WEBINAR STARTING SOON

# Managed Microsoft Defender for Endpoint

**JONATHAN TRAYERS**
Director: Security

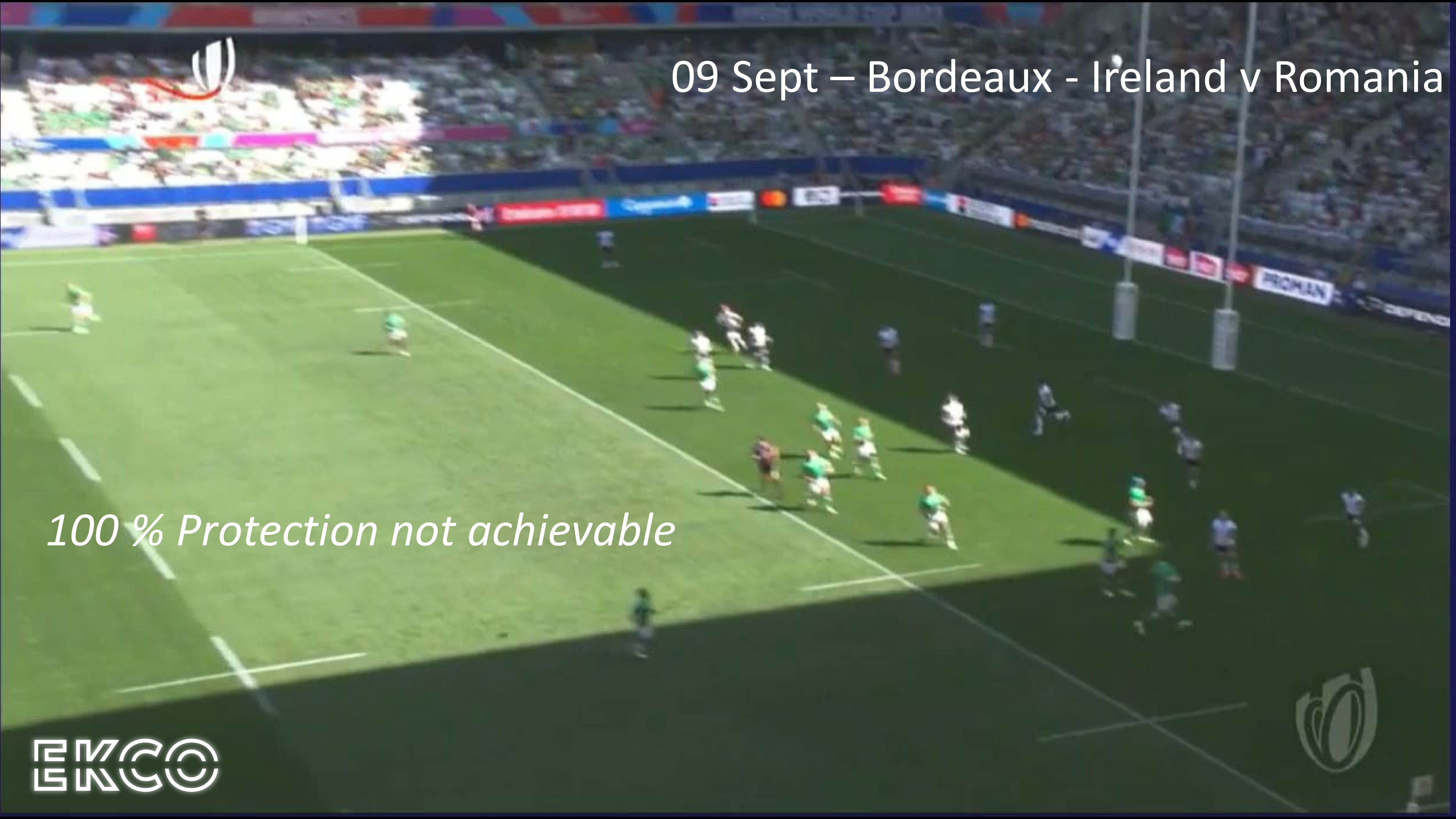
**PAUL HOGAN**
Director: MDR

**Thursday 12 October 2023 | 10.00 - 11.00**

**WEBINAR**

# Agenda

1. Three Endpoint Security Challenges
2. Key Features of a Managed EDR Programme
3. Ekco's Managed Defender for Endpoint Service
4. Key Takeaways
5. Q&A
6. Value-add for webinar attendees



