**Day 1 - Incident Response Foundations (17.6.)**

**Day 1 – Incident Response Foundations**

**1. Phases of Incident Response (based on NIST 800-61)**

**Topics**

* Overview of Incident Response lifecycle:
  + **Preparation**, **Detection & Analysis**, **Containment**, **Eradication**, **Recovery**, **Post-Incident Activities**
* Differences between event, alert & incident
* Importance of communication plans and escalation procedures
* Real-world examples of incident progression

**Webinars**:

* [NIST Cybersecurity Webcast: Incident Response Lifecycle](https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final) (Official Guide — Not a video, but gold standard reading), page 1-21
* SANS Incident Handling Process - [Incident Response SANS: The 6 Steps in Depth](https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/)

**YouTube**:

* [Incident Response Lifecycle | SANS Institute](https://www.youtube.com/watch?v=ToVVhMyU3dQ) – 00:07
* [Introduction to Incident Response | NIST 800-61 Explained](https://www.youtube.com/watch?v=IRSQEO0koYY) – 00:19

**Reading Material**:

* [NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide (PDF)](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)
* CISA Incident Response Playbooks[Cybersecurity Incident & Vulnerability Response Playbooks](https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf) – page 1-21
* [NIST Cybersecurity Framework (CSF) Overview](https://www.nist.gov/cyberframework)

**Required Infrastructure & Components**

* IR policy template & sample playbook
* IR roles & responsibilities matrix
* Access to a simulated lab environment with log files and alert data
* Whiteboard or collaborative board for mapping IR phases

**To-Dos & Steps**

1. Review and discuss the NIST 800-61 phases
2. Assign roles for an IR team and create a RACI chart
3. Walk through a sample incident (e.g., phishing or ransomware) and map to phases
4. Draft a mini playbook including triage questions and first steps
5. Reflect on importance of preparation phase & legal notification obligations

**2. Key Tools in IR: SIEM, EDR, SOAR**

**Topics**

* Role of **SIEM** (e.g., Splunk, ELK, Sentinel): Event correlation & alerting
* **EDR** tools (e.g., Defender for Endpoint, CrowdStrike): Endpoint visibility
* **SOAR** solutions (e.g., Cortex XSOAR): Playbook automation and case management
* Detection strategy design: Signature-based vs. behavioral
* Alert tuning and triage workflows

**Required Infrastructure & Components**

* SIEM dashboard demo or screenshots (Splunk, Graylog, Wazuh)
* Sample alert logs (authentication failures, malware detections)
* Optional: TryHackMe or cyber range with tool emulation
* Case triage form or ticketing board

**To-Dos & Steps**

1. Review detection rule examples and walk through correlation logic
2. Analyze SIEM alert samples and define escalation thresholds
3. Compare features of SIEM vs. EDR vs. SOAR with sample use cases
4. Draft a SOAR-style response playbook for malware
5. Practice triaging events and classifying severity

**Webinars**:

* Splunk Webinar: Splunk Security[Webinar: Splunk Security on Cloud I June 2022 I Positka](https://www.youtube.com/watch?v=RF5q4jRZBt0) – 00:57
* [Microsoft Azure Sentinel and Microsoft 365](https://www.youtube.com/watch?v=5kGN6qvj5i8) – 00:18

**YouTube**:

* [What is a SIEM? (Security Information and Event Management) – 00:14](https://www.youtube.com/watch?v=zrgBrpv4azs&t=7s)
* What is EDR? (Endpoint Detection Response)[What Is Endpoint Detection and Response (EDR)?](https://www.youtube.com/watch?v=dKNjwxpHusg) – 00:05
* SOAR Explained (Security, Orchestration, Automation & Response)[What is SOAR (Security, Orchestration, Automation & Response)](https://www.youtube.com/watch?v=k7ju95jDxFA) – 00:07

