Not the strongest

Nor the most intelligent

It is the one that is most adaptable to change

Charles Darwin

ODYSSEY™
cybersecurity

ANTICIPATING & PLANING FOR OPERATIONAL SERVICE DISRUPTIONS

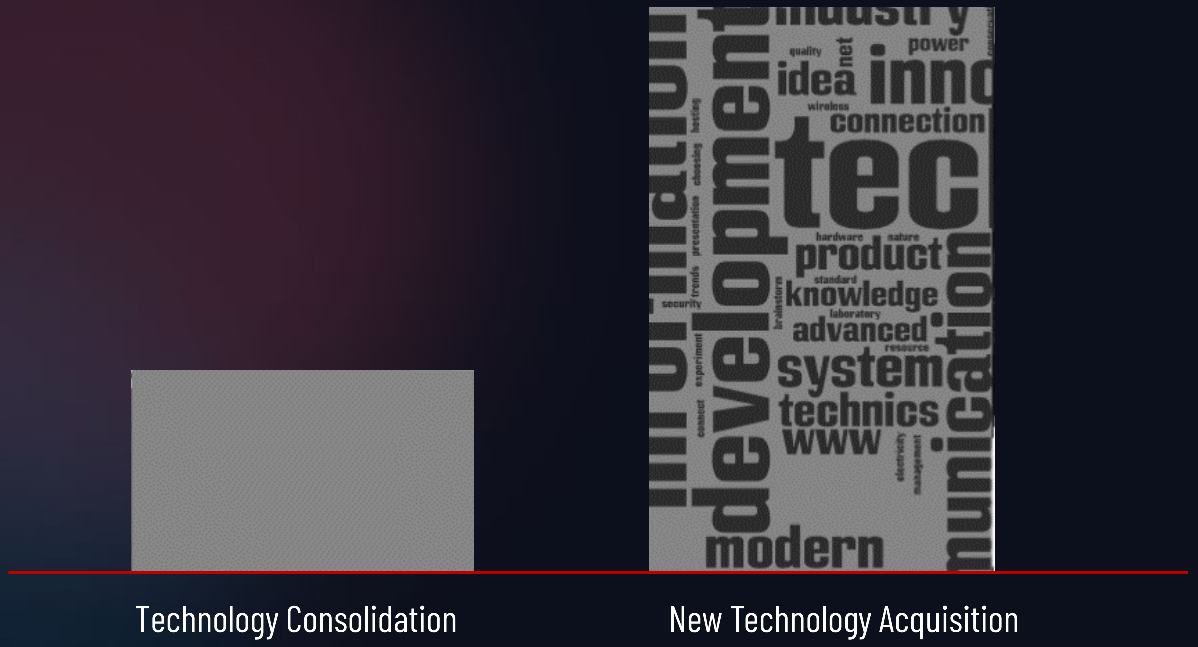
Andreas Constantinides Managed Services, Director

Myths That Prevent Cybersecurity From Unlocking Its True Value

More Tools = Better Protection?

More Technologies = Better Protection?

Gear Acquisition Syndrome



Source: Gartner 2023

Winchester Mystery House… 1884–1906

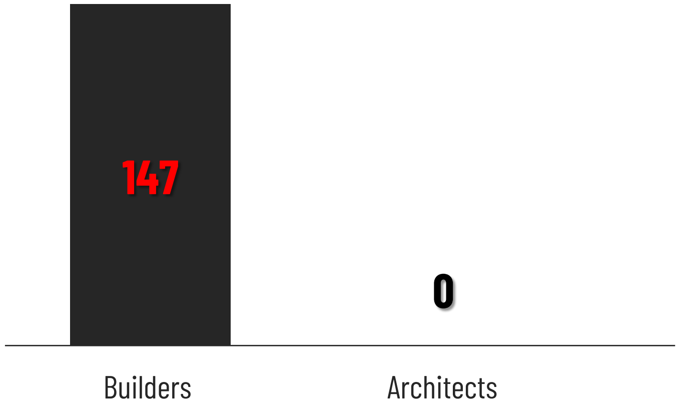
WINCHESTER MYSTERY HOUSE

An Ambitious Vision…

- ✓ 24,000 Square Feet
- ✓ 160 Rooms
- ✓ Six Kitchens
- ✓ Gas Lights
- ✓ 47 Fireplaces
- ✓ 10,000 Windows
- ✓ Wool-Wall Insulation

