RED HERRINGS
redherrings.app

COURSE PACK

Syllabus

Incident Response Fundamentals

An 8-week course from reading one EDR alert to running a ransomware incident through every NIST 800-61 phase.

Course code	[DEPT 000]
Term	[Term and year]
Instructor	[Name]
Contact	[Email]
Office hours	[Days, times, location or link]
Meeting pattern	[Days, times, room or lab]
Length	8 weeks, one lab per week
Discipline	Incident Response
Level	Upper undergraduate, graduate, or professional cohort
Prerequisites	Networking and operating systems fundamentals. Introduction to Digital Forensics is helpful but not required.
Lab time	About 7 hours of hands-on work across the term
Prepared	2026-11-12

Bracketed fields are for the adopting instructor to complete. Everything else can be used as written. Every lab in this course generates a different variant of its case for each student, with an answer key verified against that student's own evidence; grading and the student portal run on the instructor's machine.

1. Course description

This course trains the responder's first week on the job: reading detections, deciding what is real, scoping an intrusion and choosing what to do about it. It opens on single sources (an EDR alert, a SIEM queue, a packet capture) and builds to full incidents worked under time. Two 45-minute drills and a 90-minute final incident are run as timed exams in the student portal with integrity logging, because responders work on a clock. Every case is mapped to MITRE ATT&CK and the NIST 800-61 lifecycle, and every student works a different variant, so the class can be debriefed on decisions rather than on answers.

2. Learning outcomes

On completing the course a student can:

1. Triage EDR, SIEM and network evidence by severity and ATT&CK technique.

2. Scope an intrusion from initial access to impact.

3. Choose and justify containment, eradication and recovery actions.

4. Produce indicators and a breach report a manager can act on.

3. Prerequisites and materials

Prerequisites

Networking and operating systems fundamentals. Introduction to Digital Forensics is helpful but not required.

Software

All tools are free. One-run install scripts for each are on the Tools page of the product website.

Tool	Used for
Any JSON viewer	EDR and SIEM exports
jq	filtering large exports on the command line
Excel or LibreOffice	sorting and pivoting alert tables
Wireshark	packet captures
EvtxECmd	Windows event logs to CSV
Timeline Explorer	reading the CSVs and building timelines

Hardware

A laptop or lab workstation with 8 GB of RAM (16 GB for memory forensics weeks), 20 GB of free disk and permission to install the listed tools. Windows, macOS and Linux all work; some tools are Windows-only and run in a virtual machine elsewhere.

Evidence

Evidence is generated per student and handed out as a ZIP or through a private portal link each week. No textbook purchase is required; each week names its reading from the free references below.

Readings and references

No purchase is required. The texts below are free from their publishers, and each week names the part to read. Editions and addresses change; the title and publisher are the stable reference.

Title	Publisher	Use in this course
Computer Security Incident Handling Guide (SP 800-61 Rev. 2; Rev. 3 is the CSF 2.0 profile) https://doi.org/10.6028/NIST.SP.800-61r2	NIST	The lifecycle every week maps to: preparation, detection and analysis, containment, eradication and recovery, lessons learned.
MITRE ATT&CK Enterprise matrix and Getting Started https://attack.mitre.org/	MITRE	Technique ids for every detection from week 1; tactics for scoping in weeks 6 and 8.
Federal Government Cybersecurity Incident and Vulnerability Response Playbooks https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks	CISA	Decision checklists for the drills in weeks 4 and 7.
Guide to Malware Incident Prevention and Handling (SP 800-83 Rev. 1) https://doi.org/10.6028/NIST.SP.800-83r1	NIST	Malware triage and containment, week 5.
#StopRansomware Guide https://www.cisa.gov/stopransomware/ransomware-guide	CISA and partners	Response checklist for the final incident, week 8.
Windows security auditing: events to monitor https://learn.microsoft.com/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor	Microsoft Learn	Logon types and service installs for lateral movement, week 6.
Responding to a compromised email account https://learn.microsoft.com/defender-office-365/responding-to-a-compromised-email-account	Microsoft Learn (Defender for Office 365)	Mailbox rules, sign-ins and what to revoke, week 7.
Wireshark User's Guide https://www.wireshark.org/docs/wsug_html_chunked/	Wireshark Foundation	Reading the packet captures from week 3 on.
Good Practice Guide for Incident Management https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management	ENISA	Team roles and escalation; background for the breach report.

4. How a week runs

1. Each week has one lab built on a single case. Every student receives a different variant of that case: different names, hosts, timestamps and answers, generated from the same story.

