RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: AIR-W04

Incident Responder Field Guide: Lessons from a Fortune 100 Incident Responder

Tim Bandos

Director of Cybersecurity

Digital Guardian

@midnit3sec

#RSAC

Agenda

- Introductions
- Purpose
- Response Plans
- Framework
- IR Lifecycle
- Cyber Threat Hunting

Purpose

A Cyber Security Incident Response Plan provides a formal, coordinated approach to responding to cyber security incidents affecting information assets.

Defines:

- Incident classification
- Roles and responsibilities
- Incident reporting and escalation
- Communication channels for information flow
- Outlines the overall incident response processes

Who's on the IR Team?

Technical

Incident Response Manager
Security Analysts
Threat Researchers

Non-Technical

CSO
CISO
CIO

HR
Compliance
Public Affairs
Legal

Communication within and between two groups critical

What Not to Do & Do

Not To Do	To Do
Panic	Collect volatile data and other critical artifacts
Discuss the incident with others unless directed	Gather any external intelligence based on known indicators of compromise
Use domain administrative credentials to access systems	Safeguard systems and/or media for forensic collection
Shutdown affected systems	Collect any network-based logs
Execute any non-forensic type software on system	

Incident Categories, Types, & Severities

Category

- Unauthorized Access
- Malware
- Denial of Service
- Improper Usage
- Unsuccessful Attempt
- Physical Asset Loss
- Explained Anomaly

Type

- Advanced Persistent Threat
- Hacktivism Threat
- Insider Threat
- Opportunistic Threat
- Nuisance Threat
- Unattributed Threat

Severity

- Critical Impact
- High Impact
- Moderate Impact
- Low Impact

Classification of Incidents enables the prioritization of incident management while enabling meaningful metrics

Incident Taxonomy

Detection Method	Vector	Impact	Intent
▪ End User Report ▪ 3rd Party Service Provider ▪ Law Enforcement ▪ Data Leak Prevention ▪ Intrusion Prevention System ▪ Intrusion Detection System ▪ Firewall ▪ Anti-Virus ▪ Proxy ▪ Netflow	▪ Email ▪ End User Action ▪ Vulnerability Exploited ▪ Web / Drive-by ▪ USB / External Drive ▪ Brute Force ▪ Loss of Asset ▪ Unauthorized Software ▪ Weak Password	▪ Employee Dismissal ▪ HR / Ethics Violation ▪ Loss of Productivity ▪ Unauthorized Privileges ▪ Website Defacement ▪ Brand Image ▪ Lawsuit ▪ Denial of Service ▪ Compromise of IP ▪ Malicious Code Execution ▪ Privacy	▪ Non-Malicious ▪ Malicious ▪ Theft ▪ Accidental ▪ Physical Damage ▪ Fraud ▪ Defamation ▪ Espionage

An Incident Taxonomy will provide readily obtainable answers to key questions involving root cause, trends, and intelligence.

Incident Taxonomy continued…

Data Exposed	Mitigation	Root Cause
▪ Public ▪ Confidential ▪ Export Control ▪ Financial Reporting ▪ Unknown ▪ PII ▪ PCI	▪ OS Patching ▪ Application Patching ▪ User Awareness & Training ▪ Compliance to Internal Standards ▪ Host Hardening ▪ Least Privilege ▪ Technology Rule Configurations	▪ Unauthorized Action ▪ Vulnerability Management ▪ Theft ▪ Security Control Failure/Gap ▪ Disregard of Policy ▪ Non-Compliance to Standards ▪ Service Provider Negligence ▪ User Negligence

Incident Communications

Telecommunication Bridges

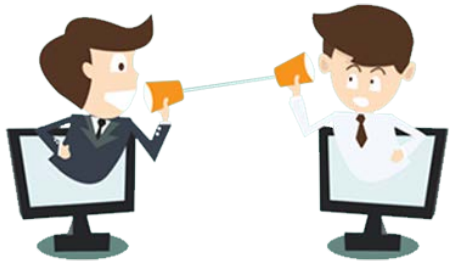
- Use pre-shared access codes for authenticating users
- Avoid using speakerphones in non-closed conference rooms or offices

Email

- Encrypted email messages when discussing IR details
- Recommend using signed and encrypted ECA PKI certificates

