Key Takeaways from SECURITY UNLOCKED: Emerging Threats, Business Risks & the Case for MDR Webinar

Insights from Featured Speakers:

Mark Sangster
Chief of Strategy, Adlumin

Troels Rasmussen
General Manager, Security Products, N-able

Rick Mutzel
Chief Information Security Officer, Omega Systems

In this document:

Speakers from Adlumin, N-able, and Omega Systems discussed the current threat landscape, how businesses are aligning their security priorities with their business needs, and the importance of managed detection and response (MDR) as an essential tool for any business's security stack.

***Responses have been edited and streamlined to allow for easier reading.*

Adlumin
adlumin.com

N-able
n-able.com

Omega Systems
omegasystemscorp.com

Key Takeaways from
SECURITY UNLOCKED: MDR Webinar

WEBINAR Q&A

What's Included?

The Current Threat Landscape

Business Challenges

- Cybersecurity: A Business Risk, Not an IT Problem
- Limited Resources & Budget Constraints
- Evolving Regulatory Requirements
- Aligning IT & Business Priorities

The Solution: Managed Detection & Response (MDR)

- Game-Changing MDR Capabilities

The Current Threat Landscape

Q : How would you describe the shift in sophistication we've seen from hackers and threats over the last 5, 10, or 15+ years?

A : "We've seen the industrial revolution of cybercrime. These groups operate like well-funded intelligence agencies. They're associated with governments in many cases. We've also seen the development of software as a service (SaaS) across these organizations. I call these guys the ‘Misfortune 500’ because they are like Fortune 500 companies. They have structures and compensation models; they know what they're doing."

— Mark Sangster, Adlumin

The Current Threat Landscape

Q : What threats or tactics are keeping you up right now?

A : "Your company's weakest link will always be your end users. Social engineering has become incredibly good, making it difficult to distinguish valid from malicious content. End-user awareness is a critical weakness, leaving 'low-hanging fruit' for attackers."

— Rick Mutzel, Omega Systems

A : "Attackers are even exploiting regulatory reporting to extort organizations after breaches. The barrier to cybercrime is lower than ever. You can buy sophisticated attacks as a service, and some businesses still have the 'it only happens to the neighbor' mentality."

— Troels Rasmussen, N-able

Q : Are AI-driven productivity apps aiding hackers in becoming more effective or deceptive?

A : “Imagine a tool that generates realistic talking faces from a single photo and voice clip. Hackers could use this to create deepfakes of executives, making phishing scams or fraudulent transfers much more believable. With such tools, it becomes harder and harder to distinguish between real and fake.”

— Mark Sangster, Adlumin

Business Challenges

Cybersecurity: A Business Risk, Not an IT Problem

Q : For C-level executives without an IT background, security threats can seem abstract. So, why should cybersecurity matter to them?

A : “Cybersecurity is not an IT problem; it's a business risk to manage. Excuses for not treating it like any other business risk—such as a natural disaster or economic headwinds—are dwindling. Ignorance is not bliss when it comes to cyber risk; it's a potential liability. As one large law firm puts it, your liability is limited only by the creativity of the plaintiff's lawyer or the aggressiveness of the regulator's auditor."

— Mark S.

A : “Cyber incidents are no longer a matter of 'if' but 'when.' Businesses need to be prepared for the inevitable aftermath. Do you have the tools, policies, and a dedicated team to manage a cyberattack? The ostrich approach of ignoring the risk won't work. Having a plan and testing it beforehand is crucial for effective incident response."

— Rick M.

A : “Just as financial security isn't only for the accounting department, security shouldn't be just an IT concern. Strong security policies and procedures are essential for any resilient business. Security is as crucial as reliable internet or functional equipment, enabling core business functions. In industries like healthcare and finance, this responsibility is even greater due to sensitive data."

— Troels R.

