Joint Solution Brief

SDG NETWITNESS

The Future of Cybersecurity: Implementing Proactive Threat Detection and Response

OVERVIEW

The Detection Challenge

The race to combat cybersecurity attacks is relentless and despite the complexity of cyber-attacks increasing, according to Help Net Security, the median attacker dwell time – the time from when an attack starts to when it's detected – has shrunk from 10 to eight days for all attacks, and to five days for ransomware attacks during the first half of 2023.

While this is commendable, it still presents a significant window of opportunity for cybercriminals, competitors, aggressive nation states, or even disgruntled employees to gain unauthorized access to your vital business systems and critical information assets.

A Proactive Defense is the Only Good Offense

The best offense to thwart a cyber-attack is a proactive defense. The goal is to significantly reduce the time it takes to identify and combat advanced cyber threats by swiftly identifying and neutralizing emerging threats before damage can occur.

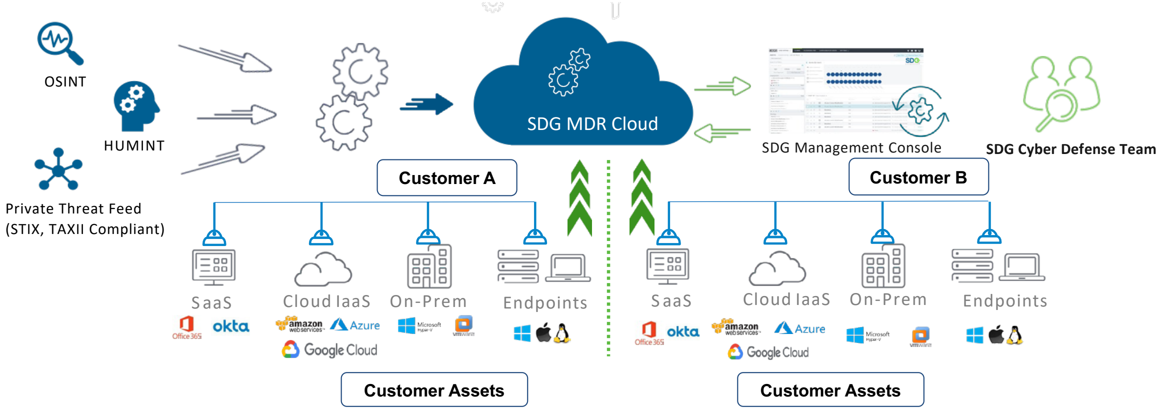
Unfortunately, few organizations have the means to hire, train, and manage the dedicated team of cybersecurity experts with the expertise and ability to vigilantly monitor their network, applications, and systems around the clock that it takes to ensure the security and resilience of their organization. This inability to proactively defend themselves leaves the organization vulnerable to downtime, data loss, and a damaged reputation.

SDG MANAGED DETECTION AND RESPONSE SERVICE

As the world continues its digital transformation, the landscape of threats is in a constant state of flux. This ever-evolving environment exposes businesses, regardless of their size, to potential cyber-attacks. The ability to detect and respond to risks in real-time has become crucial.

SDG's Managed Detection & Response service provides a comprehensive 24/7 Cyber Defense Center (CDC) that seamlessly integrates with your organization's inhouse team. By partnering with SDG, you gain access to a range of security advantages that encompass the key elements of a SOC; people, processes, and technology.

Our managed detection and response (MDR) teams consist of skilled professionals, including threat researchers, threat hunters, security analysts, administrators, product specialists, and forensic experts that work in concert to create the ultimate proactive defense against threats. Based out of our advanced Cyber Defense Center, our team leverages the logs and packets provided by the intelligence driven NetWitness XDR platform to gain complete visibility into the organization's environment. SDG's diligence combined with the NetWitness XDR platform's robust orchestration and automation, helps to ensure a near-zero blind spot. This visibility is the crucial first step to protection and crucial to detection.



NETWITNESS EXTENDED DETECTION AND RESPONSE SOLUTION

NetWitness XDR (extended detection and response) combines visibility, analytics, and automation into a single platform. This comprehensive XDR solution accelerates SDG's threat detection and response by collecting and analyzing data across all capture points (logs, packets, NetFlow, endpoint, and IoT) and computing platforms (physical, virtual, and cloud), enriching data with threat intelligence and business context.

The NetWitness "network-forward" approach allows SDG to search, correlate, and analyze the ever-increasing volumes of data generated by modern organizations. More data means more places for threats to hide, and NetWitness XDR ensures our team has internal data-driven visibility.