$5 million dollars in 1923

…Built Without a "Blueprint"…

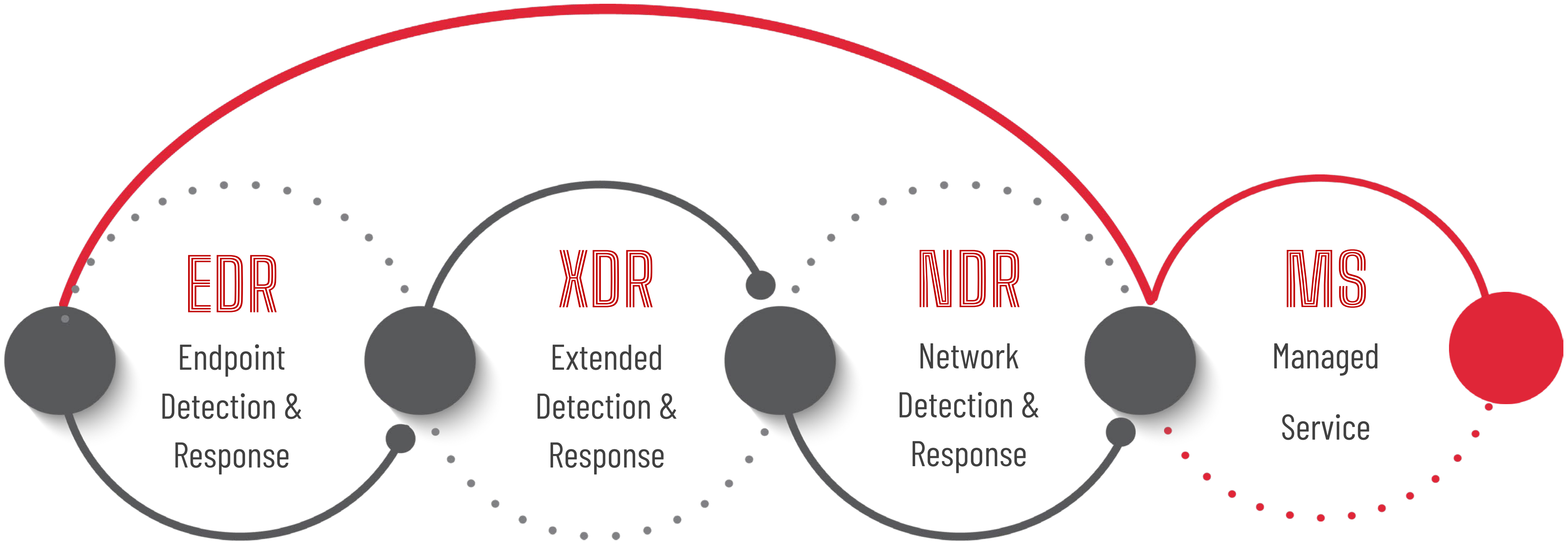


…Yields Inhospitable Results

- ✓ 65 Doors Leading to Blank walls
- ✓ 13 Staircases Abandoned
- ✓ 24 Skylights in Floors

100 Million Cost In Today's Money

Let’s Clarify the Buzz Words_



EDR

Endpoint Detection & Response

XDR

Extended Detection & Response

NDR

Network Detection & Response

MS

Managed Service

EDR combines real-time continuous monitoring with rule-based automated responses

XDR extends Endpoint Detection & Response by natively integrating multiple security products into a cohesive security operation

NDR monitors network traffic to gain visibility into potential threats.

MS combines technologies and human intelligence to intelligently analyse log and event data collected from diverse sources to respond to Eminent & Potential Cyber-Threats

The cost of a Data Breach is Rising_

Data Breaches **remain Hidden longer** and **take longer to Contain** than ever before despite the **large defensive investments** from organizations, particularly in prevention (Cyber-Defense).

