Integrity360
your **security** in mind

Welcome

5 Core trends redefining MDR in 2026

Brian Martin

Director of Product Management

Integrity360

Nick Brownrigg

Director of Solution Architecture

Integrity360

Ahmed Aburahal

Technical Product Manager

Integrity360

Agenda

- Evolving threats
- AI impact on cyber security
- Evolution of MDR architecture
- Automation vs human element
- Exposure management integration
- Real-world attack examples
- Key takeaways
- Q&A

Integrity360
your **security** in mind

Threats are evolving

- **API threats**
- **Autonomous attack by AI**
- **Targeting business use of AI**
- **Targeting AI (LLM models)**
- **Attacks Using AI**
- **Cloud Threats**

- 44% of advanced bot activity target specifically API environments, despite APIs representing only 14% of overall attack vectors
- Brute force has entered the top 3 API breach methods in 2025
- BOLA (Broken Object Level Authorisation) stays #1 API vulnerability and #1 on the OWASP top 10 API list
    - 60 million users records stolen – USPS breach
    - 15 million users records stolen – Trello breach

Integrity360
your **security** in mind

Threats are evolving

- API threats
- **Autonomous attack by AI**
- Targeting business use of AI
- Targeting AI (LLM models)
- Attacks Using AI
- Cloud Threats

- Autonomous attacks carried by AI agents
- Carnegie Mellon University research conducted in partnership with Anthropic, showed that AI could replicate the 2017 cyberattack on Equifax by autonomously exploiting vulnerabilities, installing malware and stealing data. (Attack Toolkit "Incalmo")
- The result? Threat actor can expand their campaigns without the human element limitations

Threats are evolving

- API threats
- Autonomous attack by AI
- **Targeting business use of AI**
- Targeting AI (LLM models)
- Attacks Using AI
- Cloud Threats

- Gemini Trifecta: discovered by Tenable, 3 vulnerabilities in Google’s Gemini:
  - Gemini Cloud Assist - a prompt-injection vulnerability
  - Gemini browsing tool vulnerability
  - Gemini search personalisation model – search injection vulnerability

- Amazon Q Developer compromise: *“AWS Security has inspected the code and determined the malicious code was distributed with the extension but was unsuccessful in executing due to a syntax error.”*!

Threats are evolving

- API threats
- Autonomous attack by AI
- Targeting business use of AI
- Targeting AI (LLM models)
- Attacks Using AI
- Cloud Threats

- Poisoning attacks: Poisoning attacks target the AI/ML model training data
- Evasion attacks: Evasion attacks target an AI/ML model’s input data
- Model tampering: Model tampering targets the parameters or structure of a pre-trained AI/ML model

Threats are evolving

- API threats
- Autonomous attack by AI
- Targeting business use of AI
- Targeting AI (LLM models)
- **Attacks Using AI**
- Cloud Threats

- Attacks where adversaries use AI to craft sophisticated attacks
- **LameHug** infostealer malware, By APT28, no hardcoded malicious code but talks to LLMs and sends prompts to retrieve malicious code
- Deepfakes, Social engineering, extorsion, phishing: all benefit from AI for increased efficiency and accuracy

Threats are evolving

API threats

Autonomous attack by AI

Targeting business use of AI

Targeting AI (LLM models)

Attacks Using AI

Cloud Threats

- 4 in 5 companies reported at least one cloud-related security incident in the past year (ExpertInsights, 2025)
- 68%of organisations admit they cannot detect cloud threats in real time. (AppSecure, 2025)
- 54% of cloud-stored data is classified as sensitive (AppSecure, 2025)

Defenders follow

- **SentinelOne**
  acquired Observo AI & Prompt Security (2025)
- **Crowdstrike**
  Pangea of AI security, Onum for telemetry analytics (2025), Flow Security (2024)
- **Vectra AI**
  Netography (2025)
- **Darktrace**
  Mira Security (2025)
- **Check Point**
  Lakera AI Security & Veriti for risk management (2025), Atomsec (SaaS Security, 2024)
- **Fortinet**
  Suridata (SSPM, 2025), Lacework (CNAPP, 2024), NextDLP (2024)
- **Varonis**
  Cyral (DAM) & SlashNext (AI email security), 2025.
- **Netskope**
  Wootcloud (OT sec, 2025) & Dasera (DSPM, 2024)
- **Zscaler**
  Red canary AI-driven SecOps (2025), Avalor for AI-powered data security (2024), Airgap (2024)

