# Protect your data and your mission
## DXC Cyber Defense Situational Awareness

Organizations worldwide continue to invest heavily in IT cyber defense capabilities to protect their critical assets. It doesn't matter what is being defended — from governmental and military assets to commercial brands, intellectual capital, customer information or critical infrastructure.

Security incident detection and response now must be based on near real-time situation analysis against disparate security devices, organizational, geographic and mission data. And minimum response standards must be addressed through a pre-approved playbook of courses of action tailored to the enterprise.

Security operations centers are bombarded daily with millions, and in some cases billions of pieces of information from multiple sources. The detection and response capability of organizations continues to evolve. The biggest question now is how do you manage all that information and turn disparate data into actionable intelligence that an analyst can act on?

Even more importantly, what are the anticipated effects on active missions for people and resources? Going forward, threat analysts need real situational awareness of the threats and their correlation to the mission environment.

### Know your enemy

In today's threat environment, Security Operations Center teams need to do more than just intake and analyze security-related data. They must also understand security data from a higher operational picture. That requires an ability to ingest vast amounts of data from numerous and differing sources, and to centralize that data into a single, authoritative location.

Security information should be correlated, transformed and normalized. Then security data can be overlaid on top of organizational, geographic and mission data, enabling true situational awareness across the organization's environment.

Finally, the results of those activities must be presented visually — in a way that allows operators to see security-related events not just from an IT perspective but also from an operational perspective. This situational approach helps personnel make better decisions and better support and protect vital active missions.

### Gain operational awareness

The DXC Cyber Defense Situational Awareness (CDSA) solution addresses several key issues. It fits smoothly into existing security and SOC operations and enables organizations to integrate vulnerability, threat, hardware, software, organizational, geographic and mission data. This will enable security teams to better identify, understand, prioritize and respond to threats that may impact the mission.  The underlying solution is based on an enterprise service bus configuration that can:

- Securely pull data from a single authoritative data access point (SADAP)
- Transform and normalize the data
- Analyze data against organizational and mission data
- Transport data to a dashboard
- Kick off messaging to initiate courses of action
- Delve into your environment to investigate the threat
- Alert your organization on which missions may be affected
- Track incident resolution

Another strength of a robust situational awareness security solution is the visual correlation of events to mission data. Rather than only interpreting text on a screen, plotting information geospatially provides real-time differences in digesting information to speed decision-making.

### Learn what it is, what it does, how it works

The DXC CDSA does not replace current systems; it enhances and extends SOC and response capabilities. It helps you prioritize the large amount of data being gathered from disparate sources, and to prioritize that incoming information against mission and operational data.

The CDSA then pulls in specific suggested courses of action to address the incident and provides SOC analysts with in-depth graphical and geographical inputs. A dashboard provides situational awareness reporting with views of the data that are appropriate for analysts, management and executive personnel.

To support this CDSA solution, DXC created 35 specific use cases, including:

- View current risks list, prioritized by impact and displaying geographic location
- Generate and select from course of action options
- View incidents, aggregated by network with linked views
- View historical incidents, displayed by asset

These use cases were designed and implemented to provide a complete and scalable approach to handling security incidents.

We designed, built and tested the CDSA solution in our labs using standard processes and documentation, real-world proof-of-concept testing and implementation procedures. DXC offers advisory and diagnostic capabilities based on standard assessment processes. With these we can identify data sources and any gaps in your infrastructure that may be a barrier to adopting CDSA. DXC also offers functional training for the CDSA and ongoing solution support.

### Achieve more

- Aggregation of data volumes from multiple sources
- A seamless overlay and correlation of mission and security data
- Correlation engines to transform data into actionable information
- A situational awareness portal that aggregates and displays mission-critical security data
- An enhanced ability to prioritize incidents, select optimum courses of action and escalate events
- The transformation of technical security data into strategic operational and mission insights

### Gain significant benefits

The DXC Cyber Defense Situational Awareness solution is designed to support a mature, data-driven model for incident detection and response. Our solution enables organizations to:

- Draw data from a single platform, giving security analysts full access to data that has been correlated with information from a variety of sources when investigating an alert or incident
- Prioritize threats and risk by mission, ensuring that limited skilled resources are focused on events that most affect the organization's core objectives
- Leverage geographic information to gain higher levels of situational awareness
- Reduce implementation risk by deploying a system based on similar systems successfully deployed on time and on budget for a number of U.S. Federal civilian agencies
- Minimize risk with an architecture that enables cost-efficient upgrades and provides flexibility to incorporate future changes in your security environment
- Increase the overall maturity and effectiveness of the security operations center
- Address key threat environment scenarios
- Add situational awareness to your security incident response
- Investigate and remediate external attacks
- Enable system within different security domains

### Discover the DXC difference

DXC has unmatched experience in developing, deploying and operating cyber defense situational awareness solutions in demanding threat environments.

We are truly the “safe pair of hands” — capable of reducing financial and implementation risk while ensuring that CDSA deployments yield optimal functionality on time and on budget. The world's most demanding cyber defense teams trust DXC for situational awareness technology and for some excellent reasons:

- DXC spent five years researching and developing Cyber Defense Situational Awareness technology and solutions for military, federal, state and local governments — all which also can provide value to organizations in transportation, financial services and other commercial sectors.
- We implemented similar solutions for six U.S. Federal civilian agencies.
- DXC engineered the CDSA solution to minimize technical and financial risks.
- DXC Technology is ready to support your efforts to protect your data and core operational objectives.

## Learn more at www.dxc.technology/security