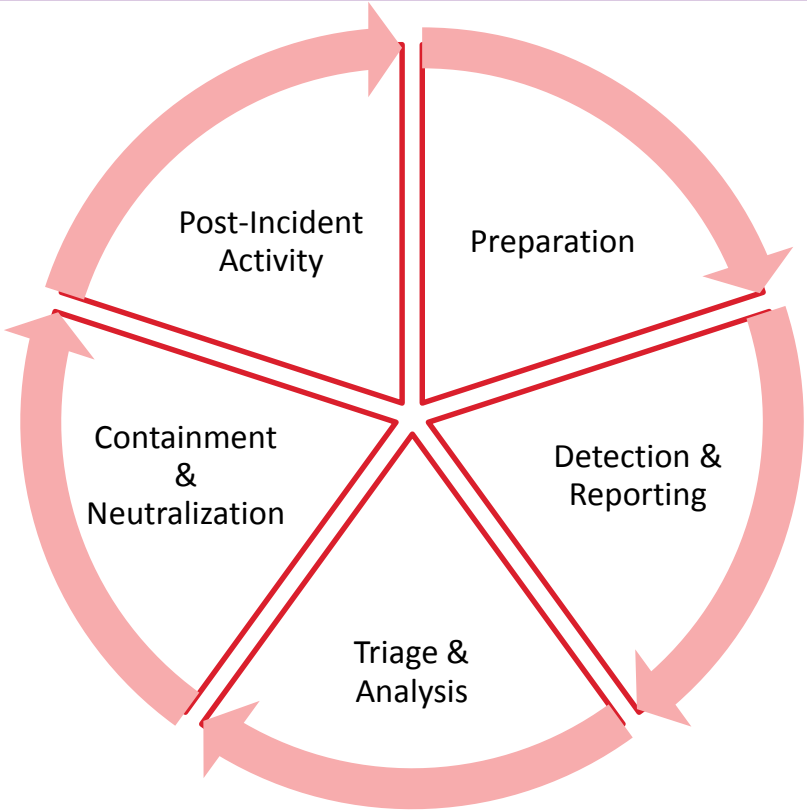
Instant Message

- Unencrypted IM messaging should be avoided at all costs

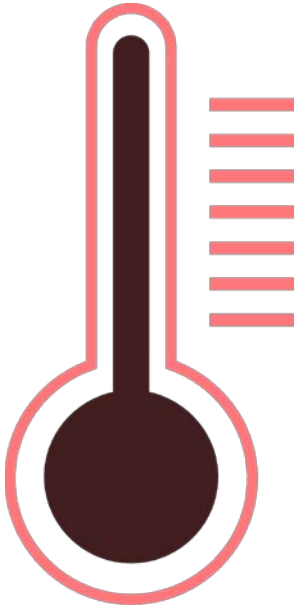


Only member's on the Incident Response team with a **need-to-know** should be included in communications regarding details.

5 Incident Response Phases



CRISIS



Preparation

Establishing policies, procedures, and agreements covering the management and response to security incidents BEFORE you need them.

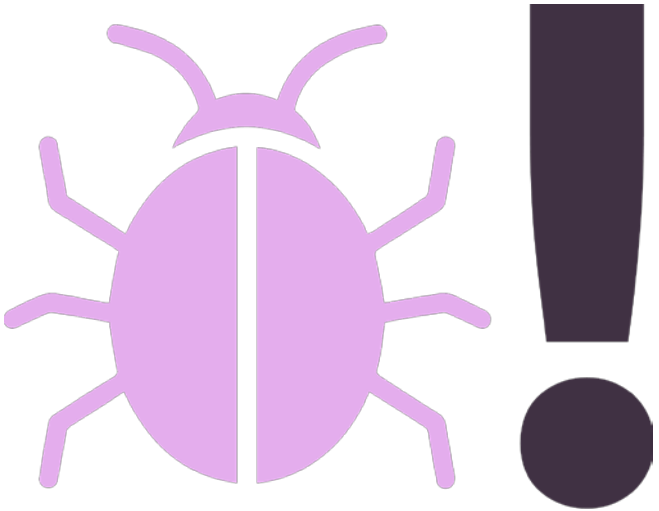
- Ongoing collection, analysis, and fusion of Threat Intelligence
- Cyber Threat Hunting Operations
- Threat Detection Capability Development
- Conduct Operational Cyber Exercises
- Ensure Vulnerability Management & Configuration Management are informed
- Documented Procedures for Incident Handling

Detection & Reporting

Monitoring and correlation of security events to detect, alert, and report on potential security incidents.

