Security-Rich: How the D2iQ Platform Meets NSA/CISA Kubernetes Security Hardening Guidelines

Cybersecurity continues to be a thorny problem for businesses and government agencies as breaches, disruptions, and data thefts continue to escalate. To help ensure that the growing number of government and private organizations implementing Kubernetes solutions have the highest possible levels of security, the National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) have issued guidelines for hardening the security of Kubernetes implementations.

The good news is that the D2iQ Kubernetes Platform (DKP) meets all the NSA/CISA guidelines, giving D2iQ customers the assurance that their environments provide military-grade security protection. How DKP addresses each of the NSA/CISA guidelines is detailed in the "How D2iQ Maps to the NSA/CISA Guidelines" section below.

Security Is Mission-Critical

The level of security an organization maintains can have a dramatic impact on the bottom line. Surveys show that the average cost of a data breach in 2021 was about $4.24 million. These costs vary according to the type and size of an organization. For example, the average cost of a data breach in the healthcare industry was $9.23 million, while the average total cost of a breach at enterprises of more than 25,000 employees was more than $5 million.

Stolen data and business disruptions resulting from security breaches take the largest toll on a business, with losses including lost customers, lost revenue resulting from system downtime, and the increased cost of acquiring new customers as a result of diminished reputation.

Remote work during COVID-19 is expected to increase data breach costs and incident response times. Having a remote workforce was found to increase the average total cost of a data breach by nearly $137,000 in 2020, for an adjusted average total cost of $4 million.

Supply Chains Targeted

Along with malicious threat actors and insider threats, the NSA/CISA report cites supply chain security as one of the major areas of concern. This is borne out in research that shows that "Supply chain attacks rose by 42% in the first quarter of 2021 in the U.S., impacting up to seven million people."

As Forbes reports, "A whopping 97% of firms have been impacted by a cybersecurity breach in their supply chain, and 93% admitted that they have suffered a direct cybersecurity breach because of weaknesses in their supply chain."

Infrastructure Makes a Difference

Traditional IT infrastructures have more inherent vulnerabilities than do modern cloud-native containerized infrastructures. As the NSA/CISA guidance notes, a Kubernetes virtualized infrastructure "can provide several flexibility and security benefits compared to traditional, monolithic software platforms."

Organizations that modernize their infrastructure security by implementing cloud-native containerized architectures and deploying advanced process automation, machine learning, and AI technologies can more effectively prevent, detect, and respond to cyber attacks.

This is reflected in the statistics that show that organizations that have not deployed security automation incur an average total cost of $6.71 million, more than double the average cost of a data breach of $2.90 million for businesses that have fully deployed security automation.

Cyber criminals are relentless in devising new ways to compromise an organization's security. This makes cybersecurity an ongoing battle that requires organizations to have the strongest and most flexible architectures, processes, and policies in place.

Organizations that lag in modernizing the security of their IT environments will run higher risks and stand to suffer greater losses. Organizations with weaker security also risk losing partnering opportunities. As Gartner predicts, by 2025, 60% of organizations will use cybersecurity risk as a "primary determinant" in choosing who they conduct business with.

How D2iQ Maps to the NSA/CISA Guidelines

D2iQ provides extensive out-of-the-box capabilities that can be integrated into the fabric of an agency's or organization's installed cyber-security controls and tooling. The following describes how DKP 2.0 maps to the NSA/CISA guidelines.

NSA/CISA Guideline:	How DKP Meets the Guideline:
Scan containers and pods for vulnerabilities or misconfigurations	Provides support for immutable operating systems such as Flatcar. Running immutable operating systems can significantly enhance your container hardening strategy and minimize the attack surface to mitigate risk.
Run containers and pods with the least privileges possible	Leverages rootless container runtime engines to reduce the attack surface and mitigate insider threats in the event a root account is compromised. DKP is FIPS 140-2 certified for securing secrets and encryption keys for SSL.
Use network separation to control the amount of damage a compromise can cause	A critical DKP capability is support for air-gapped environments. Air-gapped deployments ensure that network separation integrities remain intact. DKP also provides a FIPS 140-2 certified environment for encryption of data in transit.
Use firewalls to limit network traffic and encryption to protect confidentiality	DKP provides encryption of data in transit and also utilizes Kubetunnel, which creates an encrypted tunnel for cluster management. DKP works transparently with any current firewall implementation.
Use strong authentication and authorization to limit user and administrator access and limit the attack surface	DKP has built-in support for multifactor authentication for administrative access. DKP also provides out-of-the-box logging for role-based access and delegation of duty. DKP provides monitoring of the environment for analogous behavior.
Use log auditing so that administrators can monitor activity and be alerted to potential malicious activity	DKP provides turnkey logging capabilities for activity monitoring, role-based access, and delegation of duty. DKP includes monitoring of the environment for consistent operational practices across multiple deployments.

NSA/CISA Guideline:	How DKP Meets the Guideline:
Periodically review all Kubernetes settings and use vulnerability scans to help ensure risks are appropriately accounted for, and security patches are applied	D2iQ is an Embargo partner and can quickly react in the event of a known exploit. The DKP platform is FIPS 140-2 certified. The DKP platform provides RBAC (role-based access controls) to restrict who and what has access to the Kubernetes infrastructure.

3 Major Threats

The NSA/CISA guidelines cite three major types of threats:

- Supply chain
- Malicious threat actors
- Insider threat

DKP addresses each of these threats in the following ways:

Supply Chain

- D2iQ is a CNCF embargo partner and can respond rapidly to Day 0 security exploits through software patches.
- DKP goes through vigorous and continuous vulnerability scanning with every point release.

Malicious Threat Actors

- DKP is preconfigured with known security practices to ensure that Kubernetes components are free from common misconfigurations that a malicious actor could exploit.
- DKP is FIPS 140-2 certified.
- DKP provides role-based access control (RBAC) to govern who and what has access to the Kubernetes infrastructure.

Insider Threat

- D2iQ highly recommends ongoing cybersecurity training for all employees to prevent inadvertent events such as phishing, malware, and human error.
- The DKP platform provides multifactor authentication for administrative delegation of duty and abides by the Presidential Cybersecurity Executive Order, which includes the following:
  - Multifactor authentication: DKP platform supported.
  - Data-in-motion encryption: DKP platform supported; DKP is FIPS certified.
  - Data-at-rest encryption: DKP transparently integrates with existing data-at-rest capabilities.
  - Zero trust architecture principles: DKP supports air-gapped deployments out of the box for network segmentation and enables platform observability out of the box through monitoring and logging.

D2iQ's Security Commitment

The NSA/CISA hardening guidelines are welcomed by D2iQ as we have always prided ourselves as a security-first Kubernetes organization. D2iQ is a longstanding and recognized leader in the Cloud Native Computing Foundation (CNCF) Kubernetes ecosystem, continues to be a leading contributor to CNCF, and provides CNCF certified training and services. D2iQ will continue to contribute to CNCF and monitor future NSA/CISA Kubernetes hardening suggestions.

To learn more about how D2iQ can be your partner in the cloud native journey, go to www.D2iQ.com.