

Incident Response Maturity – From Planning to Remediation



Matthew McGill
Sr. Information
Security Consultant

Agenda

- Incident Response Lifecycle
- Strategic Planning & Preparation
- Detection & Alerting
- Coordinated Response
- Recovery and Remediation
- Continuous Improvement
- Practical Guidance & Key Takeaways

The Incident Response Lifecycle



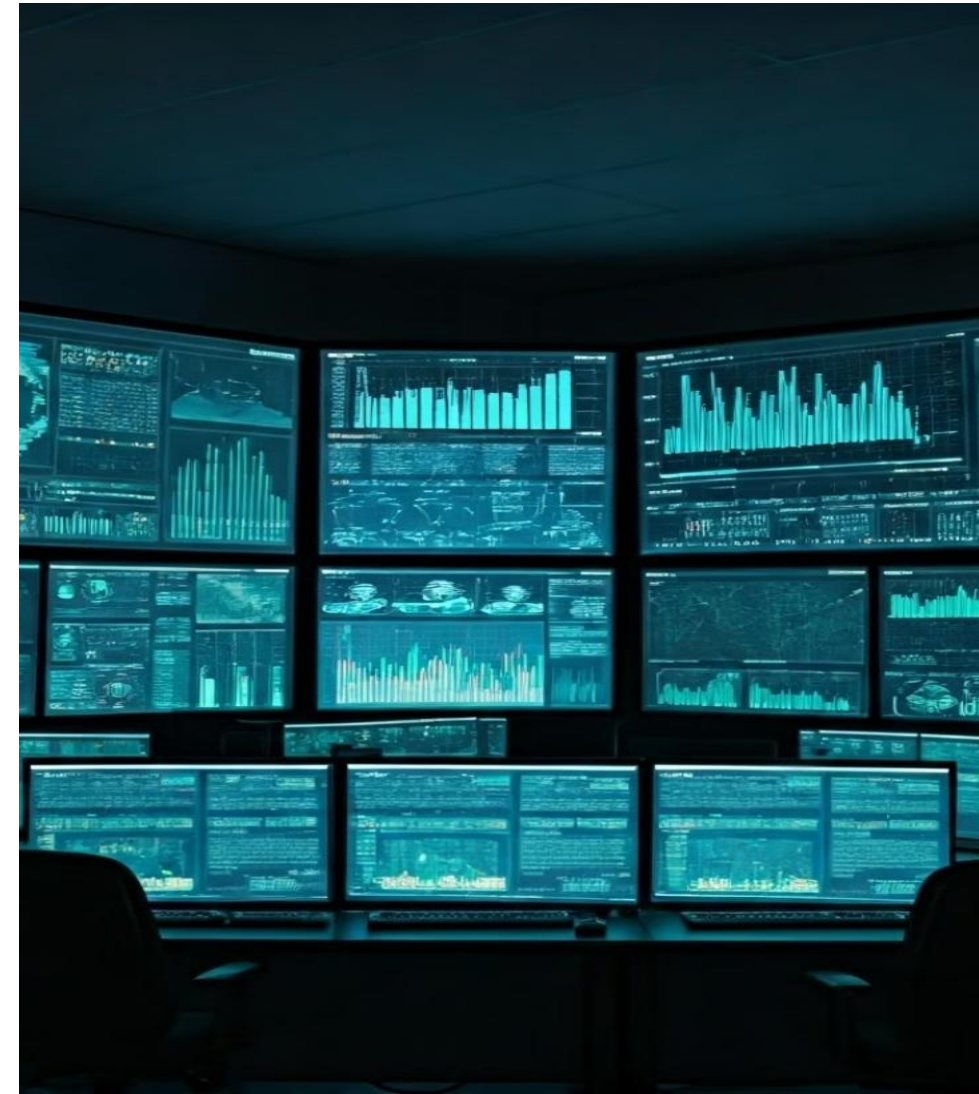
Strategic Planning & Preparation

- Developing an Incident Response Plan aligned to business priorities & compliance requirements
- Defining roles and responsibilities (internal teams, external partners, regulators, legal, cybersecurity insurance provider, etc.)
- Distinguishing between **event** and **incident**
- Building incident classification & severity models
- Importance of tabletop exercises & simulations