**Reading Material**:

* Splunk Security Operations Guide[The Fundamental Guide to Building a Better Security Operations Center (SOC)](https://www.splunk.com/en_us/pdfs/resources/e-book/the-fundamental-guide-to-building-a-better-security-operation-center-soc.pdf) – 8 pages
* MITRE Engenuity ATT&CK Evaluations for EDR Tools[MITRE Engenuity ATT&CK evaluation - N-able](https://www.n-able.com/de/resources/mitre-engenuity-attck-evaluation) – 1 page
* SOAR Buyer’s Guide by Palo Alto Networks[SOAR buyer’s guide: 11 security orchestration, automation, and response products — and how to choose | CSO Online](https://www.csoonline.com/article/3622920/soar-buyers-guide-11-security-orchestration-automation-and-response-products-and-how-to-choose.html) – 00:16
* [Elastic SIEM Documentation (Free and Open SIEM)](https://www.elastic.co/what-is/siem)

**3. Playbook Creation & Detection Strategy**

**Topics**

* Anatomy of a detection playbook: Trigger → Analysis → Response → Documentation
* Mapping use cases to detection rules (e.g., brute-force, lateral movement)
* Leveraging frameworks: MITRE ATT&CK, D3FEND
* Prioritizing detection logic: asset value vs. likelihood

**Required Infrastructure & Components**

* Detection use case template
* MITRE ATT&CK Navigator access
* Playbook design tool (e.g., Lucidchart, Miro)
* Reference: Sigma rules or example log patterns

**To-Dos & Steps**

1. Select a common incident type and build a simple response playbook
2. Map detection logic to MITRE ATT&CK tactics
3. Use a playbook builder to visualize detection-to-response flow
4. Review gaps in visibility and plan additional telemetry sources
5. Present detection logic to peers for feedback

**Webinars**:

* MITRE ATT&CK Deep Dive: Tactics and Techniques[Logpoint’s Top Ten MITRE ATT&CK Techniques - Logpoint](https://www.logpoint.com/en/blog/logpoints-top-ten-mitre-attck-techniques/) – 00:14
* SANS Detection Engineering Webcast [SANS Webcast | Detection Engineering in the Cloud: A Defenders Wonderland](https://www.youtube.com/watch?v=1yG49PfRZmQ) – 00:47

**YouTube**:

* [MITRE ATT&CK Framework Explained](https://www.youtube.com/watch?v=iOkkAfVAFyc) – 00:17
* How to build detection Playbooks[(231) Playbooks for Password spray, Endpoint detection, and Typo-squatted domain - Demo webinar - YouTube](https://www.youtube.com/watch?v=mRwCwD-cY4E) – 00:32

**Reading Material**:

* MITRE ATT&CK Navigator (Tool for Mapping Detections)<https://mitre-attack.github.io/attack-navigator/>
* D3FEND Framework by MITRE (Countermeasure Matrix)<https://d3fend.mitre.org/>
* [Sigma Rule Collection (Open Detection Rules)](https://github.com/SigmaHQ/sigma)[What Are SIGMA Rules: Beginner's Guide | SOC Prime](https://socprime.com/blog/sigma-rules-the-beginners-guide/)
* [Elastic SIEM Detection Rule Repository](https://github.com/elastic/detection-rules) [Create a detection rule | Elastic Docs](https://www.elastic.co/docs/solutions/security/detect-and-alert/create-detection-rule)

**Afternoon Lab: TryHackMe – Incident Response Room**

* Hands-on scenario walk-through: IR lab simulating attack lifecycle
* Collect indicators, analyze logs, perform containment decisions
* Identify missed detections and recommend monitoring improvements
* Reflect on timeline and response gaps

TryHackMe: Incident Response Lab *(Hands-on Guided Lab)*<https://tryhackme.com/room/adventofcyber2024>

**🎯 End-of-Day Goal**

Participants should be able to:

* Describe and apply each phase of the NIST incident response process
* Understand and compare key IR tools (SIEM, EDR, SOAR)
* Build and explain a detection-focused IR playbook
* Apply detection and triage concepts in a guided lab
* Recognize the value of preparation and structured IR handling