2. Before the lab, read the briefing and the week's preparation notes, and confirm the listed tools open on your machine.

3. During the lab, work the evidence with the listed tools and record each answer with the artifact and method that proves it.

4. Submit through the student portal link for that week, or hand in the worksheet. Portal submissions are graded against your own answer key the moment you submit.

5. After release, review the walkthrough for your variant: where each answer was, and how it was found.

5. Assessment and grading

Component	Weight	Details
Weekly labs (5)	50%	Best 4 of 5 count. Auto-graded on submission; each lab is up to 20 questions on that week's case.
Timed drills (2)	30%	Weeks 4 and 7. Two 45-minute exams in the portal, 15% each, each ending in a containment or response decision.
Final incident	20%	Week 8. A 90-minute timed exam on a live ransomware chain, plus a breach report due one week later.

Grading scale

A	90 to 100
B	80 to 89
C	70 to 79
D	60 to 69
F	below 60

Timed assessments are graded on submission in the portal. Reports are graded with the rubric in section 8. Scores export to the institution's LMS from each week's job.

6. Course policies

Collaboration

Discussing tools and technique with classmates is encouraged. Answers aren't transferable: each variant has its own evidence and its own key, and a submission that matches another student's variant rather than your own is flagged by the collusion report and treated as academic misconduct.

Late work

Labs are due at the end of the week they're set. Late labs lose 10% per day for three days and aren't accepted after that. The lowest lab scores are dropped as stated in the assessment table, which covers illness and emergencies without paperwork for short absences.

Timed assessments

Timed exams run in the student portal with a fixed clock, shuffled question order and integrity logging (tab switches, full-screen exits and pastes are recorded). Arrive with your tools installed and tested.

Resubmission

One lab per term may be resubmitted within a week of feedback for up to 80% of full credit.

Evidence handling

Evidence files are synthetic. Treat them as you would real evidence anyway: verify hashes, work on copies, and document every step. That habit is assessed.

Accommodations

[Insert the institution's disability accommodation and extended-time statement. The portal supports per-student time extensions.]

Academic integrity

[Insert the institution's academic integrity statement.]

7. Schedule

One case per week. The mode and time budget are set when the course is generated; the deliverable is what the student hands in.

Wk	Topic	Case	Mode	Assessment
1	Reading an EDR alert	First Look: Reading an EDR Alert	Practice, about 33 min	Lab 1
2	The SIEM queue	First Look: Reading a SIEM Alert	Practice, about 33 min	Lab 2
3	Beacons in web traffic	First Look: One Beacon in the Web Traffic	Practice, about 38 min	Lab 3
4	Phishing to foothold	Phishing to Foothold	Timed exam, 45 min	Drill 1 (15%)
5	Malware triage	Malware Triage: From Alert to Verdict	Practice, about 55 min	Lab 4
6	Lateral movement	Lateral Move to the File Server	Practice, about 76 min	Lab 5
7	Business email compromise	Business Email Compromise: Wire Fraud	Timed exam, 45 min	Drill 2 (15%)
8	Final incident: ransomware	Ransomware Before Coffee	Timed exam, 90 min, with report	Final 20%

Week by week

Each week below lists its objectives, the case and what it contains, what students should do beforehand, what they hand in, and a note for the instructor.

Week 1: Reading an EDR alert

Objectives

• Triage by severity and read a process tree.

• Map a detection to an ATT&CK technique.

Case

First Look: Reading an EDR Alert. Your first shift on the SOC queue. One endpoint threw a short stack of EDR detections. Read the feed the way a responder does, triage by severity, read the process tree and the ATT&CK technique on each one, and decide whether this is a real incident or noise.

Practice, about 33 min · Up to 15 questions · Tools: Any JSON viewer, jq, Excel

Reading

SP 800-61r2 section 3.2 (detection and analysis). ATT&CK: Getting Started and the Execution tactic.

Before the lab

Read the NIST 800-61 incident lifecycle summary and the ATT&CK matrix overview.

Deliverable

Lab 1 answers, each with the ATT&CK technique id.

Instructor note

Insist on technique ids from day one; the rest of the course assumes the vocabulary.

Week 2: The SIEM queue

Objectives

• Read a SIEM alert export.

• Separate a true positive from noise.

Case

First Look: Reading a SIEM Alert. Your first shift on the SOC queue. One correlated SIEM export is waiting with a short stack of alerts. Read it the way a responder does: sort by severity, open the worst alert, and pull its rule, technique and the source, destination and user entities so you can escalate cleanly.

