splunk> | Deloitte.

SOLUTION GUIDE

The New Evolution of Managed Detection and Response: Deloitte MXDR

Splunk: Helping to Power MXDR by Deloitte

As the pace of change quickens and disruption becomes the norm, digital transformation is the key to making organizations across industries more agile and efficient. Yet digital transformation initiatives can also create new cybersecurity challenges that threaten profitability, competitive advantage, and reputation.

Cyberattacks are becoming more frequent and increasingly sophisticated even as the bar to entry for malicious hackers gets lower thanks to “innovations” such as ransomware-as-a-service. In addition, IT infrastructure continues to grow in scale, and complexity becomes the nemesis to effective, efficient, and easy to use security.

To combat these challenges without increasing the burden on overtaxed IT teams, Deloitte created the managed extended detect and respond (MXDR) platform, a set of composable and modular Software-as-a-Service (SaaS) business applications that helps drive measurable cybersecurity outcomes—all enabled by industry-leading cybersecurity technology like Splunk.

Helping to power MXDR by Deloitte, Splunk Enterprise Security (ES) on Splunk Cloud, MXDR by Deloitte provides continuous intelligence, threat visibility and telemetry across their clients' IT and operational technology (OT) assets, from the cloud to the ground to the edge, so clients can see where threats lie and gain sophisticated defensive capabilities. Deloitte's US and Global SOCs provide 24x7x365 L1, L2, and L3 prevention, detection, response, and remediation, using Splunk as the analytical nucleus of MXDR's modular set of FedRAMP-authorized and commercially available cloud-native and SaaS-based services.

Benefits

- Outcome-focused capabilities that provide resolutions to incidents and threats across a client's organization
- Near real-time breadth & depth of visibility into threats and enhanced analytics
- Advanced & industry-leading technology capabilities
- Full visibility and collaboration with 24x7x365 service delivery

Services	Capability Descriptions
Unified Extended Detection and Response (XDR)	Central XDR security information and event management (SIEM)/logging/analytics management combines agent, agentless, Endpoint Detection & Response (EDR), Network Detection & Response (NDR) data fusion and 24x7x365 SLA-driven support to improve the mean time to prevent, detect, and respond to cyber attacks
Digital Risk Protection	Continuous digital asset monitoring that is operationalized with analytics & actionable intelligence to promptly identify and decrease the impact of exposed data
Cyber Threat Intelligence	Predictive cyber threat intelligence informed by adversary tactics, techniques and procedures (TTPs), tailored analysis, and malware analysis
Insider Threat Detection	Evaluate the environment to identify users and roles with relevant access and implement controls
Adversary Pursuit: Proactive Hunting	Continuous hunting leveraging intelligence, artificial intelligence/machine learning, and a hypothesis driven approach with the Deloitte Threat Hunting Platform and Master Hunter Operator trained teams
Cloud SaaS: Prevention, Detection and Response (PDR) Hunting	Leverage cloud access security broker (CASB) and data loss prevention (DLP) technology to detect and respond to SAAS targeted attacks
Cloud Security: PDR	Initiate service discovery to learn what is and is not secured, along with supporting instances, containers, cloud services, serverless, various cloud platforms and operating systems
Zero Trust: Identity PDR	Provide visibility into identity, anomalous behavior, detection of lateral movement, and advanced threats to detect compromised identities
Enterprise PDR	Support assets both on and off network to prevent both malware and ransomware attacks using next generation antivirus and end point detection & response
Attack Surface & Vulnerability Management	Bolster host and network endpoint and virtual and private clouds across multiple technology environments providing real time visibility into vulnerabilities, asset tracking, and rogue system detection
Incident Response (IR)	Identify incident management gaps in current processes and procedures, and streamline response to adversary techniques to provide containment, eradication, and remediation actions to remove the adversary from the client environment
Master Operator & Hunt Training	Provide advanced training to equip security analysts and operators with hands-on technical skills to defeat various adversaries

Why Deloitte and Splunk?

As a leading global systems integrator and Splunk elite level alliance, Deloitte applies its breadth of industry and technology experience to help their clients increase client security, responsiveness, and value. Deloitte helps clients enhance business outcomes by integrating leading technologies with Splunk ES at the core. As the leading security analytics platform, Splunk ES is the prefered choice to drive threat detection and investigation together with Deloitte's professional teams to provide comprehensive cybersecurity outcomes and help clients reimagine how work gets done, deliver material improvements in revenue and reduce costs with higher job satisfaction.

The MXDR by Deloitte platform represents a new evolution of managed security services: an all-cyber approach to help meet current and future cybersecurity challenges. MXDR provides a customized interface that offers rapid analytics and reporting with high availability. It is designed to improve mean time to prevent, detect, contain, and respond to cyberattacks against your security assets with a consolidated set of tools that reduces complexity and total cost of ownership.

To learn more about the MXDR by Deloitte platform and Splunk Cloud and ES, contact us!

Tim Duffy
Global Partner Development Manager
tduffy@splunk.com

Alicia Henneberry
Partner Development Manager
ahenneberry@splunk.com

Rob Joseph
Alliance Sales Manager, Public Sector
rjoseph@splunk.com

Curt Aubley
Managing Director
Detect & Respond Leader
caubley@deloitte.com
Deloitte & Touche LLP

Mike Morris
Managing Director
Technology & Solutions Leader
micmorris@deloitte.com
Deloitte & Touche LLP

Steve Mahar
Managing Director & Sales Leader
Detect & Respond
smahar@deloitte.com
Deloitte Services LP

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

22-22217-Splunk-Deloitte Guardian Detect and Respond Services-SG-101