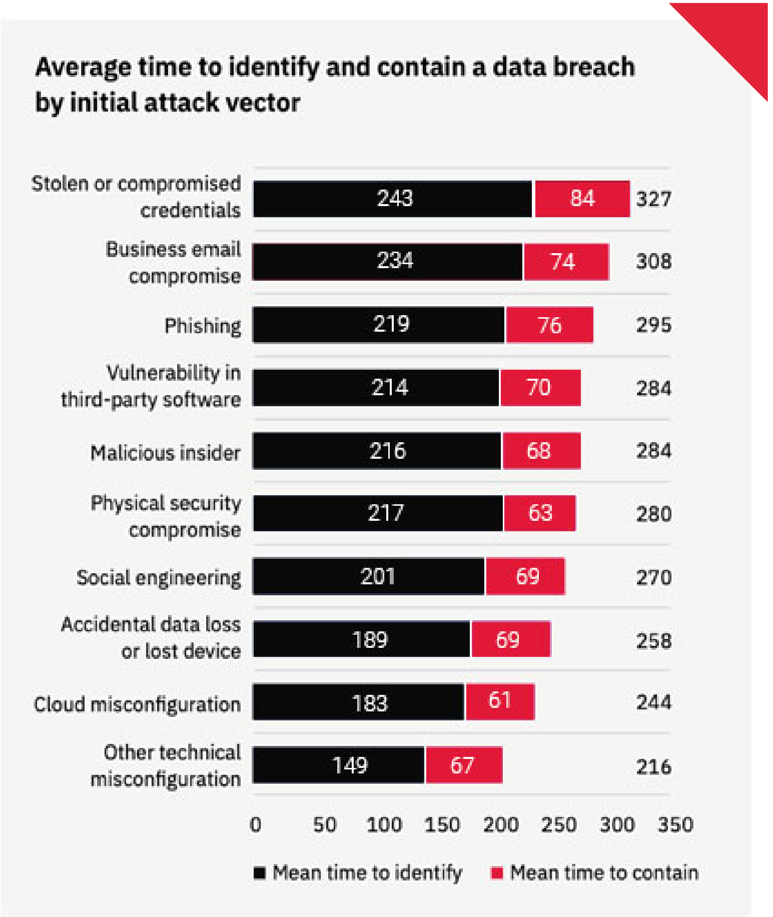

Average time to identify and contain a data breach by initial attack vector

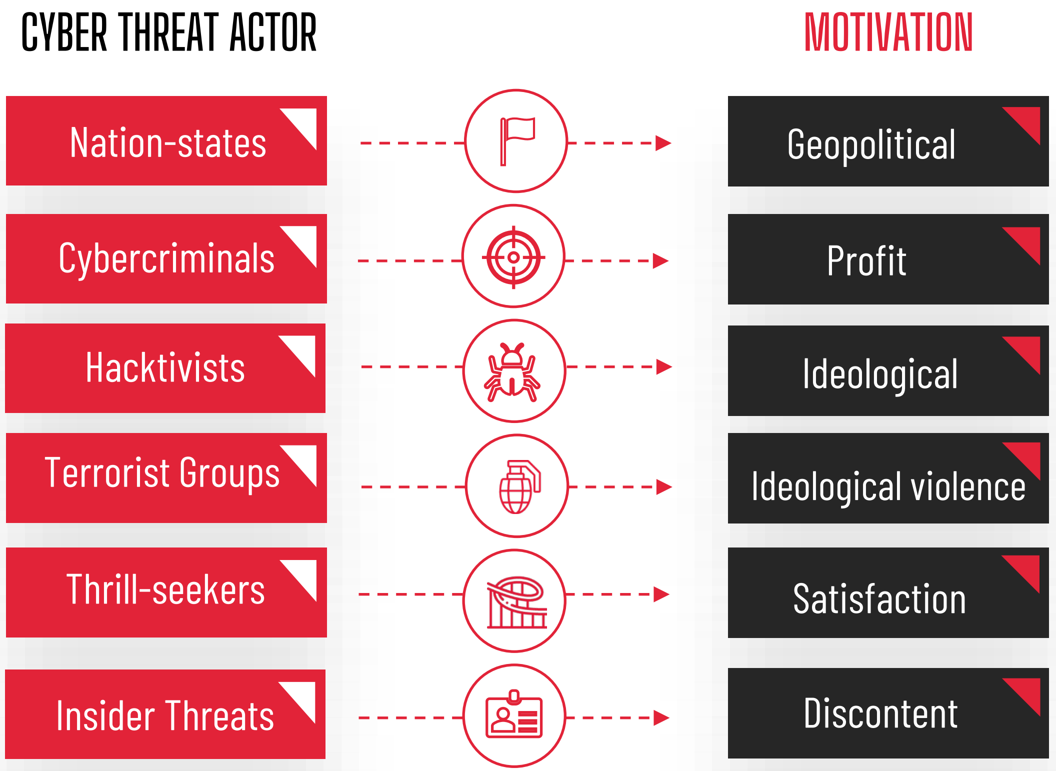
Figure 12: Measured in days

Source IBM: Cost of a Data Breach report 2022

Motivations behind Cyber Attacks

CYBER THREAT ACTORS

- Nation state cyber threat actors are geopolitically motivated.
- Cybercriminals financially motivated.
- Hacktivists ideologically motivated.
- Terrorist groups motivated by ideological violence.
- Thrill-seekers are often motivated by satisfaction.



CYBER THREAT ACTOR	MOTIVATION
Nation-states	Geopolitical
Cybercriminals	Profit
Hacktivists	Ideological
Terrorist Groups	Ideological violence
Thrill-seekers	Satisfaction
Insider Threats	Discontent

First-Mover Advantage
Zero-day Exploits_

With the First-Mover Advantage “FMA”, Threat-Actors enjoy continued success in penetrating systems and applications DESPITE THE ENORMOUS INVESTMENTS from Organizations in Cyber Defenses.

WHY?

C-Level CONFUSION

It does not matter what it is called.
Security Professionals & Businesses need to be able to DETECT THREATS, INVESTIGATE those threats and effectively RESPOND to them

Decipher the Evolution of the Threat Landscape

“To Accelerate Threat Detection, Investigation & Response”

Past, Present and Future…

The PRESENT!