09 Sept – Bordeaux - Ireland v Romania

*100 % Protection not achievable*

# Endpoint Security Challenges

### Changing Threat Landscape

UNDERSTAND YOUR RISKS & EXPOSURE

### Legacy Approaches

ORGANISATIONS MUST HAVE THE RIGHT PROTECTIONS IN PLACE

### Security Specialists

PROTECTION ISNT ENOUGH – NEED TO DETECT & RESPOND

## Can you answer these questions ?

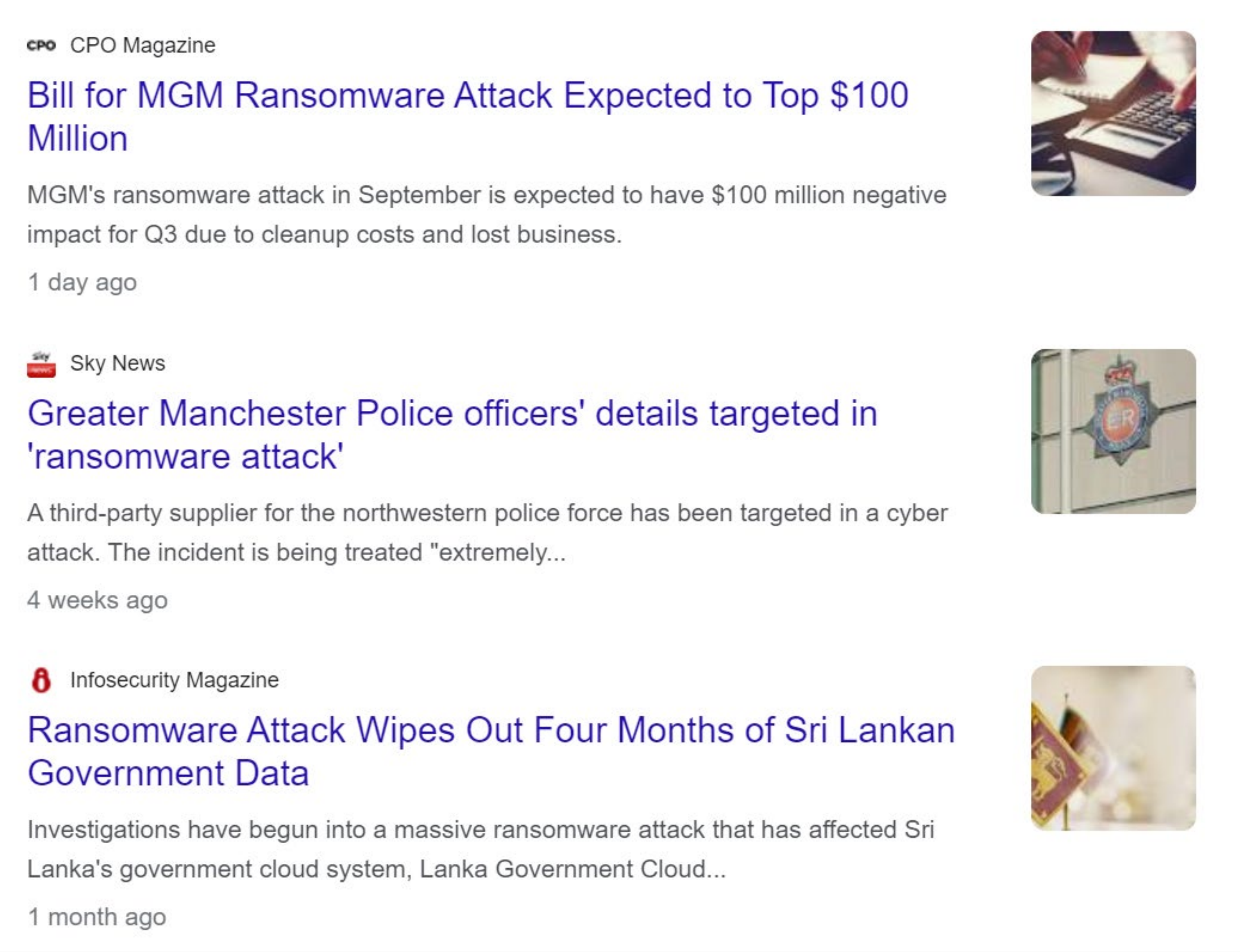
- What are the major risks and vulnerabilities?
- Are we configured to protect against advanced threats?
- Are we in compliance
- What security incidents are happening right now?
- What is the impact to the organisation?

# Endpoint Security Challenges

## Changing Threat Landscape

**UNDERSTAND YOUR RISKS & EXPOSURE**

- Nature of work has changed, and Endpoints represent a significant attack surface.
- Majority breaches are **due existing vulnerabilities or misconfigurations**
- **Ransomware attacks and threat actors** continues to grow, costs of data breaches and regulation are increasing.
- **Cyber insurance** is setting the bar higher.



CPO Magazine

Bill for MGM Ransomware Attack Expected to Top $100 Million

MGM's ransomware attack in September is expected to have $100 million negative impact for Q3 due to cleanup costs and lost business.

1 day ago

Sky News

Greater Manchester Police officers' details targeted in 'ransomware attack'

A third-party supplier for the northwestern police force has been targeted in a cyber attack. The incident is being treated "extremely...

4 weeks ago

Infosecurity Magazine

Ransomware Attack Wipes Out Four Months of Sri Lankan Government Data

Investigations have begun into a massive ransomware attack that has affected Sri Lanka's government cloud system, Lanka Government Cloud...

1 month ago

# Global Threat Landscape

## Microsoft Digital Defence Report – October 2023

- Cybercriminals are leveraging **the cybercrime-as-a-service** ecosystem to launch attacks at scale.
- **Ransomware operators are shifting heavily toward hands on keyboard attacks,** using living-off-the- land techniques and remote encryption to conceal their tracks, and exfiltrating data to add pressure to their ransom demands.
- And cybercriminals are **improving their ability to impersonate or compromise legitimate third parties**, making it even harder for users to identify fraud until it's too late.

80-90%

of all successful ransomware compromises originate through unmanaged devices

70%

of organisations encountering human-operated ransomware had fewer than 500 employees

Human-operated ransomware attacks are up more than

200%

Password-based attacks spiked in 2023

# Endpoint Security Challenges

## Legacy Approaches

**ORGANISATIONS MUST HAVE THE RIGHT PROTECTIONS IN PLACE**

- Most organisations have basic EPP solutions in place but it's not enough. **46% of compromised systems had no malware on them**
- **Vulnerabilities and misconfigurations on the endpoint** expand the attack surface.
- Organisations need **EDR and VM to extend EPP.**

