

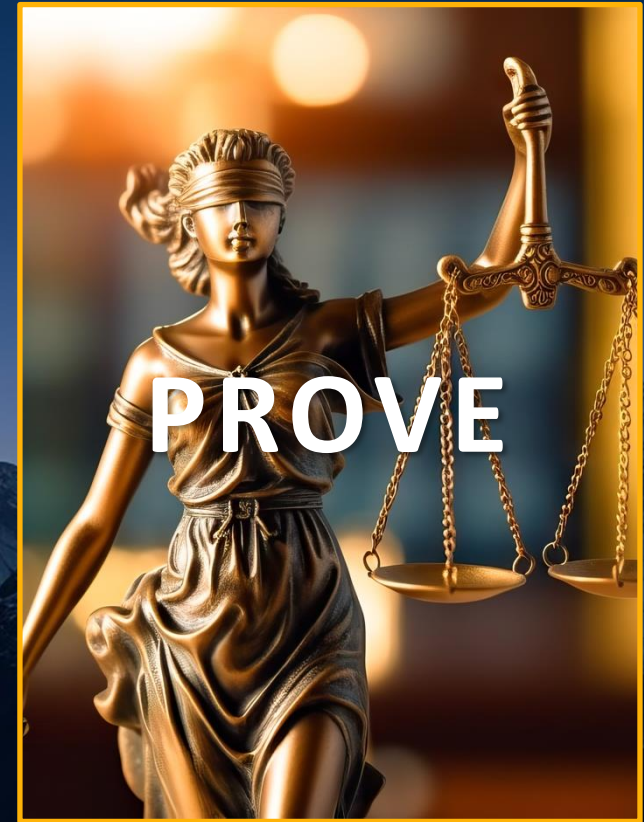


**Cybersecurity**  
is not an IT problem to solve.

It's a **Business Risk**  
to manage.



# Cybersecurity is more than an IT problem



# Organizations struggle to manage security



THREATS