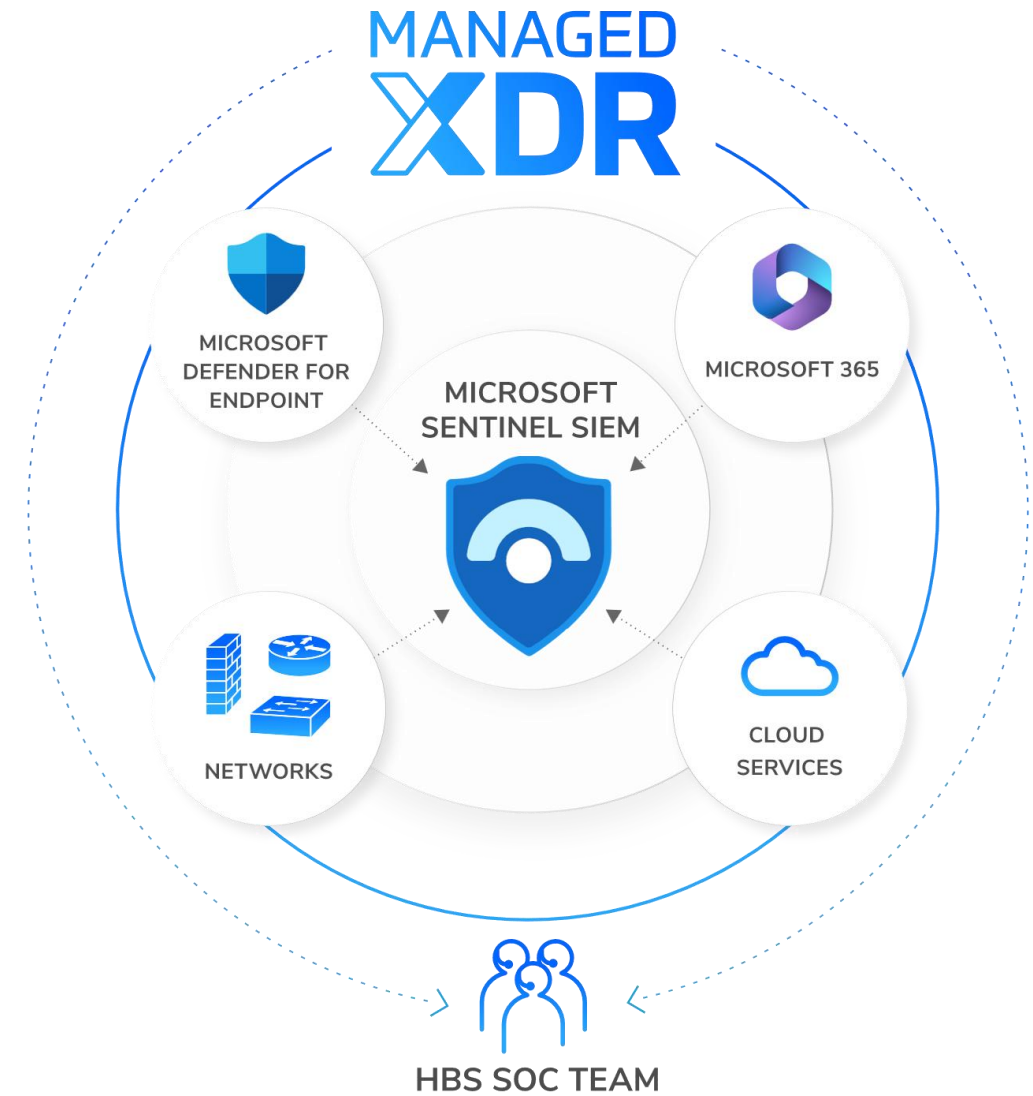
Proactive Defense – Defending with Data

- Detects Events/Incidents Early
 - Identify and stop attacks before they escalate
 - Reduce dwell time and limit exposure
 - Enable faster containment and rapid response
- Allows for Alert-Driven Security Operations
 - Real-time visibility into suspicious activity
 - Empowered response via SOC and SOAR
 - Identifies gaps and policy violations
- Drives Remediation and Improvement
 - Informs needed configuration changes, playbook updates, and patching needs
 - Strengthens future detection rules



Logging & Monitoring for Incident Response

- Why Logging Matters During Incidents
 - Provides forensic evidence for root cause analysis
 - Enables timeline reconstruction of attacker activity
- Monitoring Enables
 - Identify misconfigurations
 - Validate containment success and verify remediation
- Diversified vs. consolidated vendor approach



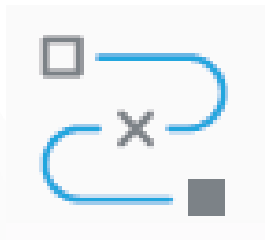
Coordinated Response

- IR requires a LOT of coordination
 - Internal coordination: IT, security, legal, HR, communications
 - External coordination: law enforcement, vendors, regulators, customers
- Overlaps with business continuity strategies
- Example workflows for ransomware, insider threats, and phishing
- Cybersecurity Insurance – Verify that forensic investigations are included and if not, establish a trusting relationship and partner

Incident Response Focus Points	
Business Email Compromise (BEC)	Advanced Persistent Threats (APT)
Phishing Attacks	Employee Data Theft
Malware Attacks	HR Issues
Ransomware	Industrial Espionage

Recovery & Remediation

- Root cause analysis and corrective actions
- Eradication of threat actor presence
- System recovery and validation
- Post-incident communication: executives, regulators, customers
- Ensuring business continuity during and after incidents



Continuous Improvement

- Post-incident reviews and lessons learned
- Updating the IR plan and playbooks
- Leveraging threat intelligence for proactive defense
- Building a culture of resilience

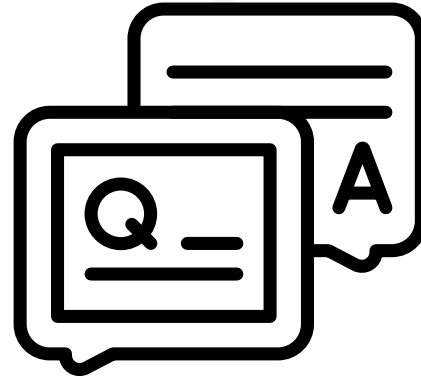


Practical Guidance & Key Takeaways





**SECURE
IOWA**
CONFERENCE



Discussion



Thank you!

We're happy to answer any questions.



COMPLIMENTARY

60 Minutes with a CISO

Spend an hour with an HBS Virtual Chief Information Security Officer (vCISO) to get expert insights and strategic recommendations for enhancing your cybersecurity measures.

During the hour, we will:

- Open the floor for your questions and provide expert CISO advice.
- Identify and prioritize key areas to address immediately.
- Deliver strategic recommendations to enhance your cybersecurity measures.