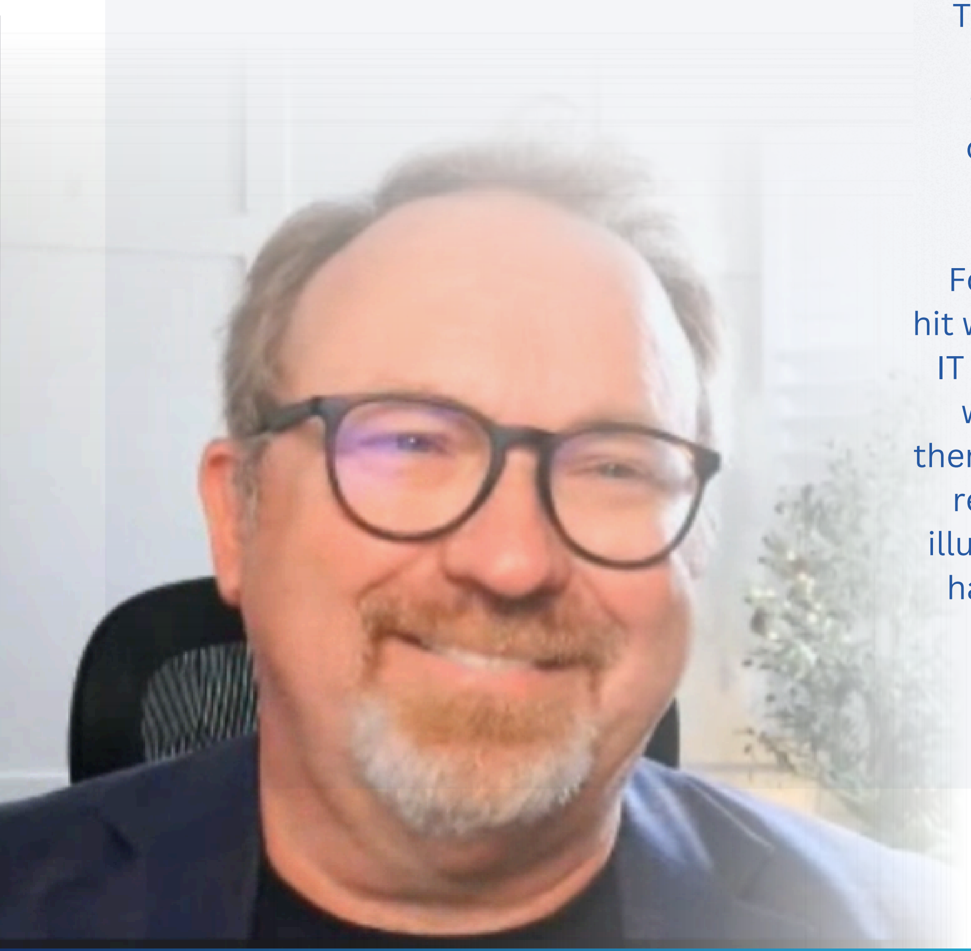
Business Challenges

Limited Resources & Budget Constraints

Q : “I don't have the money, expertise, or bandwidth to stay ahead of today's threats.” What's your response to that perspective and how do you coach both C-level executives and IT leaders who are trying to make the case internally for more investments in proactive security?

A : “Technical leaders have crucial information, but they often speak a different language than business leaders. We need to translate tech details into business terms. Comparing costs and outcomes of similar incidents helps make risks relevant.

Instead of bombarding with statistics, share relatable stories. If crime statistics don't catch their attention, mentioning a neighbor's robbery will. The same principle applies to cybersecurity.



Tabletop exercises or simulations work because they demonstrate that most decisions in a security crisis are business decisions, not just IT decisions.

For instance, a top global law firm hit with a ransomware attack had its IT employee put up a warning sign, which a client photographed and then posted online, causing a public relations nightmare. This incident illustrates that decisions on how to handle breaches often impact the entire business."

— Mark S.

Business Challenges

Evolving Regulatory Requirements

Q : Regulations around cybersecurity and risk management are becoming stricter. How are these evolving regulatory requirements impacting security standards for businesses?

