SIMPLIFYING CYBER SECURITY
SOFTGEN AUSTRALIA

XDR-AS-A-SERVICE

“Single Pane of Glass to analyze, investigate and responds to security alerts detected across the different security solutions”

WHY DOES YOUR BUSINESS NEED XDR AS A SERVICE?

Your business is growing, and so as your endpoints, networks, cloud infrastructure, and applications. XDR as a Service is an essential tool for businesses looking to protect their growing network of endpoints, networks, cloud infrastructure, and applications. While traditional security services such as EDR and MDR provide rapid prevention, detection, response, and threat-hunting solutions, they are often seen as limited point solutions that address only a single aspect of network security. XDR addresses these limitations by pulling together the capabilities of multiple security solutions, such as Managed Detection and Response (MDR), Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), User Behavior Analytics (UBA), Network Detection and Response (NDR), Network Flow Analytics, System X Threat Containment, and Dark Web Monitoring, into a single platform. XDR provides a more unified and holistic approach to defending against all types of attacks, including standard cyberattacks, misuse of networks, unauthorized access, and more. It also helps to expedite the speed of detection and remediation of known and unknown threats. By consolidating multiple security solutions into a single platform, XDR enables businesses to more effectively protect their growing network of endpoints, networks, cloud services and applications.

DO YOU KNOW?

- **As per the SANS, only 40 % of SOC have an incident response capability**
- **Security Services supported by AI can reduce the cost by 60%**
- **93% of organizations failed to respond to threats on the same day**
- **9 in every 10 analysts acknowledge the need for automation in threat management**

XDR-AS-A-SERVICE: SOLUTION TO A NEW WORLD SECURITY CHALLENGE

Conventional security solutions, such as Endpoint Detection and Response (EDR), User Behavior Analytics (UBA), Network Detection and Response (NDR), and Security Information and Event Management (SIEM), only provide a fragmented view of potential attacks and infections. This fragmentation can lead to several problems for the SOC team:

- The high volume of false positive incidents generated by these tools can lead to wasted time spent on triaging and investigating these alerts, which can take away from investigating actual incidents.
- The high number of false positives and need for complex investigations can lead to longer response and containment times for a breach.
- The use of multiple tools can make it difficult for the SOC team to have a comprehensive view of the security posture of the IT infrastructure, and they spend a lot of time switching between different consoles.

XDR addresses these challenges by integrating multiple security solutions and bringing all relevant security information to a single pane of glass. This integration:

- Reduces the response time for alerts by bringing information from all security solutions into one place
- Reduces alert fatigue for Security Operation Center Analysts
- Out-of-the-box integration and automation of XDR helps Security Operation Center team in daily and routine reports.

With XDR, the SOC team can easily and quickly identify and respond to potential threats, reducing the risk of data breaches and improving overall security posture.

EXTENDED DETECTION & RESPONSE – BENEFITS

- **Single Pane of Glass for all Security Solutions**
  XDR integrates all security solutions and provides a single pane of glass to analyze, investigate and mitigate security risks.
- **Expedite Response Time**
  XDR decreases response time to alerts by aggregating and correlating data from multiple security solutions. It also detects and correlates abnormal behavior with well-known attacks.
- **Easy Deployment in Cloud Environment**
  XDR is a turnkey service with zero-touch deployment. Businesses do not need any additional infrastructure on-premises and can easily integrate currently deployed solutions.
- **Expose Stealthy Threats**
  XDR provides extensive knowledge about the abnormal behavior to the IT Team and helps to contain the threat before they cause any damage.
- **Increase SOC Productivity**
  XDR increases the productivity of the SOC team by eliminating the need for analysts to switch between different consoles. It also helps them grasp knowledge from each console, reducing false positives.
- **Behavioral Rules to Stop Future Attacks**
  XDR provides functionality to identify a behavioral baseline of identities in the IT environment over time, creating rules to identify non-traditional and zero-day threats that can bypass conventional signature-based methodology.

MANAGED XDR-AS-A-SERVICE - FEATURES

- A SOC 2 Type II and ISO 27K1 Certified SOC
- Industry Beating Priced Premium Quality Service
- Simple Per-Asset Pricing Model
- 1000+ customers across 20+ countries
- Global Locations
- Vulnerability & Patch Mgmt Solution Agnostic Service
- Fixed Monthly Fee (No Nickel-&-Dime!)
- Fully-Managed Turnkey/Co-Managed Options
- 15-Min Gold SLA
- GDPR and Local Privacy Laws Compliant

SUPPORTED XDR PRODUCTS

TREND MICRO™

CROWDSTRIKE

CORTEX

SOPHOS

cynet

McAfee™

FIREEYE™

CONTACT US

CONTACT US NOW!

+61 2 9416 0416

sales@sgen.com.au

www.sgen.com.au