Zero Trust Architecture Strategy: Interdisciplinary Approaches to Widespread Integration and Confronting Trending Cyber Infrastructure Maneuvers

Paul M. Brown
Old Dominion University

Abstract

Modern IT environments are shifting, if not already, into a cloud prioritized architecture which can follow with heavier use of complex technological solutions like containerization. Local infrastructure is, as well, able to leverage container technology and orchestration systems like Kubernetes. The increased use of these technologies across all infrastructure types is evident by the fast adoption and widespread increase in the implementation of Kubernetes observed over recent years -- *and ongoing*. This event has caused a breaking point for two sub sequential directive consequences: first, the focus of sophisticated hackers with ill-intent has also gravitated with this increase; second, high-capability security embedded in Kubernetes upon baseline implementation has not been considered under scope of scale and type of use it now realizes. We should now have a collective goal in the greater field of cybersecurity to address a reasonable approach to aligning a baseline for cyber hygiene in modern IT environments. This includes maintaining ongoing efforts to achieve Zero Trust Architectures (ZTA) across the Nation. Embedding ZTA principles into Kubernetes deployments is an essential component to that maintenance in modern IT environments. A possible approach is realizing the most secure state imaginable and working backwards to implement strategic, achievable security states (accumulation of improvements over time) until a satisfactory baseline is met. The baseline would represent deterring the threat actors interest in attacking Kubernetes coupled with advances in introducing innovative security solutions for Kubernetes to achieve a secure by default posture. This paper demonstrates two small steps in architectural inclusion that are two giant leaps in security software engineering for Kubernetes and beyond. Policy-as-code will be demonstrated using Open Policy Agent (OPA). In addition, Gravitational's access management solution Teleport will be demonstrated. Each will be introduced and describe from a perspective with the aforementioned collective goal in mind. The focus is to target fundamental security issues in Kubernetes' default implementation in which the underlying problem has already been logically solved and, in the two examples I have selected, already been developed into production security tools. This is why OPA's Gatekeeper tool and Gravitational's Teleport will be demonstrated in this manuscript. Security policy enforcement and access management are extremely powerful security controls. These are among other of the most effective fundamentals in container security. There are additional areas of security that could be considered as impactful and categorized as fundamental. Secrets management is just one example. Understand that research and innovative development must occur as a unitary movement across an accumulative Kubernetes' security efforts. That requires interdisciplinary collaboration both in the sense of special knowledge areas within cybersecurity and in a larger group scheme involving cybersecurity with external fields of study. Possibly the most significant example is between cybersecurity and computer science. It is significant due to so much overlapping responsibility and straightforward collaborative needs between the two fields of study. An argument can be made for more niche collaborations as well. An effort involving cybersecurity with art communications may determine an optimal method for portraying technical security information in context of Zero Trust Architecture (ZTA) principles. This can lead to general awareness through the connective communication medium of art. It will ignite understandings about the security *'how'* of applications any given person may be using daily.

Zero Trust Architecture Strategy: Interdisciplinary Approaches to Widespread Integration and Confronting Trending Cyber Infrastructure Maneuvers

Information technology environments are adapting to the rapid innovation space enabled by internet-connected systems. Containerization is a particularly useful example. It was first developed by Docker in 2013. Although, containerization as an idea can be traced back to earlier technologies. Containerization is a ground-shattering technology for DevOps given the ability to package, deploy, and test applications consistently and with swift efficiency regardless of underlying infrastructure. Containerization was also realized to address inherent challenges of deploying applications in cloud environments. For instance, containerization helps activate scalability benefits of cloud computing. Ultimately, containerization has really revolutionized software development, deployment, and management of modern IT environments.

Part 1: Modern Cloud Architecture

Kubernetes has become the de facto standard for container orchestration. Orchestration just means the process of managing, deploying, and scaling containers in a distributed computing environment. It is not extremely important to try visualizing this "distributed computing environment". Clustering is a technique used in Kubernetes and the cluster represent this environment which can include a grouping of virtual machines. The grouping of virtual machines become the Kubernetes cluster upon implementation. Depending on the perspective it can be confusing to imagine this computing environment as distributed given the virtualized representation. However, it begins to become clear that *Kubernetes* is *orchestrating containers* that are deployed on two or more *clustered virtual machines* that are operating upon *cloud computing resources*. This is a case by which Kubernetes is deployed on cloud infrastructure. The characteristics of containerization and orchestration remain across different infrastructure

