Getting to Grips with Incident Response Management

14th April 2021

Integrity360

your security in mind

Getting to Grips with Incident Response Management

Patrick Wragg

Cyber Incident Response Manager

Mark Wiley

Senior Account Manager

- Attack Techniques
- Recent Attacks
- Assessing your need for IR
- Pitfalls of managing IR

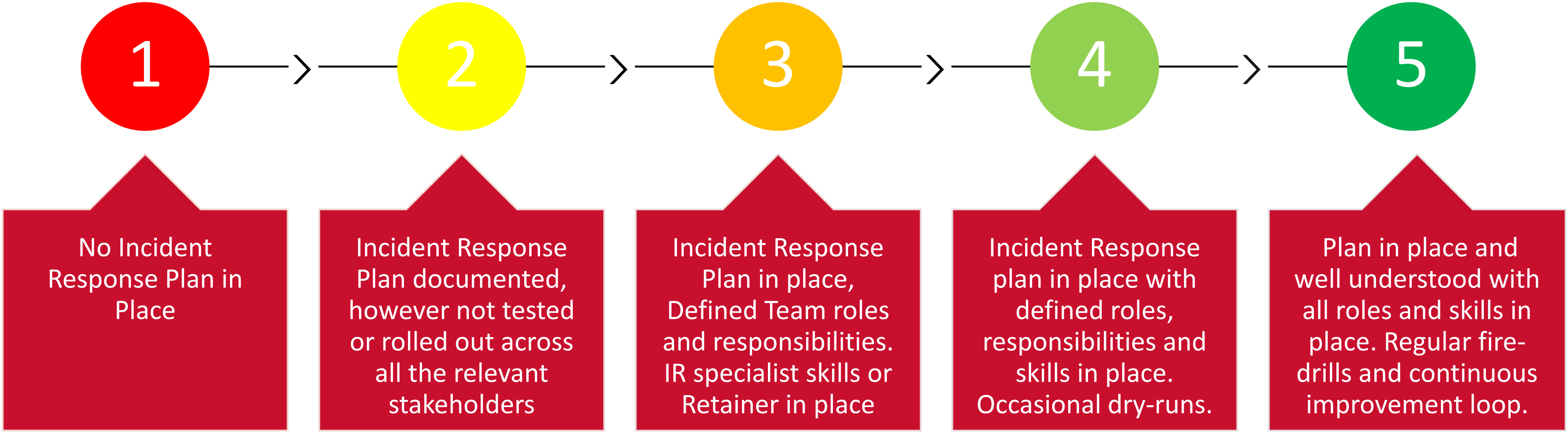
Integrity360

your **security** in mind

Incident Response Drivers

- Ransomware 2.0 model adoption - Maze Group
- Dwell time increasing – 66 Days in 2020 EMEA (M-trends 2021 Report)
- Business email compromise – MFA on O365
- Vulnerabilities in 3rd Party Software – Solarwinds, Microsoft
- Remote working – RDP access
- Scattergun approach – size doesn't matter

Incident Response Maturity



1. No Incident Response Plan in Place

2. Incident Response Plan documented, however not tested or rolled out across all the relevant stakeholders

3. Incident Response Plan in place, Defined Team roles and responsibilities. IR specialist skills or Retainer in place

4. Incident Response plan in place with defined roles, responsibilities and skills in place. Occasional dry-runs.

5. Plan in place and well understood with all roles and skills in place. Regular fire-drills and continuous improvement loop.