COMPLIANCE

VS



CAPACITY



BUDGETS

# Common cyber misconceptions



We have nothing worth stealing.



Breaches are the result of mistakes.



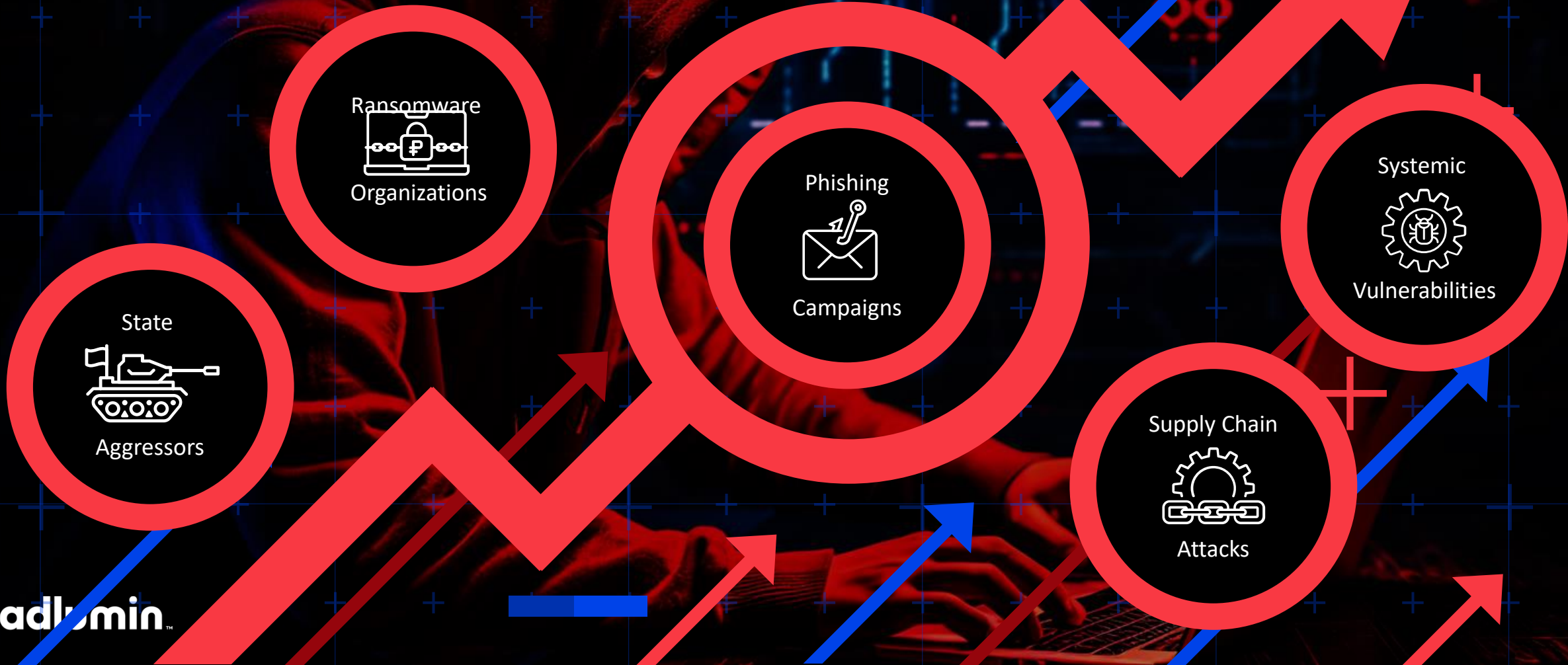
There were no suspicious signs.



