Improvements in Efficacy and Efficiency yields security efficacy and efficiency benefits for organizations. This is achieved through a highly automated approach to threat detection and response that aggregates data and technologies. The research sought to uncover whether an organization’s detection and response strategies, processes, and tools have an impact on security outcomes.

On behalf of Trend Micro, ESG conducted a research survey of 1,000 enterprise respondents. The study found that organizations with high maturity in XDR experienced numerous benefits, including better security posture, improved detection and response, and reduced dwell time.

The Need for XDR

Security teams are facing unprecedented challenges and changes:

- **85%** of respondents say threat detection and response is getting harder, outnumbering those saying easier by 4:1.
- **Teams need a force multiplier more than ever** to keep up with the changing threat detection and response landscape (43% versus 22%).
- Organizations with high maturity are **2x more likely** to describe their detection and response as effective (70% versus 35%).
- Organizations with high maturity are **2.2x more likely** to report a short attack dwell time (i.e., a few days or less) (65% versus 29%).
- Organizations with high maturity are **2x more likely** to be very confident in their ability to keep up with the changing threat detection and response landscape (43% versus 22%).

Measuring XDR Maturity

Organizations were placed into one of three XDR maturity stages based on their responses to two questions:

1. **Question 1:** How would you describe the process of integrating and aggregating data from your security, threat detection, and response controls?
   - **Low XDR Maturity:** Fragmented/Siloed
   - **Mid-level XDR Maturity:** Fragmented/Aggregated
   - **High XDR Maturity:** Integrated/Aggregated

2. **Question 2:** How would you describe your ability to quickly integrate and respond to security alerts you ignore?
   - **Low XDR Maturity:** Manual
   - **Mid-level XDR Maturity:** Semi-automated
   - **High XDR Maturity:** Fully automated

Outcomes Correlated with XDR Maturity

**Efficiency:**

- Organizations with high maturity cut the number of successful attacks experienced in the last 12 months by 55% (on average relative to those with low maturity 1.5x versus 13.2 attacks on average).
- Organizations with high maturity are **2x more likely** to report a short attack dwell time (i.e., a few days or less) (65% versus 38%).
- Organizations with low maturity are **2.6x more likely** to be overwhelmed by the number of alerts and response teams as typically overwhelmed (59% versus 22%).
- Organizations with high maturity cut the number of successful attacks experienced in the last 12 months by 55% (on average relative to those with low maturity 1.5x versus 13.2 attacks on average).
- Organizations with high maturity are **2x more likely** to report a short attack dwell time (i.e., a few days or less) (65% versus 38%).

**The Bigger Truth**

Outcomes are a result of proactive planning and building the necessary foundation for XDR. Organizations that have invested in strong security postures, robust and efficient technologies, and a comprehensive strategy are better equipped to detect, respond, and recover from attacks. The research findings highlight the importance of prioritizing XDR maturity to enhance security outcomes.