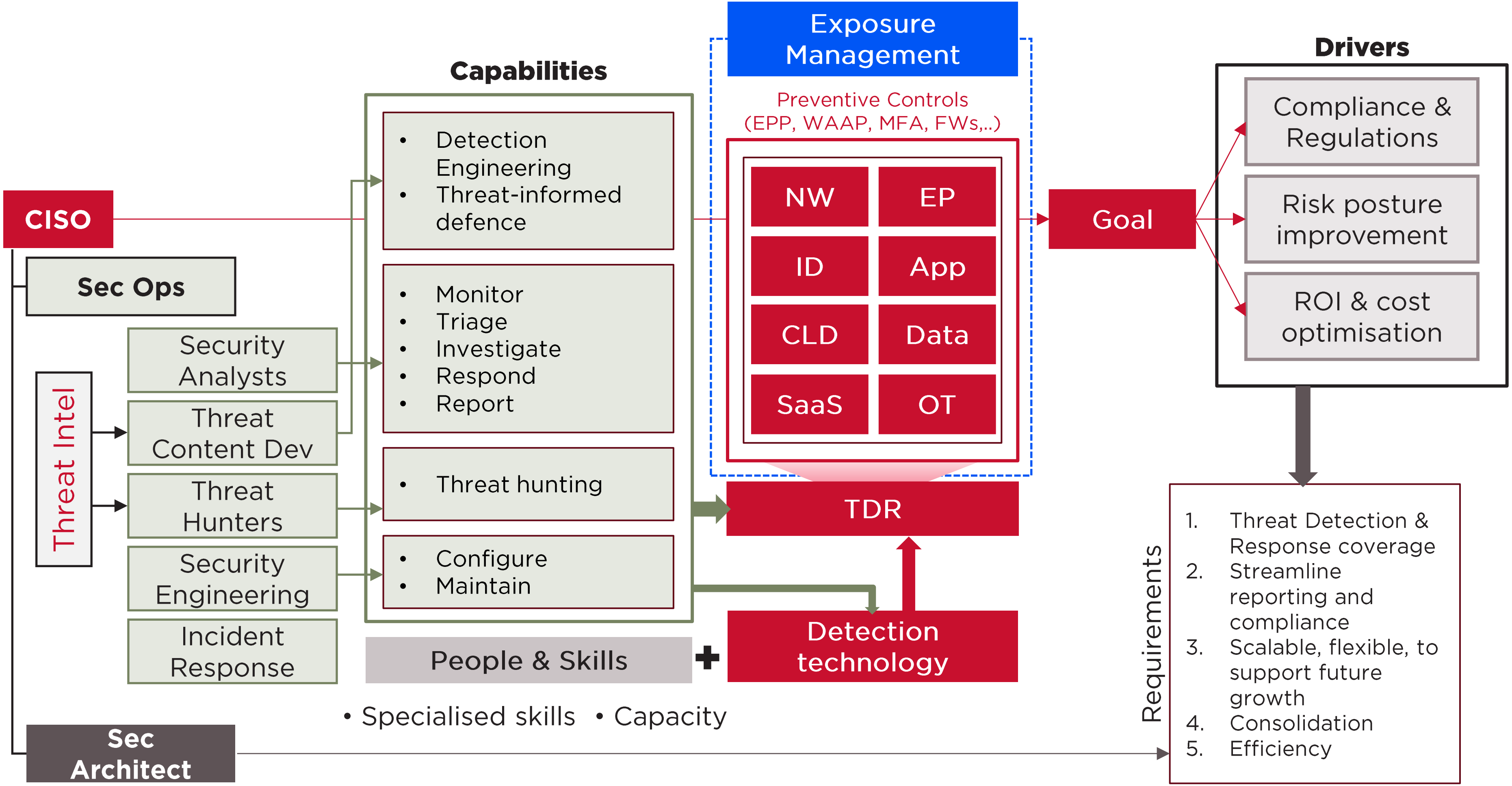
Cyber security vendors are racing to acquire AI capabilities, complete their coverage, and move into a consolidated platform play ..
But can they win the race?

AI vs AI

Integrity360
your security in mind

- Criminal GPT (Worm GPT, ..)
- Prompt injection, poisoning,..
- Deepfakes, social engineering,..

- Gen AI user controls
- AI-powered MDR
- AISPM
- Security Copilot
- AI analytics



CISO

Sec Ops

Threat Intel

Security Analysts

Threat Content Dev

Threat Hunters

Security Engineering

Incident Response

Sec Architect

Capabilities

- Detection Engineering
- Threat-informed defence

- Monitor
- Triage
- Investigate
- Respond
- Report

- Threat hunting

- Configure
- Maintain

People & Skills ✚

- Specialised skills
- Capacity

Exposure Management

Preventive Controls (EPP, WAAP, MFA, FWs,..)