We have insurance and backups.

# INDUSTRIALIZED CYBERCRIME

State-sponsored actors and gangs operate on the same principles as legitimate businesses in pursuit of profit. They participate in an ecosystem that shares criminal expertise, licenses malicious technology and brands, and traffics in stolen assets.



IN 2023

**CYBER CRIMINALS**

**TARGETED**

**76%**

**OF**

**ORGANIZATIONS**

**2.5K**

**Vulnerabilities**

Per month to investigate

**1.0K**

**Critical Alerts**

Per month requiring action

**30<sup>sec</sup>**

**TRIAGE**

Time to identify threats

**15<sup>min</sup>**

**CONTAIN**

Dangerous threats

**\$1.2<sup>M</sup>**

**COST**

Annual DIY Operations



VPN



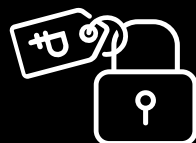
POWERSHELL



CLOUD EMAIL



CLOUD APPS



RANSOMWARE



EXFILTRATION



DATA EXPOSURE



REPUTATION

# Gartner®

The rise in ransomware drives the demand for 24/7 managed detection and response (MDR) services.



**CONFUSES**  
EDR, MDR & XDR



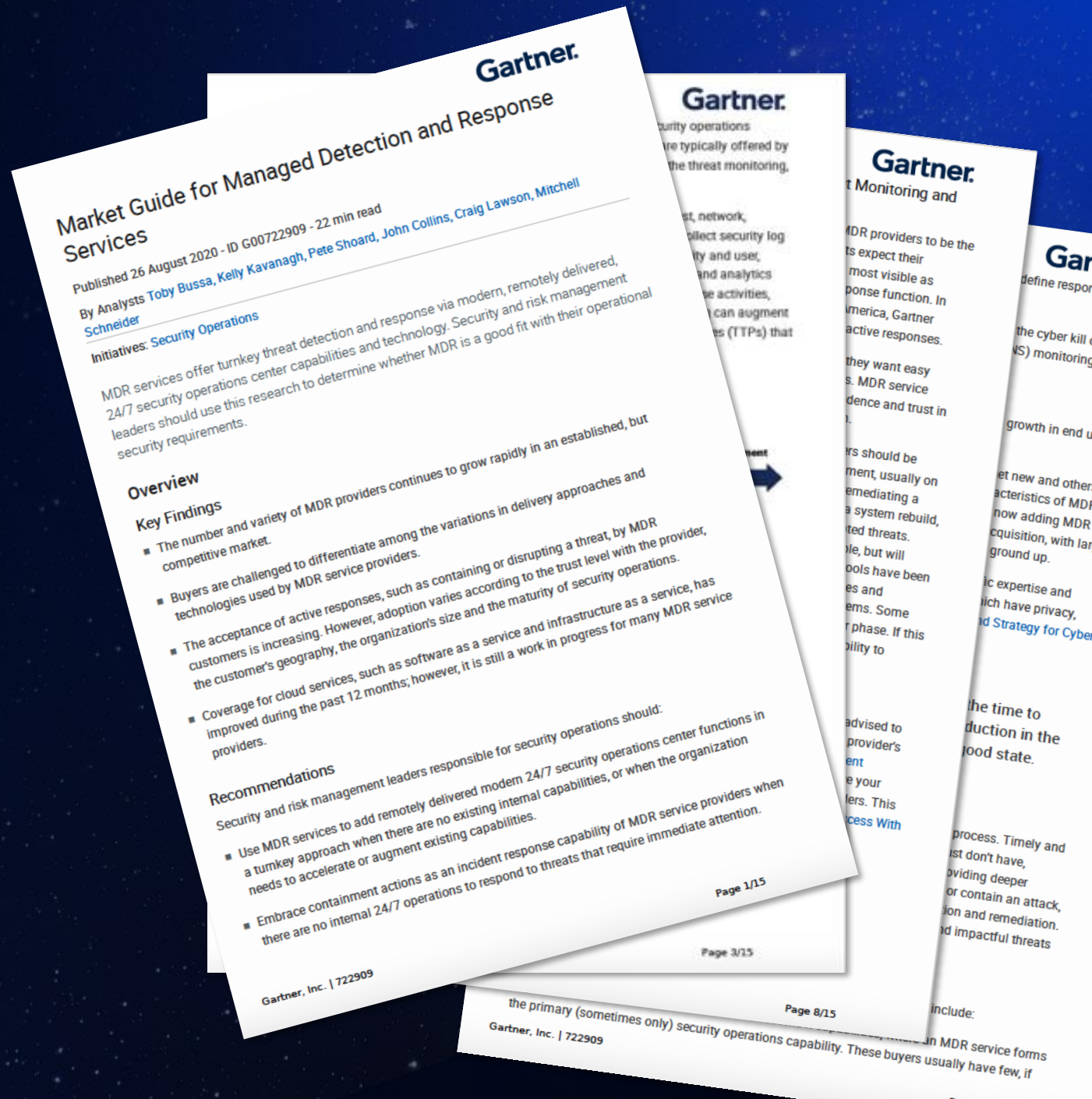
**SACRIFICES**  
VISIBILITY & CONTROL



**LACKS**  
MSP INTEGRATION

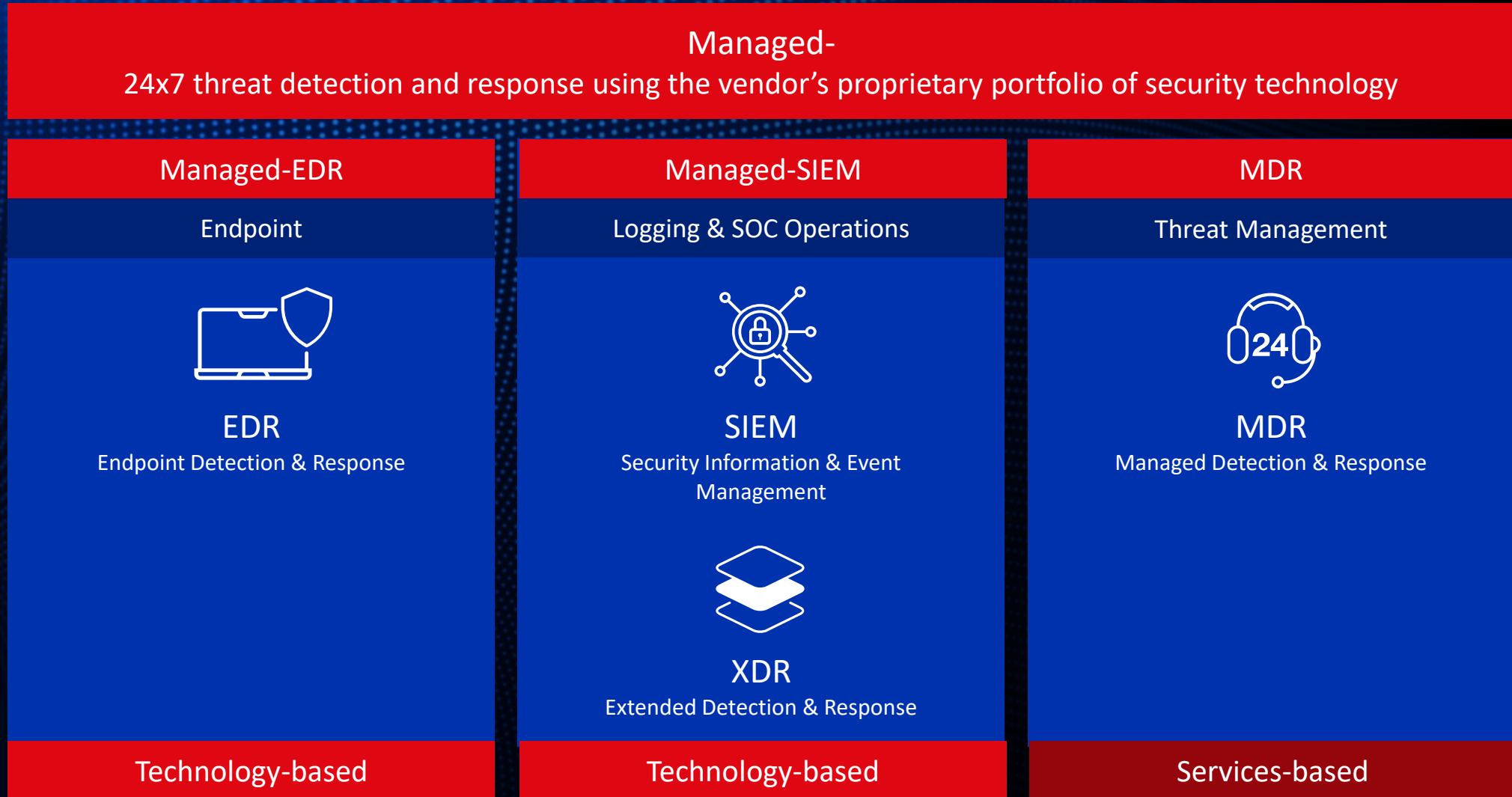
“ MDR services offer turnkey threat detection and response via modern, remotely delivered, 24/7 security operations center capabilities and technology. ”

- ✓ External SOC or augments internal capabilities
- ✓ MDR evolved from MSSP
- ✓ MDR lacks a clear service definition across vendors
- ✓ Differentiation is difficult across varied approaches