types. This can be a local hardware server running clustered virtual machines, multiple local hardware servers clustered, or other variants of physical and virtual IT structures. The point of Kubernetes maintaining its role multiplies the impact of solving fundamental security issues in default Kubernetes. In their 2022 State of Kubernetes security report RedHat presents key findings including 53% of organizations in the study detecting a Kubernetes misconfiguration in the last 12 months and 51% of surveyed organizations require developers to use validated images. These two findings in particular exemplify the need for tools like OPA's Gatekeeper to be properly implemented for maximizing security. The specifics for OPA's Gatekeeper will be described in a later section of this report. Point now being related to improving Kubernetes security by means of policy so that the 12-month percentage of detected misconfigurations is reduced, and the required use of validated images is increased. RedHat's report continues to state, "The majority of survey respondents (55%) have had to delay an application rollout because of security concerns over the last 12 months." (RedHat, 2023) Again OPA Gatekeeper or similar policy enforcing tools can assist in "shifting security left" to address security concerns before the development lifecycle begins. Access management is additionally extremely impactful in this scenario. There can be daily operation delays due to considering security too late in the lifecycle but there can also be larger security events like active attack campaigns. Tools like Gravitational's Teleport significantly decrease the possibility of a larger security event that leads to more extensive delays. When access management is properly considered using a robust tool such as Teleport it demands much more from potential attackers and will often result in attackers veering their malicious focus elsewhere.

Attackers are also aware of the amount of misconfigurations in Kubernetes deployments. In combination with the increasing use of Kubernetes in all infrastructure types these facts

portray containers as easy targets to sophisticated enough malicious hackers. It would be unacceptable to leave such awareness unaddressed. There must be specification when progressing large efforts surrounding cyber infrastructure security. For instance, the White House issued an executive order (EO) in 2021 that included requirement of federal agencies to adopt zero trust architecture (ZTA). Everyone who is knowledgeable about true ZTA understands the magnitude of potential overhauls for the least cyber healthy agencies. This is an extremely significant requirement and completely necessary. However, specification of security in more granule context such as container configuration compliance requirements by way of EO would be beneficial. The Cybersecurity and Infrastructure Security Agency (CISA) released a pre-decisional draft of their Zero Trust Maturity Model which serves to support Federal Civilian Executive Branch (FCEB) agencies in responding to the 2021 EO. In addition to the EO this is also extremely significant. There would be an expectation for a similar style model for the proposed granularity of maintaining a ZTA across containerized applications. Which should encompass solving, in part, Kubernetes (and containerization more generally) security misconfigurations. Further, I would propose the progression to compliance law for any enterprise use of Kubernetes. However, this law must not stand as a hurdle for small and medium sized businesses and non-profit organizations. Therefor, additional stabilizing efforts must follow. One approach may be to scale up existing services and products offered by agencies like CISA. Extending assistance by incorporating new services and products that are more intentional may also contribute to an achievable baseline for the mentioned business categories. For example, offering free baseline auditing and guidance for container compliance would ensure the technology remains approachable for organizations.