NW	EP
ID	App
CLD	Data
SaaS	OT

TDR

Detection technology

Goal

Drivers

Compliance & Regulations

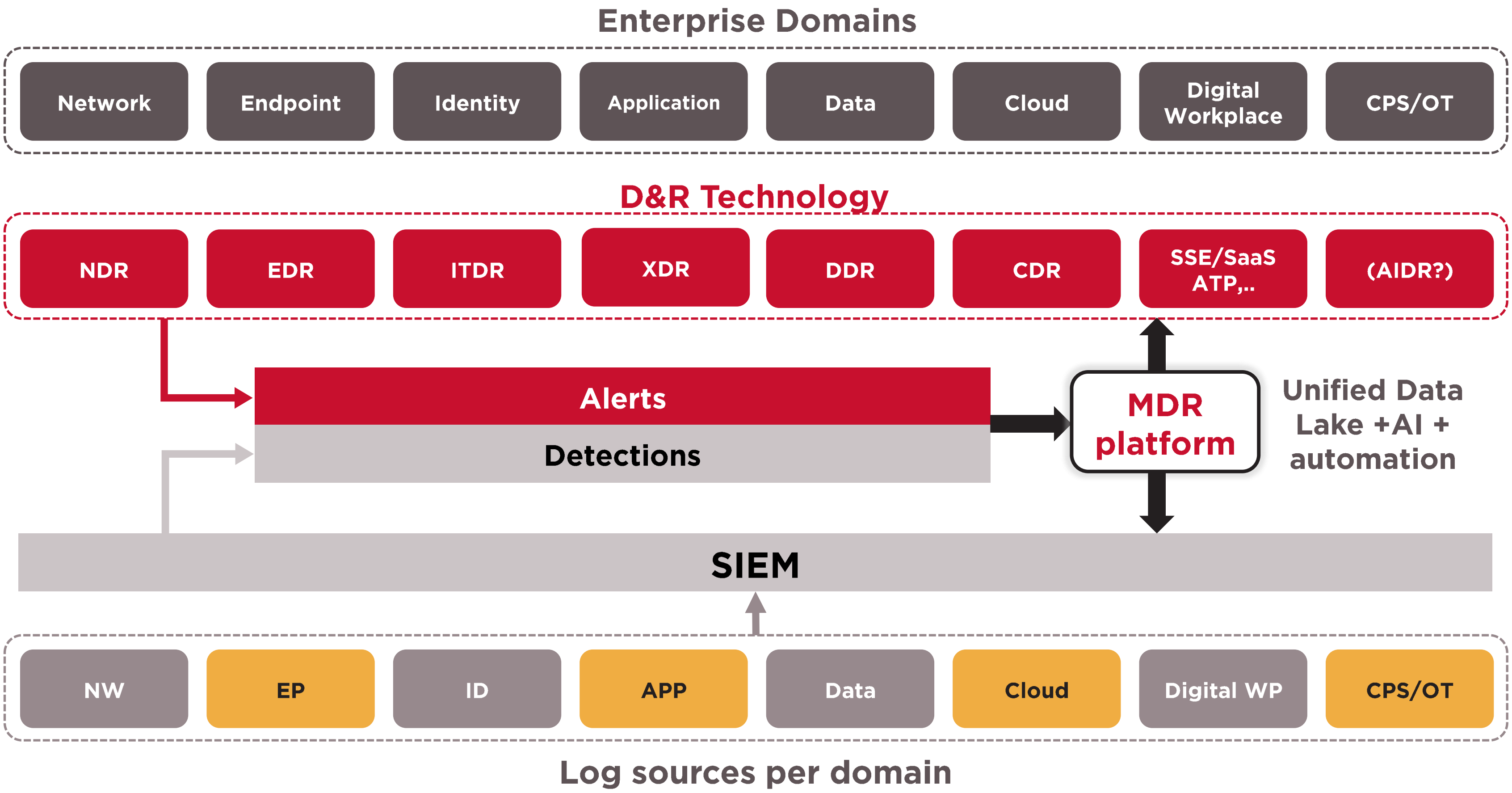
Risk posture improvement

ROI & cost optimisation

Requirements

1. Threat Detection & Response coverage
2. Streamline reporting and compliance
3. Scalable, flexible, to support future growth
4. Consolidation
5. Efficiency

MDR Architecture



Enterprise Domains

Network | Endpoint | Identity | Application | Data | Cloud | Digital Workplace | CPS/OT

D&R Technology

NDR | EDR | ITDR | XDR | DDR | CDR | SSE/SaaS ATP,.. | (AIDR?)

Alerts

Detections

MDR platform

Unified Data Lake +AI + automation

SIEM

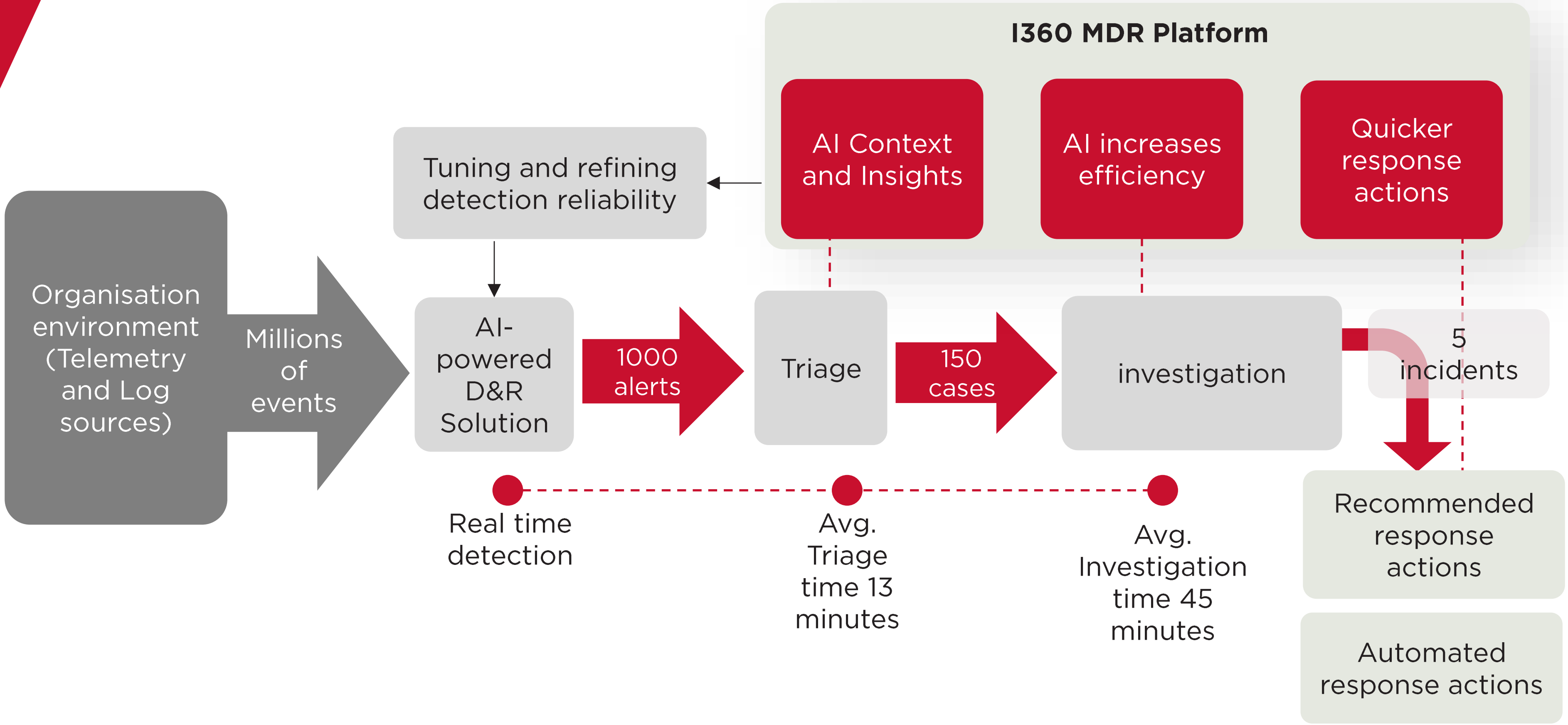
NW | EP | ID | APP | Data | Cloud | Digital WP | CPS/OT

