MEASURING THE XDR PAYOFF:
Hard Data Shows Better Efficacy and Efficiency Improvements

On behalf of Trend Micro, ESG conducted a research survey to better understand the efficacy and efficiency benefits for organizations of implementing XDR (XDR: X, Threat Detection and Response). The research sought to uncover whether an organization’s detection and response strategies, processes, and tools are effective. The research was based on survey responses from 500 security and IT professionals responsible for their organization’s various security, threat detection, and response controls.

Outcomes Correlated with XDR Maturity

**Efficacy:**
- Organizations with high maturity are 2.6x more likely to replace their automated systems in the last 12 months (16% vs. 38%)
- Organizations with low maturity are 2.2x more likely to keep up with thechanging threat landscape and response timelines (65% vs. 29%)
- Organizations with high maturity are 2x more likely to be very confident in their ability to keep up with changing threat detection and response timelines (43% vs. 22%)
- Organizations with high maturity are 2.6x more likely to cut the number of successful attacks experienced in the last 12 months by 55% on average relative to those with low maturity (3.5 versus 14.2 attacks on average)
- Organizations with low maturity are 2.5x more likely to have less than one security professional to respond to alerts and are overburdened (36% versus 22%)
- Organizations with high maturity are 2.2x more likely to report a shorter attack dwell time (3 days or less) (58% vs. 22%)
- Organizations with low maturity are 2.5x more likely to describe their detection and response teams as typically overwhelmed (58% vs. 22%)
- Organizations with high maturity cut the number of security alerts they ignore nearly in half (20% versus 38%)
- Organizations with low maturity are 2.6x more likely to have more than 50 security and automation/technology staff per 8 full-time employees to replace their automated systems.

**Only 21%** reported their organization excelled in both areas, earning a high maturity designation for XDR maturity.

**The Bigger Truth**
XDR is a paradigm shift in the operation of security teams to effectively detect and respond to threats across the enterprise. This needs to be supported by investments in people, processes, and technologies. Organizations are quickly discovering that XDR is the only way to move past overwhelmed, stressed-out security teams and achieve meaningful outcomes. Organizations need to take a serious look at their current security posture and consider the potential investments needed to achieve a balanced and effective solution.

---


© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.