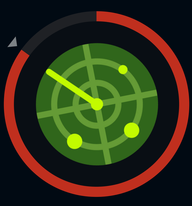
ESG Enterprise Strategy Group | Getting to the bigger truth.™

MEASURING THE XDR PAYOFF:

Hard Data Shows Better Efficacy and Efficiency Improvements

On behalf of Trend Micro, ESG conducted a research survey of 500 security and IT professionals responsible for their organization's detection and response strategies, processes, and technologies. The research sought to uncover whether an approach to threat detection and response that aggregates data across many security controls in a highly automated fashion yields security efficacy and efficiency benefits for organizations.



The Need for XDR

SECURITY TEAMS ARE FACING UNPRECEDENTED CHALLENGES AND CHANGE:

85%

of respondents say threat detection and response is getting harder, outnumbering those saying easier by 43:1.

THE REASONS:

Bad actors' attacks continue to be more sophisticated while organizations grapple with security stack complexity and a skills shortfall.

THREAT COMPLEXITY

+

ATTACK SURFACE

At the same time, the attack surface in most organizations is rapidly expanding, with more diversity in device types and cloud services in use than ever before.

Measuring XDR Maturity

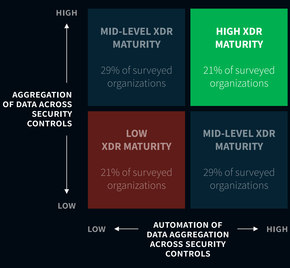
RESPONDENTS WERE PLACED INTO ONE OF THREE STAGES OF XDR MATURITY BASED ON THEIR RESPONSES TO TWO QUESTIONS:

QUESTION 1:
How would you describe the information/data in your organization's various security, threat detection, and response controls?

ANSWER OPTIONS:
A. Fragmented/Siloed
B. Integrated/Aggregated

QUESTION 2:
How would you describe the process of integrating and aggregating data from your organization's various security, threat detection, and response controls?

ANSWER OPTIONS:
A. Manual
B. Automated



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

Outcomes Correlated with XDR Maturity

EFFICACY:

DEFENSE

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 (6.5 versus 14.3 attacks on average).

KEEPING UP

Organizations with high maturity are **2x more likely** than those with low maturity to be very confident in their ability to keep up with the changing threat detection and response landscape (43% versus 22%).

DWELL TIME

Organizations with high maturity are **2.2x more likely** than those with low maturity to report a short attack dwell time (i.e., a few days or less) (65% versus 29%).

EFFICIENCY:

OVERWHELMED

Organizations with low maturity are **2.6x more likely** than those with high maturity to describe their detection and response teams as typically overwhelmed (58% versus 22%).

ALERTS

Organizations with high maturity cut the number of security alerts they ignore **nearly in half (20% versus 38%).**

AUTOMATION

Organizations with high maturity believe that it would take the equivalent of **8 full-time employees** to replace their automated systems.

The Bigger Truth

XDR promises a new level of automation and fidelity for security teams that are struggling to keep up with the rapidly expanding and complex threat landscape. With no end in sight for the skills shortage and accelerating timelines for digital transformation initiatives, security teams need a force multiplier more than ever.

READ THE REPORT

TREND MICRO

Source: ESG Research Insights Report commissioned by Trend Micro, *The XDR Payoff: Better Security Posture*, September 2020.