Log sources per domain

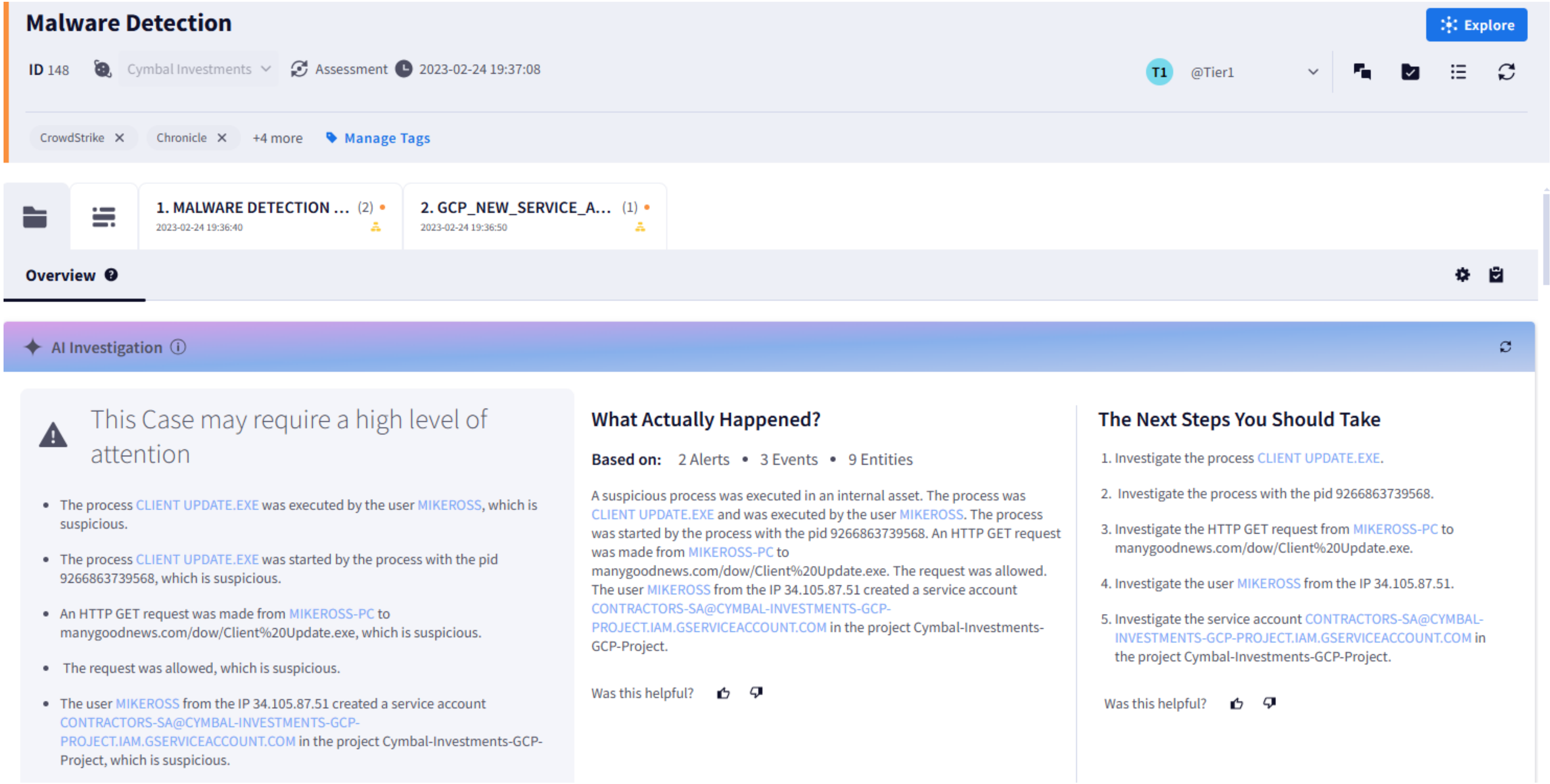
How AI Enhances MDR Capabilities

How AI & Automation powered MDR improves incident lifecycle

Integrity360
your security in mind


I360 MDR Platform
AI Context and Insights
AI increases efficiency
Quicker response actions
Tuning and refining detection reliability
Organisation environment (Telemetry and Log sources)
Millions of events
AI-powered D&R Solution
1000 alerts
Triage
150 cases
investigation
5 incidents
Recommended response actions
Automated response actions
Real time detection
Avg. Triage time 13 minutes
Avg. Investigation time 45 minutes