Organisational Maturity of Incident Response Capability

Poll

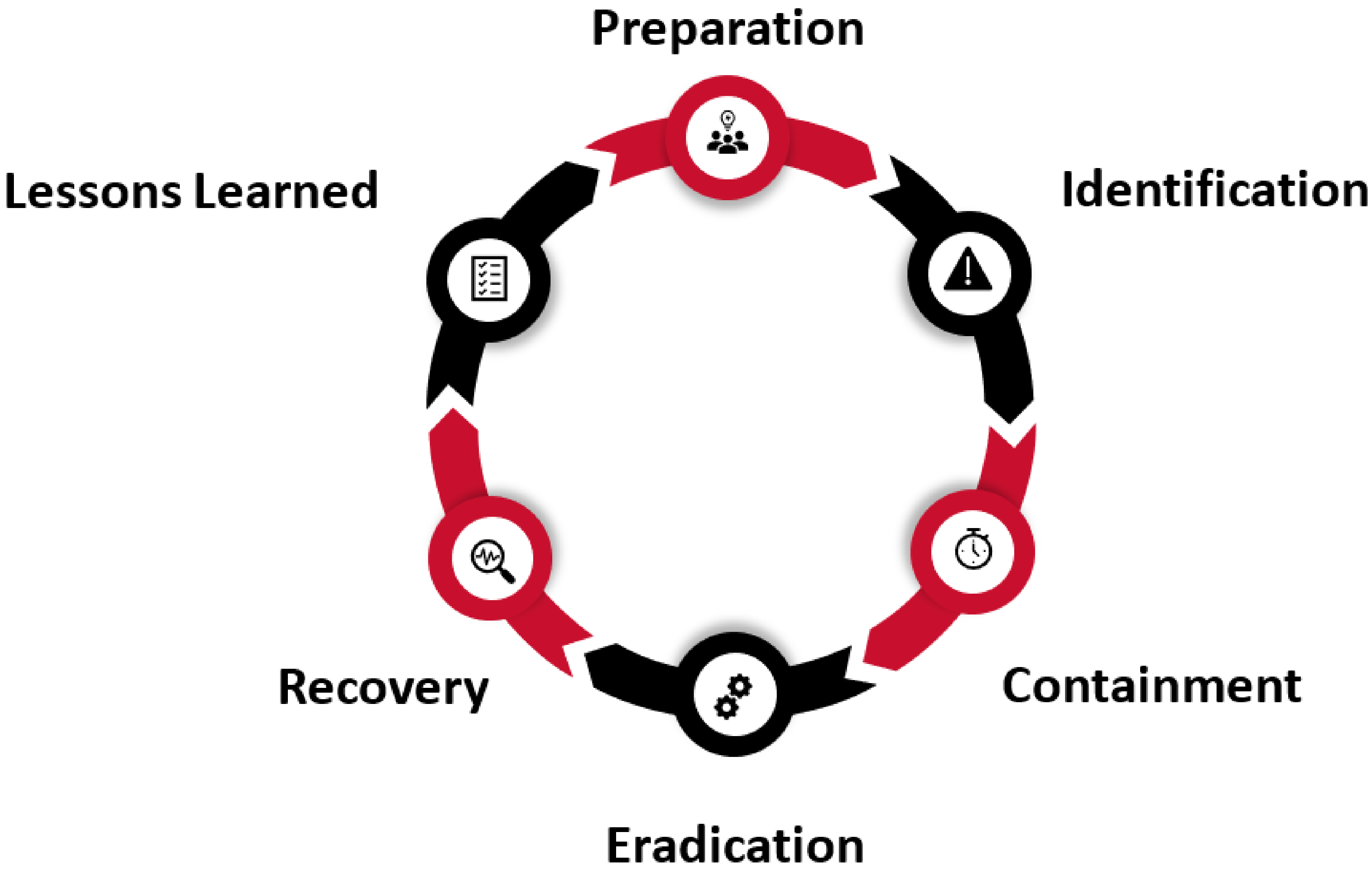
Integrity360
your security in mind

About me

Patrick Wragg

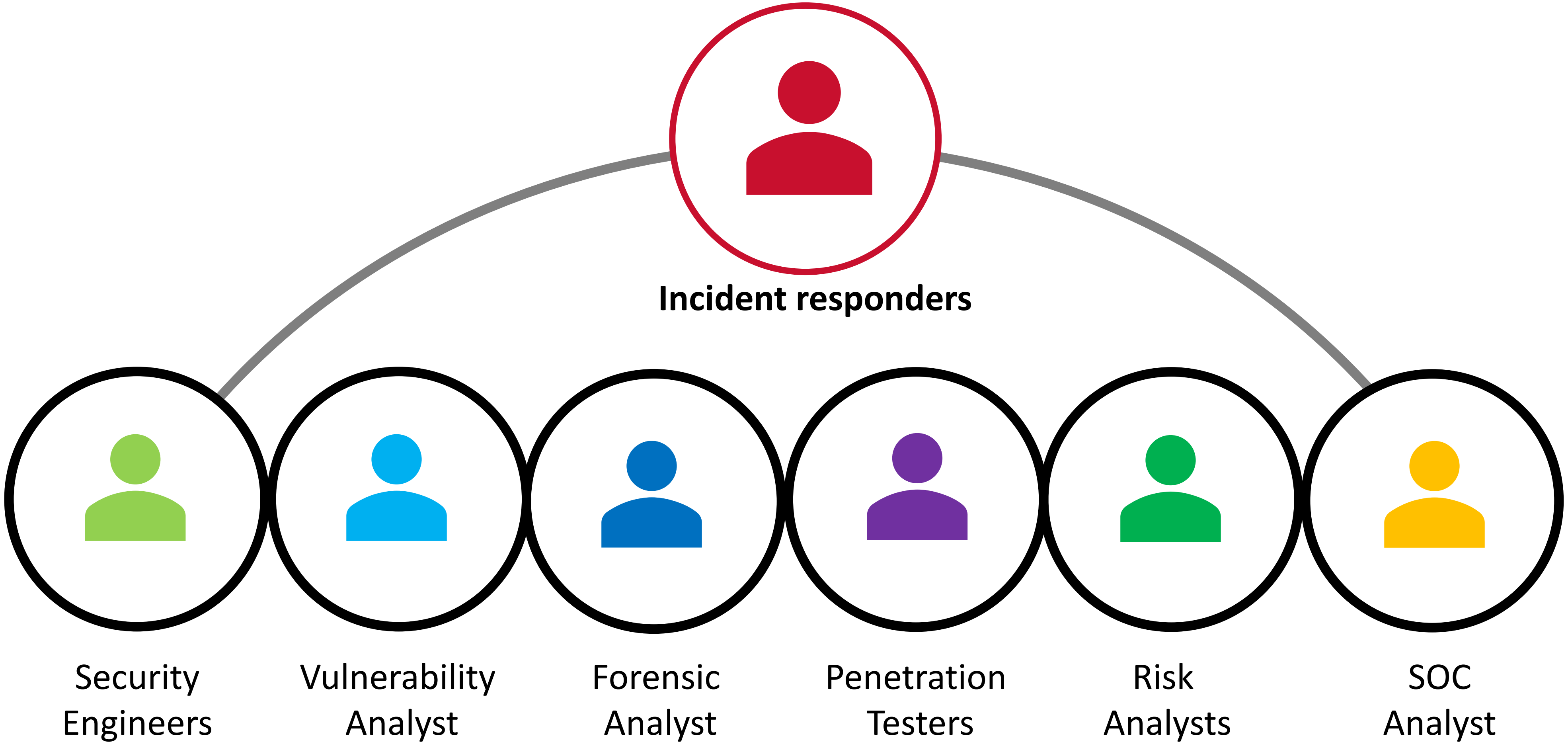
Cyber Incident Response Manager

What is Incident Response?