Timely Detection & Response to cyber, insider and 3rd party threats

PRESENT

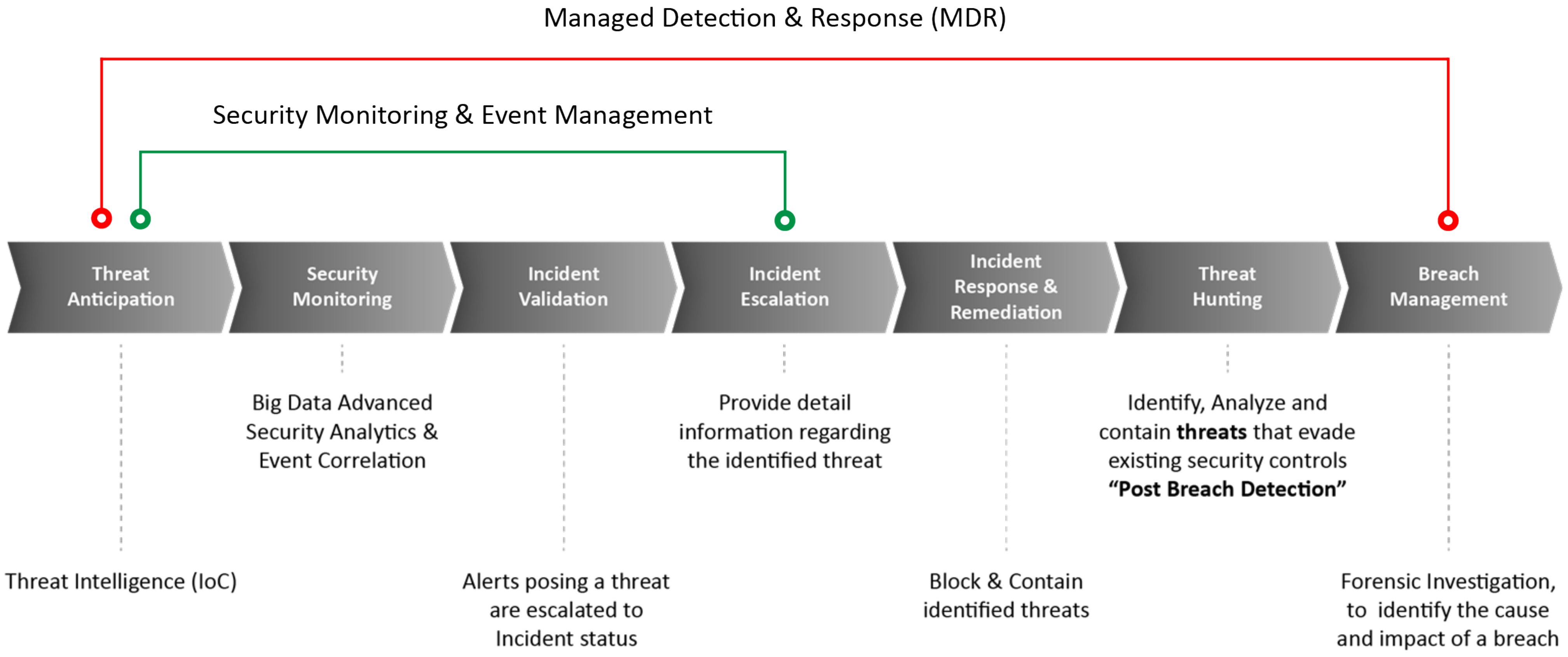
Managed Detection & Response (MDR)

The Benefits

- ✓ Advanced Threat Detection
- ✓ 24/7 Monitoring
- ✓ Rapid Response
- ✓ Enhanced Security Posture

SECURITY OPERATIONS

Managed Detection & Response



Managed Detection & Response (MDR)

Security Monitoring & Event Management

Threat Anticipation → Security Monitoring → Incident Validation → Incident Escalation → Incident Response & Remediation → Threat Hunting → Breach Management

Threat Anticipation: Threat Intelligence (IoC)

Security Monitoring: Big Data Advanced Security Analytics & Event Correlation

Incident Validation: Alerts posing a threat are escalated to Incident status

Incident Escalation: Provide detail information regarding the identified threat

Incident Response & Remediation: Block & Contain identified threats

Threat Hunting: Identify, Analyze and contain **threats** that evade existing security controls **“Post Breach Detection”**

Breach Management: Forensic Investigation, to identify the cause and impact of a breach

Understanding Telemetry = Cross-Layered Visibility_

SIMPLE

Log and event data from endpoints (limited visibility, so potentially a false indicator that “All is Good”)

MODERATE

Log and event data from endpoints, plus security tools (Moderate visibility, but missing visibility from network, and application-specific visibility

