Despite Investments, Security Operations Is More Difficult

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

Rethinking Program Strategies

Attack surfaces and the threat landscape are evolving, making it crucial for organizations to adapt and improve their security programs. With the increasing number of threats, organizations need to rethink their approaches to security operations.

- **Top five reasons SecOps is more difficult today than it was two years ago**:
  - Top five key drivers for MDR engagement:
    - 41% 
      - Demonstrate a critical need for overall visibility and management.
    - 39% 
      - Provide continuous monitoring for threats.
    - 37% 
      - Improve organizational posture.
    - 34% 
      - Improve regulatory compliance.
    - 33% 
      - Deliver actionable and context rich threat intelligence.

- **New Requirements for MDR**
  - More than half of organizations are either already engaged with an MDR provider or plan to engage in the next 12 months.
  - Top five reasons SecOps is more difficult:
    - 49% 
      - The complexity of security operations tasks.
    - 45% 
      - Regulatory requirements.
    - 39% 
      - The volume and sophistication of alerts.
    - 34% 
      - The ability to manage and respond to threats.
    - 33% 
      - The number of threat vectors.

- **Key value drivers for MDR engagement**:
  - **Operational Improvement and Efficiency**:
    - MDR solutions provide organizations with real-time visibility and control over security operations in several ways. Each solution is intended to achieve the "right thing," and the implementation of the technology stack will be critical to success.
  - **Improved Responsiveness and Resilience**:
    - MDR solutions can help organizations stop threats already in progress, improve detection of potential threats, and provide proactive protection strategies, including proactive threat hunting and risk analysis.

- **Primary reasons behind organizations' usage of MDR plans for managed services**:
  - 52% 
    - MDR solutions provide organizations with advanced threat detection and prevention capabilities.
  - 49% 
    - MDR solutions help organizations quickly and efficiently analyze and respond to threats.
  - 42% 
    - MDR solutions enable organizations to reduce overall security costs.

New Requirements for MDR

Many organizations are looking for new requirements and expectations of MDR providers to help them meet their operational needs.

- **Key considerations for MDR providers**:
  - 61% 
    - 24/7 monitoring of events and logs.
  - 55% 
    - Regulatory compliance reporting.
  - 51% 
    - Detailed, real-time analysis based on threat intelligence.
  - 45% 
    - 24/7 monitoring of events and logs.
  - 43% 
    - Analysis capabilities in multi-cloud and hybrid cloud environments.
  - 40% 
    - Intrusion attack tools.

- **Key skills for security operations**:
  - 52% 
    - Knowledge of cloud architecture.
  - 49% 
    - Knowledge of security operations technologies.
  - 46% 
    - Knowledge of cloud environments.

- **MDR Augmentation**:
  - 54% 
    - Augmentation: 49%
      - My organization wants to focus more strategic security operations tasks.
    - 55% 
      - My organization believes we can do a better job with security operations.
    - 52% 
      - My organization believes service providers can help with security operations.
  - **Key value drivers for MDR engagement**:
    - 49% 
      - Demonstrate a critical need for overall visibility and management.
    - 48% 
      - Improve regulatory compliance.
    - 47% 
      - Deliver actionable and context rich threat intelligence.

The Bigger Truth

As the risk landscape changes, so do the ways organizations approach security. The increased adoption of cloud-native applications and microservices has led to a shift in security strategies, with a greater focus on automation and machine learning to detect and respond to threats in real-time.