

# 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.

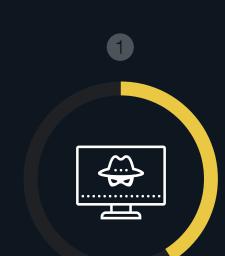
# Despite Investments, Security Operations Is More Difficult



### **MORE THAN HALF**

of respondents think SecOps is more difficult today than it was two years ago.

» Top five reasons SecOps is more difficult.



41% The threat landscape is evolving and changing rapidly



39% The attack surface is continuously changing

and evolving



37% The volume and complexity of security alerts have increased



34% My organization's increased use of public

cloud services



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 riskcentric approach to prioritization and mitigation.



24/7 monitoring of events and logs.



activity and alerts by volume, location, and type.

Fast and high-visibility information on suspicious



and threat analysis.

Continuous and scalable network monitoring



response options.

Al-driven recommendations for contextual



Regulatory compliance reporting.



with in-house teams.

Vulnerability assessments, prioritization,

"Human" security advisors in direct contact



detection, triage, investigation, and forensics.

Detailed, real-time analysis based on threat

and mitigation guidance.

organizations should look for partners that can deliver:

When considering the large number of potential service providers that can deliver some, most, or even all outsourced MDR capabilities,



Contextual threat intelligence.



coverage area, vertical market, and regulatory profile.

Proven track record in the organization's geographic



Demonstrated threat-hunting capabilities.

Extensive capabilities in multi-cloud and



A proven ability to scale their service over time,

A long-term commitment to cloud-based MDR.



shared responsibility model of cloud security.

hybrid cloud environments, zero trust, and the



and demonstrated expertise by its people.

based on innovative technology, proven processes,

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

The Bigger Truth

**D<**LLTechnologies