Utilising AI in SecOps



Malware Detection

ID 148 Cymbal Investments Assessment 2023-02-24 19:37:08

CrowdStrike ✕ Chronicle ✕ +4 more Manage Tags

1. MALWARE DETECTION ... (2) 2023-02-24 19:36:40

2. GCP_NEW_SERVICE_A... (1) 2023-02-24 19:36:50

Overview

AI Investigation

This Case may require a high level of attention

- The process CLIENT UPDATE.EXE was executed by the user MIKEROSS, which is suspicious.
- The process CLIENT UPDATE.EXE was started by the process with the pid 9266863739568, which is suspicious.
- An HTTP GET request was made from MIKEROSS-PC to manygoodnews.com/dow/Client%20Update.exe, which is suspicious.
- The request was allowed, which is suspicious.
- The user MIKEROSS from the IP 34.105.87.51 created a service account CONTRACTORS-SA@CYMBAL-INVESTMENTS-GCP-PROJECT.IAM.GSERVICEACCOUNT.COM in the project Cymbal-Investments-GCP-Project, which is suspicious.

What Actually Happened?

Based on: 2 Alerts • 3 Events • 9 Entities

A suspicious process was executed in an internal asset. The process was CLIENT UPDATE.EXE and was executed by the user MIKEROSS. The process was started by the process with the pid 9266863739568. An HTTP GET request was made from MIKEROSS-PC to manygoodnews.com/dow/Client%20Update.exe. The request was allowed. The user MIKEROSS from the IP 34.105.87.51 created a service account CONTRACTORS-SA@CYMBAL-INVESTMENTS-GCP-PROJECT.IAM.GSERVICEACCOUNT.COM in the project Cymbal-Investments-GCP-Project.

Was this helpful?

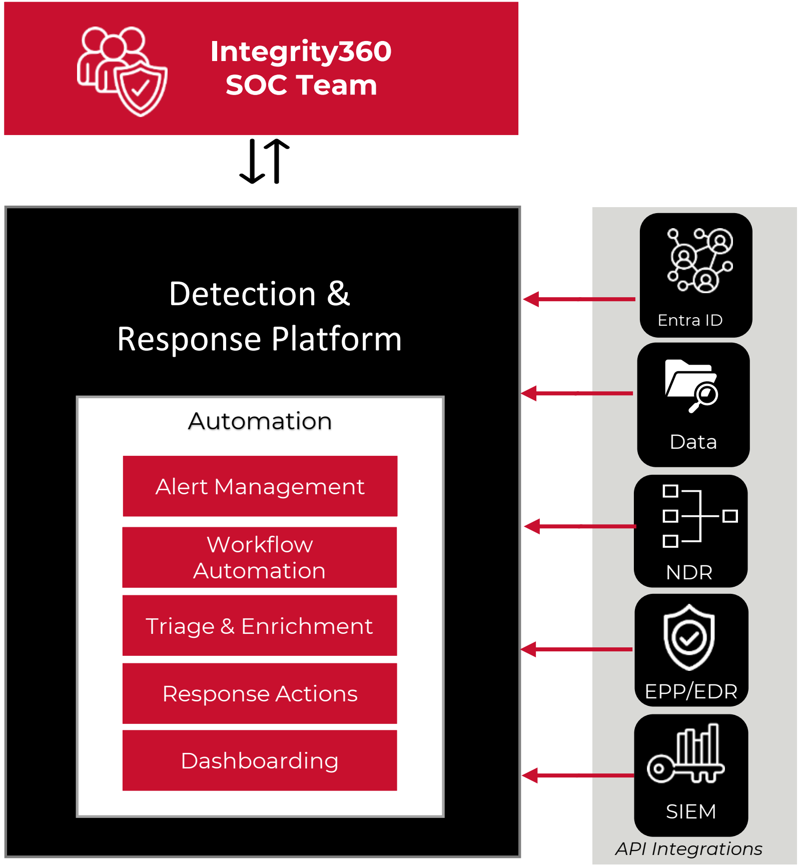
The Next Steps You Should Take

1. Investigate the process CLIENT UPDATE.EXE.
2. Investigate the process with the pid 9266863739568.
3. Investigate the HTTP GET request from MIKEROSS-PC to manygoodnews.com/dow/Client%20Update.exe.
4. Investigate the user MIKEROSS from the IP 34.105.87.51.
5. Investigate the service account CONTRACTORS-SA@CYMBAL-INVESTMENTS-GCP-PROJECT.IAM.GSERVICEACCOUNT.COM in the project Cymbal-Investments-GCP-Project.

Was this helpful?