**The days of just having antivirus are dead!**

## Endpoint Protection (EPP) vs Endpoint Detection & Response (EDR)

**MORE SOPHISTICATED ATTACKS**

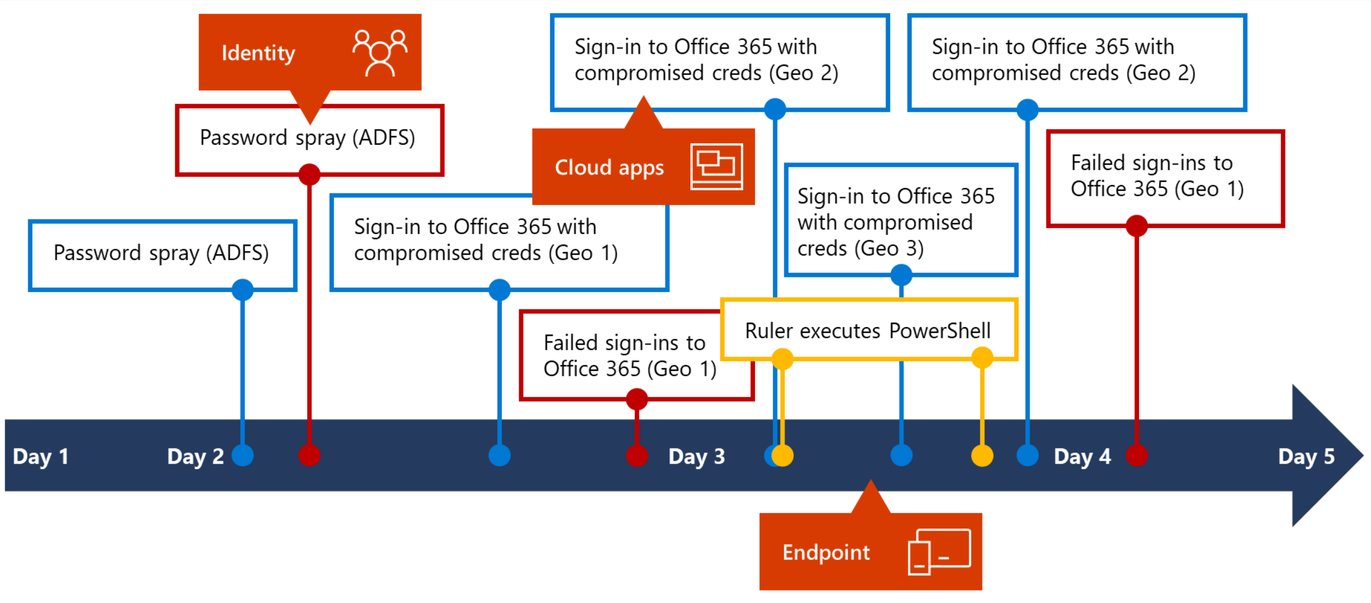
- EPP primarily focus on preventing known threats, utilising **a database of known malware signatures** to block malicious activities before they can execute on the host.
- EDR continuous monitors and responses to advanced threats, employing **behavioural analysis and anomaly detection** to identify and mitigate threats.

# Endpoint Security Challenges

## Security Specialists

**PROTECTION ISNT ENOUGH – NEED TO DETECT & RESPOND**

- **100% protection is impossible**, Incidents happen, so as well as technology you need an **IR capability** that detects and responds to incidents 24x7.
- **Threats are complex** and organisations **lack the expertise to manage EDR on a 24x7x365 basis.**
- Access to Incident Response Specialists is essential in modern enterprises.


Identity
Password spray (ADFS)
Password spray (ADFS)
Sign-in to Office 365 with compromised creds (Geo 1)
Cloud apps
Sign-in to Office 365 with compromised creds (Geo 2)
Failed sign-ins to Office 365 (Geo 1)
Ruler executes PowerShell
Sign-in to Office 365 with compromised creds (Geo 3)
Sign-in to Office 365 with compromised creds (Geo 2)
Failed sign-ins to Office 365 (Geo 1)
Endpoint
Day 1
Day 2
Day 3
Day 4
Day 5

# Managed Detection and Response

## Key Features of a Managed EDR & VM programme

Endpoint detection & response

Next generation protection

Attack Surface Reduction

Auto investigation & remediation

Threat and Vulnerability Management

Threat Hunting

24x7x365

Search
Vulnerability Management dashboard
Filter by device groups (17/17)
Top security recommendations
Recommendation
Exposed devices
Threats
Impact
Tags
Update Apple Mac Os
Update Apple Safari for Mac
Update Microsoft Windows 10 (OS and built-in applications)
Show more
Show exceptions
Microsoft Secure Score for Devices
Your score for devices: 51%
Application
OS
Network
Accounts
Security controls
Exposure score

# Protecting Endpoints from Cyberattacks

## A Managed Microsoft Defender for Endpoint (MDE) Solution from Ekco

# Microsoft Defender for Endpoint (MDE)

## An industry leader in endpoint security

FORRESTER

Forrester names Microsoft a Leader in 2021 Endpoint Security Software as a Service Wave

Forrester names Microsoft a Leader in 2020 Enterprise Detection and Response Wave

Forrester names Microsoft a Leader in Extended Detection and Response Q4 2021

Gartner

Gartner names Microsoft a Leader in 2022 Endpoint Protection Platforms Magic Quadrant

MITRE | ATT&CK

Microsoft leads in real-world detection in MITRE ATT&CK evaluation

Microsoft anti-malware capabilities consistently achieve high scores in independent tests

