perspecta

Security operations center services

Security incident analysis and response management

Benefits

- In-depth engineering, architecture and installation expertise supporting ArcSight and Splunk
- Over 300 standard correlations provide alerts that are custom-tuned to your environment and needs
- 24 / 7 / 365 monitoring performed by CONUS-based U.S. citizen staff pre-cleared with a minimum 6C Public Trust clearance

When talking about cybersecurity, proactive detection and an immediate response to threats is becoming essential. But with a surplus of security sensors and tools gathering an overwhelming amount of data, IT teams are being inundated with information and alerts. To make matters worse, with the shortage of qualified cybersecurity professionals, organizations either don't have the expertise, or lack the time and resources to sift through the data and focus on the information that matters most. Additionally, organizations are being challenged to meet a growing number of legislative requirements, technical standards and processes, putting further strain on existing cybersecurity staff.

Strike a balance

With Perspecta's security operations center (SOC) services, you can rely on cybersecurity experts to provide you with a comprehensive view of your security posture, so you can correlate and monitor critical security event data in near real time while acting on events in real time.

Our SOC offering includes an advisory and diagnostic assessment of your environment to create and design a solution that works for you. Perspecta will work with your team to install a security information and event management (SIEM) solution that works for you. We'll deploy log-gathering solutions to ensure a stable detailed feed into the security SIEM and assist with the testing of the environment to ensure that all logging and correlations of the SIEM solution are working correctly.

Once we've confirmed that the environment is stable and processing logs correctly, we can work with your team to turn over the SIEM solution, this includes teaching your team how to use and administer the tool, and working with them to understand how to create and implement correlations.

Additionally, we can provide insight into how to monitor and triage events which optionally includes assisting with incident response management. This also allows Perspecta to work with your teams to engage and educate on proper incident response management so that your team's expertise can continue to grow. With Perspecta's SOC services and experts on your side, you can get out of weeds and start focusing on more strategic, high-value work.

Alternatively, Perspecta can provide operation and management support for your SOC.

Making the most of your SIEM investment

With Perspecta's decades of experience and expertise working with well over 150 public sector customers to implement SIEM and SOC solutions, we are uniquely capable of standing up and supporting a security event monitoring and response management solution based on your needs.

To get the most from your SIEM investment, the Perspecta team has created more than 300 custom correlations that are a part of our standard offering. Our deep understanding of your logging requirements allows for a quick and seamless implementation of industry leading SIEM products to monitor new vulnerabilities and threats on an on-going basis. Our 24 / 7 / 365 availability to assist and augment your existing or evolving SOC to create a mature SIEM offering goes beyond out of the box setup and generic content.

Our work in action

Perspecta's security incident analysis and response management team has a history of providing solid security support against an ever-changing threat landscape. A few of our results are listed below:

- First to detect enterprise wide penetration test for large federal customer. During the initial reconnaissance phase, Perspecta rapidly detected and escalated the penetration test to the customer as well observed and reported on further indicators of compromise (IOC) across the cyber kill chain
- Leveraged our tools and expertise to proactively work with csutomer teams to complete compliance assessments such as annual standards audits, ATO's, POA&M's, and CAPA's.
- Our team regularly performs proactive threat hunting by writing custom signatures in YARA and Snort to detect on-going and emerging threats across our environment. We contribute those signatures to the greater open source threat intelligence cyber analysis platforms, where appropriate. We then analyze the findings matching these rules statistically and dynamically for IoCs, which are imported into SIEM correlation rules. This process of threat hunting has lead the Perspecta SOC to discover indicators of APT-related campaigns and malware before mainstream cyber threat Intelligence sources

Why Perspecta

Perspecta works with the ever-changing cybersecurity landscape to create and implement a custom solution tailored to your environment.

Our expertise in security operations and incident response management augments and enhances your team's capabilities ensuring that in the event of a cybersecurity incident, remediation happens as quickly as possible.

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