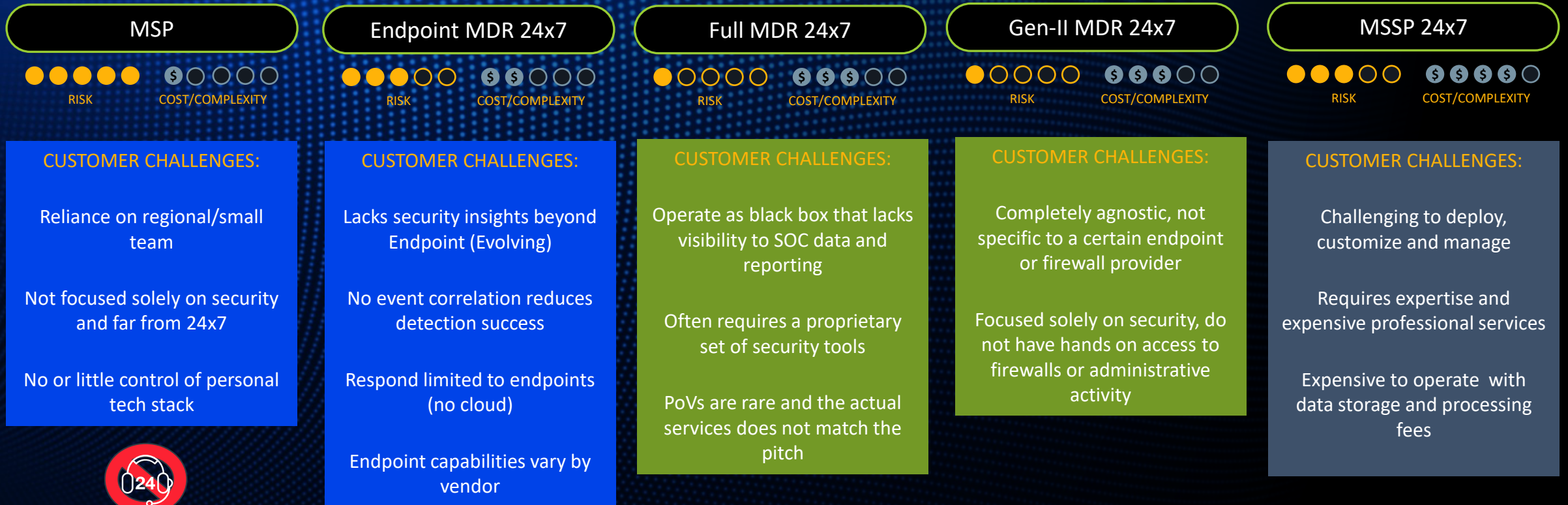




# M- is the management and operations layer



# Stages of Managed Security

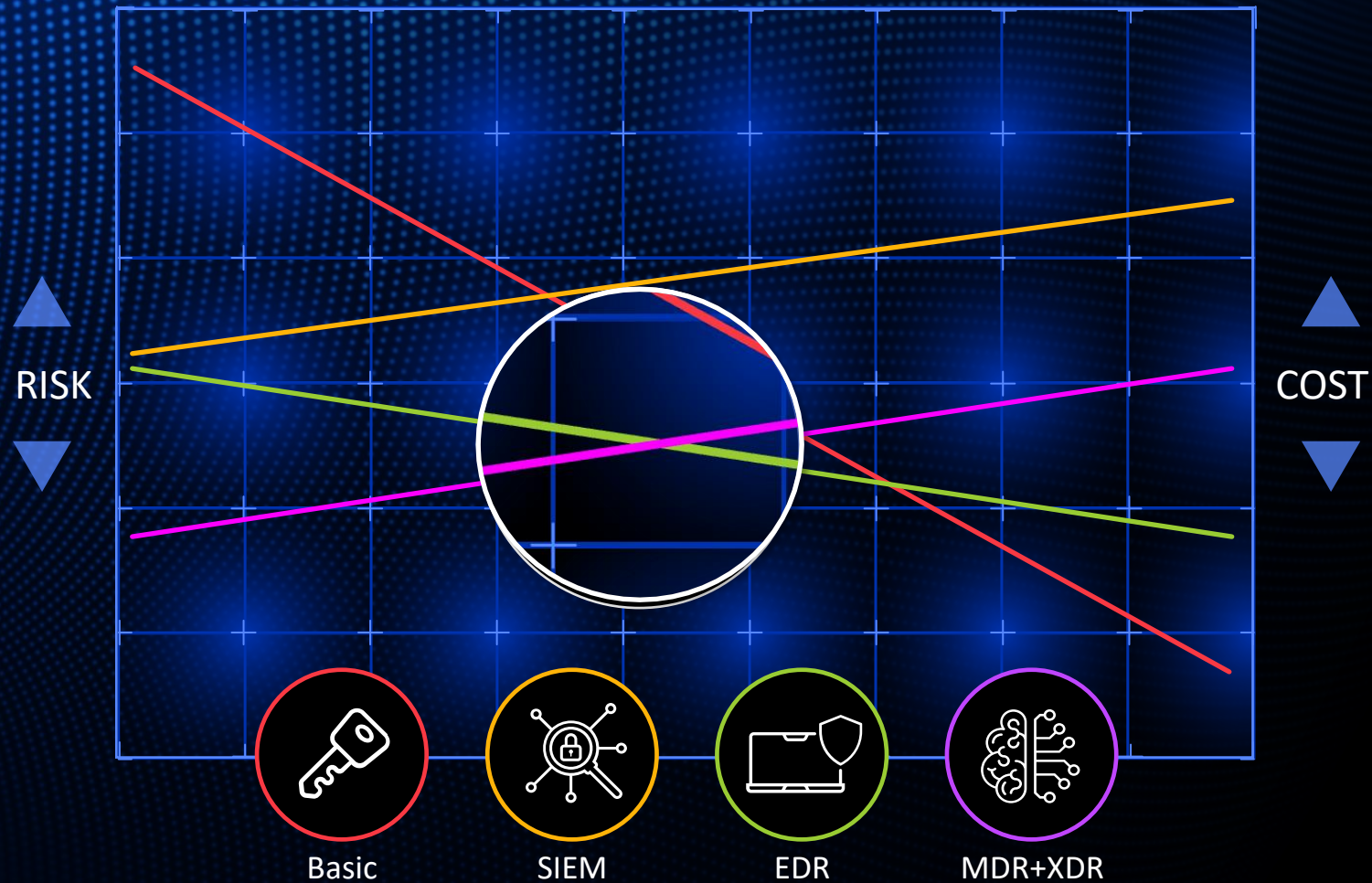


## Examples

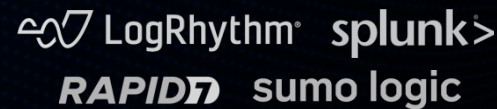
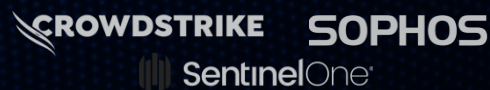


# The evolution of MDR services as risk mitigation

How much risk can we mitigate and what's it going to cost me?



# The evolution of MDR services as risk mitigation



# Security is in our DNA



**ROBERT JOHNSTON**  
Chief Executive Officer


Former National Security Agency (NSA)  
U.S. Cyber Command

Stood up the first U.S. Cyber Command  
Cyber Protection Team (CPT) 81, NSA

Director, Marine Corps Red Team,  
USMC

While Principal Consultant with  
CrowdStrike, led Multiple High Profile  
Investigations including Breach of  
Pentagon Joint Chiefs of Staff by  
Russian GRU, and the Breach  
Investigation against the Democratic  
National Committee

**BuzzFeed News**  
REPORTING TO YOU



**He Solved The DNC Hack. Now He's Telling His Story For The First Time.**

Less than a year before Marine Corps cyberwarrior Robert Johnston discovered that the Russians had hacked the Democratic National Committee, he found they had launched a similar attack at the Joint Chiefs of Staff.

Via Skype  
Toronto  
10:34 AM ET