What is an incident responder?

Integrity360
your **security** in mind



Incident responders

Security Engineers

Vulnerability Analyst

Forensic Analyst

Penetration Testers

Risk Analysts

SOC Analyst

Example Attack Techniques

Integrity360

your **security** in mind

Phishing

Mitigations

1. Awareness training
2. Email security gateway
3. Implement anti-spoofing technology (SPF/Dmarc)

Integrity360
your **security** in mind

Ransomware

Mitigations

1. Backup regularly
2. Have an incident response plan in place
3. Implement "least privilege" access principle and network segmentation

Integrity360
your **security** in mind

Password Spraying

Mitigations

1. Have a strong password complexity requirement
2. Use multi-factor authentication
3. Implement SIEM monitoring use cases

Integrity360
your **security** in mind

Zero Days

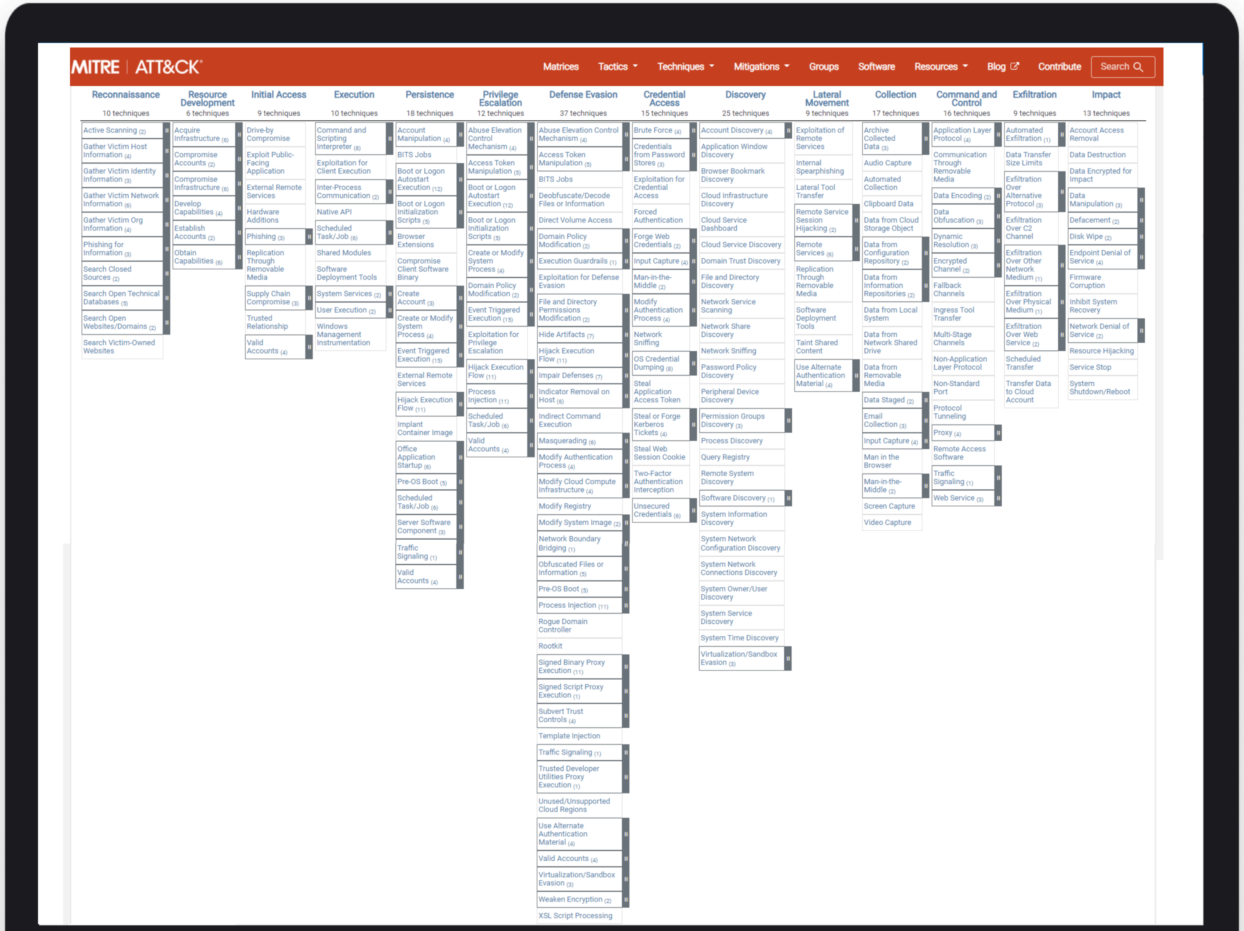
Mitigations

1. Regular vulnerability scanning
2. Patch Management

Aside from regular vulnerability scanning and patch management, there are no known mitigations against 0 days by nature of definition.

