



Stronger Together, Building the Future of Cyber Resilience

A discussion on modern cyber threats, resilience strategies, and the role of Open XDR

Gareth Young

The Cyber Threat Landscape

- *Why is cyber resilience more critical than ever?*
- Cyber Stats
 - Average time to detect is 212 days
 - 67% Surge in ransomware
- The increasing complexity of attack surfaces
- The failure of traditional defensive security models



What is Cyber Resilience?

- *Cyber resilience is an organisation's ability to anticipate, withstand, recover from, and adapt to cyber threats.*
- Four Pillars of Cyber Resilience:
 - Anticipate – Proactive threat intelligence and detection
 - Withstand – Strong security architecture and response capabilities
 - Recover – Fast response, containment, and mitigation
 - Adapt – Continuous learning and improvement
- Common gaps in resilience that lead to breaches



The Tooling Problem in Cybersecurity

- Organisations rely on multiple security tools (EDR, SIEM, SOAR, NDR, IDS/IPS) which creates challenges, and a fragmented approach leads to a lack of visibility.
- Slow response times due to manual correlation and swivel chair syndrome
- Alert fatigue and inefficiencies in the security operations centre
- There is a growing need for a unified approach to security



Introduction to Open XDR

- 
- What is Open XDR?
 - Why 'Open' matters: Integrates with existing security tools
 - Centralised detection, analysis, and response
 - AI-driven automation for faster threat mitigation
 - How Open XDR enhances visibility, efficiency, and response speed

Strengthening Cyber Resilience

- Anticipate Threats with AI & UEBA
 - AI-driven anomaly detection
 - User and Entity Behaviour Analytics (UEBA)
- Withstand Attacks with NDR and Automated Detection
 - Network Detection & Response (NDR) for real-time threat visibility
 - Automated threat hunting
- Recover Faster with Automated Response
 - AI-powered incident prioritisation
 - Automated workflows to contain threats instantly
- Adapt with Continuous Intelligence
 - Learning from every incident
 - Enabling proactive security strategies

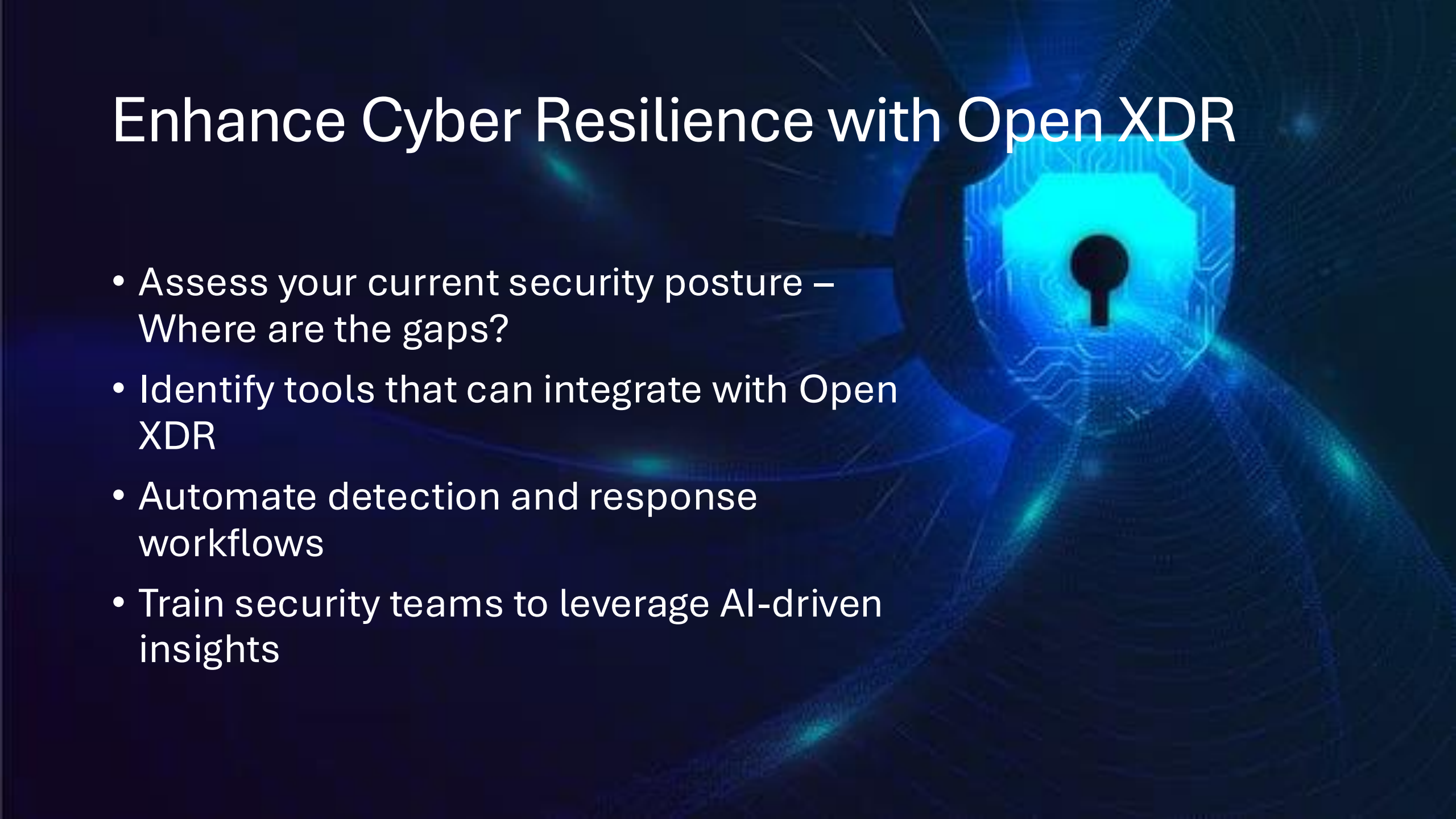


The Benefits of an Integrated Solution



- Up to 90% reduction in alert noise
- Threat detection and response 20x faster
- Lower operational costs by consolidating tools
- Better attack surface coverage across cloud, endpoint, network, and identity

Enhance Cyber Resilience with Open XDR



- Assess your current security posture – Where are the gaps?
- Identify tools that can integrate with Open XDR
- Automate detection and response workflows
- Train security teams to leverage AI-driven insights

Evolving the SOC

- Evolving from Narrow AI to Autonomous Agents
- Human-Guided Hyper-automation
- Amplifying Security Through Collaboration



Overcoming the Barriers to Adoption



- Common misconceptions about Open XDR
 - "Does it replace my existing security tools?" (No, it enhances them)
 - "Is it only for large enterprises?" (No, scalable for all sizes)
 - "Is it difficult to implement?" (No, plug-and-play integrations)
- Why **now is the right time** to adopt Open XDR



Open Security Initiatives and A Smarter Path to Cyber Resilience

- Fosters collaboration
- Enable flexibility and future-proofing
- Avoids reliance on a single vendor's roadmap or priorities
- Encourages transparency, innovation, and sharing
- Supports integration through open standards and interoperability





STELLAR CYBER®

Final Reflections – Building Resilience Together