**RANSOMWARE ATTACKS**  
CYBER CRIMINALS TARGET VITAL INFRASTRUCTURE AND BUSINESSES  
Mark Sangster | Author, "No Safe Harbor"

LIVE  
CNN  
10:34 AM ET  
540p



**RUSSIA CONNECTION**  
ROBERT JOHNSTON | CEO  
ADLUMIN

LIVE  
MSNBC  
10:39 AM MT



# Adlumin Managed Detection and Response (GEN-II MDR)

Adlumin was founded in 2016 by two NSA veterans who bring the unique counterpoints of a cyberattack squadron commander and national cyber defense leader. Based on their expertise, they designed a platform that could prevent attacks for a fraction of the cost of a significant incident or breach.



## Extended Detection and Response (XDR)

Centralized XDR that consolidates SIEM and SOAR for threat detection, investigation, and response

The Security Operations platform streamlines data ingestion, analysis, and security workflows— illuminating unseen threats, system vulnerabilities, and IT operations, so your path to response and compliance becomes clear.



## Managed Detection and Response (24x7 SOC)

24x7 Security Operations Center (SOC) providing monitoring, investigation, and response

Most managed services providers give you partial or bare-minimum visibility into your environment. With Adlumin MDR Services, you get round-the-clock coverage and access to the same platform as our SOC analysts.