MITRE ATT&CK Framework

Integrity360
your security in mind



Reconnaissance
10 techniques

- Active Scanning (2)
- Gather Victim Host Information (4)
- Gather Victim Identity Information (3)
- Gather Victim Network Information (6)
- Gather Victim Org Information (4)
- Phishing for Information (3)
- Search Closed Sources (2)
- Search Open Technical Databases (5)
- Search Open Websites/Domains (2)
- Search Victim-Owned Websites

Resource Development
6 techniques

- Acquire Infrastructure (6)
- Compromise Accounts (2)
- Compromise Infrastructure (6)
- Develop Capabilities (4)
- Establish Accounts (2)
- Obtain Capabilities (6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (3)
- Replication Through Removable Media
- Supply Chain Compromise (3)
- Trusted Relationship
- Valid Accounts (4)

Execution
10 techniques

- Command and Scripting Interpreter (8)
- Exploitation for Client Execution
- Inter-Process Communication (2)
- Native API
- Scheduled Task/Job (6)
- Shared Modules
- Software Deployment Tools
- System Services (2)
- User Execution (2)
- Windows Management Instrumentation

Persistence
18 techniques

- Account Manipulation (4)
- BITS Jobs
- Boot or Logon Autostart Execution (12)
- Boot or Logon Initialization Scripts (5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (3)
- Create or Modify System Process (4)
- Event Triggered Execution (15)
- External Remote Services
- Hijack Execution Flow (11)
- Implant Container Image
- Office Application Startup (6)
- Pre-OS Boot (5)
- Scheduled Task/Job (6)
- Server Software Component (3)
- Traffic Signaling (1)
- Valid Accounts (4)

Privilege Escalation
12 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- Boot or Logon Autostart Execution (12)
- Boot or Logon Initialization Scripts (5)
- Create or Modify System Process (4)
- Domain Policy Modification (2)
- Event Triggered Execution (15)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (11)
- Process Injection (11)
- Scheduled Task/Job (6)
- Valid Accounts (4)

Defense Evasion
37 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (7)
- Hijack Execution Flow (11)
- Impair Defenses (7)
- Indicator Removal on Host (6)
- Indirect Command Execution
- Masquerading (6)
- Modify Authentication Process (4)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry
- Modify System Image (2)
- Network Boundary Bridging (1)
- Obfuscated Files or Information (5)
- Pre-OS Boot (5)
- Process Injection (11)
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution (11)
- Signed Script Proxy Execution (1)
- Subvert Trust Controls (4)
- Template Injection
- Traffic Signaling (1)
- Trusted Developer Utilities Proxy Execution (1)
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material (4)
- Valid Accounts (4)
- Virtualization/Sandbox Evasion (3)
- Weaken Encryption (2)
- XSL Script Processing

Credential Access
15 techniques

- Brute Force (4)
- Credentials from Password Stores (3)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (2)
- Input Capture (4)
- Man-in-the-Middle (2)
- Modify Authentication Process (4)
- Network Sniffing
- OS Credential Dumping (8)
- Steal Application Access Token
- Steal or Forge Kerberos Tickets (4)
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials (6)

Discovery
25 techniques

- Account Discovery (4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (1)
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (3)

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (2)
- Remote Services (6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)

Collection
17 techniques

- Archive Collected Data (3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (2)
- Data from Information Repositories (2)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (2)
- Email Collection (3)
- Input Capture (4)
- Man in the Browser
- Man-in-the-Middle (2)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (4)
- Communication Through Removable Media
- Data Encoding (2)
- Data Obfuscation (3)
- Dynamic Resolution (3)
- Encrypted Channel (2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (4)
- Remote Access Software
- Traffic Signaling (1)
- Web Service (3)

Exfiltration
9 techniques

- Automated Exfiltration (1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (1)
- Exfiltration Over Physical Medium (1)
- Exfiltration Over Web Service (2)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

