

# Unlock the Power of XDR to Maximize Protection Against Cyberattacks

Today, organizations are embracing extended detection and response (XDR) to better combine telemetry data from SIEM, NDR, EDR, and threat intelligence feeds. XDR also helps to build powerful endpoint detection and response strategies against advanced threats.

**52%** of security personnel are confident in XDR's capability to supplement their existing security operations technologies

## Top Drivers for Security Leaders to Adopt XDR

### Security Tools Complexity

**51%**

Agreed that existing tools struggle to detect & investigate advanced threats

### Need for Expert Security Skills

**38%**

Agreed that specialized skills are required to harness current tools

### Event & Threat Correlation

**36%**

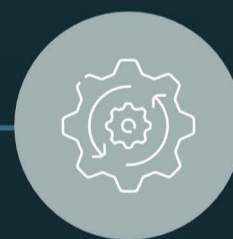
Agreed that current tools lack the ability to efficiently correlate alerts

## How XDR Helps Businesses to Improve Cyber Resilience



### Clear Visualization

Presents a simple visualization of complex attacks and their trajectory across a kill chain



### Response Automation

Automates response to block ongoing attacks



### Advanced Analytics

Offers advanced analytics to detect and tackle sophisticated & persistent attacks

SAMI-AEC's Security Operations Centre as a Service can help businesses to integrate visualization, advanced analytics, and automation in its cybersecurity offerings, equipping them with robust threat detection and response capabilities.