SC MEDIA

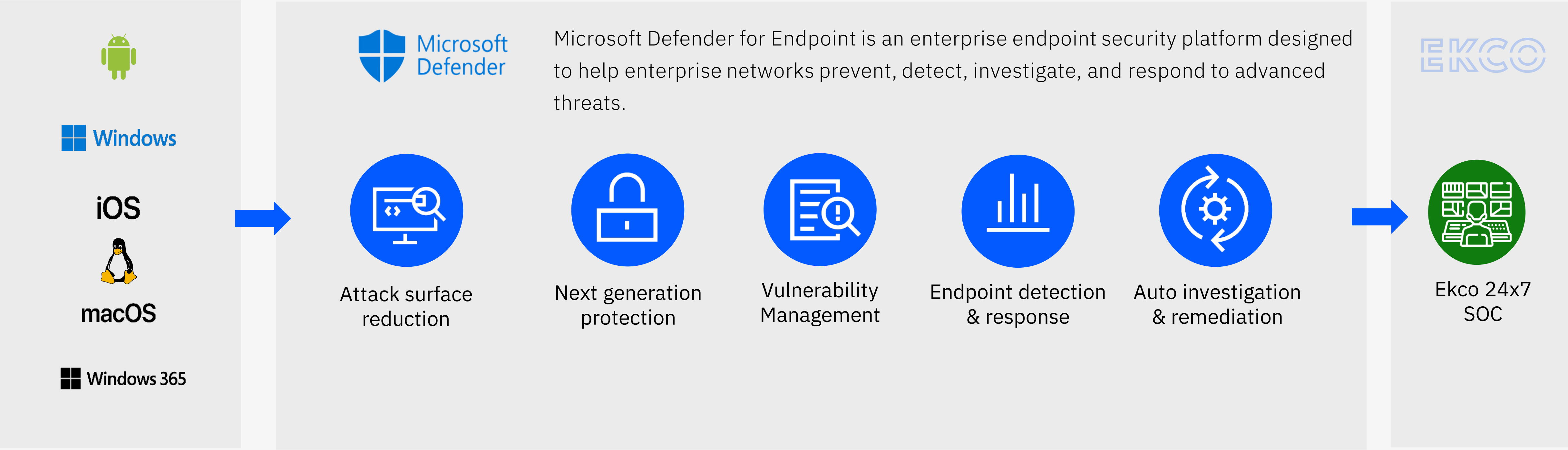
Microsoft Defender for Endpoint awarded a perfect 5-star rating by SC Media in 2020 Endpoint Security Review

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2021

Microsoft won six security awards with Cyber Defense Magazine at RSAC 2021

# Managed Detection and Response (MDR)

## Microsoft Defender for Endpoint (MDE)



Windows

iOS

macOS

Windows 365

Microsoft Defender

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

Attack surface reduction

Next generation protection

Vulnerability Management

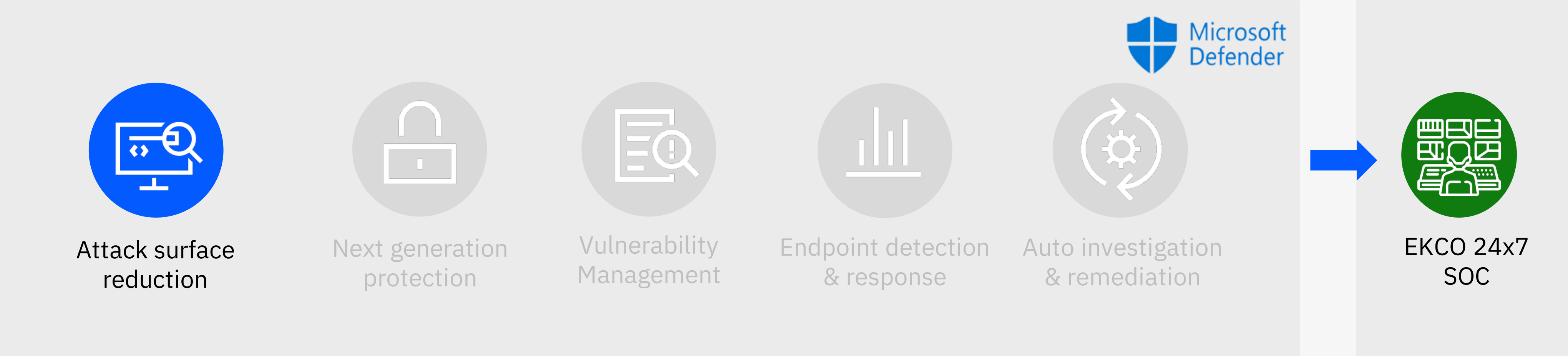
Endpoint detection & response

Auto investigation & remediation

Ekco 24x7 SOC

# Attack surface reduction

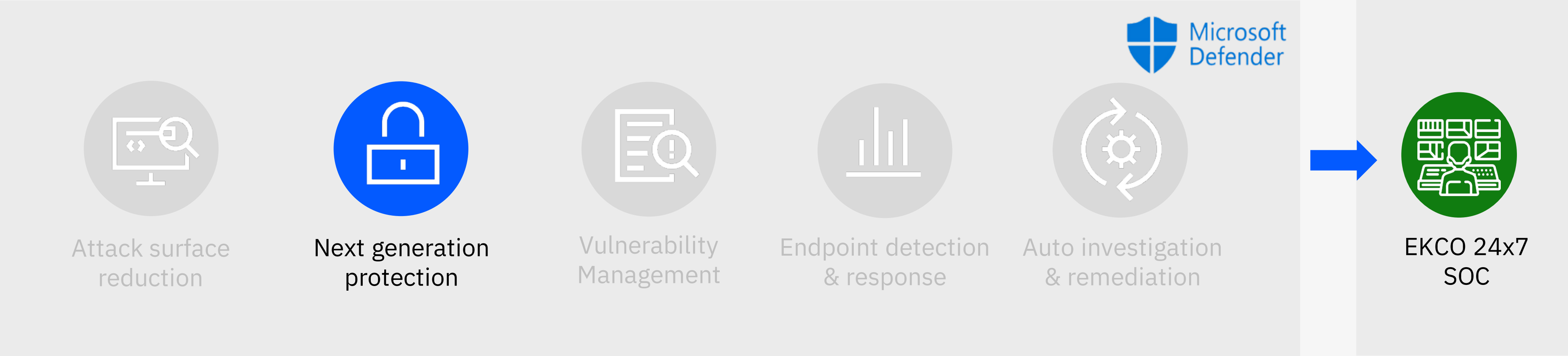
## Eliminate risks by reducing the surface area of attack