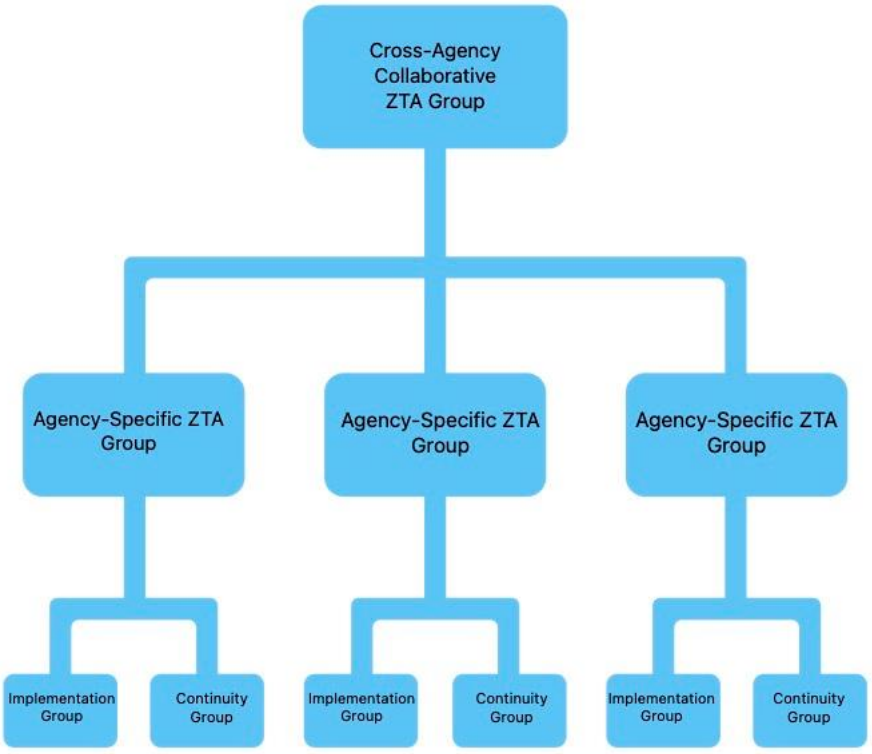
Of course, the software developers of container tools are certainly responsible for some level of embedded security. There is a reason I have engaged the idea of compliance for organizations by law. I believe the underlying technology should remain under free and open philosophies. This means that the tools can be used by anyone in any situation. The proposition of law is necessary when the tools are implemented in situations which turn profit or in situations of use by non-profit organizations that contain some definition of a full-scale IT environment. There is only a small amount of cyber expertise required to research and implement additional tools to reach a reasonable container security baseline. This can be completed by employed cyber professionals or by contracting third-parties. Later sections of this manuscript will demonstrate the ease in implementing two profoundly effective security solutions for Kubernetes and container security. There is certainly an assumption made about scaling this implementation out to a production environment. Acknowledging that there would be some degree of inherent rise in complexity I suggest there would remain an unscaled expertise hurdle. As in, the increasing complexities of production deployment is more concerned with human power and workforce-unique challenges opposed to knowledge of what to do for security.

Part 2: ZTA Integration: Developing a Strategic Workforce

Government is understandably first responsible for paving a path to optimal cyber hygiene within its own domain. There must also be a collective effort to achieve generalized optimal cyber hygiene by all organizations operating in cyber space. There is a particularly useful structure to the documentation and tutorials offered by Teleport for the use of their software solutions. This includes the guidance used for the demonstration of Teleport explored in a proceeding section of this manuscript. I suggest it can be used to model a knowledge database

with more accessible and actionable steps towards attaining ZTA. This could initially be explored by government in an effort to streamline the response to EO 14028. Furthermore, I would advise for dedicated expertise to address various component efforts to the ZTA shift. Figure 1 outlines one possible structure for the larger effort.

Figure 1:

