GlobalTech Ransomware DFIR Playbook

Project 8: DFIR Playbook

Group Members: D'Marco Rodgers, Duran Anderson

What Is DFIR?

DFIR = Digital Forensics & Incident Response

- Incident Response handles **what to do during an attack**
- Digital Forensics focuses on **collecting and analyzing evidence**
- A DFIR playbook gives a **step-by-step response plan**

Project Goal

Goal of the Project

- Design a DFIR playbook for ransomware incidents
- Follow the full Incident Response lifecycle
- Show how evidence is collected and analyzed
- Use real tools and realistic artifacts

Incident Response Lifecycle

IR Lifecycle Used (NIST-based)

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Ransomware Scenario

Why Ransomware?

- One of the most common attacks today
- Encrypts files and disrupts business
- Often spreads quickly across networks

Evidence & Logs

Forensic Evidence Collected

- Memory (RAM) images
- Disk images
- Windows Event Logs
- Sysmon logs
- Network logs

Tools Used

DFIR Tools Referenced

- FTK Imager – disk & memory acquisition
- WinPMEM – live memory capture
- Volatility – memory analysis
- Autopsy – disk forensic analysis
- Sysmon – detailed system logging

Sample Artifacts

Project Artifacts

- Sample log files
- Simulated ransomware indicators
- Chain-of-custody template
- IR workflow diagrams

Why a Playbook Matters

Why DFIR Playbooks Are Important

- Ensures a structured response
- Prevents evidence loss
- Reduces downtime
- Improves recovery and future security

Conclusion

- Built a realistic DFIR ransomware playbook
- Aligned with industry standards
- Includes procedures, tools, and evidence handling
- Helps organizations respond to attacks confidently

Links/Refrences

NIST SP 800-61 Rev. 2. (2012). *Computer Security Incident Handling Guide.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST SP 800-86. (2006). *Guide to Integrating Forensics Techniques into Incident Response.* National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

RFC 3227. (2002). *Guidelines for Evidence Collection and Archiving.* Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc3227

MITRE ATT&CK Framework. MITRE Corporation. https://attack.mitre.org

CrowdStrike. (2024). *Global Threat Report.* CrowdStrike Inc. https://www.crowdstrike.com/resources/reports/global-threat-report