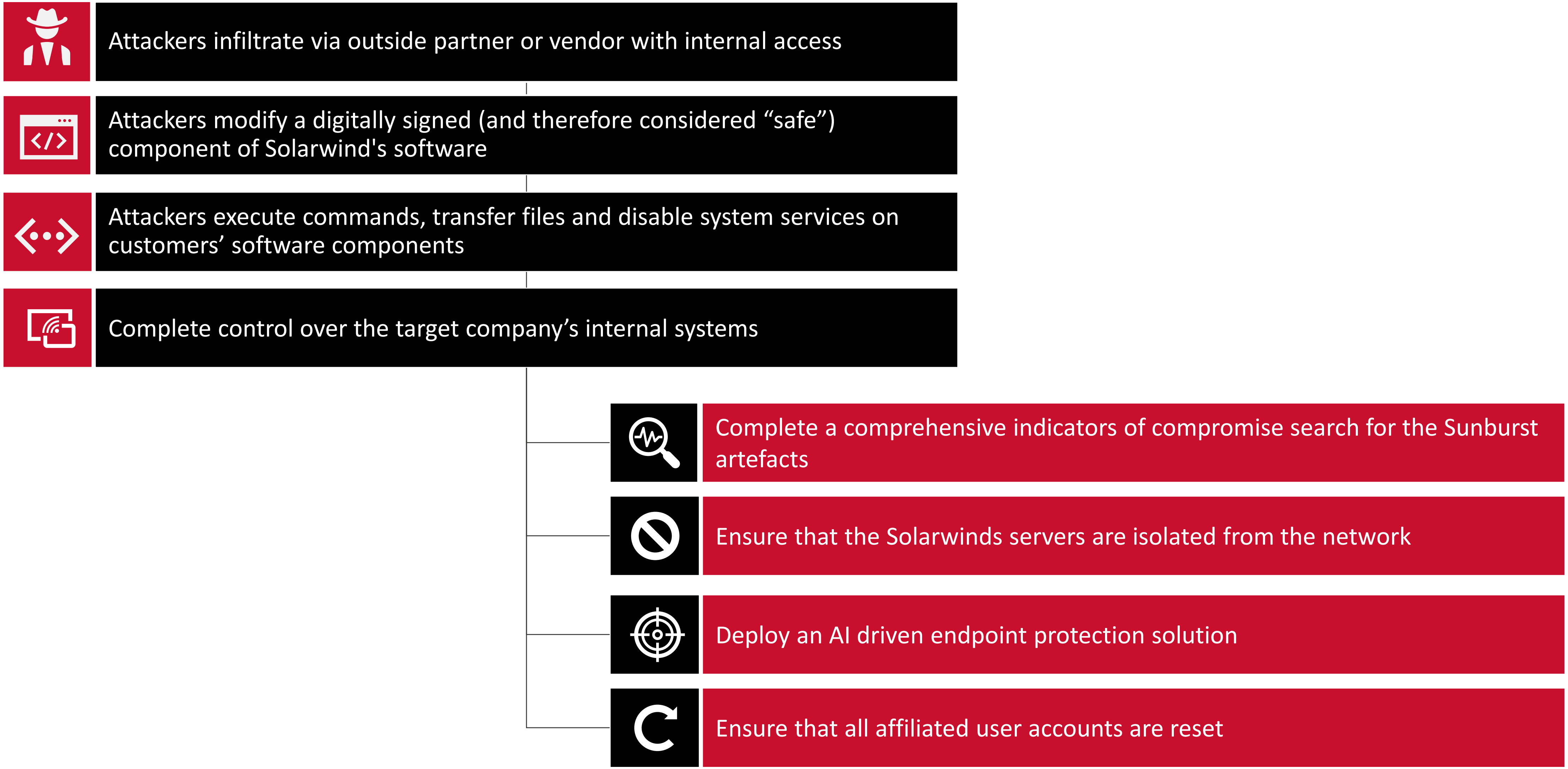
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (3)
- Defacement (2)
- Disk Wipe (2)
- Endpoint Denial of Service (4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Tactics
Techniques
Procedures

ATT&CK®

Recent Attacks

Sunburst – Supply Chain Attack



Attackers infiltrate via outside partner or vendor with internal access

Attackers modify a digitally signed (and therefore considered “safe”) component of Solarwind's software

Attackers execute commands, transfer files and disable system services on customers’ software components

Complete control over the target company’s internal systems

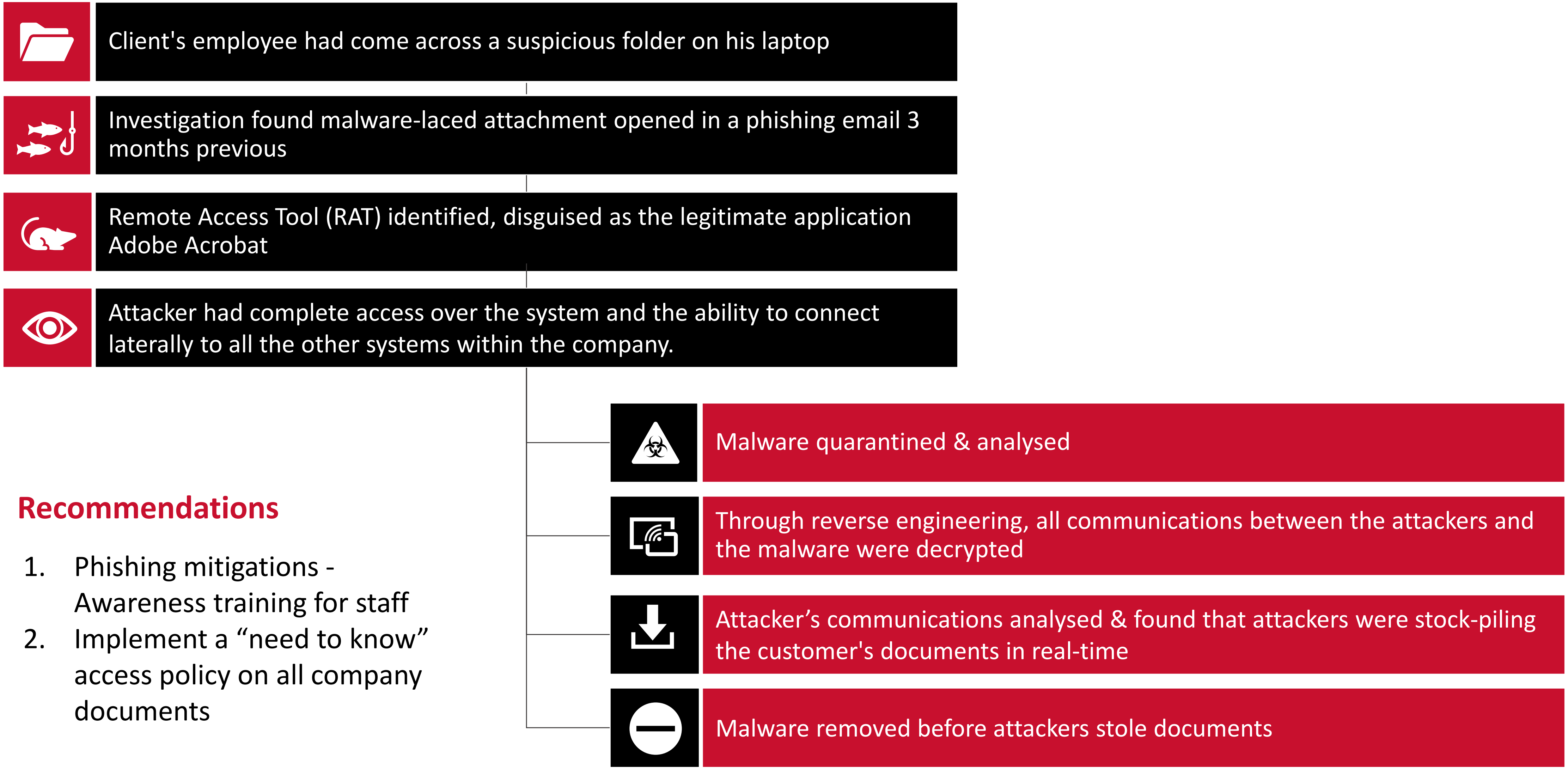
Complete a comprehensive indicators of compromise search for the Sunburst artefacts