Events generated from:

- Intrusion Prevention / Detection Systems
- Anti-Virus Logs
- Firewall Logs
- Data Leak Prevention Logs
- Vulnerability Management Systems
- Netflow Logs



Triage & Analysis

Examination of event/log data to confirm whether the detected activity is indeed a security incident.

Endpoint Analysis

- Forensic Acquisition & Analysis
- Memory Analysis
- Timeline/Artifacts

Binary Analysis

- Static/Dynamic Analysis
- Reverse Engineering

Enterprise Hunting

- Apply IOC's across Enterprise
- Leverage SIEM for Traces

Containment & Neutralization

Strategy development based upon all the intelligence gathered throughout the Triage & Analysis phase. Coordination and notification of all involved or affected entities with details on how to effectively neutralize the threat.

Items to Consider:

- System Backup – Note: May introduce risk from infection
- Risk to continued Operations
- Changing Passwords /ACL's on compromised systems
- Development of new detection capabilities for Post-Incident Monitoring
- Process for wiping systems and Rebuilding OS
- Issuing Threat Mitigation Requests

Post-Incident Activity

Documentation and dissemination of an incident report, identifying lessons learned including successful and unsuccessful actions taken in response.

Items to Consider:

- Development of new security initiatives to prevent future incidents.
- Updating Threat Detection Watchlists / Feeds
- Closely Monitor Activity Post Incident
- Coordination among organization to implement any process improvement activities

Cyber Hunting Safety: Cyber-Threat Tracking and Hunting

Agenda

- Groundwork
- Building Blocks
- Supplies, Preparation, Ammunition, Armory
- The Prey, Bird Dogs
- Stories from the Field
- Facing your Adversary
- Questions

Groundwork

- Incident Response
  - Formalized Plan
  - Well Defined
  - Business Wide Initiative
- Threat Hunting
  - Mission
  - Fewer Boundaries
  - InfoSec Centric

Building Blocks to Threat Hunting

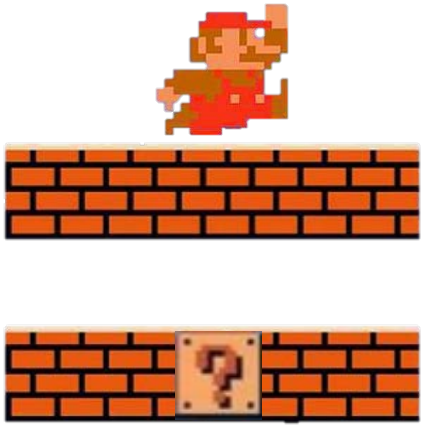
Build Architecture

Implement Passive Defense

Develop Active Defense Program

Drive Intelligence

The Equation



Intent

Capability

Opportunity

Supplies and Preparation

- What are the tools
  - Bare minimum
  - Nice to haves
  - Luxury goods

Logs, Logs, Logs

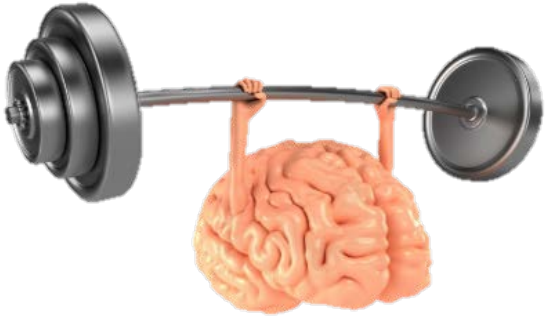
SIEM

Machine Learning

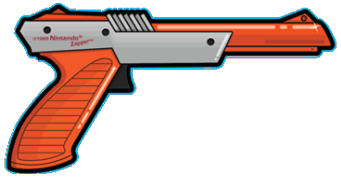
Log Consumer

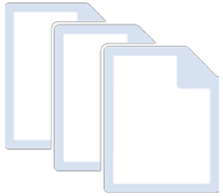
Data Analytics

- Skills you should have
  - Innovative Analysts
  - Active Defense & Intelligence
  - Familiarity with Enterprise
  - Ability to Hypothesize
  - Statistics



