The prevention, detection, assessment, and remediation of cyberincidents are top priorities for the United States and essential to national security. This IDC Technology Spotlight looks at how extended detection and response solutions can help.

Federal Agencies Can Ensure Cyber-Resiliency Through Extended Detection and Response

September 2021

Written by: Adelaide O’Brien, Research Director, Government Digital Transformation Strategies

The New Battlefield: Detection and Response at Speed

Reliance on digital channels, ecommerce, remote work, and other virtual interactions exposes new attack surfaces and vulnerabilities that can be exploited by sophisticated global actors. The bleeding edge of digital transformation — hybrid work models and constituent self-service — heightens the potential risk to personal information. Ransomware, phishing, email compromise, insider threats, and nation-state attacks are increasingly common events that cause significant disruptions, high costs, and reputational damage.

Federal agencies face inherent constraints that make protecting their networks and infrastructure challenging and costly. In addition to cybersecurity skill shortages, it is often difficult for agencies to readily hire qualified talent. Also, many agencies have overly complicated IT architectures and environments that are expensive and difficult to protect as well as procurement systems that delay and encumber the acquisition of emerging cybersecurity technologies to combat new threats.

These factors leave too many federal agencies reliant on highly manual processes, outdated technologies, and understaffed and undertrained security operations centers (SOCs) to protect a fragmented environment against a growing number of more sophisticated attacks. This exposure leads to unacceptable risk for agencies and their constituents.

The Executive Order on Improving the Nation’s Cybersecurity (EO 14028), issued on May 12, 2021, makes the prevention, detection, assessment, and remediation of cyberincidents the top priorities for agencies and essential to national security. As a result, there is increasing recognition that detection and response at speed is the new battlefield because the ability to detect and respond quickly can dramatically reduce the potential damage inflicted by cybercriminals.

Subsequently, the release of Memorandum M-21-31 on August 27, 2021, addresses the detailed logging, log retention, and log management requirements of Section 8 of EO 14028 — breaking down what fields are most important to be captured for visibility before, during, and after a cybersecurity incident.
Zero Trust Takes Center Stage

Continued reliance on firewalls and similar border protections alone leaves organizations vulnerable and unprotected. Shifting the focus from perimeter security to more adaptive approaches such as zero trust offers more multifaceted and pervasive defenses. This shift is driven by the need to protect increasingly distributed and virtual cloud-based environments from more numerous and cunning cyberattacks.

Zero trust provides a model for data protection, network security, and identity and access management solutions to work together at scale to secure the enterprise. In a zero trust design, every device, user, network connection, and data exchange is authenticated and authorized. XDR can build upon this layered, risk-based approach to data access with integrated threat intelligence, automation, and analytics to more quickly detect and eradicate specific threats, giving agencies the ability to reduce their risk exposure.

XDR Definition

Many enterprises utilize managed detection and response (MDR) services, which IDC defines as a subset of managed security services (MSS) that encompasses a combination of tools, technologies, procedures, and methodologies to provide full cybersecurity life-cycle capability for an organization. MDR services include a 24 x 7 x 365 cybersecurity staff in a SOC. Service providers can deploy MDR utilizing a mixture of clients' existing capabilities and cybersecurity tools or services and private intellectual property.

According to IDC's Security ServicesView, the number 1 reason to invest in MSS is to improve performance and efficiencies of the following:

» Detection and response
» Emerging security tools
» 24 x 7 support
» Mean time to detect (MTTD)
» Mean time to respond (MTTR)

XDR extends MDR by bringing in various telemetry sources such as messaging, firewall logs, endpoint, network, and identity and access management correlation; integration with data protection platforms; and smart integrations with web and email service providers, threat intelligence, and intrusion detection systems/intrusion prevention systems. XDR provides real-time correlation and analytics across these data sources to detect otherwise unseen intrusions with automated responses used to eradicate the identified threat. In addition to offering the features that an XDR platform provides, some MSS providers supply threat hunting and incident response through retainer, investigation, and forensics capabilities.

An appealing aspect of XDR is that its architecture is made up of endpoint detection response, plus security information and event management (SIEM), plus security orchestration, automation, and response (SOAR). Logs are necessary for compliance and as a reservoir for search, especially when new malware and threats are found. SIEM platforms either natively have SOAR and case management functions or are widely integrated through APIs to initiate response. XDR improves malware detection and antivirus capabilities over reactive endpoint solutions by deploying high-grade security solutions that proactively identify and collect security threats and employ strategies to detect future cybersecurity risks.
External threat intelligence is a valued feature of XDR. The proliferation of cybergangs and adversarial nation-states necessitates that when context is added to full packet collection or metadata collection using the MITRE adversarial tactics, techniques, and common knowledge (ATT&CK) framework, analysis and adapting defenses using artificial intelligence (AI) is expedited.