Ensure that the Solarwinds servers are isolated from the network

Deploy an AI driven endpoint protection solution

Ensure that all affiliated user accounts are reset

Adobe Acro-RAT



Client's employee had come across a suspicious folder on his laptop

Investigation found malware-laced attachment opened in a phishing email 3 months previous

Remote Access Tool (RAT) identified, disguised as the legitimate application Adobe Acrobat

Attacker had complete access over the system and the ability to connect laterally to all the other systems within the company.

Malware quarantined & analysed

Through reverse engineering, all communications between the attackers and the malware were decrypted

Attacker’s communications analysed & found that attackers were stock-piling the customer's documents in real-time

Malware removed before attackers stole documents

Recommendations

1. Phishing mitigations - Awareness training for staff
2. Implement a “need to know” access policy on all company documents

Assessing your need for IR

Integrity360

your **security** in mind

Key IR requirements

24/7 availability

Do you have a dedicated incident response team ready at very short notice?

Skills and experience

Do your team members have the necessary technical knowledge and accreditations to perform investigations?

Sufficient Security Tooling

Does your business have access to industry leading cyber security tools?

Key IR requirements

Reporting capabilities

Does your internal team have the time and resources to effectively conclude all evidence and findings in a report?

Regulatory compliance

What stakeholders/ regulatory practices are to be informed when a breach takes place?

Access to latest tailored threat intelligence

Does your business have access to the latest threat intelligence?

Efficient/automated IR process

Does your incident response process address every stage of an investigations in great detail?

Poll

Integrity360
your security in mind

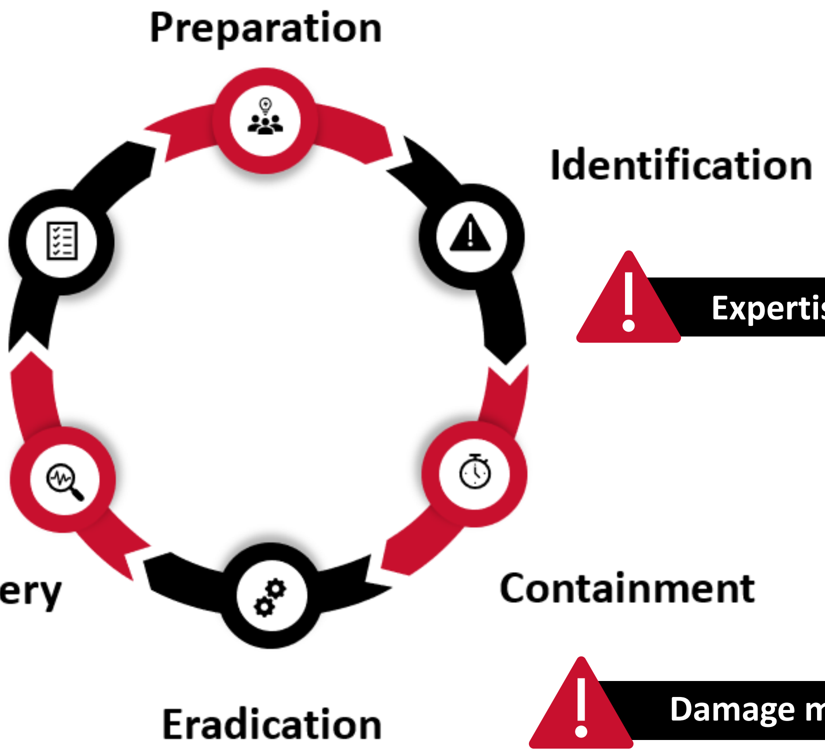
The Pitfalls of managing IR

Integrity360
your security in mind

Incident Response Pitfalls

Integrity360
your **security** in mind

⚠ Fully documented incident response playbook



⚠ Learn from history

⚠ Expertise in analysing security logs

⚠ Fully documented process to get back to full working capacity

⚠ Damage mitigation

⚠ Eliminating the root cause of the breach

Key Takeaways

Integrity360
your security in mind

1 Create an Incident Response Plan

2 Produce Threat-Specific Incident Response Playbooks

3 Create a Communication Plan

4 Outsource to a MSP If You Don’t Have the Necessary Expertise

5 Keep Your Incident Response Process **Simple**

Incident Response Services

Integrity360
your security in mind

	Reactive	Proactive
Description	“Break-glass” services to assist customers and clients in the event of their experiencing cyber incidents and security breaches	Annual Incident Response Retainer so you can prepare for the eventuality in advance
Response Time 24x7	Best Efforts	4 hours
Prepaid hours	None	40/80/120
Minimum hours per invoked incident	40	16
Procurement & Legal documentation completion	Completed at start of engagement	Completed in advance
Incident Response Preparedness Assessment	No	Included
Proactive cyber security incident response preparedness services*	Not applicable	Yes
Unused hours apply to other services**	Not applicable	Yes