Microsoft Defender
Attack surface reduction
Next generation protection
Vulnerability Management
Endpoint detection & response
Auto investigation & remediation
EKCO 24x7 SOC

- Attack surface reduction (ASR) is a collection of controls that restrict common malware and exploit techniques
- The attack surface reduction set of capabilities provides the first line of defense in the stack.
- By ensuring configuration settings are properly set and exploit mitigation techniques are applied, the capabilities resist attacks and exploitation.
- This set of capabilities also includes network protection and web protection, which regulate access to malicious IP addresses, domains, and URLs.

# Next Generation Protection

## Blocks and tackles sophisticated threats and malware

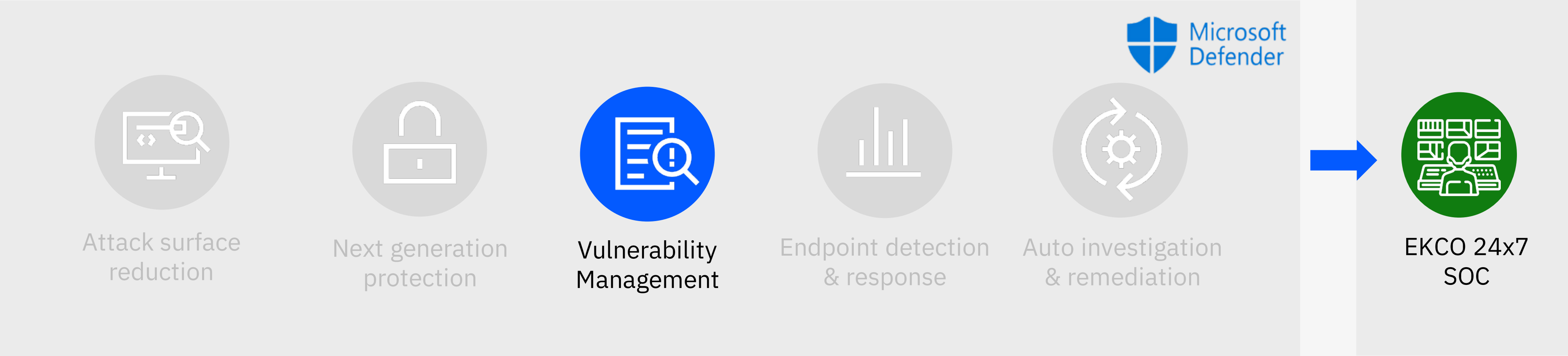


Microsoft Defender
Attack surface reduction
Next generation protection
Vulnerability Management
Endpoint detection & response
Auto investigation & remediation
EKCO 24x7 SOC

- Behavioral based real-time protection – dynamic heuristics rather than static signatures
- Blocks file-based and fileless malware
- Stops malicious activity from trusted and untrusted applications

# Vulnerability management

## A risk-based approach to prioritize and remediate your vulnerabilities

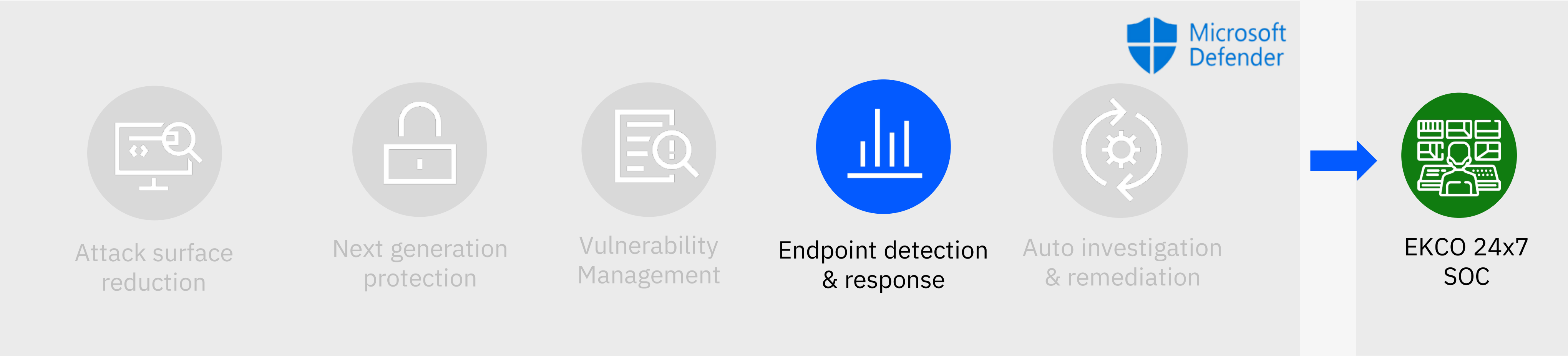

Microsoft Defender
Attack surface reduction
Next generation protection
Vulnerability Management
Endpoint detection & response
Auto investigation & remediation
EKCO 24x7 SOC

Built-in core vulnerability management capabilities use a modern risk-based approach to the discovery, assessment, prioritisation, and remediation of endpoint vulnerabilities and misconfigurations.