HOLISTIC

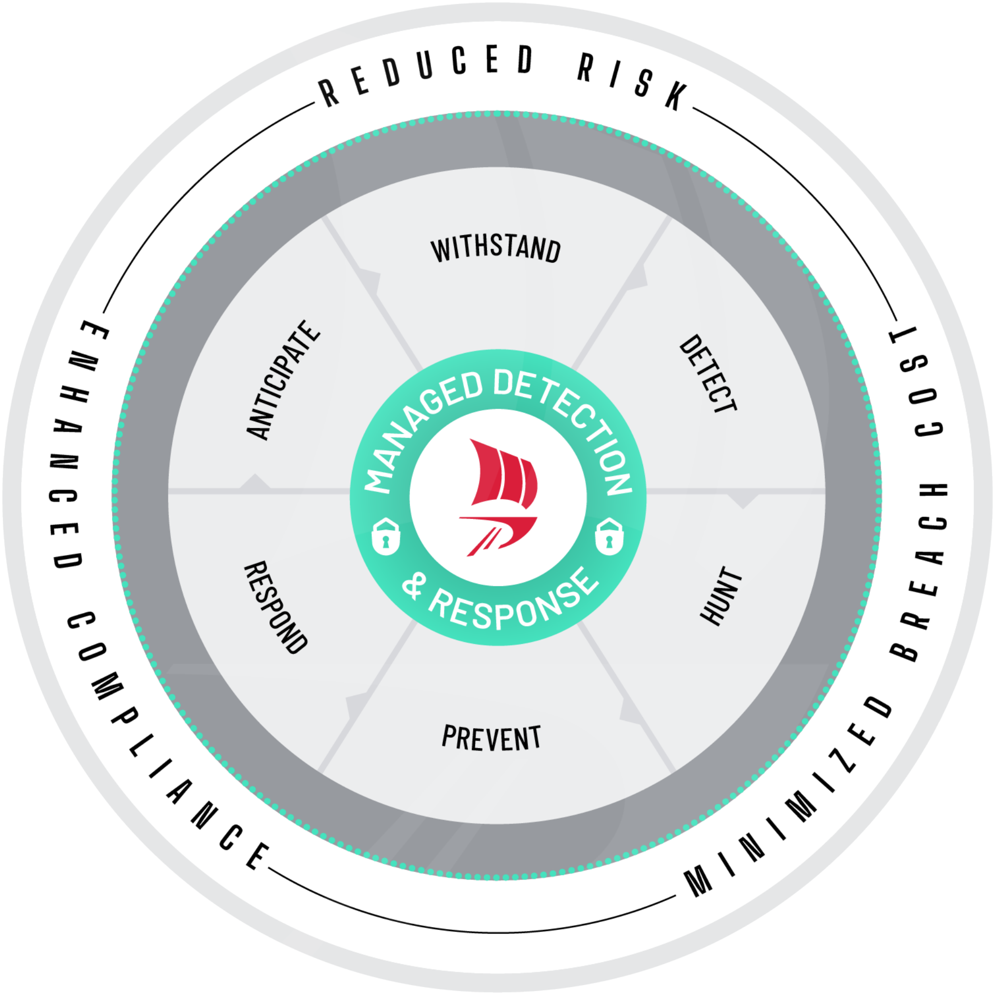
Log and event data from endpoints, security tools, network, applications, cloud, industry-specific, and vulnerability information (Full Visibility)

The higher the level of Telemetry, the easier it is to promptly

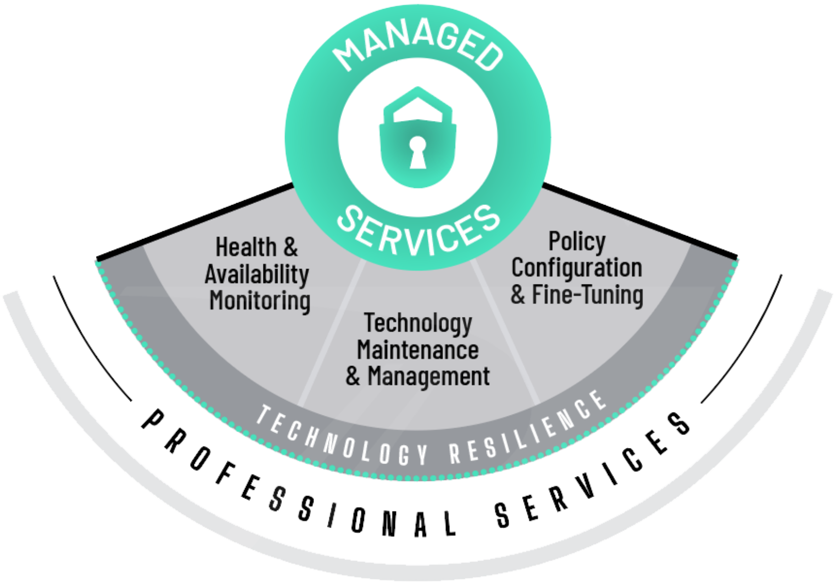
Identify, **Hunt** and **Confirm** THREAT-ACTOR presence