*Proactive hours

*Proactive services include:

- IR process development
- Table-top exercises
- IR awareness training
- Security testing

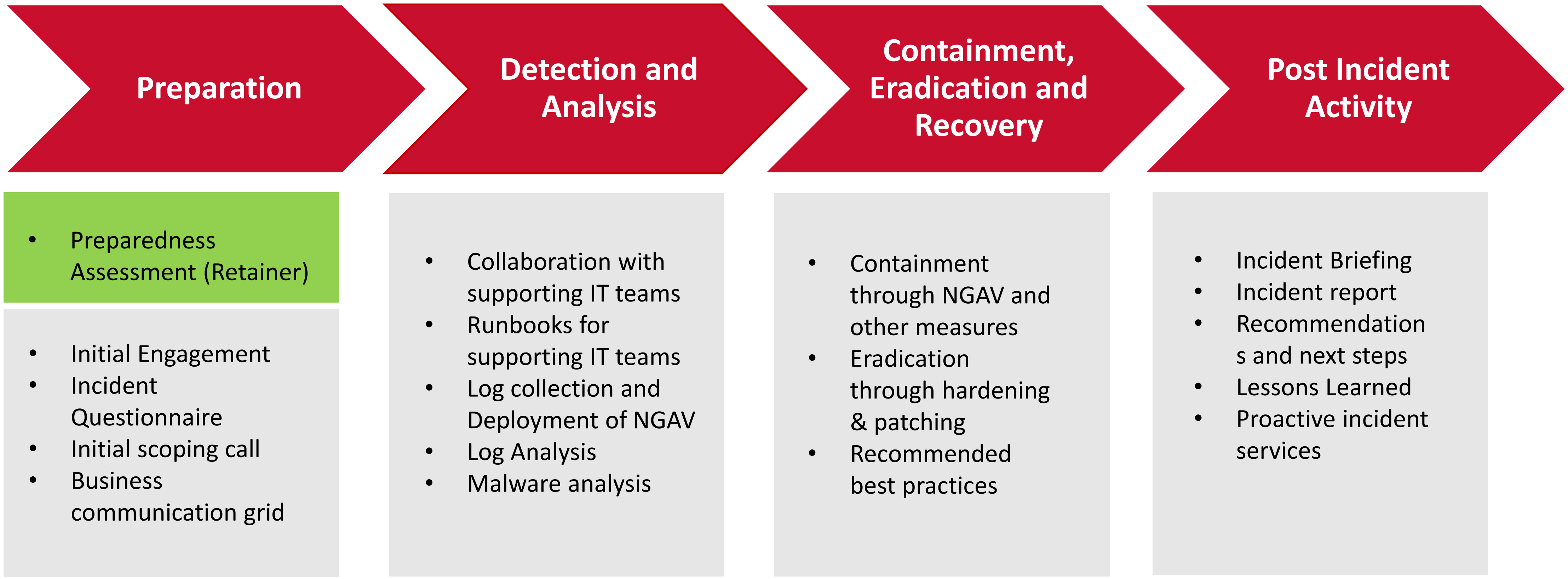
**Unused hours

Unused hours can be used for:

- IR Table-Top exercises
- Vulnerability Assessment
- Penetration testing
- Red-team exercise
- Compromise Assessment
- Incident Response (IR) Preparedness
- IR Technology Assessment
- IR Capability Development
- IR Awareness training

Incident Response Engagement

Integrity360
your security in mind



Preparation

- Preparedness Assessment (Retainer)

- Initial Engagement
- Incident Questionnaire
- Initial scoping call
- Business communication grid

Detection and Analysis

- Collaboration with supporting IT teams
- Runbooks for supporting IT teams
- Log collection and Deployment of NGAV
- Log Analysis
- Malware analysis

Containment, Eradication and Recovery

- Containment through NGAV and other measures
- Eradication through hardening & patching
- Recommended best practices

Post Incident Activity

- Incident Briefing
- Incident report
- Recommendations and next steps
- Lessons Learned
- Proactive incident services

Upcoming Webinar & available resources

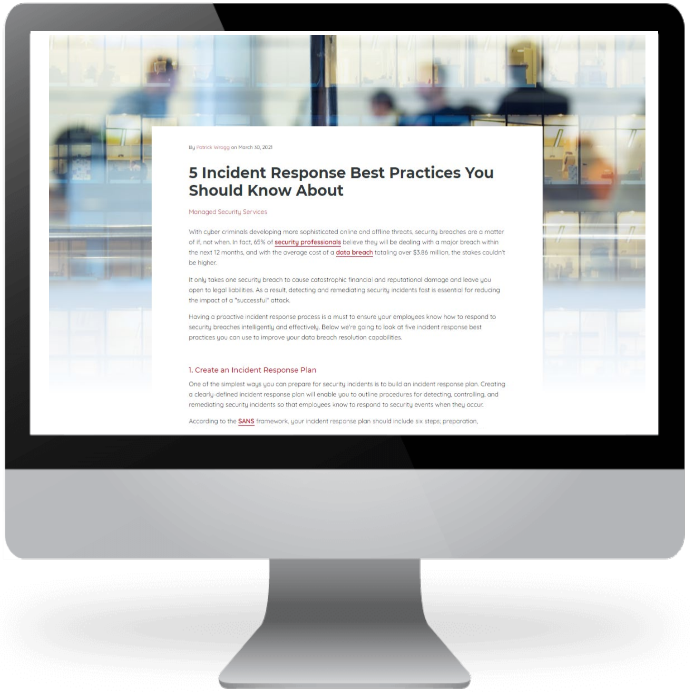
Incident Response Management – Preparing for the inevitable - 19th of May 2021 @ 11am