- Continuous real-time discovery
- Context-aware prioritization
- Built-in end-to-end remediation process

# Endpoint Detection & Response (EDR)

## Detect and investigate advanced persistent attacks



Microsoft Defender

Attack surface reduction

Next generation protection

Vulnerability Management

Endpoint detection & response

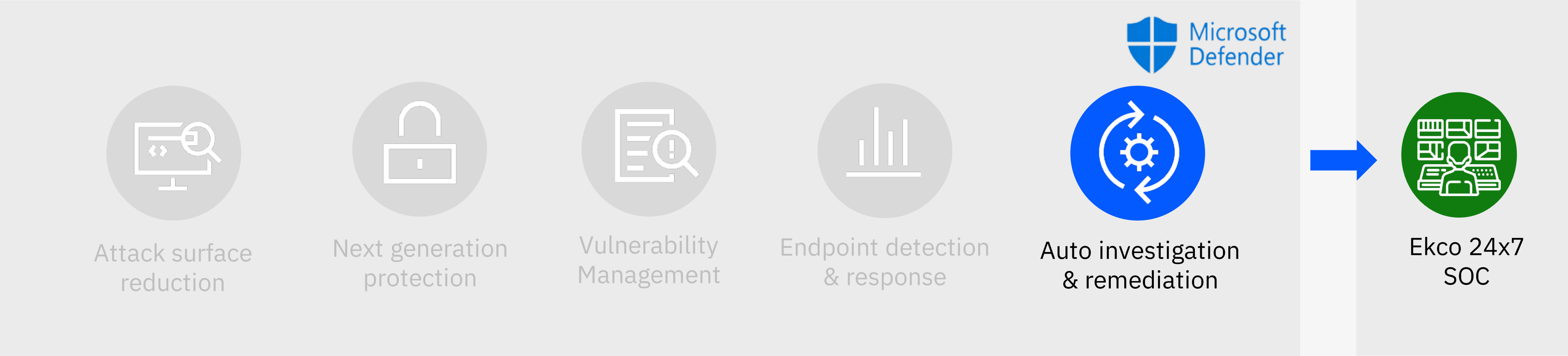
Auto investigation & remediation

EKCO 24x7 SOC

- Correlated Behavioural Alerts
- Investigation and hunting over six months of data
- Rich set of response actions
- Demonstrated industry-leading optics and detection capabilities in MITRE ATT&CK-based evaluation
- Live Response
- Advanced Hunting
- Deep file analysis

# Auto Investigation & Remediation (AIR)

## Automatically investigates alerts and remediates complex threats in minutes


Microsoft Defender
Attack surface reduction
Next generation protection
Vulnerability Management
Endpoint detection & response
Auto investigation & remediation
Ekco 24x7 SOC

- Automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale.
- Mimics the ideal steps analysts would take
- Tackles file or memory-based attacks
- Works 24x7, with unlimited capacity

✓ **Security automation is...**
mimicking the ideal steps a human would take to investigate and remediate a cyber threat

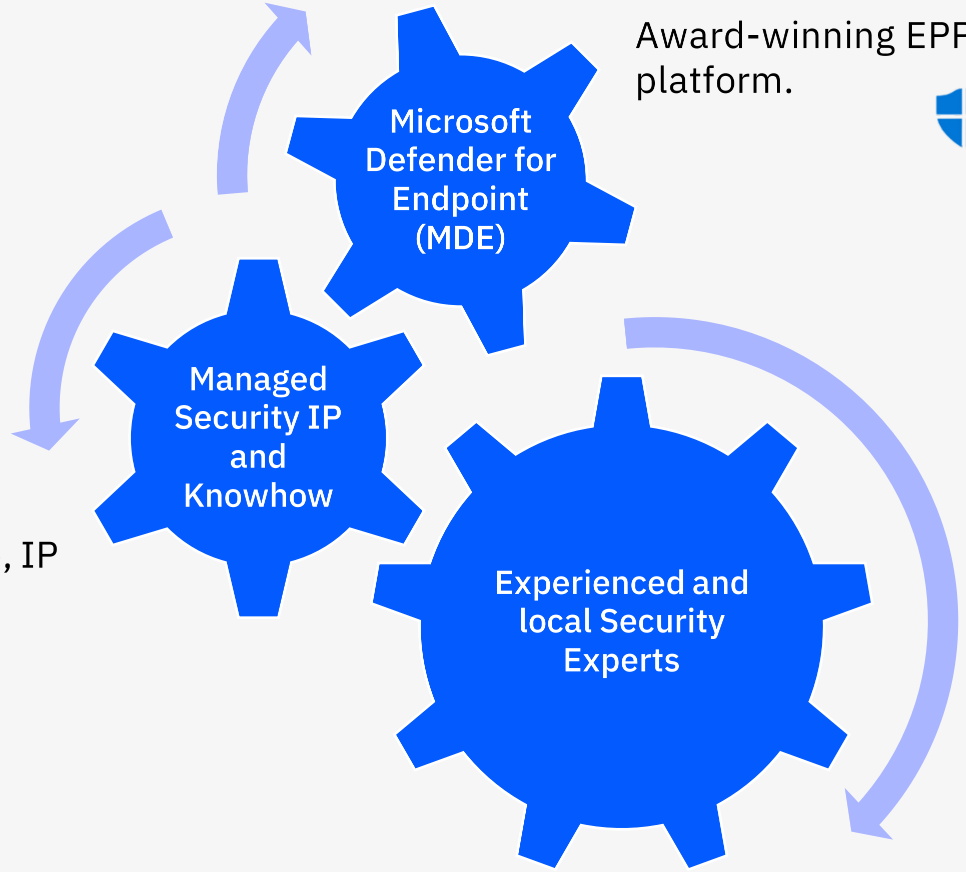
✗ **Security automation is not...**
if machine has alert → auto-isolate

# Ekco SOC

## 24x7 SOC located in Ireland – Digital Forensics and Incident Response

Award-winning EPP and EDR platform.