MDR: Service Delivery Approach

- **ANTICIPATE:** Machine Learning, Contextual Threat Intelligence, Indicators of Attacks
- **WITHSTAND:** Review key Assets Operations and Security
- **DETECT:** Analytics, Use Cases, Play Books , Vulnerability Management, Taxonomy
- **HUNT:** Active Defense
- **PREVENT:** SOAR, Identity & Access, EDR
- **RAPIDLY RESPOND:** Incident Response and Digital Forensics



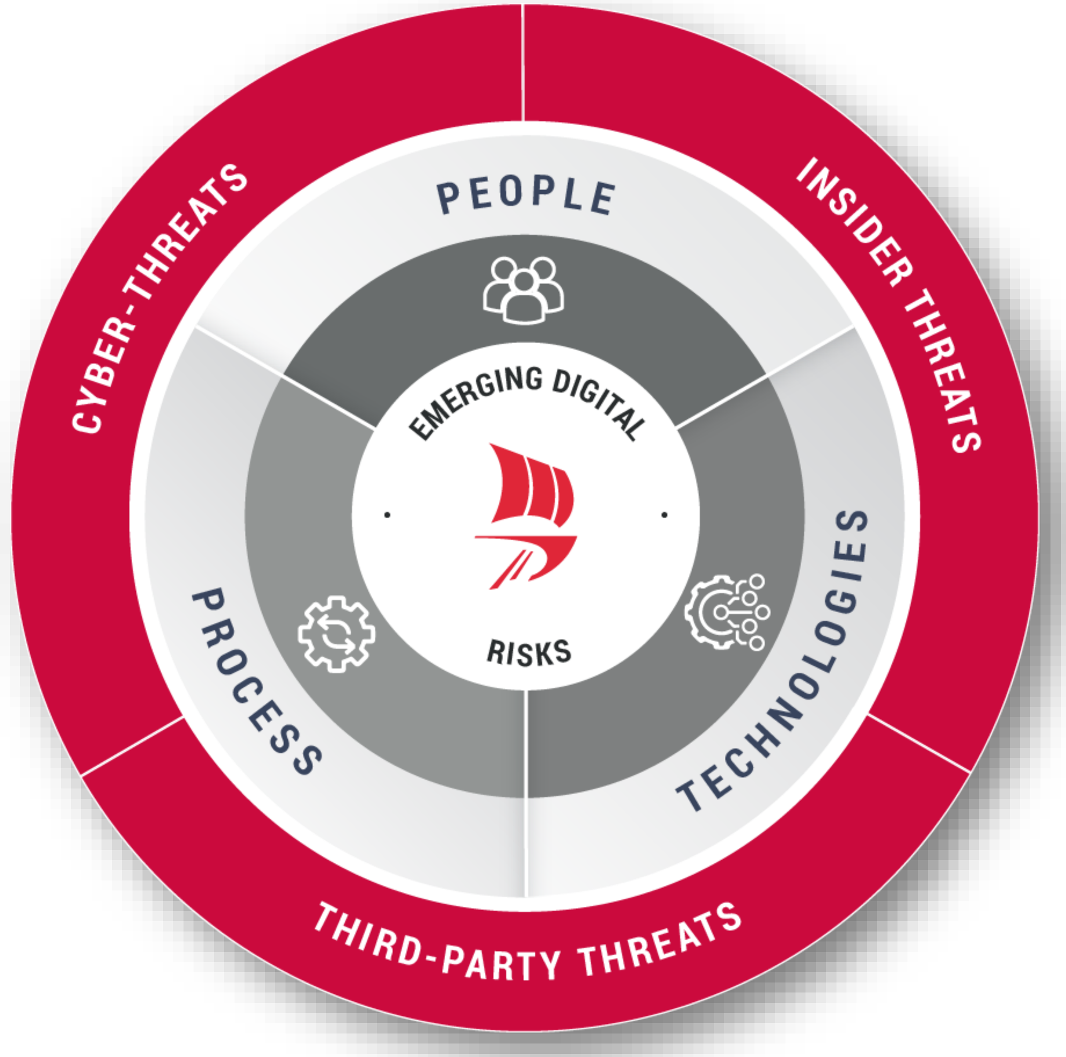
Ensure Optimal Performance & Protection


MANAGED SERVICES
Health & Availability Monitoring
Technology Maintenance & Management
Policy Configuration & Fine-Tuning
TECHNOLOGY RESILIENCE
PROFESSIONAL SERVICES

The Value

- ✓ Disaster Recovery Preparedness
- ✓ Adaptive Security Measures
- ✓ Comprehensive Risk Assessment
- ✓ Regulatory Compliance

To effectively minimize your OPERATIONAL RISK from this new diverse set of DIGITAL RISKS.