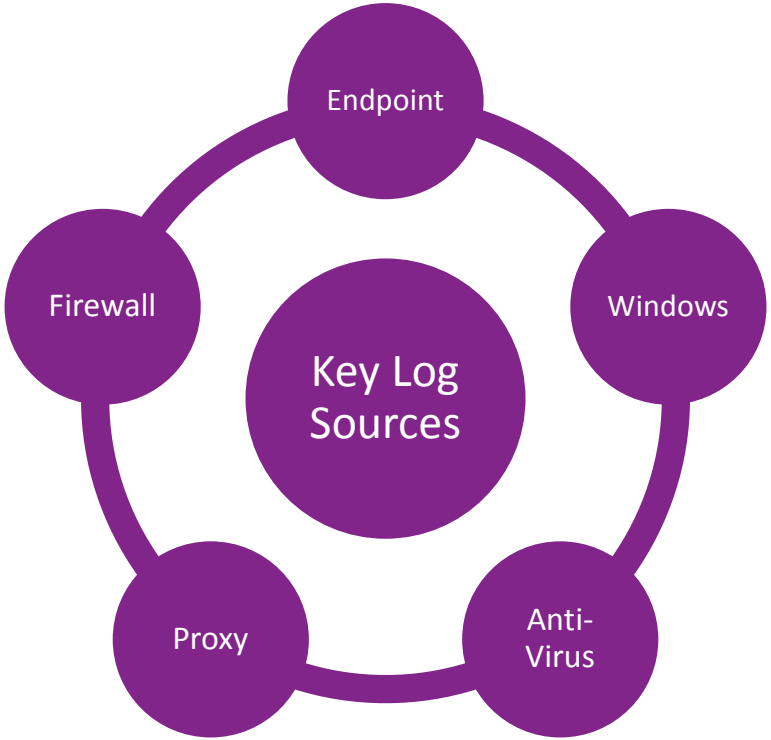
Ammunition





Hunters require data; providing the ability to pivot from individual pieces of information into links and correlations to reveal the threat.

- **Logs**
- **Alerts**
- **Netflow**
- **Forensic Images**
- **Memory Captures**



Armory

Tools

- **SIEM:** ELK Stack (Elastic Search, Logstash, Kibana)
- **Log Forwarder:** NxLog
- **Log Parser:** Log Parser 2.2 Microsoft
- **Log Capture:** Digital Guardian, duhh (or Sysmon)
- **Host Forensics:** Encase / Sleuth Kit / FTK Imager
- **Memory Forensics:** Volatility / Mandiant's Redline
- **Timeline:** Log2timeline
- **Registry:** RegRipper

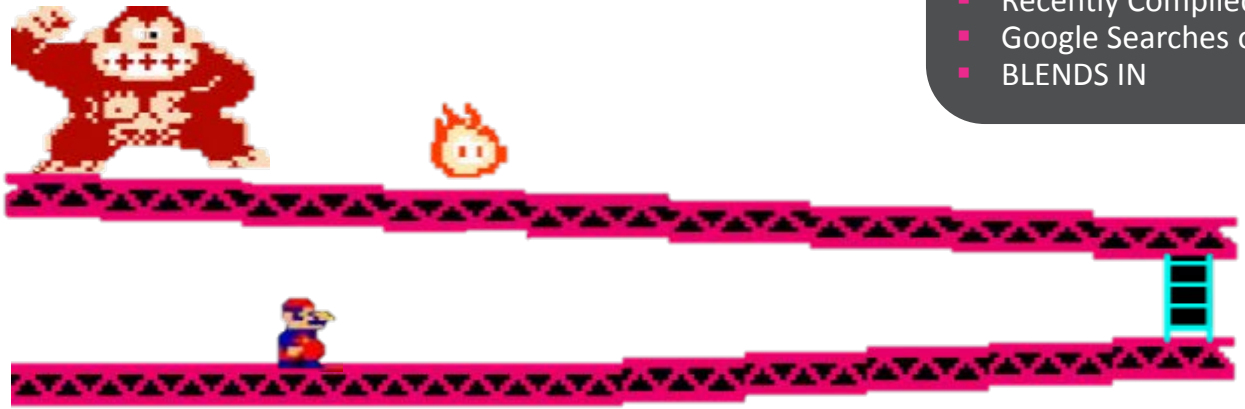
The Prey

Known

- Matches an Indicator / Signature
- Antivirus is Aware / Submitted to Virus Total
- Your Level 1 Analyst Detects Them
- FireEye has a Blogpost About Them
- Easy to Detect & Out in the Open

Unknown

- Leverages New Techniques for Persistence / C2
- Works through encrypted channels
- Authorized Use Activity
- Maintains inside a Baseline
- Recently Created Command & Control
- Recently Compiled Toolsets
- Google Searches on MD5's = Nothing
- BLENDS IN



