What to Expect When You're Not Expecting
The Reality of Incident Response

Lou Smith
Cyber Incident Response Team (CIRT) Operational Team Lead

May 08, 2026

Discussion Goals

- Whoami
- Defining Incident Response (IR)
- IR Steps
- IR Plans
- Evidence Preservation & Collection
- Tooling
- Full Disk Analysis v. Rapid Triage
- Open-source Intelligence (OSINT)
- External Assistance

“All we seek is one goal, one goal / All we need is one goal”

• Eifel 65, *One Goal* (2001)

Whoami

- **Center for Internet Security (CIS) CIRT**
  - Since 2018
- **Background**
  - Communications, marketing, and journalism
- **Degrees**
  - A.A. in Humanities
  - B.S. in Digital Forensics
- **Certifications**
  - GSEC / GPEN / GCFE / GBFA
- **Motivators**
  - Art (music, literature, and film)
  - Travel (culture, cuisine, and characters)
  - Greater Good (SLTT v. Corporate)

"But who am I to say, what a girl is to do / God, I need some answers"

• Britney Spears, *Overprotected* (2001)

Defining Incident Response (IR)

- **Definition**
  - "…the steps used to prepare for, detect, contain, and recover from a [data] breach"
- **IR v. Threat Hunting**
  - Confirmed cyber incident v. review of systems that aren't showing signs of being impacted

- **Goals**
  - Have plans in place to cut down on response time
  - Identify "patient zero"
  - Contain impacted device(s)
  - Assess damage/downtime
  - Identify Indicators of Compromise (IOCs)

"You know us we the usual suspects / The real definition of success"

• Nas, *The Usual Suspects* (2009)

IR Steps

- **Preparation**
  - Risk assessments, identify mission-critical assets, define incidents by severity, etc.
- **Identification**
  - Collect evidence, establish type and severity, document, etc.
- **Containment**
  - Isolate the impacted network segment or device
- **Eradication**
  - Remove malware from impacted systems, identify root cause, etc.
- **Recovery**
  - Bring impacted production systems back online
- **Lessons Learned**
  - Prepare complete documentation of the incident, investigate further

"Baby step back, baby step back / Either step up or step back"

• Gordon Lightfoot, *Baby Step Back* (1982)

IR Plans

- **Remember**
  - IR Plans need to be as comprehensive *and* practical
  - Based on the nature of the incident not all steps might be necessary
- **Testing**
  - Walk through your IR Plan
  - Consider incorporating the CIS CIRT into your IR Plans and/or to review your current plan

- **Tips**
  - Work to identify who is involved (Cyber Insurance, SMEs, Third-Party Vendors, etc.) and then develop a contact list
  - Delegate responsibilities
  - Don't be afraid to revisit the IR Plan

"Baby, I got a plan / Run away as fast as you can"

• Kanye West, *Runaway* (2010)

Evidence Preservation & Collection

Overview

- **Visibility**
  - Have information on-hand
  - Backups, rollover, etc.
- **Target**
  - Based on the nature of the case, what evidence should you collect
  - Have external drives available
  - Isolate v. shutdown
- **Etc.**
  - Network Diagram
  - SMEs or Vendors
  - Contact Information
  - Scope Creep
  - Communication & Delegation

"Well, nobody knew where to find him / No evidence was found"

• Phil Collins, *Don't Lose My Number* (1985)

Evidence Preservation & Collection 2

Windows Event Logs

- **The Big Three**
  - Application
  - Security
  - System
- **Log Retention / Rollover**
  - Varies based on the log source and what is being recorded
  - Can be manually cleared
- **Remember**
  - 200+ more “custom” Windows Event logs
  - Windows logs *everything*
  - Visibility and accessibility are key
  - Tooling options

“I’m the main event / Still grindin’ in the streets like I ain’t made a cent”

• Chamillionaire, *The Main Event* (2017)

Evidence Preservation & Collection 3

Windows Master File Table (MFT)

- **Function**
  - Records when files are written to the disk, which include initially created, updated, etc.
- **Usefulness**
  - Chronological order of files written following an incident, can help with scoping of infection, etc.

