Cyber Defense Situational Awareness

Protect your data and your mission

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. A consistent response from all warfighters — from the boots on the ground in the theatre of war to the operations team at headquarters — is a necessity.

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, but how can you manage all that information and turn disparate siloed data into actionable intelligence?

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 to better support and protect vital active missions.

Gain operational awareness

The Perspecta Cyber Defense Situational Awareness (CDSA) solution addresses these 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 architecture 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 securely
- Utilize a security canonical model to support solution flexibility and consistency
- Delve into your environment to investigate any indicators of compromise
- Relate incident data to your cybersecurity landscape

perspecta

perspecta

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

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

Perspecta's CDSA solution 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 prioritize that incoming information against mission and operational data.

CDSA then initiates specifically suggested courses of action to address the incident and provide the warfighter with a workflow to consistently mitigate and remediate threats. 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, Perspecta 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 and relationships to other incidents
- View of current threats and incidents that place a mission in jeopardy

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. Perspecta offers advisory and diagnostic capabilities based on standard assessment processes. With these processes we can identify data sources and any gaps in your infrastructure to help facilitate adopting CDSA quickly. Perspecta 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 Perspecta CDSA 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 leveraging functionality 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
- Bring all of your security data into one big picture view

Discover the Perspecta difference

Perspecta 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 Perspecta for situational awareness technology:

- Perspecta spent five years researching and developing our CDSA technology and solutions for military, federal, state and local governments — all of which can provide value through commercial partnership to organizations in transportation, financial services and other commercial sectors
- We implemented similar solutions for six U.S. federal civilian agencies. We were the first to have our system reach operational readiness. Perspecta is currently and was the first to report all CDM systems for all of its agencies up to the DHS Federal Dashboard
- Perspecta engineered the CDSA solution to minimize technical and financial risks. All 35 gate reviews were passed on the first attempt
- We are ready to support your efforts to protect your data and core operational objectives. Perspecta was one of the few CDM integrators to utilize transparent encryption to protect data at rest

Learn more at perspecta.com

perspecta.com | contactus@perspecta.com
15052 Conference Center Drive
Chantilly, Virginia 20151