Topics discussed during the session will include:

- Important factors to consider before a breach
- IR industry best practices
- How to develop an effective IR plan
- Questions you need to ask your IR provider

Eric Barnes
Cyber Services Architect

Register Now



By Patrick Wragg on March 30, 2021

5 Incident Response Best Practices You Should Know About

Managed Security Services

With cyber criminals developing more sophisticated online and offline threats, security breaches are a matter of if, not when. In fact, 65% of security professionals believe they will be dealing with a major breach within the next 12 months, and with the average cost of a data breach totaling over $3.86 million, the stakes couldn't be higher.

It only takes one security breach to cause catastrophic financial and reputational damage and leave you open to legal liabilities. As a result, detecting and remediating security incidents fast is essential for reducing the impact of a "successful" attack.

Having a proactive incident response process is a must to ensure your employees know how to respond to security breaches intelligently and effectively. Below we're going to look at five incident response best practices you can use to improve your data breach resolution capabilities.

1. Create an Incident Response Plan

One of the simplest ways you can prepare for security incidents is to build an incident response plan. Creating a clearly-defined incident response plan will enable you to outline procedures for detecting, controlling, and remediating security incidents so that employees know to respond to security events when they occur.

According to the SANS framework, your incident response plan should include six steps; preparation,

Integrity360
your security in mind

Case Study

Service: Incident Response
Practice: Managed Security
Client: Wholesaler client

OVERVIEW

Our client was concerned when it became apparent that an invoice generated by its accou department was used to extract money from o of its customers. Our client assumed that they had a breach and called us to investigate. the breach occurred internally or externally.

Because of the lack of log data maintained by t client it was difficult to determine who had acc to the invoice in question. Additionally, due to t lack of procedures that existed in the company was impossible to tell whether the breach occu internally or externally.

CHALLENGE

Our client's accounts department routinely generates invoices and sends them out to its customers via post, fax or email.

On one occasion, what appeared to be an offici notice, went to one of its customers advising th that the company's bank details had changed and that they should make payments to a new fraudulent bank account instead.

Integrity360
your security in mind

Case Study

Service: Incident Response
Practice: Managed Security
Client: E-commerce Retailer

OVERVIEW

The client proactively reviewed their network after hearing that its main competitor had been compromised in a cyber attack. They found that they too had been compromised.

Integrity360's Incident Response team was called to site and isolated the system, analysed the logs, found the root cause and removed the threat.

A series of lessons learned exercises followed to ensure that the same attack will not happen to the client again.

CHALLENGE

As a solely online transaction based company the client depended on 100% availability of its website to generate revenue. After a competitor announced that their online servers had been compromised and that credit card details were stolen without their knowledge our client wanted to ensure that the power to ensure would not happe

HOW TH WAS AD

The client first ev became apparent leaving the organ to Integrity360.

The next step wa still taking place. were called to sit door was found i From firewall and identify custome

The server was in that no other info images of the ma for root cause. Fo understanding of

Integrity360
your security in mind

Case Study

Service: Incident Response
Practice: Managed Security
Client: Non-profit client

CHALLENGE

Integrity received a call from the CEO of a charity who had fallen victim of a cyber attack. The organisation had money transferred from their bank account and needed assistance in understanding what had happened and how it could be remediated.

The organisation's technology was managed by an IT specialist who was only available once a week. In their absence, Integrity360 spent two days investigating and remediating their incident, working closely with both the the organisation itself and the authorities.

HOW THE CHALLENGE WAS ADDRESSED

It became evident that the orgnisation had fallen victim to a phishing attack several months prior to the money transfer.

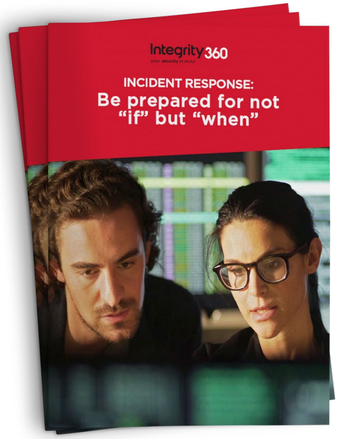
Once access had been gained by phishing, the threat actor was logging in daily to their systems to monitor user activity.

Subsequent phishing was then carried out on a senior manager and at the opportune time, the threat actor sent an email from the Head of Finance to a financial controller with a request to transfer a significantly large sum of money to a bank account overseas. The financial controllor believed the request came from the head of finance and actioned the request.

Integrity360 took back control of the compromised accounts and worked with the orgnisation to do a full review of their security posture to ensure that all evidence of compromise was remediated and their network was adequately secured.

The incident response team also worked closely with the authorities and the organisation to ensure that the financial implications were minimused and the transfers reversed.

The organisation was supported at the end of the engagement with a next steps action plan on how they could further futureproof their security to avoid any similar incidents.



Integrity360

INCIDENT RESPONSE:
Be prepared for not "if" but "when"

Q&A

Patrick Wragg

Cyber Incident Response Manager

Mark Wiley

Senior Account Manager

Thank you

Integrity360

your **security** in mind