Automation benefits

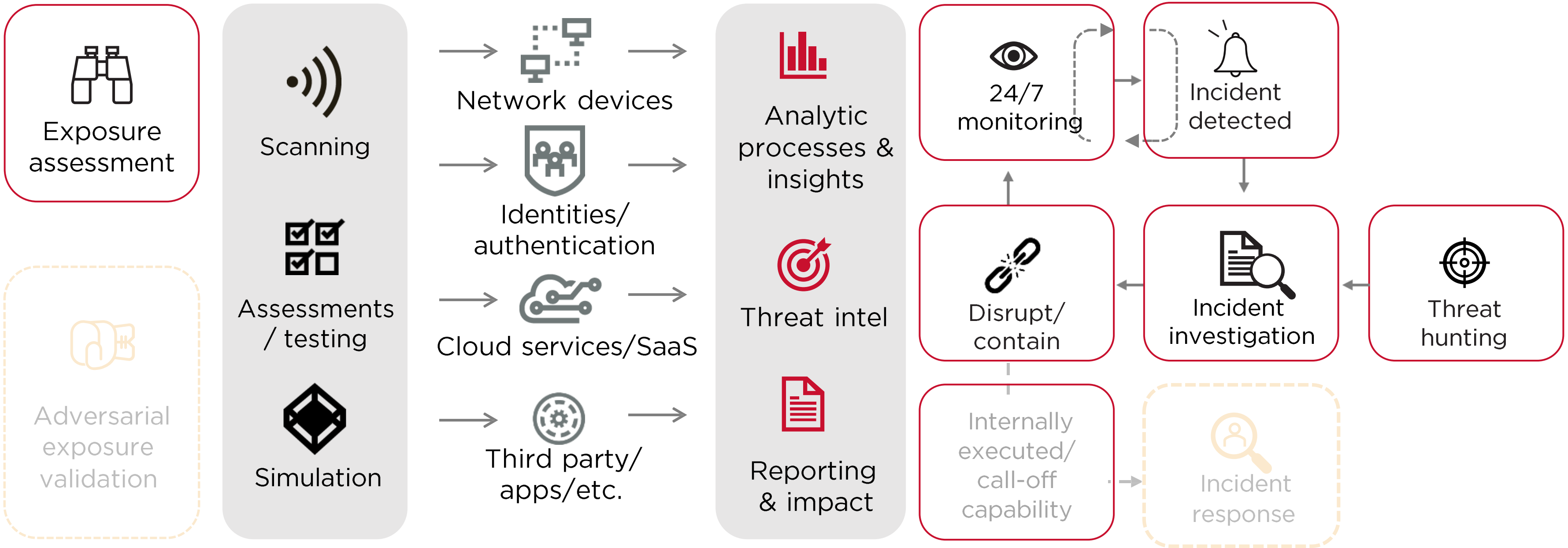
- Use not replace on existing detection technologies
- Consistent outcomes across techs
- Rapid view of collated information
- Rapid enrichment information
- Rapid timeline view
- Enables faster precise decisions making
- Positive impact on staff retention
- Enables proactive threat hunting
- Enables continuous threat detection evolution



Integrity360
your security in mind

Now is the time for MDR to become proactive

🟥 Core MDR 🟧 Adjacent services



Exposure assessment

Adversarial exposure validation

Scanning

Assessments / testing

Simulation

Network devices

Identities/ authentication

Cloud services/SaaS

Third party/ apps/etc.

Analytic processes & insights

Threat intel

Reporting & impact

24/7 monitoring

Incident detected

Disrupt/ contain

Incident investigation

Threat hunting

Internally executed/ call-off capability

Incident response

Proactive capability

Reactive capability

Gartner

Integrity360

your **security** in mind

> “By 2026, organisations prioritising their security investments based on a continuous exposure management programme will be three times less likely to suffer from a breach.”

Gartner

Integrity360

your security in mind

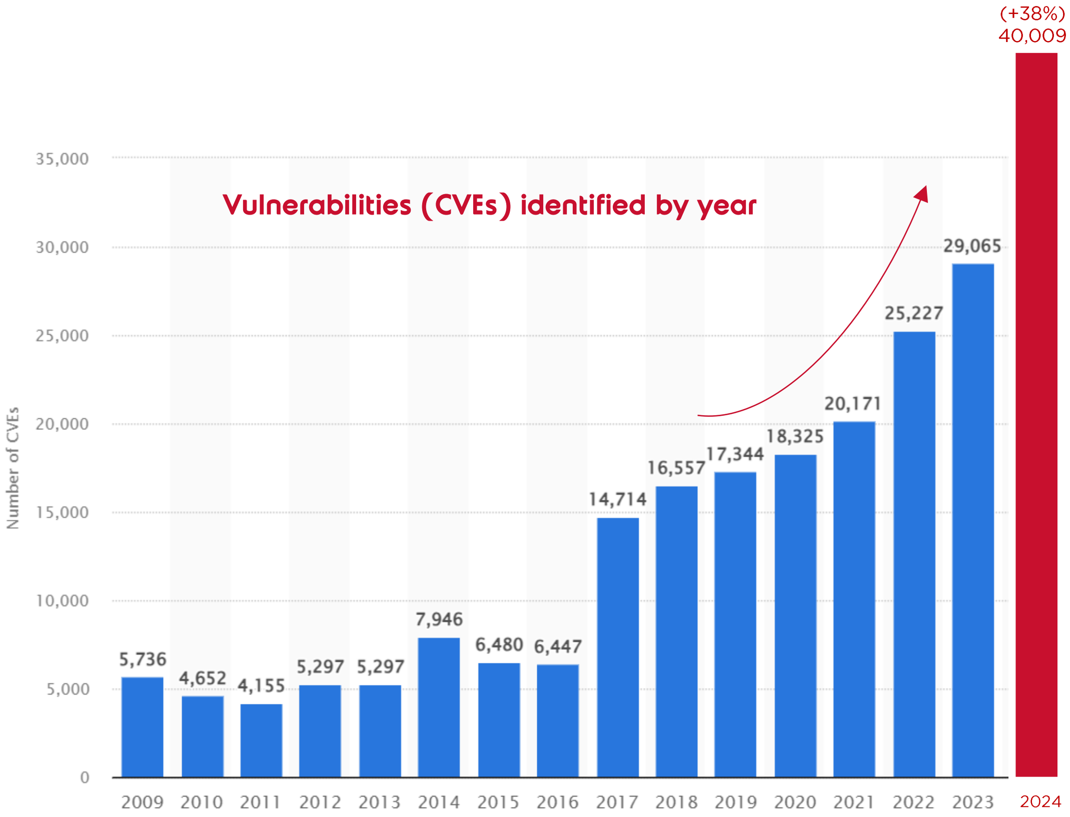
> “By 2028, 50% of findings from managed detection and response providers will be focused on, or include detail on threat exposures, up from 10% today.”