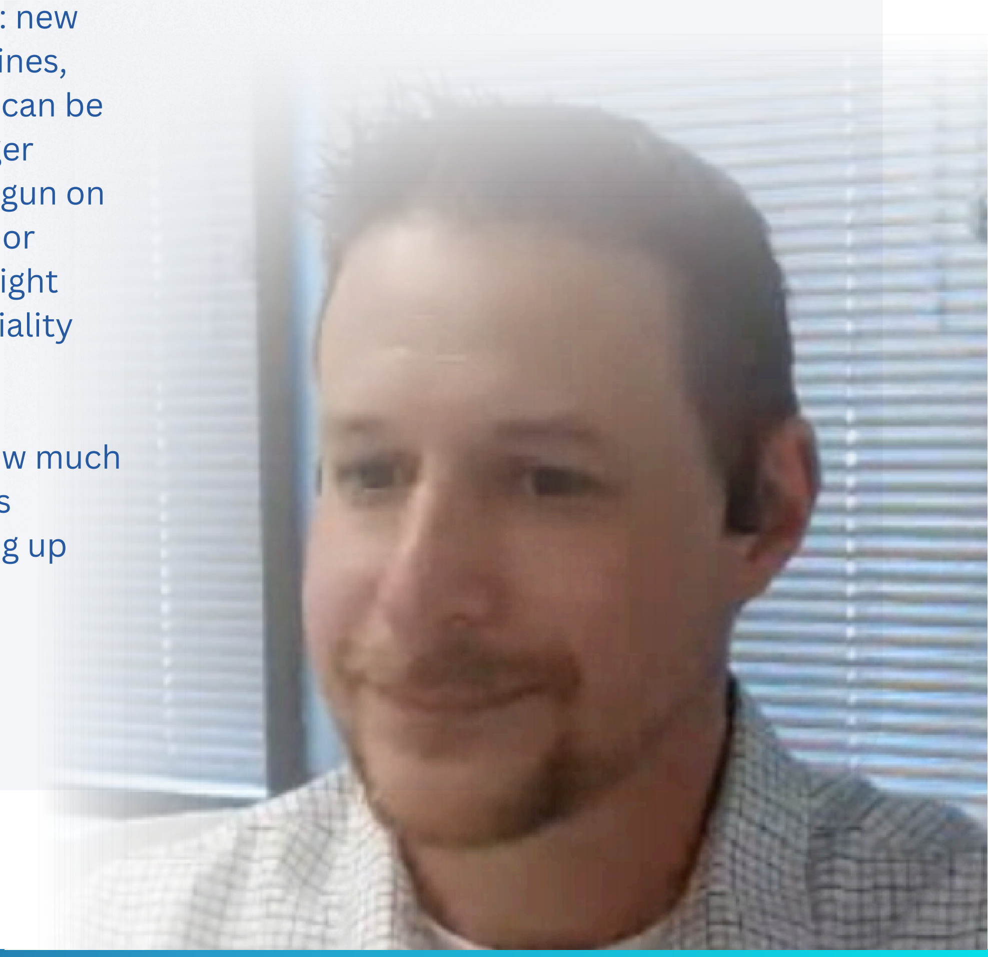
A : “Regulations are tightening and extending into new industries. Take car dealerships, for example. Previously, their security practices were inconsistent, but now the FTC is introducing structure with its GLBA safeguard standards.

The SEC is also raising standards and accountability. Previously, CISOs bore blame for breaches, but now board members must take responsibility for cybersecurity. Understanding materiality is crucial—assessing the breach's impact on the company and its customers.

But here's the tricky part: new incident disclosure timelines, like the SEC's 4-day rule, can be tough, especially for bigger companies. Jumping the gun on reporting can lead to major fallout, and without the right tools, determining materiality can be a challenge.

These shifts show just how much the cybersecurity game is changing and why keeping up with compliance is more important than ever.”