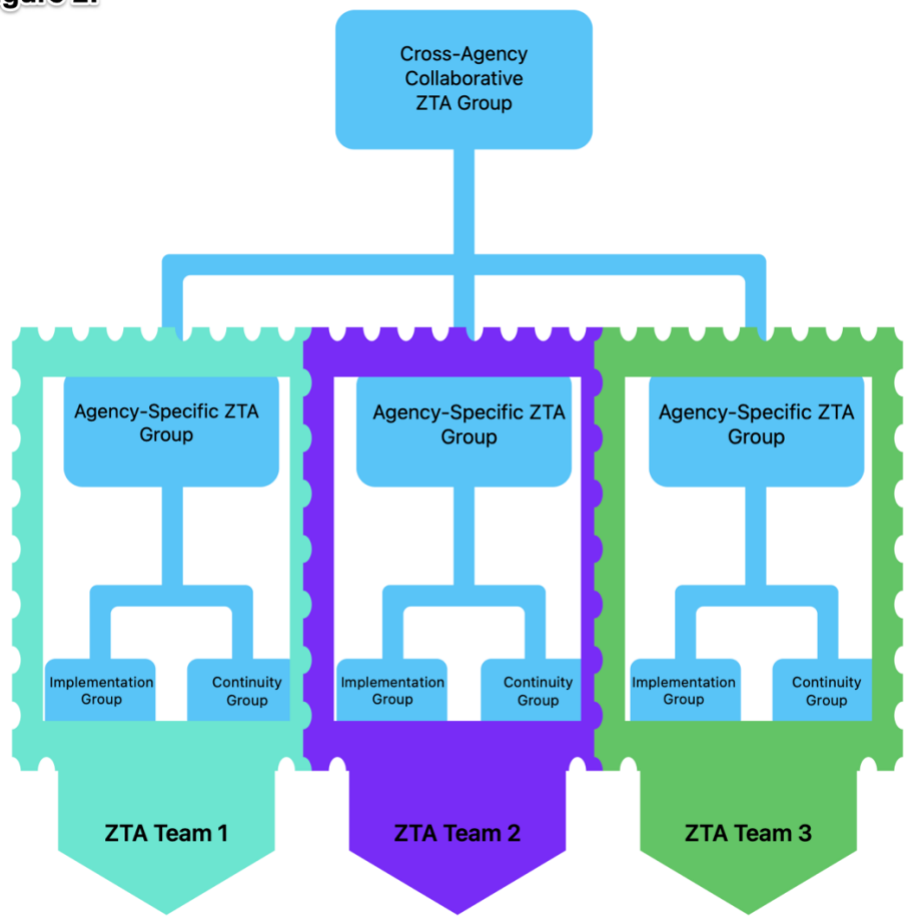


The suggested groups would represent specific knowledge pools for ensuring a robust effort in upgrading the whole of government to ZTA. Foremost, a cross-agency collaborative ZTA group would contain ZTA experts across cyber relevant agencies such as the National Security Agency (NSA) and CISA. This group would be expected to build out and maintain a centralized internal ZTA knowledge base. The expectation is that the knowledge base would be structured in a digestible and straightforward manner as was mentioned with Teleport's documentation. Across the FCEB each organization would be expected to put together their own ZTA management group as well as an implementation and continuity group. The agency-specific

ZTA management group would be expected to translate the information and guidance from the cross-agency collaborative ZTA group into their own unique infrastructure. This management group would also hold the responsibility of carrying out the effort to transition to true ZTA. The implementation group will largely be concerned with the initial rollout. These IT infrastructure and cybersecurity professional should specialize in overhauling IT environments to retroactively incorporate foundational structures such as zero trust. Finally, the continuity group would be in charge of ensuring the achieved ZTA is not undermined as IT systems and processes progress over time.

In case it is not obvious there is an explanation for shifting in and out of container security (expressed through Kubernetes policy and access management) and ZTA as the focused topic. There are similarities in solving problems faced by ZTA and faced by container security. ZTA has gained attention and traction in efforts to uplift the Nations cyber defenses. Container security should be explored in as critical a manner since it can be thought of as a granular component part of the ZTA umbrella within environments that run containerized applications. If structured, robust efforts are explicitly outlined for achieving granular security control over technology within a given IT environment then big picture ZTA can more easily be realized. So, the meaning of diverging into ZTA and outlining strategic approaches for implementation is to offer an assumed solution to the previously mentioned human power and workforce-unique challenges of achieving a particular security posture. This would need to be creatively scaled out to organizations outside of the government domain as well. See figure 2 for a possible continuation strategy for the government.

Figure 2:



After the rapid overhaul of infrastructure within the government domain to attain ZTA best practice the constructed groups can redirect efforts. CISA's mission statement is as follows, "We lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure." (cisa.gov/about) Cyber agencies like CISA could include a new service to their customer base that targets critical infrastructure (CI) operators with the most need for assistance. The responsibilities of each established group would remain intact. A team would be deployed to the CI operator to assess, plan, and upgrade the infrastructure to a robust ZTA baseline. Following the upgrade the team would also advise the CI operators on hiring recommendations for their own ZTA continuity group.

In summary, there is a widespread shift to cloud infrastructure and increasing use of Kubernetes for container orchestration across all infrastructure types which requires thoughtful security consideration to maintain ongoing security progressions such as with the ZTA evolution. A 2015 article, *Zero Trust: An Alternative Network Security Model*, states "...Zero Trust model takes into account both external and internal threats, ensuring that malicious insiders cannot access information they are not authorized to access, thus reducing the exposure of vulnerable systems and preventing the lateral movement of threats throughout the network." The article also explains the origin of the concept surfaced from Forrester Research in 2010. (Odell, et al.) Acknowledging today's understand of ZTA and supporting technologies is much more advanced it is still important to note the understandings from 8 years ago and point to some of the earliest ideas over 10 years ago. Efforts in cybersecurity need to become more proactive opposed to an aftermath EO to ignite impactful action. Emerging technology must already have security plans and strategies associated with each. In other words, the shift to cloud and containerization boom need to have existing strategic models to maintain true ZTA across containers as the adoption occurs. Future technologies must be addressed in research and development of security strategy. For example, this integration model for ZTA in the government domain or any existing strategic model for ZTA could have been realized and constructed in 2010. It is reasonable to assume a possible future state of technology with some degree of variability and effectively construct baseline models for strategic security efforts. The foundational models can be adapted and tweaked as the futures appear in different forms. It is assumed that the level of effort would be much lower opposed to developing strategy from scratch after advanced technologies emerge. For example, developing a strategic model for ensuring new security best practices are followed in a post quantum-classical mixed information technology ecosystem. There should be some