+ Total Ransomware Defense

+ Incident Response

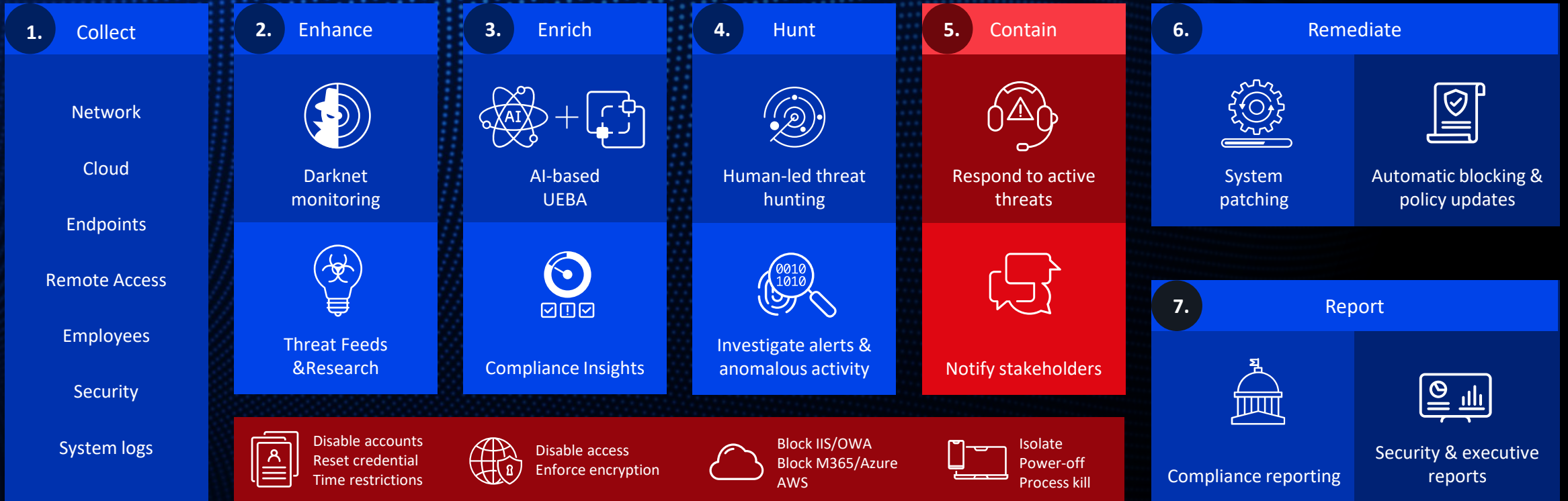
+ Vulnerability Management

+ Penetration Testing

+ Security Awareness Training

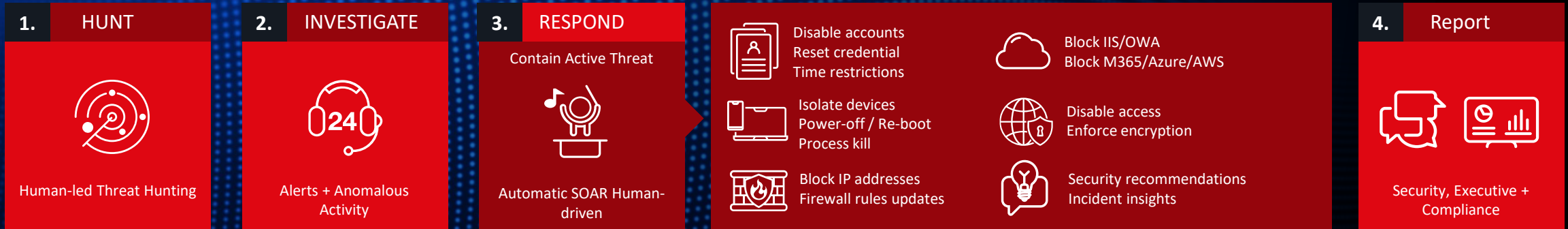
# Detecting the signs to contain attacks early

Adlumin MDR detects a trail of attack pre-cursors to stop attacks from becoming business disrupting

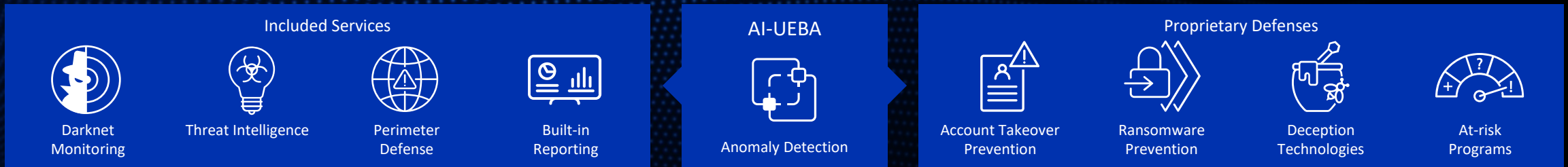


# Adlumin XDR platform and MDR Response

Adlumin XDR Platform deploys in 90-minutes and sending detections in seconds



## MDR Rapid Response



## XDR Platform



# There were plenty of signs before the ransomware attack

Criminals use sophisticated methods to gain access. Your insurer's Incident Response investigators will discover this evidence.