Microsoft Defender



Microsoft Defender for Endpoint (MDE)

Managed Security IP and Knowhow

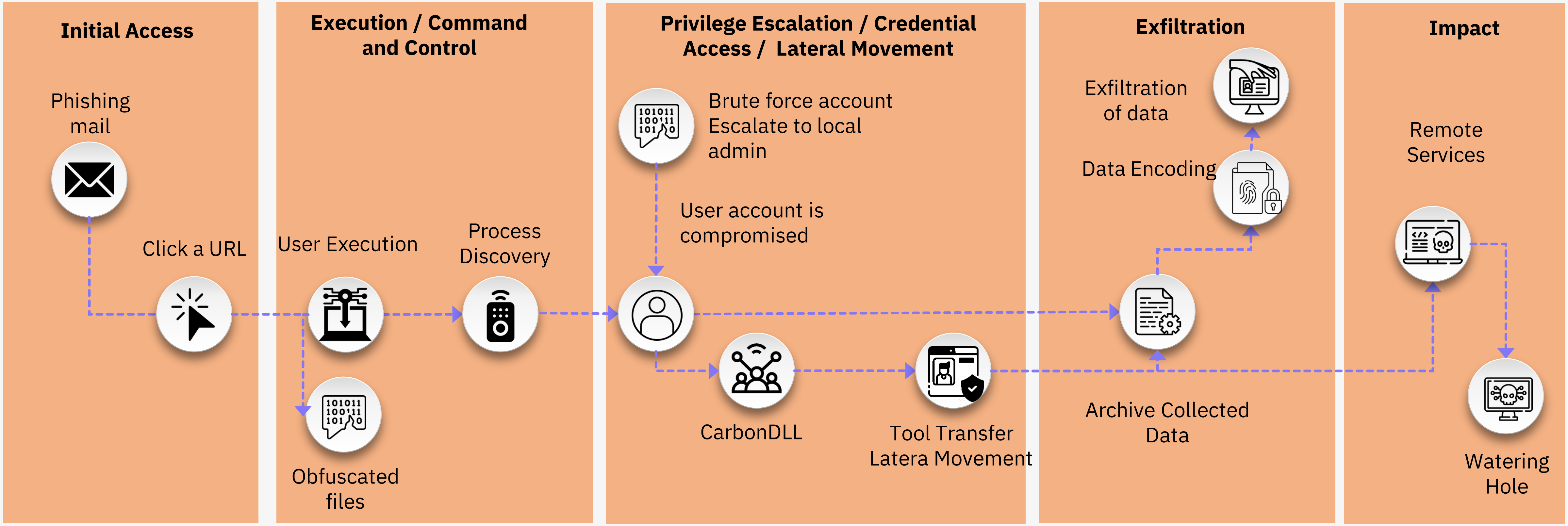
Experienced and local Security Experts

Comprehensive knowledge, IP and know-how

24x7 SOC located in Ireland. Staffed with expert and experienced analysts, leveraging extensive skill base.

# Managed MDE in Action

## MITRE ATT&CK – Turla Attack (Simplified)



# Service Description: MDR Microsoft Defender for Endpoint.

| | Essentials<br>(P1) | Advanced<br>(P2) | Add-Ons |
|---|---|---|---|
| **Microsoft Defender for Endpoint Deployment and onboarding**<br>Initial setup of Microsoft Defender for Endpoint (MDE). | ✓ | ✓ | |
| **Next Generation Protection**<br>Blocks sophisticated threats and malware with machine learning and behavioral based real-time protection | ✓ | ✓ | |
| **Attack Surface Reduction**<br>Minimise risks by reducing the surface area of attack, resisting attacks and exploitations | ✓ | ✓ | |
| **Managed Incident and Alert Monitoring and Triage – Incident Response**<br>A 24x7 XDR service protect detect with manual response actions. | ✓ | ✓ | |
| **24x7 SOC**<br>A 24x7 MDR service with around the clock detection and response from experienced threat experts | ✓ | ✓ | |
| **Incident Response Retainer***<br>IR service activation with 5 hours draw down time | ✓ | ✓ | |
| **Endpoint detection & response**<br>Rapidly detect, investigate, and respond to advanced threats. | | ✓ | |
| **AIR**<br>Automatic Investigation and remediation. | | ✓ | |
| **Threat and Vulnerability Management**<br>Discovery, assessment, prioritisation, and remediation of endpoint vulnerabilities and misconfigurations | | ✓ | |
| **Advanced Threat Hunting**<br>Experts proactively hunt to spot anomalies or known malicious behavior | | ✓ | |
| **Microsoft Secure Score for Devices**<br>reflects the collective security configuration state of your devices | | ✓ | |
| **Microsoft Defender for Office 365**<br>24x7 XDR service protect detect with manual response actions on email. | | | ✓ |
| **Microsoft Defender for Data Loss Prevention / Cloud / Identity**<br>Ekco have a 24x7 XDR service protect detect with manual response actions to all Defender products | | | ✓ |

* Core IR retainer can be upgraded

# Ekco Emergency Incident Response Services

## Reduce the time to detect, respond to, and recover from Cyber Security incidents.

## PREPARATION

### PLAN / ONBOARDING

Incident response plan and strategy. Create / review policy that details the activities to classify, prioritise and respond to an incident.

### IR TABLETOP EXERCISE

Bespoke scenario-based exercise to ensure that your key technical team incident stakeholders are practices the procedures required of them in the event of an incident or event.

## RESPONSE

### IR SPECIALISTS ON-CALL

Retainer based access to incident response specialists on call who have necessary skills and experience.