amount of research capability into the subject now and strategic security models should begin emerging ahead of that reality.

The remainder of this manuscript will express the importance of policy management and access management in Kubernetes. Furthermore, this document concludes with other fundamental security areas to consider in Kubernetes. Kubernetes and container security more generally will be essential to address in order to maintain true ZTA in modern IT environments.

Part 3: Policy Management in Kubernetes Architecture

Traditionally, policy controls refer to a set of rules, guidelines, and procedures that are implemented to guide and regulate behavior within an organization. In computer systems, policy controls typically refer to a set of rules and procedures that are designed to regulate access to data and resources, as well as to ensure the security and integrity of computer systems and networks. *The Ultimate Guide to Policy-based Governance, Security & Compliance for Kubernetes* explains, "In Kubernetes, policies are a special type of configuration resource that control other configuration or runtime behaviors. For example, a simple policy declaration may be, 'HTTP (non-encrypted) endpoints are not allowed'." (nirmata, 2023) One of the most effective means to managing policies in Kubernetes is by code. Policy-as-code (PaC) is an approach to managing policies that involves representing policies as code, which can be automatically enforced by computer systems. This approach enables scalability and efficiency of managing policies in complex modern IT environments. Under a PaC approach, policies are defined as code that can be versioned, tested, and deployed like any other software coded solution. This allows for ease in maintaining and updating policies over time. Some PaC approaches involve defining policies in a dedicated policy language and other approaches use

existing programming languages such as Python or YAML to define policies. Overall, PaC is an emerging approach to policy management that offers a number of benefits, including improved scalability, greater automation, and better alignment between policies and the underlying systems they govern.

Open Policy Agent (OPA) is an open-source project that provides a general-purpose policy engine for enforcing policies across a wide range of computing environments, from cloud-native applications to microservices and APIs. OPA was originally created in 2016 by Tim Hinrichs and Torin Sandall. OPA was designed to provide a more flexible and extensible approach to policy enforcement, based on the principles of declarative programming. OPA is an example of a PaC approach that uses a dedicated policy language called Rego. Since its initial release, OPA has gained a significant following within the cloud-native and DevOps communities. To enforce policies in Kubernetes, OPA is typically integrated with the Kubernetes API server using a component called the OPA Kubernetes Admission Controller. This component intercepts requests to the Kubernetes API server and checks them against OPA policies defined using Rego. One of the key benefits of using OPA for Kubernetes policy enforcement is its flexibility and extensibility. OPA policies can be easily modified and updated to reflect changes in the underlying Kubernetes environment, and can be extended to cover new types of policies or resources as needed. Gatekeeper is OPA's policy enforcement tool which can serve as an admission controller. It is built on top of OPA and is designed to be highly flexible and extensible.

OPA Gatekeeper allows administrators to define policies in a declarative way using a dedicated language called Constraint Language (CIL). CIL is used to define constraints that can be applied to Kubernetes resources, such as Deployments, Services, and ConfigMaps. These

constraints define rules that must be satisfied before a Kubernetes resource can be created or updated. Once policies have been defined using CIL, they can be deployed to the Kubernetes cluster and enforced by Gatekeeper. When a user attempts to create or update a Kubernetes resource, Gatekeeper intercepts the request and checks it against the defined policies. If the request violates any of the policies, it is rejected and an error message is returned to the user. I have demonstrated OPA's Gatekeeper in an elementary scenario here.

