchert; S. Mitchell; S. Connelly; National Institute of Standards and Technology SP 800-207 *Zero Trust Architecture*, USA, August 2020, *https://doi.org/10.6028/nist.sp.800-207*
6 *Ibid*.
7 The US White House, "Executive Order on Improving the Nation's Cybersecurity," USA, 12 May 2021, *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*
8 US Executive Office of the President, Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, USA, 26 January 2022, *https://zerotrust.cyber.gov/downloads/M-22-09%20Federal%20Zero%20Trust%20Strategy.pdf*
9 US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), *Zero Trust Maturity Model (No. 1)*, USA, June 2021, *https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf*
10 *Ibid*.
11 Petersen, R.; D. Santos; M. C. Smith; K. A. Wetzel; G. Witte; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181 Revision 1 *Workforce Framework for Cybersecurity (NICE Framework)*, USA, November 2020, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf*
12 National Institute of Standards and Technology, NIST Risk Management Framework Control Overlay Repository, USA, *https://csrc.nist.gov/projects/risk-management/sp800-53-controls/overlay-repository*
13 ISACA, *COBIT® for Small and Medium Enterprises Using COBIT® 2019*, USA, 2021, *https://www.isaca.org/resources/cobit*