Gartner

An exposure is anything that may be exploited by a bad actor to achieve their objectives

Type of exposure: Vulnerabilities

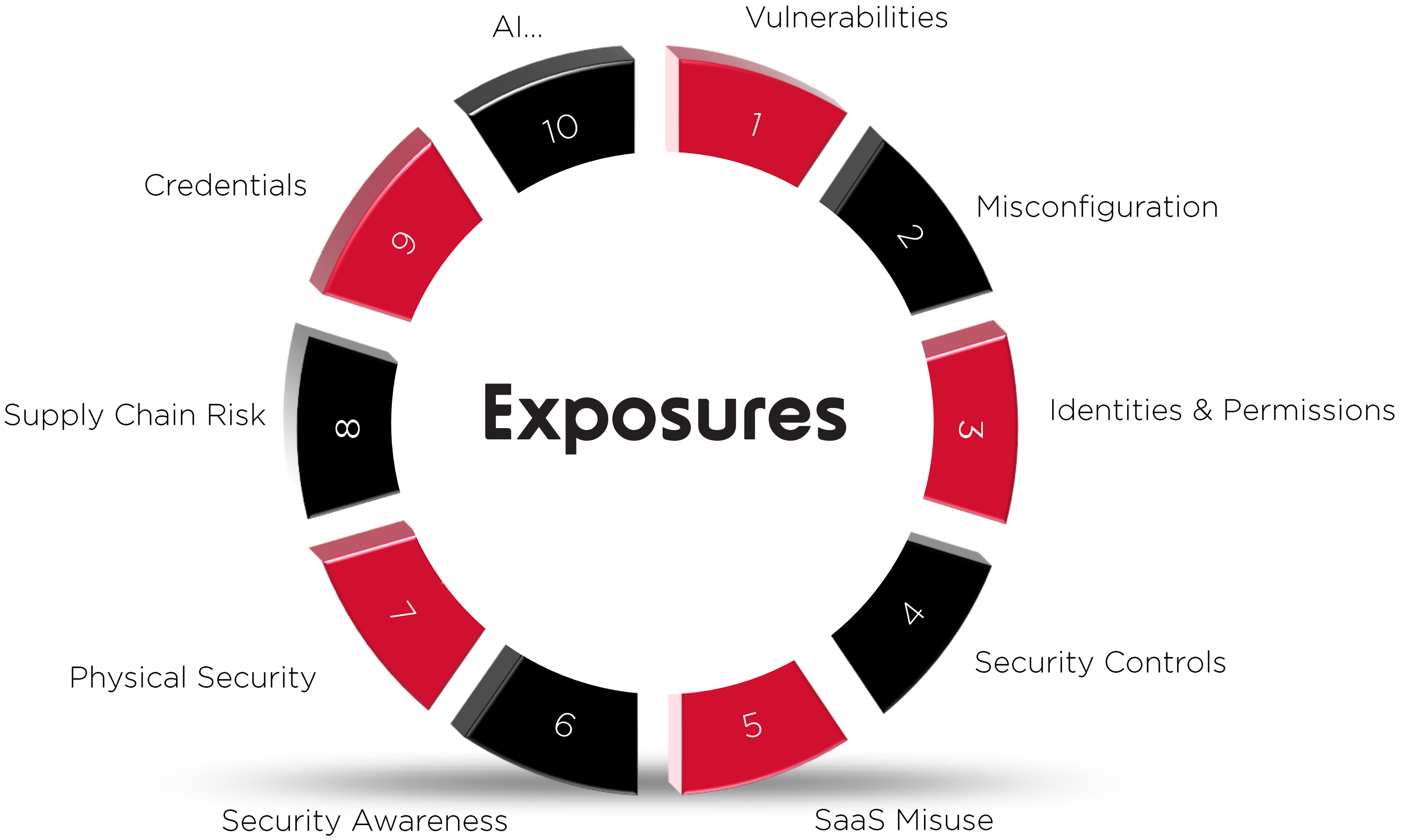
Vulnerability Management as a problem is not going away



