Enterprise Strategy Group | Getting to the bigger truth.™

Closing Security Operations Gaps with MDR

As the escalating risk of damaging cyber-attacks steals mindshare and budget from core business objectives, organizations must respond by strengthening cybersecurity programs. Central to all cybersecurity programs is security operations (SecOps), responsible for monitoring and protecting all facets of the digital attack surface.

Despite Investments, Security Operations Is More Difficult

MORE THAN HALF of respondents think SecOps is **more difficult** today than it was two years ago.

» **Top five reasons SecOps is more difficult.**

1. **41%** The threat landscape is evolving and changing rapidly
2. **39%** The attack surface is continuously changing and evolving
3. **37%** The volume and complexity of security alerts have increased
4. **34%** My organization's increased use of public cloud services
5. **33%** It is difficult to keep up with the operational needs of security operations technologies

Rethinking Program Strategies

Attack surfaces and the threat landscape have grown in both size and complexity and so has the utilization of security controls, generating thousands of alerts and massive amounts of security data. Security teams are rethinking overall program operations to further incorporate asset and risk data from IT and line-of-business teams to focus on those threats that pose the most significant risk to organizational objectives.

98% of organizations are either already engaged with an MDR provider or plan to engage in the next 12 months.

88% of these organizations plan to increase MDR use over the coming 12 months.

» **Key value drivers for MDR engagement.**

OPERATIONAL IMPROVEMENT AND EFFICIENCY.
MDR can help organizations reduce the total cost of security operations in several ways, such as infrastructure, personnel, and management. It can also address the "alert fatigue" issue and improve the likelihood that false positives will be reduced significantly.

IMPROVED CYBERSECURITY EFFICACY AND REDUCED RISK.
MDR can help organizations stop threats already in progress, improve detection of potential threats and advanced persistent attacks, activate proactive threat hunting, and institutionalize stronger controls to identify and prevent future attacks.

» **Primary reasons behind organizations' usage of or plans for managed services.**

55%
Focus:
My organization wants to focus its security personnel on more strategic security initiatives rather than spend time on security operations tasks.

52%
Services:
My organization believes service providers can do a better job with security operations than we can.

49%
Augmentation:
My organization believes that a service provider can augment our SOC team with security operations.

42%
Skills:
My organization doesn't have adequate skills for security operations.

> **Many 'Generation 1.0' MDR solutions were designed and implemented for a different era:** less data, fewer threats, simpler detections."
>
> *- Dave Gruber, ESG Principal Analyst*

New Requirements for MDR

Many "Generation 1.0" MDR solutions were designed and implemented for a different era: less data, fewer threats, simpler detections. The next generation of MDR solutions must be equipped to protect a more diverse attack surface, detect more complex threats, and leverage a more risk-centric approach to prioritization and mitigation.

- 24/7 monitoring of events and logs.
- Continuous and scalable network monitoring and threat analysis.
- Regulatory compliance reporting.
- Detailed, real-time analysis based on threat detection, triage, investigation, and forensics.
- Fast and high-visibility information on suspicious activity and alerts by volume, location, and type.
- AI-driven recommendations for contextual response options.
- "Human" security advisors in direct contact with in-house teams.
- Vulnerability assessments, prioritization, and mitigation guidance.

When considering the large number of potential service providers that can deliver some, most, or even all outsourced MDR capabilities, **organizations should look for partners that can deliver:**

- Contextual threat intelligence.
- Demonstrated threat-hunting capabilities.
- Extensive capabilities in multi-cloud and hybrid cloud environments, zero trust, and the shared responsibility model of cloud security.
- Proven track record in the organization's geographic coverage area, vertical market, and regulatory profile.
- A long-term commitment to cloud-based MDR.
- A proven ability to scale their service over time, based on innovative technology, proven processes, and demonstrated expertise by its people.

The Bigger Truth

As the escalating risk of damaging cyber-attacks steals mindshare and budget from core business objectives, organizations must strengthen cybersecurity programs. While use cases vary, most are leveraging MDR service providers to grow and scale their programs.

The Dell Technologies approach to managed detection and response combines flexible, intelligent, and scalable technology with experienced cybersecurity professionals, helping organizations of all sizes and resource profiles accelerate and strengthen security programs.

LEARN MORE

DELL Technologies

Source: ESG Complete Survey Results, SOC Modernization and the Role of XDR, August 2022.