INVESTIGATING AND RESPONDING TO LIVE ATTACKS AND THREATS

20
24

HOW IMPORTANT IS TO UNDERSTAND THE PAST & PREDICT THE FUTURE?

Proactively identify risks before they can escalate into full-blown attacks

DARK WEB SOCIAL MEDIA NEW MALWARE STRAINS ZERO-DAY VULNERABILITIES EXPLOIT KITS ATTACK CAMPAIGN INFORMATION LEAKED DATA DISCUSSIONS IN UNDERGROUND FORUMS

PAST

FUTURE

Silent Threat Surveillance

Key Benefits:

- ✓ Enhanced Detection Capabilities
- ✓ Quicker Response Times
- ✓ Deeper Security Insights

Identify vulnerabilities & configuration weaknesses

FUTURE

Continuous Threat Exposure Management

Key Benefits:

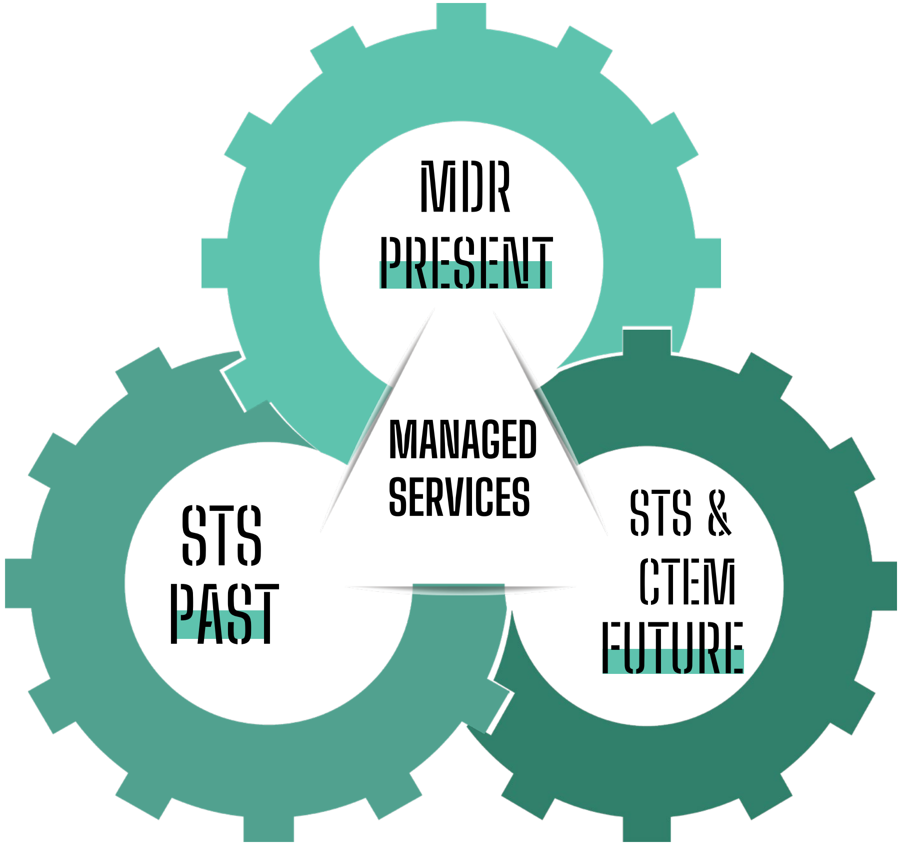
- ✓ Proactive Risk Identification
- ✓ Enhanced Visibility and Awareness
- ✓ Improved Security Posture Over Time