**Benefits of XDR**

By extending MDR, bringing in various telemetry sources for detection and response, and collecting and automatically correlating data across multiple security layers, XDR provides many benefits, including:

- Strengthening IT and security resilience by making fuller use of cloud-provided features and services
- Providing a 360-degree view of the security environment
- Enabling agencies to deploy the latest security techniques as a service without significant investments in security technologies and undergoing a lengthy procurement process
- Reducing the time-and-effort requirement of chasing spurious alerts, freeing highly skilled experts to tackle more high-value tasks
- Enabling agencies to detect, defeat, and recover from attacks faster and more confidently
- Improving overall performance, financial predictability, and cost effectiveness through MSS automation and analytics
- Providing high-performing incident response, a capability that takes time and skilled personnel, which many agencies lack (MSS can offer various levels of support for deeper investigation analysis along with enhanced guidance on containment, remediation, and future mitigation, expanding agency cybersecurity staff skills and capabilities.)
- Meeting the need to prevent, detect, assess, and remEDIATE cyberincidents as required by EO 14028

**XDR Case Study: National Gallery of Art**

One of the biggest security challenges that the National Gallery of Art in Washington, D.C., faced prior to deploying an XDR solution was having the expertise and resources needed for 24 x 7 audit log monitoring on its network, according to CISO Nabil Ghadiali. The CIO staff of this small agency appreciates the advantages of SOC as a service, which provides speed of detection and speed of remediation, as well as having the SOC analysts review alerts and make sure they are not false positives. Another benefit is the agency doesn't have to purchase and install a SIEM tool, onboard staff who understand how to operate the tool, and make sure the software is up to date and secure. Members of senior management value the XDR solution because deploying their own audit and logging service was cost prohibitive and having the SOC resources and intelligence at their disposal was, as Ghadiali said, "phenomenal." He continued, "One of the greatest things about XDR is that it is organically growing into something that is bigger than any one of us could have stood up independently, and we are seeing this value again and again."
**Trends**

The federal government spends more than $100 billion on IT and cyber-related investments annually. However, when it comes to cybersecurity, many federal agencies have failed or performed poorly, been inadequately managed, and possess security weaknesses, according to a March 2021 report by the U.S. Government Accountability Office (GAO).

As agencies increasingly use hybrid cloud and multclouds and deploy a growing number of applications in their cloud environment, they are confronted by an evolving cyber-risk environment. Early priorities around information security and data protection were mainly focused on compliance, but the threat landscape has proven to be dynamic and increasingly sophisticated. The GAO indicates that more than 28,000 security incidents were reported by federal executive branch civilian agencies to the U.S. Department of Homeland Security (DHS) in fiscal year 2019.

Threat actors may insert adversary-controlled credentials into a cloud account to maintain persistent access and instances within the environment. In December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive and alert about an advanced persistent threat actor. This malicious entity was observed leveraging a software supply chain compromise of an enterprise network management software suite, SolarWinds Orion products, to conduct a cyberattack campaign against U.S. government agencies.

Historically, agencies purchased discrete solutions to address specific threats. But today the security landscape is changing. Data is growing rapidly and is highly fragmented across different departments. Organizations must keep up with the pace of cybersecurity technology to defend themselves against cybercriminals and meet the requirements of EO 10428.

**Considering Accenture XDR for Government**

Accenture provides global, one-stop, end-to-end solutions to help organizations protect entire ecosystems and value chains. Its security services portfolio includes categories such as managed threat operations, managed identity, managed application security, and managed risk. The company provided $3 billion+ in security-related services in FY20 and has more than 8,000 security professionals as well as 880 active and pending patents related to security. Accenture has more than 30 ecosystem partners in security and deploys a market- and capability-focused acquisition strategy, integrating people and technology into its platform.

Accenture also operates eight global cyber fusion centers; two cybersecurity R&D centers (Tel Aviv and Washington, D.C.); and three ICS cyber ranges (Houston, Sydney, and Essen, Germany).

**Accenture Federal Services**

Accenture Federal Services is a wholly owned subsidiary of Accenture, focused on the unique requirements of the U.S. federal government. The company provides Accenture XDR for Government as a FedRAMP Moderate authorized managed service. Accenture XDR for Government can be purchased and deployed in a plug-and-play manner as a vendor-agnostic solution. It is architected today to operate at a FedRAMP High level and integrates natively with the Accenture Insights Platform for Government (AIP.IQ) for enhanced analytics.
Accenture XDR for Government is fully compliant with EO 14028 and provides the following capabilities:

- Full attack-chain visibility for continuous endpoint monitoring, proactive threat mitigation, and vulnerability protection
- Advanced security analytics processes to analyze log data from security controls, network infrastructure, and endpoints to identify events of interest
- A threat intelligence platform that provides insight into threats impacting similar industries and geographies as well as adversary tools techniques and procedures
- 24 x 7 alert monitoring and analysis to identify and escalate incidents (Alert monitoring is automated to improve repeatability efficiency and effectiveness.)
- Threat hunting to identify compromises through targeted proactive discovery across the kill chain, including known and unknown threats
- User behavior analytics through applied machine learning (ML) to identify anonymous user activity to support threat identification
- Tier EL3 advanced logging capable, designed to include a minimum of 12 months of active storage and 18 months of cold storage
- Detection and response integration to detect, analyze, and remove threats from endpoints and networks, such as servers and laptops, leveraging Accenture's XDR solution or a detection response solution from an agency or a client
- Incident response by performing incident triage prioritization and response (i.e., disable user accounts, quarantine hosts, malware detonation) to notable events
- Tailored use cases and playbooks that develop and continuously refine rules, triggers, and responses by applying threat hunter methodology and feedback
- A customer portal with a comprehensive view of agencies' security postures, including risk scoring, detailed analysis of incidents, and recommendations tailored specifically for each agency's environment (The portal provides near-real-time updates to ongoing investigations and metrics.)
- Interactive dashboards that offer a single-pane-of-glass view into an organization's current security posture, including:
  - Real-time performance and status reporting
  - Logging quality metrics
  - Insight into specific incidents and recommendations
  - Incident trending data
  - Industry intelligence on active threats and other security news
As seen in Figure 1, Accenture offers the following metrics comparing industry averages to Accenture XDR responses.