Part 4: Access Management in Kubernetes Architecture

Access management, similar to policy management, can be traced back to the early days of computing. As computers became widely adopted for business and industry the need for access management grew as well. Simple username and password authentication was an early accepted solution for access management. It was quickly discovered that this was weak access management for any adept, malicious hackers. Systems requiring access management were also becoming more complex. Role-Based Access Control (RBAC) was a respectable early access management system and is used in more evolved forms today. RBAC allows administrators to define roles that correspond to different levels of access, and then assign users to those roles based on their job responsibilities and level of authority. Over time, RBAC has been augmented in various ways. For instance, policy defined requirements for authentication controls in RBAC systems became harmonious. This enables defined enforcement for controls like multi-factor authentication (MFA).

Authorization in Kubernetes is based on the RBAC model. RBAC policies can be defined for specific resources, such as Pods, Deployments, or Services, as well as for specific actions, such as create, read, update, or delete. Policies are defined using Kubernetes manifests, which

are YAML or JSON files that describe the desired state of Kubernetes resources. "Access Control for Kubernetes Clusters: An Empirical Study of an RBAC Policy Model for Kubernetes" by Tiago de Mello et al. (2021), suggests several areas of improvement for the RBAC policy model for Kubernetes access management. the authors suggest that improvements to RBAC policy management, authorization granularity, policy evaluation performance, and policy versioning and management could help enhance the effectiveness and usability of the RBAC model for Kubernetes access management. The authors suggest that improvements to RBAC policy management, authorization granularity, policy evaluation performance, and policy versioning and management could help enhance the effectiveness and usability of the RBAC model for Kubernetes access management. In addition to RBAC, Kubernetes also supports other access control mechanisms, such as Network Policies, which allow administrators to define rules for network traffic between Pods, and Service Accounts, which allow Kubernetes resources to authenticate with other resources in the cluster. Teleport simplifies access management in Kubernetes by providing a unified platform for managing authentication, authorization, and auditing across multiple clusters and environments. Teleport's RBAC, SSO, MFA, and auditing capabilities make it a popular choice for organizations that need to secure access to cloud-native infrastructure.

Teleport provides several key features, as mentioned, that address common challenges in Kubernetes access management. SSO through Teleport can harden the access security of Kubernetes service application dashboards that would otherwise not support the feature. This is true for other features supported by Teleport as well, such as MFA. Using a robust access management tool like Teleport can harden a Kubernetes deployment against insider threats, credential theft, man-in-the-middle attacks, and malicious code execution. Teleport's RBAC

policies allow administrators to restrict access to sensitive resources and limit the actions that users can perform. MFA provides an extra layer of security that can help protect against credential theft. Even if an attacker steals a user's password or other credentials, they would still need to provide a second factor, such as a token or biometric identifier, to gain access to the system. Teleport encrypts all network traffic between clients and servers, which can help prevent attackers from intercepting or tampering with the traffic. Teleport also uses TLS certificates to ensure that clients are communicating with the correct servers, which can help prevent man-in-the-middle attacks. By restricting access to sensitive resources using Teleport's RBAC policies Teleport can help prevent attackers from executing code that could compromise the security of the cluster. Overall, Teleport is an extremely impressive security software solution that can help ensure true ZTA is maintained across cloud-native and Kubernetes architectures. Similar to OPA's Gatekeeper I have completed a simple demonstration of the tool, here.

Part 5: Additional Security Fundamentals in Kubernetes, and Interdisciplinary Approaches for Resilient Cyber Defense and Awareness

True zero trust in an IT environment can only be achieved by accumulative effort and strategic compound solutions. The two areas of security explored so far, policy management and access management, are fundamental control categories in building towards true ZTA. Continuous monitoring and analytics needs to be recognized as fundamental to ZTA as well. Continuous monitoring involves the collection, analysis, and reporting of security-related data from multiple sources in real-time. This data can include logs, network traffic, user behavior, and system performance metrics, among others. By continuously monitoring this data, organizations can identify anomalous behavior that may indicate a security threat, such as unusual login

activity, unauthorized access attempts, or data exfiltration. A simple explanation for the ZTA requirement can be understood by determining no continuous monitoring and analytics would be trusting the underlying processes to maintain ZTA without verifying that is true. This is simply a plain language representation of principles majorly represented by technical controls when discussing ZTA. In Kubernetes there are many cloud-native solutions like Prometheus, Falco, Open Raven, Kubescape, and many others that contribute to monitoring and analytics for security.

