CYBERFORCE|Q

CYBERFORCE|Q AND ELASTIC COLLABORATION

The collaboration between CyberForce|Q and Elastic offers significant advantages for SLED (State, Local, and Education) clients by delivering innovative technologies that integrate seamlessly with their existing environments. Elastic's powerful Search, Observability, and Security solutions along with CyberForce|Q's Security Operations Center 24x7x365 Monitor, Detect, Analyze, and Response services provide robust cybersecurity advancements.

Working together our clients receive resources for architecting, designing, and implementing the Security Information and Event Management (SIEM) solution seamlessly into their operations.

CJIS SIEM DEPLOYMENT OVERVIEW

CyberForce|Q and Elastic together offer tailored solutions for organizations seeking to architect and deploy Security Information and Event Management (SIEM) technology to achieve compliance with the Criminal Justice Information Services (CJIS) requirements. With expertise in both cybersecurity and regulatory compliance, we provide comprehensive SIEM solutions designed to help organizations to meet and demonstrate compliance for:

- FBI CJIS Security Policy (CJISSECPOL) Policy Area 4: Accounting and Accountability
- The Bureau of Criminal Apprehension's (BCA) Minnesota Justice Information Services (MNJIS) minimum level of information technology (IT) security requirements 2.1.1 & 2.1.3

SIEM Deployment and Management

CyberForce|Q cybersecurity engineers provide end-to-end managed services for Elastic SIEM technology, covering its design, implementation, and ongoing maintenance to meet the standard requirements for CJIS Compliance based on BCA standards.

CJIS COMPLIANT EVENT LOGGING & DASHBOARDS

CyberForce|Q will implement the event logging and dashboards for organizations to easily demonstrate compliance with (CJISSECPOL) Policy Area 4: Accounting and Accountability requirements and Minnesota BCA requirements 2.1.1 & 2.1.3.

Sample Dashboards Available Include:

- Successful Log-on Attempts
- Failed Log-On Attempts
- Successful Actions by Privileged Accounts
- Create Permission User
- User Created
- File Permission Accessed
- User Permission Accessed
- Permissions Changed File/Registry
- Create Permission User
- Permissions User Right Assigned
- Permissions Created Directory
- Permissions Deleted Directory Service Object
- Permissions User Account Changed
- Successful Password Account Change
- Permissions Deleted Directory Service Object- 2
- Permissions Deleted User Right
- Permissions Deleted User Account
- Failed Actions by Privileged Accounts
- Failed Password Account Changes

Upon implementation, dashboard charts will be adjusted for the data fields available. Dashboards are tagged by compliance requirements for easy searching. All dashboards can be exported in CSV or PDF files. The dashboards can be shared directly with team members or auditors.

COLLABORATION USER GROUP

CyberForce|Q and Elastic host quarterly user group meetings for participants focusing on compliance and cybersecurity collaboration. Participants engage in structured discussions to address implementation and advancement strategies. Fostering continuous improvement and accountability.

REACH OUT FOR MORE INFORMATION: John Kelley - jkelley@cyberforceq.com - 586.907.9751