**FIGURE 1: **Response Time Comparisons

<table>
<thead>
<tr>
<th>METRICS THAT MATTER</th>
<th>INDUSTRY BENCHMARKING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean time to Detect</td>
<td>Industry Average: 7 Days</td>
</tr>
<tr>
<td>Alert Coverage</td>
<td>Industry Average: 44%</td>
</tr>
<tr>
<td>Mean time to Respond</td>
<td>Industry Average: 30 Days</td>
</tr>
<tr>
<td>True Positive Rate</td>
<td>Industry Average: 75%</td>
</tr>
<tr>
<td>Automation</td>
<td>Industry Average: 54%</td>
</tr>
<tr>
<td>Mean time to Resolution</td>
<td>Industry Average: 50 Days</td>
</tr>
<tr>
<td>Eco System coverage</td>
<td>Industry Average: 60%</td>
</tr>
</tbody>
</table>

40% of respondents cited that they didn’t have a system in place to track cyber metrics.

24% of respondents cited that have a mature Cyber metrics programs in place

- 2020 Ponemon Institute (581 companies)

*Source: Accenture, 2021*

Accenture Federal Services' Cybersecurity Services include the following capabilities:

- **Strategy & Risk** assesses risks and helps protect mission assets, enabling federal government clients to tap into the robust experience of the firm's global security strategists.

- **Zero Trust** provides data, network, and identity and access management solutions at scale.

- **Application Security** helps clients accelerate release cycles with resilient mission applications.

- **Cyber Defense** enables a proactive approach for clients that builds resilience and speed across networks, infrastructure, and endpoints including cloud, mobile, Internet of Things (IoT), and operational technology/ICS.

- **Operational Technology Security** provides strategies, engineering, and managed services to monitor, protect, and defend industrial control systems and other operational technologies.

- **Full Spectrum Cyber** delivers frameworks, computer network operations, and multidisciplinary tools to dynamically disrupt, mitigate, and neutralize vulnerabilities and attacks.

- **Cloud Monitoring, Visibility, and Management** furnishes capabilities that extend and integrate into multiple IT environments via SaaS, PaaS, and IaaS, seamlessly enabling multiple cloud implementations.
Challenges
As agencies identify gaps in their organization’s cybersecurity practices and undertake a systematic approach for identifying, assessing, and managing cybersecurity risks, they have many choices. With the ongoing changes occurring in today’s security landscape, along with the rapidly evolving pace of technology, organizations must evaluate offerings for today and for the future. It’s important that Accenture inform agencies that its XDR solution meets all requirements of EO 14028. The company also needs to reiterate its commitment to constantly evolve detection, incident response, and recovery processes with the changing threat landscape and in response to these changes continue to embed enhanced AI/ML technologies to advance detection and response capabilities.

Conclusion
EO 14028 makes the prevention, detection, assessment, and remediation of cyber incidents the top priorities for federal agencies and essential to national security. As a result, there is increasing recognition that detection and response at speed is critical to dramatically reduce the potential damage inflicted by cybercriminals. XDR enables improved risk management decisions through reduced time to identify, protect against, detect, respond to, and recover from cybersecurity attacks.

As a managed security services provider, Accenture has the ability to utilize proven cutting-edge security tools as the technology backbone for its managed XDR solution is compelling. The federal government’s security requirements will continue to grow exponentially. IDC believes that to the extent that Accenture can address the challenges described in this paper, as well as continue to invest in the next generation of cybersecurity technologies, the company has a significant opportunity for success in helping government agencies improve their protection of national and economic security.

About the Analyst

Adelaide O’Brien, Research Director, Government Digital Transformation Strategies
Adelaide O’Brien is Research Director for IDC Government Insights responsible for Government Digital Transformation Strategies. Ms. O’Brien assists clients in understanding the full scope of efforts needed for digital transformation and focuses on technology innovations such as Big Data, AI, cybersecurity, and cloud in the context of government use cases such as customer experience, data-driven benefits and services, and public health protection.
MESSAGE FROM THE SPONSOR

Accenture Federal Services’ XDR for Government is available as a managed service via established government contracting vehicles, such as NASA’s Solution for Enterprise-Wide Procurement Government-Wide Acquisition Contract (GWAC). Learn more at accenturefederal.com or contact us at XDR.info@accenturefederal.com.