TO ANTICIPATE

BE PROACTIVE

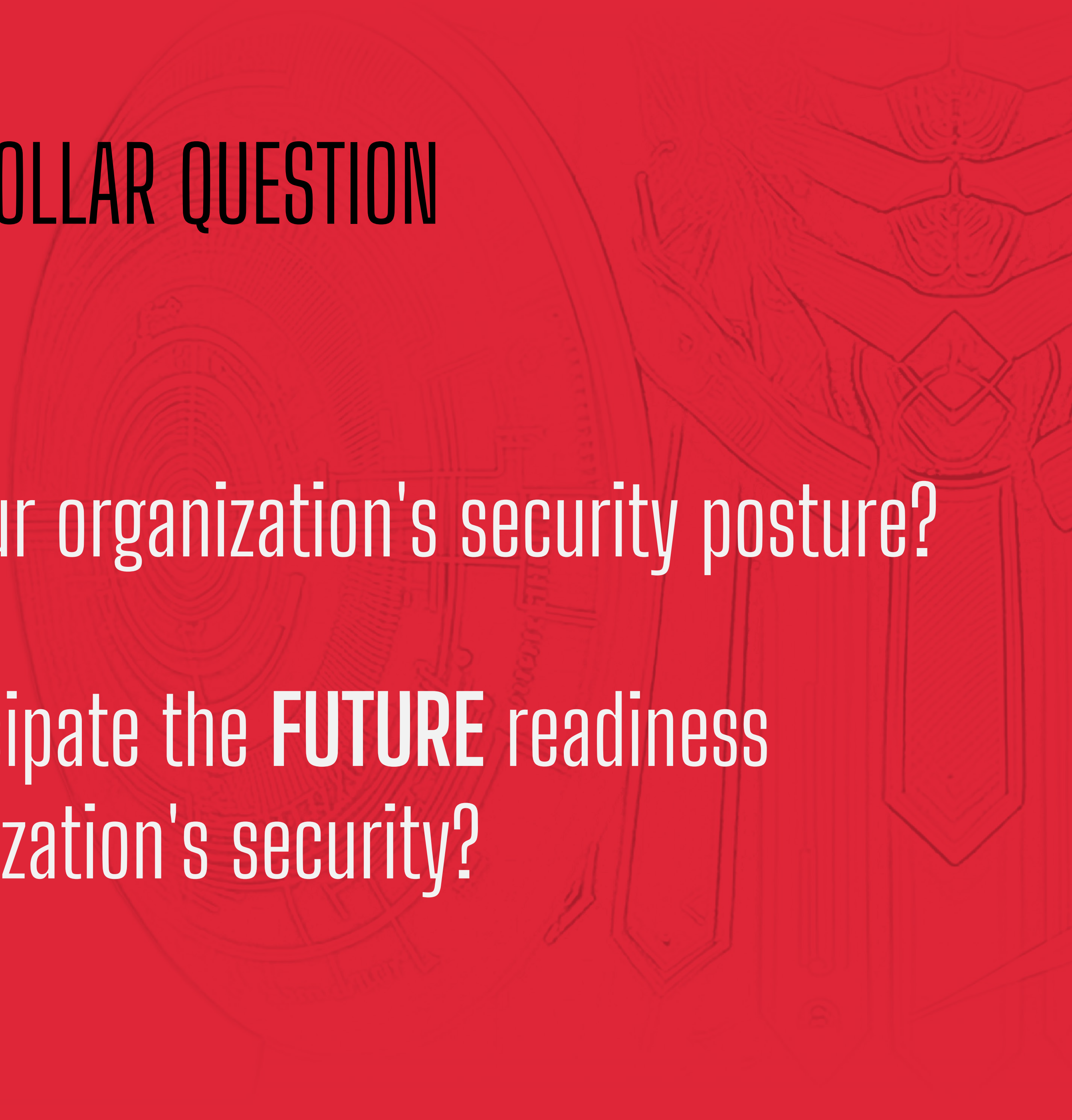
Managed Services

Delivering Peace Of Mind



Empower your defenses against increasingly sophisticated Eminent & Potential destructive Cyber-Threats

A MILLION DOLLAR QUESTION



Do you have a clear view of your organization's security posture?

Are you prepared to anticipate the **FUTURE** readiness of your organization's security?

BUILDING A STRONG SECURITY OPERATIONS

20
24

EXPERIENCED PERSONEL

Managing SOC monitoring services **24/7.**

HOLISTIC TELEMETRY

Implementing holistic telemetry for comprehensive visibility.

INCIDENT RESPONSE

Enhancing incident response and contamination capabilities.

TO ANTICIPATE & PREDICT

HOLISTIC VISIBILITY

Enhancing Visibility into Exposed Data

CONTINUOUS THREAT EXPOSURE MANAGEMENT

Identify vulnerabilities and configuration weaknesses by regularly scanning your critical technology assets

CONTEXTUAL THREAT INTELLIGENCE

What happened in the past and what is expected in the future

IS YOUR COMPANY IN THE SHADOWS?

DISCOVER IF YOU'RE A TARGET ON THE DARK & DEEP WEB

Join our Workshop

Today 14.30 – 15.30 Hall 2

ODYSSEY™
cybersecurity

WE SECURE YOUR CYBER RESILIENT FUTURE

20
24

شكرا

DIOLCH köszönöm MULȚUMESC mahalo SPASIBA

TAKK SKAL DU HA xie xie GRAZIE ĎAKUJEM GRACIAS

THANK YOU

tänan BEDANKT ŞUKRAN toda TAKK TERIMA KASIH RAHMAT merci ŞUKRAN Kiitos PALDIES

KHAWP KHUN ARIGATOU

OBRIGADO DHUN YUH VAAD dzięki TEŞEKKÜRLER

S' EFHARISTÓ DANKE SALAMAT

děkuji vám GAHM SA HAB NI DA

20
24