Furthermore, secrets management is another fundamental security requirement for attaining true ZTA. Secrets management is the practice of securely storing, managing, and distributing sensitive information, such as passwords, API keys, certificates, and other credentials, used by applications and services to access protected resources. Secrets management aims to provide a secure and auditable way to handle sensitive data, preventing unauthorized access, data breaches, and data leaks. As seen with the other security categories there are many existing open-source tools that contribute to this goal for secrets management. One note-worthy solution is from HashiCorp in form of "Vault". The solution can integrate with other HashiCorp tools and cloud-based Kubernetes architecture to achieve truly effective secrets management. There is a great video introduction to understand Vault, here. It is a few years old but offers a truly great demonstration for conceptualizing the problems Vault solves. Vault works by providing a central repository for secrets that is accessible only to authorized users and applications. The secrets are stored in an encrypted format, and access to them is controlled by policies that define who can access what secrets under what circumstances. Further, Vault can generate and manage dynamic secrets, such as temporary database credentials or AWS access

keys, on-demand, reducing the risk of credential theft and simplifying the management of secrets.

In addition to the composition of multiple technical security integrations in cyber there is an interdisciplinary requirement in operationalizing cybersecurity solutions and raising general awareness. The most evident need is cross-collaboration between software development and cybersecurity. Software engineers and cybersecurity professionals can work together to solve security issues in software solutions by collaborating at every stage of the software development lifecycle. Other fields of study such as behavioral psychology, game theory, mathematics, and philosophy can all find a place in offering unique perspectives to solve security problems in the cyber domain. Incorporating insights and perspectives from other fields of study can help cybersecurity professionals develop more effective and holistic solutions that take into account the diverse and evolving challenges of cybersecurity. By drawing on knowledge and expertise from a wide range of disciplines, we can create more robust and resilient systems that promote the safety and well-being of individuals and organizations.

Moreover, art and communication can play an important role in raising awareness about cybersecurity to the public. Visual storytelling, creative metaphors, interactive exhibits, public campaigns, and other art or non-artistic communicative mediums can assist in connecting cyber to a wider audience. By collaborating with artists, designers, and communicators, cybersecurity professionals can create more effective and impactful strategies for raising awareness and promoting cybersecurity education. Rafael Lozano-Hemmer has created some masterpieces with focuses on security adjacent topics in technology. His work "Data Shadow" visualizes the digital traces we leave behind in our daily lives, such as social media activity and GPS location data. This brings security and privacy concerns into awareness for an art-sophisticated audience. This

community may otherwise be less interested in technical fields like cybersecurity. An effort to incorporate these cyber topics in exhibits may lead to influence for additional artists to find a way to keep the messaging momentum in their own work. The alignment of strategic, interdisciplinary efforts and technical security integrations will guide in significant change for cyber defenses such as in widespread graduation to true ZTA across the Nation.

References

Complete guide to kubernetes policy management & security. Nirmata. (n.d.). Retrieved April 5, 2023, from https://info.nirmata.com/guide-kubernetes-policy-governance-management

HashiCorp. (n.d.). *Hashicorp Vault - Manage Secrets & Protect Sensitive Data*. HashiCorp. Retrieved April 5, 2023, from https://www.hashicorp.com/products/vault

Kubernetes in Microservices. (n.d.). Retrieved April 5, 2023, from https://www.researchgate.net/publication/365344228_Kubernetes_in_Microservices/fulltext/636fd6d0431b1f53009268df/365344228_Kubernetes_in_Microservices.pdf

Odell, L. A., Farrar-Foley, B. T., Fauntleroy, J. C., & Wagner, R. R. (2015). Zero Trust: An Alternative Network Security Model. In *In-Use and Emerging Disruptive Technology Trends* (pp. 13–16). Institute for Defense Analyses. http://www.jstor.org/stable/resrep36523.7

Open Policy Agent. (n.d.). Retrieved April 5, 2023, from https://www.openpolicyagent.org/docs/latest/

Open raven: Cloud native data discovery and classification tool. Open Raven: Cloud Native Data Discovery and Classification Tool. (n.d.). Retrieved April 5, 2023, from https://www.openraven.com/

Production-grade container orchestration. Kubernetes. (n.d.). Retrieved April 5, 2023, from https://kubernetes.io/

Prometheus. (n.d.). *Overview: Prometheus*. Prometheus Blog. Retrieved April 5, 2023, from https://prometheus.io/docs/introduction/overview/

State of kubernetes security report. Red Hat - We make open source technologies for the enterprise. (n.d.). Retrieved April 5, 2023, from https://www.redhat.com/en/resources/state-kubernetes-security-report