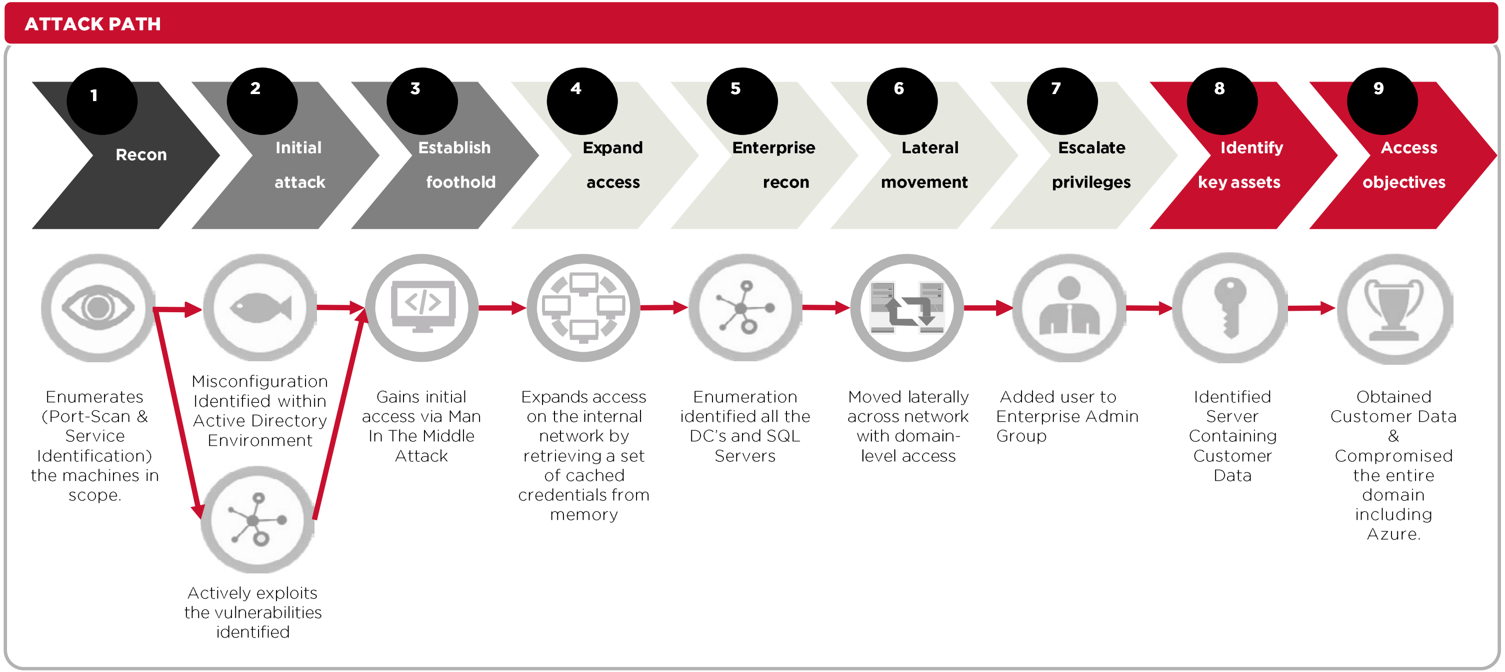
Source: Statista.com

> “Even taking a risk-based vulnerability management (RBVM) approach might not be sufficient. Fixing every known vulnerability has always been operationally infeasible.
>
> *- GARTNER*

Exposures extend beyond vulnerabilities



Attackers chain exposures to build attack paths



ATTACK PATH

1 Recon

2 Initial attack

3 Establish foothold

4 Expand access

5 Enterprise recon

6 Lateral movement

7 Escalate privileges

8 Identify key assets

9 Access objectives

Enumerates (Port-Scan & Service Identification) the machines in scope.

Misconfiguration Identified within Active Directory Environment

Actively exploits the vulnerabilities identified

Gains initial access via Man In The Middle Attack

Expands access on the internal network by retrieving a set of cached credentials from memory

Enumeration identified all the DC's and SQL Servers

Moved laterally across network with domain-level access

Added user to Enterprise Admin Group

Identified Server Containing Customer Data

Obtained Customer Data & Compromised the entire domain including Azure.

MITRE ATT&CK

The fight back along the kill chain is underway

Not convinced?

Oct 2025: Qilin stole ~9,300 files

Qilin frequently uses phishing (incl. tailored spear-phishing) and abused leaked or purchased legitimate credentials to gain a foothold (MITRE T1566 / T1078)

Mitigating factor: Digital Risk Protection

Jun 2025: Multi-country data breach discovered. ShinyHunters. Registration of likely phishing domains and setup of exfil/collection infrastructure in a narrow window.

Mitigating factor: Digital Risk Protection

LOUIS VUITTON

Jan 2024 Midnight Blizard, gained access to corporate email accounts via password spraying, spear-phishing via Teams/RDP lures, credential theft from legacy/test accounts.

Mitigating factor: **Use Microsoft** properly or CCM e.g., XMCyber.

Microsoft

Aug 2024:Salt compromised at least nine major U.S. telecommunications firms. exploiting zero-day vulnerabilities in network equipment, intercepting metadata of users' calls and text messages.

Mitigating factor: Continual External Attack Surface Scanning.

US TELECOM
SERVICES
KEEPING PEOPLE CONNECTED

ticketmaster® X INGRAM MICRO® QANTAS Collins Aerospace DELL Technologies

Key takeaways

- Evolving threats require consolidated D&R
- Attackers already using AI, embrace defender-side usage
- Automation won’t replace the human SOC, but can augment it
- Integrate Exposure Management with MDR to cover proactive and reactive risk reduction
- Ensure MDR provider is evolving in line with modern requirements