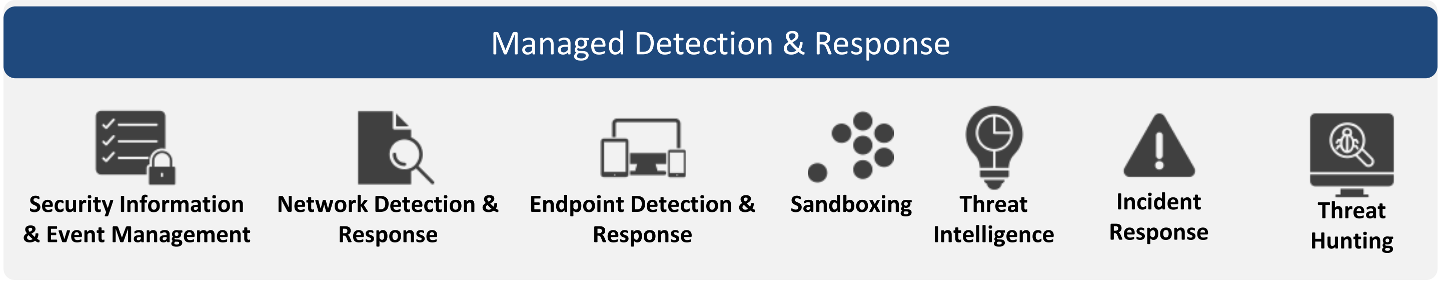
With a SaaS-based pay-as-you-go pricing model, pre-built content, and research-driven use cases, SDG can tap into the power of the New-gen Cyber Defense Center for cost-effective, scalable results.

SDG'S APPROACH

Implementing and Managing Advanced Cyber Defense

SDG's comprehensive Managed Detection & Response Service delivers swift implementation and seamless operation of a comprehensive Cyber Defense Center (CDC). Our experts diligently operate and manage the CDC 24 hours a day, 365 days a year so organizations can focus on their business strategies centered on revenue and success.

- **Collaborating with you to design data collection methodologies**, which encompass defining the systems to be monitored, determining the triggering events for alerts, and establishing routine operational tasks like updates. Additionally, we implement the necessary technology/tools for efficient data collection.
- **Working closely with you to develop a cyber-threat model** that serves as the foundation of optimizing the XDR system. We then proceed to implement the required XDR configuration based on this model.
- **Monitoring, detecting, and analyzing security events** within your organization in real-time. Our vigilant team keeps a constant watch to ensure prompt identification and response to any potential threats.
- **Securely managing the data collected** from your organization, which includes employing encryption techniques and securely transmitting it to SDGs MDR Platform. Here, comprehensive log & telemetry correlation takes place, integrating data from various security systems.
- **Continuously adapting the data** collection methodology and system configuration to align with evolving threat landscape and your organization's changing needs. This ensures ongoing optimization and effectiveness.
- **Providing access to detailed reports and interactive dashboards**, enabling you to keep your board members and executives well-informed about the security posture and relevant insights.



Managed Detection & Response

Security Information & Event Management

Network Detection & Response

Endpoint Detection & Response

Sandboxing

Threat Intelligence

Incident Response

Threat Hunting

THREAT INTELLIGENCE AND ANALYSIS

Through our advanced data analytic capabilities with the NetWitness platform, we integrate various components such as SIEM, network security monitoring, endpoint monitoring, UEBA, payload analysis, and offline big data analytics into an intelligence-driven approach. To enhance our ability to detect the most sophisticated advanced persistent threats, we employ the following strategies: vv

- Implementation of focused detection rules tailored to the client's IT environment and the evolving threat landscape.
- Deep understanding of the context, incorporating threat intelligence and knowledge of applications within the attack perimeter.
- Efficient response mechanisms by establishing strong links with IT Service Management and the security team.

- Utilization of security analytics that prioritize user behavior analysis, identification of external attacks, application monitoring, and DNS malware detection to identify hosts infected with malware.
- Predictive attack discovery facilitated by SDG Attack Surface Discovery Tool in combination with network of honeypots and mapping it to the MITRE ATT&CK framework.

CONCLUSION

Data driven intelligence lies at the core of SDG's success in managed detection & response. SDG, a distinguished managed detection and response service provider, in partnership with NetWitness XDR technology, allows organizations to transition from being the hunted to becoming threat hunters themselves.

To cater to an organization's specific security requirements, SDG offers a flexible delivery approach that accommodates various scenarios, be it on-prem, SaaS-based, or hybrid. With a comprehensive portfolio of cybersecurity solutions, SDG can assist organizations throughout their cybersecurity journey, from devising strategies to managing secure hybrid environments that promote a security-first approach.

ABOUT NETWITNESS

NetWitness is a network security company that provides real-time network forensics automated threat detection, response, and analysis solutions.

ABOUT SDG

SDG is a leading provider of technology, consulting, and managed services that enable organizations to confidently execute cybersecurity, identity, and risk management solutions to mitigate risk, protect assets, and grow securely. To learn how SDG can help your organization, visit SDGC.com or call us, +1 203.866.8886.

SDG

75 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com