Teleport. (n.d.). *Introduction to teleport.* Teleport Docs. Retrieved April 5, 2023, from https://goteleport.com/docs/

University, A. R. A., Rahman, A., University, A., University, S. I. S. A., Shamim, S. I., Tech, D. B. B. V., Bose, D. B., Tech, V., Github, R. P., Pandita, R., Github, & Metrics, O. M. V. A. (n.d.). *Security misconfigurations in open source Kubernetes Manifests: An empirical study*. ACM Transactions on Software Engineering and Methodology. Retrieved April 5, 2023, from https://dl.acm.org/doi/10.1145/3579639

YouTube. (2018, March 23). *Introduction to Hashicorp Vault with Armon Dadgar*. YouTube. Retrieved April 5, 2023, from https://www.youtube.com/watch?v=VYfl-DpZ5wM&t=94s

Figures

Figure 1:

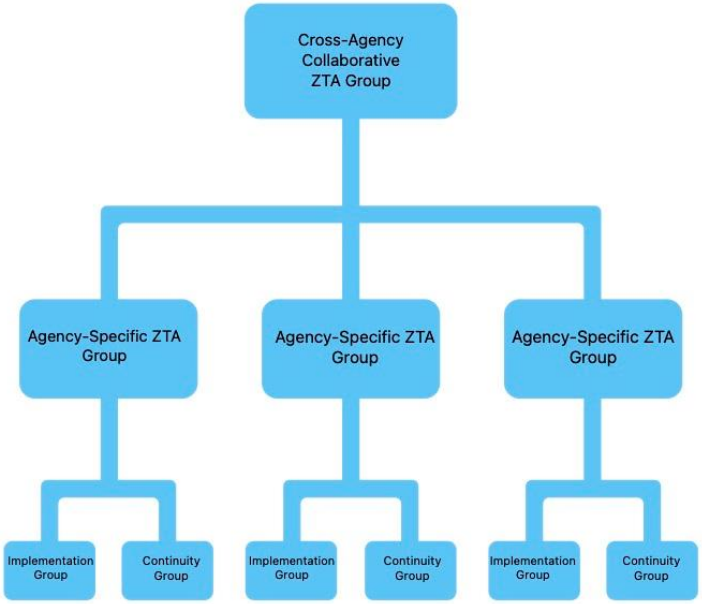


Figure 2:

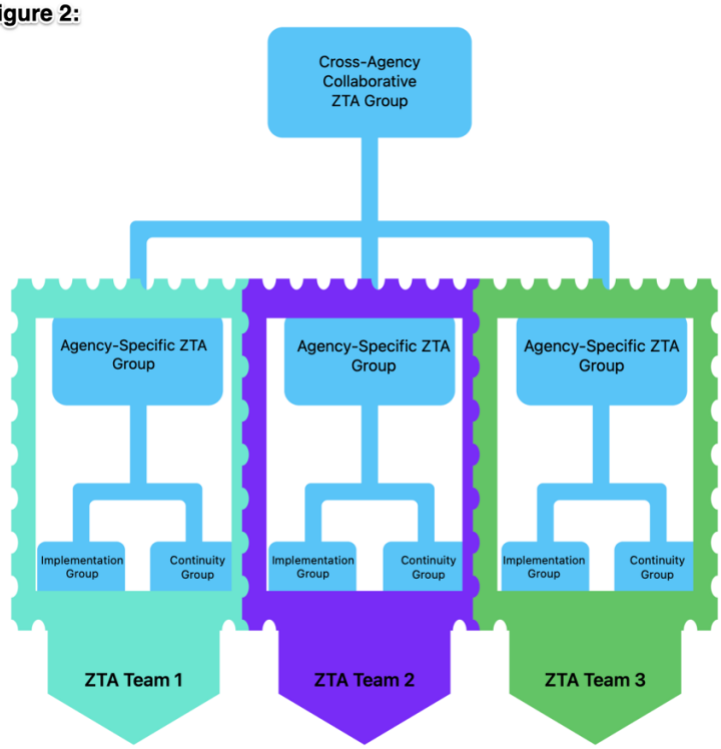


Figure 1. A proposed workforce strategy for integrating ZTA in the Government domain.
Figure 2. A proposed continuation for integrating ZTA for CI operators most in need.