## Compliance & Risk Management

MDR  
24x7 SOC



Threat  
Hunting



Detection  
Investigation



Active Threat  
Containment



Incident  
Reporting

XDR  
Platform



Threat  
Research



AI-UEBA  
Detections



Automated  
Response



Live  
Reporting



Physical



Access



Users



Cloud

## Security Consolidation



90-min  
Deployment



Full Visibility &  
Console Access



Multi-Tenant  
Management



"Competitive security services compared to its peers."



"Adlumin offers competitive security services that are cost-effective compared to its peers."

– Kiwi J., Security Administrator

"Excellent product and value."



"We barely used our old SIEM due to difficulty getting usable information, and the price kept growing. With Adlumin I can jump in and see what I need in minutes."

– Administrator in Construction

"Adlumin is the best!"



"Adlumin staff is so helpful in any situation; their response time is great, and their team is very friendly. Software is easy to use and intuitive."

– Administrator in Computer & Network Security



# Try Adlumin in Your Environment

Adlumin provides a 14-day POV with unlimited log collection. Our customer success team will guide you through onboarding and extend your team with our security operations platform and solutions.



## Kick-off & Installation

- Stand up tenant
- Create user accounts
- Set incident contacts
- Agent deployment
- Virtual Syslog collector
- API credentials (cloud, M365, etc.)



## Get to Know the Platform

- Network Health
- Reporting
- Baseline scoring
- Risk assessment
- Compliance review
- Set-up reports



## The Platform & MDR

- Detection and investigations
- Event investigation
- Log Management
- Containment
- Defense strategies
- SOAR



## Kick-off & Installation

- Finalize purchase
- Assign customer success manager
- Establish production Rules of Engagement for switchover

# MDR is the management and operations layer

## Managed

Managed services provides turnkey 24x7 device management, threat detection and response, using the portfolio of managed security technology (typically, the vendor's proprietary offerings).

### Endpoint

#### Endpoint Protection Platform (EPP)

Often referred to as a next-generation anti-virus, an EPP is a solution to detect malicious activity, and provide investigation and remediation capabilities

#### Endpoint Detection & Response (EDR)

EDR continually monitors an endpoint to identify threats through data analytics and prevent malicious activity with rules-based automated response capabilities

**Common Vendors:** Bitdefender, Cisco AMP, CrowdStrike, Cylance, Huntress, Malwarebytes, Microsoft Defender, Palo Alto Cortex, Sentinel One, Sophos, and VMware CarbonBlack.

### Logging & SOC operations

#### Security Information & Event Management (SIEM)

SIEM services support threat detection, compliance, and security incident management by collecting and analyzing security events, network logs, and other data sources.

#### Security Orchestration, Automation, and Response (SOAR)

SOAR combine incident response, orchestration, and automation of investigation and response capabilities in a single platform. Common Vendors

**Common SIEM Vendors:** ConnectWise, LogRhythm, Splunk, and Sumo Logic.

**Common SOAR vendors:** Anomali, Cyware, Fortinet, Palo Alto Networks, Rapid7, Splunk, and Sumo Logic.

### Detection & Response

#### Managed Detection & Response (MDR)

Detection and containment offered as a turnkey services, using a proprietary security technology stack for detection, and SOC for 24x7 monitoring.

#### Extended Detection & Response (XDR)

First coined by Palo Alto, XDR collects security data from network points, operating systems logs, application logs, cloud, endpoints, and other sources to apply threat detection analytics to this data lake.

**Common MDR Vendors:** Arctic Wolf, eSentire, Critical Start, Red Canary, Reliaquest.

**Common XDR Vendors:** Cisco, FireEye, Fidelis, Fortinet, Palo Alto Networks, Rapid7, and Sophos.