### INCIDENT MANAGEMENT

Incident management activities to contain and eradicate and forensics determination of root cause. Systems recovery/rebuild. Threat hunting with MDE. DF with Magnet Axiom Cyber.

## POST INCIDENT

### REPORT & REMEDIATION ADVICE

Incident timeline, root cause identification, and remediation advice an activities to improve security posture.

# Managed EDR (MDR) with Microsoft Defender for Endpoint

## Benefits of the Ekco Service

- 24/7 Threat Detection powered by real-time analytics
- Round-the-clock Incident Response
- Security Threat Focused – Advanced analytics to detect complex threats
- Incident Containment & Triage
- Automate Containment Response to block threats
- Improved Speed of detection & response
- Security Provider First – Expert level threat monitoring & analysis
- Reduced Cost & Complexity
- Simple Pricing structure

Our Managed EDR with Microsoft Defender for Endpoint offers an always-on, prevention-first endpoint security solution with supplemented threat detection and incident response capabilities.

Microsoft Defender

# Key Takeaways

# Q&A

# Value-add for webinar attendees

# Two-week free trial of Managed Microsoft Defender for Endpoint

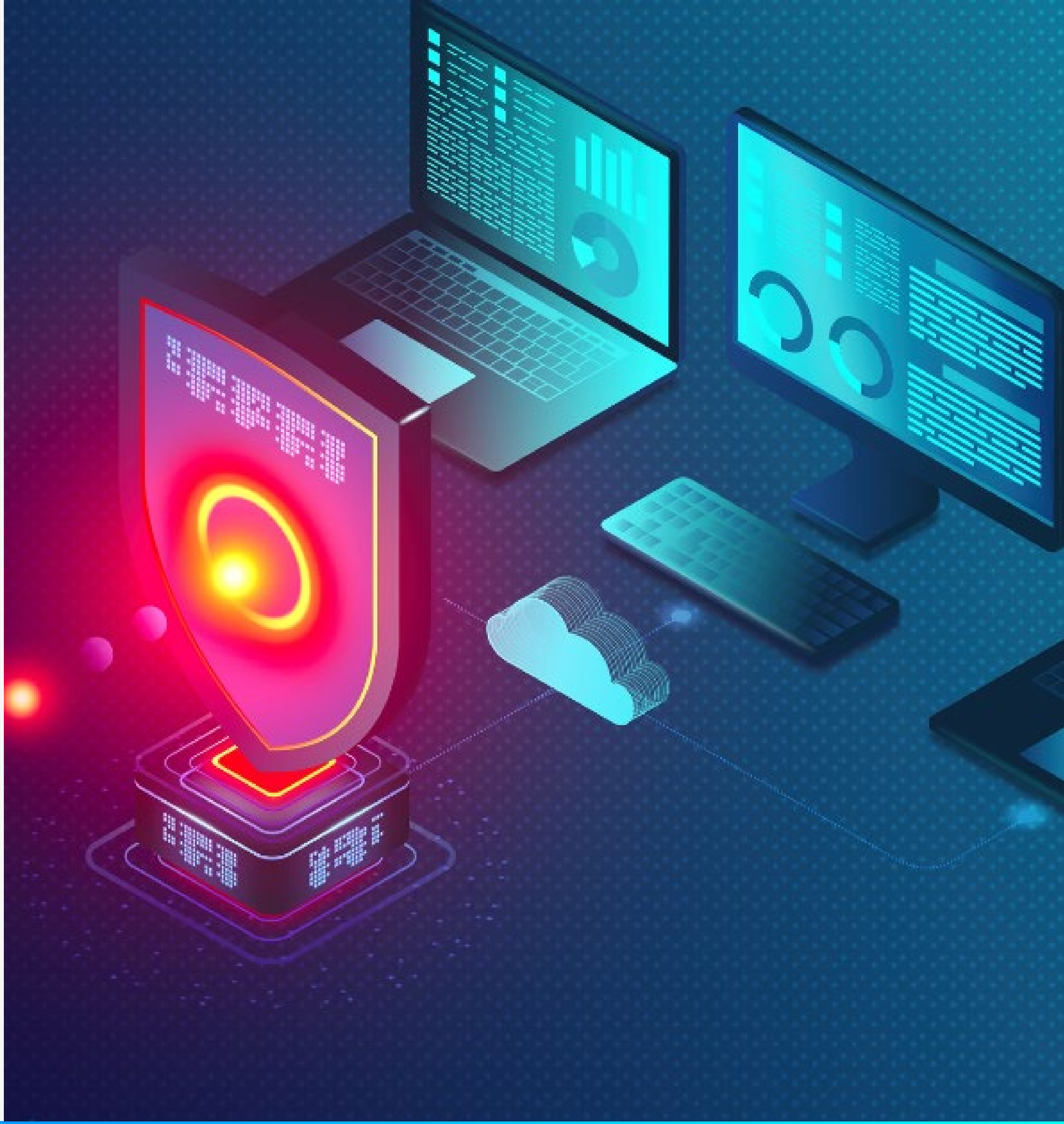
## You'll get to try out Ekco's Managed Microsoft Defender for Endpoint for yourself.

All webinar attendees will receive a two-week free trial

**This will include:**

- ✓ Review of your current endpoint configuration
- ✓ MDR service with auto investigation and response
- ✓ Technical and management report

You'll need to have a Microsoft Defender for Endpoint licence to take up the service



# Find out more

**More information on our Managed Microsoft Defender for Endpoint Service is on www.ek.co**

**Resources include:**

Datasheet: Ekco Managed MS Defender for Endpoint

Ebook: Supercharge your Security with Managed EDR

Ebook: The Ekco IT Security Guide to Getting More Sleep

# Thanks for joining us

www.ek.co