— Rick M.



Business Challenges

Aligning IT & Business Priorities

Q : How can IT leaders effectively communicate the importance of operational resilience and the risks of ignoring cybersecurity to the board and business leadership?

A : “Conduct tabletop exercises at least twice a year and involve all executives and even board members. It's surprising how quickly people can lose their heads in a crisis.

Security should be like muscle memory; everyone needs to know who makes critical decisions when key personnel are unavailable. For example, who takes charge when the CEO is on vacation?

Tabletops help us understand not just how to respond to incidents, but also the business decisions involved. Understanding the potential impact of incidents—from inconvenience to existential threats—is crucial for prioritizing investments in cybersecurity.

By framing cybersecurity discussions in terms of the potential impact on the business and the cost of mitigating risks, we can more effectively align our cybersecurity investments with the organization's goals and priorities.”

— Troels R.

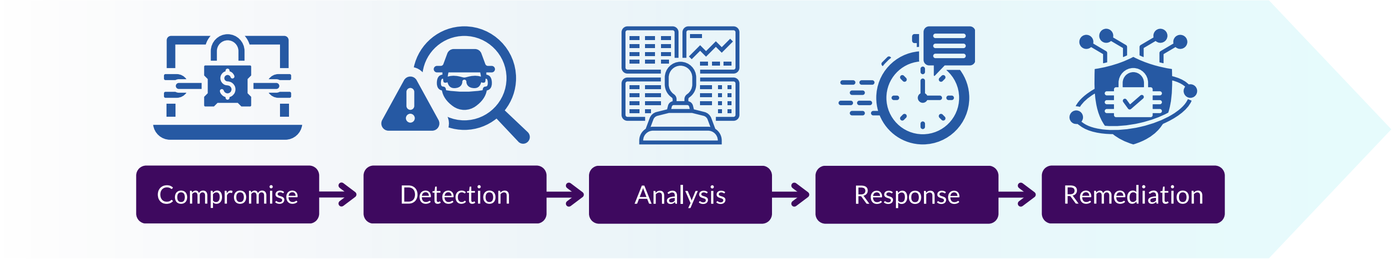
The Solution: Managed Detection & Response (MDR)

Q : Given the challenges facing IT security today, such as more sophisticated threats, resource constraints, and increasing regulations, what's your perspective on the role of managed detection and response (MDR) as a potential solution?

A : "Gartner coined 'managed detection and response' as a turnkey service offering 24x7 protection, plus detection and containment for clients. When a system alerts, an expert can identify malicious activity and contain the threat before it disrupts operations. This expertise is crucial in preventing significant business disruptions."

— Mark S.

Managed Detection and Response



Compromise → Detection → Analysis → Response → Remediation

Q : Can you explain the benefits of the Security Operations Center (SOC) in MDR solutions and how it offers a cost-effective alternative to building an internal SOC team?

A : “Finding and retaining skilled security personnel and managing a 24x7 SOC is costly and complex. Outsourcing is sensible, especially for small to mid-sized businesses lacking resources. It lets companies focus on core operations while specialized providers handle security. This requires a strong relationship with a trusted provider, as the company’s reputation and incident recovery depend on their performance.”

— Rick M.

Managed Detection & Response

Game-Changing MDR Capabilities

Q: From your experience, which MDR capability stands out the most?

A: "Real-time reporting. It offers the ability to see what the security operations team sees at any given time, without relying on another party to pull or curate that information for you."

— Mark S.

A: “UEBA (user and entity behavior analytics). Extending on what Mark said, there's a lot of sophistication in the tool that allows you and your team to be so effective when operationalizing and scaling.”

— Troels R.

A: “SOAR (security orchestration, automation, and response). I'm a big fan of automation whenever possible. The sooner we can mitigate the dwell time of a threat actor or potential incident, the better. SOAR significantly reduces response time through automated processes, leveraging UEBA and real-time reporting data.”

— Rick M.