Bird Dog

- Bird Dog – dogs trained to retrieve birds

Strategic Goal

- Hunting processes have been operationalized
- Continual improvement of existing processes
- Development of new hunting tactics
- Actively seeking out adversaries on a daily basis

Hunting Examples

Proxy Logs

- Traffic being sent out port 22
- Network connections with same pattern of bytes in and bytes out
- Dynamic DNS visits
- Unique User Agent Strings
- Base64 Encoded Strings in URLs
- Executables being Downloaded

Windows Logs

- Explicit Logon Attempts (4648 / 552)
- Users added to Privileged Group (4728, 4732, 4756)
- Failed Logon Attempts via Multiple Accounts
- Log Clearing Activity (104, 1102)
- EMET Crash Logs (1, 2)
- Application Crashes & Hangs (1000, 1002)
- Windows Defender Errors

Hunting Examples

Anti-Virus

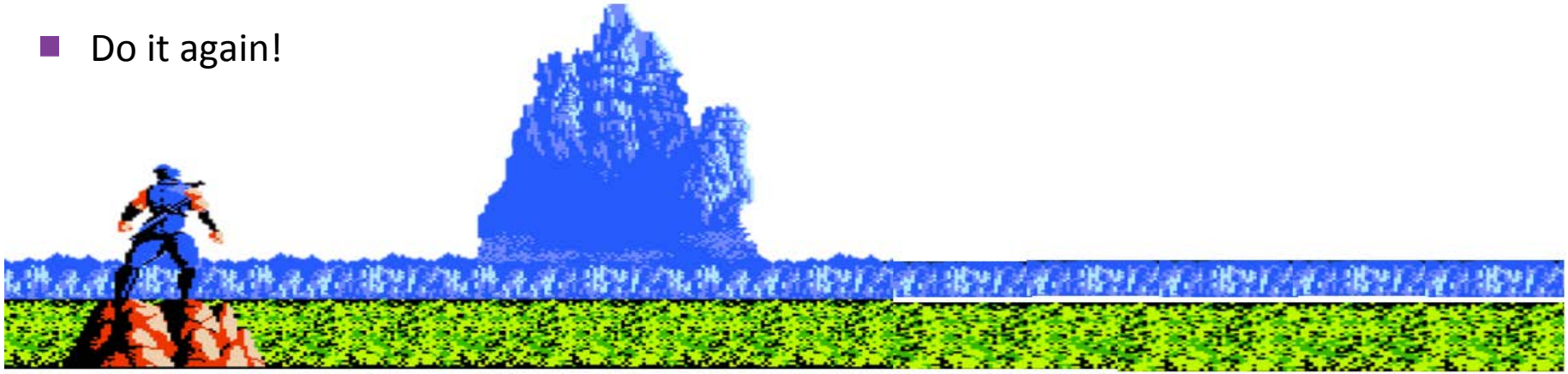
- Password Dumping Programs
- Specific Backdoors Detected (PlugX, 9002, Derusbi, Nettraveler, Winnti, Pirpi)
- Detections with Dropper in the name
- Custom Detection Creation

Digital Guardian

- Execution from temp with no Company Name or Version information
- Svchost launching without Services being its parent
- Process launches from odd directories (%windows\fonts, %windows\help, %windows\wbem\, %windows\addins, %windows\debut, %windows\system32\tasks)
- Rar being executed to compress files
- Rare process execution events
- Execution of PowerShell with suspicious commands
- Scheduled AT jobs with suspicious commands

You Found Something; Now What

- Gather Information & Engage Forensic Ninjas
- Research Intelligence via OSINT sources
- Execute IR Plan
- Neutralize Bad Guy
- Do it again!



Facing Your Adversary

- Learn from their Behaviors
- Document their Tactics, Techniques, Procedures
- Organize & Manage Threat Indicators Associated to their Activity
- Develop a Profile:
  - Region of Operation
  - Motive
  - Intent
  - Capability
- Disrupt their Operations

- Offensively Hack Back
- Immediately shut down systems
- Block an Indicator without knowing full scope
- Call Ghostbusters for IR services

Apply What You've Learned Today

- Next week you should
  - Define your Incident Response plan
  - Receive support from the executive team and business leaders
- In the next three months you should have
  - An established IR team in place
  - Actively engaging in the five phases of IR
- In the next six months you should be actively hunting threats while identifying active attacks and responding accordingly