- **Remember**
  - If a file is deleted, review of the USN Journal (“$J”) will assist in providing additional evidence
  - “Timestomping” has been a known method employed by TAs and can be identified through the MFT

“She ran underneath the table / You could see she was unable”

• Michael Jackson, *Smooth Criminal* (1987)

Evidence Preservation & Collection 4

Additional Evidence Sources

- **Firewall Logs**
  - Retention
  - Parsing
- **Web Server Logs**
  - IIS / WC3
  - Scoping
- **Microsoft O365**
  - UAL

- **Remember**
  - Just because you can export everything doesn't mean you should
  - Scoping & Queries
  - Licensing
  - Vendor Support

"Truth or consequence, say it aloud / Use that evidence, race it around"

• Foo Fighters, *My Hero* (1997)

Tooling

- **Triage Tools**
  - Kroll's KAPE
  - BasisTech's Cyber Triage
- **Scripts**
  - Volatility Framework
  - ESENTUTL
- **Forensic Suites**
  - Exterro's Forensic Toolkit (FTK)
  - Magnet AXIOM
- **Imaging**
  - Exterro's FTK Imager
  - Arsenal Image Mounter

"As of now, I am a tool / Of severe impact"

• Fear Factory, *Body Hammer* (2003)

Full Disk Analysis v. Rapid Triage

- **Full Disk**
  - *Pros*
    - Captures EVERYTHING
    - For use with advanced threats, criminal cases, or if rapid triage doesn't yield results
  - *Cons*
    - Captures EVERYTHING
    - Time consuming
- **Rapid Triage**
  - *Pros*
    - Lightweight and speedy
    - Easy to parse the data
  - *Cons*
    - Doesn't capture everything
    - Not for every single case

"Here today, tomorrow gone / To the triage tent in the great beyond"
• Walter Becker, *Medical Science* (1994)

Open-source Intelligence (OSINT)

- **Uses**
  - The community of practice has several blogs/forums/etc. where useful data can be harvested
  - Helpful when cross-referencing possible IOCs or behavior that have been discovered
- **Warning**
  - Not all blogs/forums/etc. are created equal, pull from several sources
  - Don't use any OSINT resources as the "silver bullet" with analysis and/or reference

"Damaged goods are good for nothing / Watch your intelligence"

• Robyn Hitchcock, *Watch Your Intelligence* (1991)

External Assistance

Cyber Insurance

- **Benefits**
  - Extra resources
  - May assign forensics or IR team
  - May ask that you work with the assigned teams for liability and claim reasons
  - May offer ransom negotiations
- **Remember**
  - Not all insurance carriers are created equal
  - The “cheapest” option might not be the best
  - Communication (immediate v. delayed)

“A license to love, insurance to hold / Melts all your memories and change into gold”

• Sade, *Smooth Operator* (1984)

External Assistance 2

Third-Party Vendors

- **Remember**
  - Choose a firm that fits the needs of your organization and budget
  - Gauge how easily they can be accessed versus level of support and testimonials
  - “Cheaper” isn’t necessarily always better
- **Tips**
  - Develop a firm understanding for what the vendors *can* and *cannot* do before deciding
  - For pre-existing firms, don’t be afraid to access if they are still necessary/fit after major updates to your environment

“All you pretty pretenders, negligent vendors / I have no need for anger”

• Indigo Girls, *Reunion* (1994)

Contact Info & Questions

- **Membership**
  - Email: info@cisecurity.org
- **Contact Info (CIRT & SOC)**
  - Email: cirt@cisecurity.org / soc@cisecurity.org
  - Phone: 866-787-4722

- **Questions?**

“I’ve got a question / Would you ever dance with me like that?”

• Neon Trees, *Girls and Boys in School* (2010)

Thank You