Practice, about 33 min · Up to 15 questions · Tools: Any JSON viewer, jq, Excel

Reading

SP 800-61r2 section 3.2.4 (incident analysis) and 3.2.6 (prioritization).

Before the lab

Open the sample SIEM export in a JSON viewer and in a spreadsheet; decide which you prefer.

Deliverable

Lab 2 answers and a one-line triage note per alert: true positive, benign, or needs more data.

Instructor note

Most of the queue is noise by design; grade the dismissals as carefully as the escalation.

Week 3: Beacons in web traffic

Objectives
• Spot periodic egress in a packet capture.

• Pull a C2 indicator set.

Case
First Look: One Beacon in the Web Traffic. A workstation's outbound traffic for one hour was captured off the sensor. Most of it is ordinary browsing. Read the capture the way a responder reads a proxy log: rule out the normal destinations and pull indicators for whatever's left.

Practice, about 38 min · Up to 15 questions · Tools: Wireshark, tshark, NetworkMiner

Reading
ATT&CK: Command and Control tactic, T1071 and T1573. Wireshark User's Guide chapter 6.

Before the lab
Read the ATT&CK pages for T1071 and T1573 with periodicity, jitter and user-agent anomalies in mind.

Deliverable
Lab 3 answers and an indicator list (domains, IPs, user agents) ready to block.

Instructor note
Have students compute the beacon interval by hand once before letting a tool do it.

Week 4: Phishing to foothold

Objectives
• Follow a phish through delivery, execution and persistence.

• Make the first containment call under time.

Case
Phishing to Foothold. A user clicked. Walk the intrusion end to end: read the phishing email, follow what ran on the endpoint, and pull the indicators the team needs to block.

Timed exam, 45 min · Up to 20 questions · Tools: Thunderbird, Any JSON viewer, jq, Excel

Reading
SP 800-61r2 section 3.3 (containment). CISA playbook: incident response, containment step.

Before the lab
Review weeks 1 to 3. Read SP 800-61r2 section 3.3 on choosing a containment strategy.

Deliverable
Drill 1 submitted in the portal within 45 minutes, including the containment call.

Instructor note
Exam mode. Debrief the containment decisions as a group; there's more than one defensible answer.

Week 5: Malware triage

Objectives
• Go from alert to verdict with hashes, signatures and behavior.

Case
Malware Triage: From Alert to Verdict. A single endpoint threw a short stack of EDR detections. Work it from alert to verdict: find the worst severity and the technique, read what the sensor actually did, pull the offending process, its hash and parent, pin the first-detection time, and set the incident severity.

Practice, about 55 min · Up to 20 questions · Tools: Any JSON viewer, jq, Excel, Timeline Explorer

Reading
SP 800-83r1 sections 3 and 4 (detection, containment, eradication of malware).

Before the lab
Read SP 800-83r1 section 4 with hashes, signatures, behavior and when to stop in mind.

Deliverable
Lab 4 answers and a verdict with severity.

Instructor note
The case rewards stopping at a verdict; students who try to reverse the sample run out of time.

Week 6: Lateral movement

Objectives
• Pair 4624 logons with 7045 service installs.

• Scope which hosts the attacker reached.

Case
Lateral Move to the File Server. An unusual service started on the file server. Using the Security and System logs, the registry and Prefetch, work out where the session came from, what ran, and what was left to survive a reboot.

Practice, about 76 min · Up to 20 questions · Tools: Event Viewer, EvtxECmd, Registry Explorer, PECmd

Reading
Microsoft events to monitor: 4624 logon types, 4648, 7045, 4698. ATT&CK: Lateral Movement, T1021.

Before the lab
Install EvtxECmd and Timeline Explorer. Read the Microsoft events to monitor entries for 4624 logon types and 7045.

Deliverable
Lab 5 answers and a scoping table of hosts reached, with the evidence for each.

Instructor note
The scoping table is the artifact a real responder hands to leadership; grade it as such.

Week 7: Business email compromise

Objectives
• Trace a fraudulent wire request through mail, browser and phone evidence.

• Decide what to do first.

Case
Business Email Compromise: Wire Fraud. A finance controller wired a vendor payment to an account nobody recognizes, after an urgent request from an executive and new bank details from the vendor.

Timed exam, 45 min · Up to 20 questions · Tools: Thunderbird, DB Browser for SQLite, ALEAPP

Reading
Microsoft: responding to a compromised email account. ATT&CK: T1114 and T1564.008.

Before the lab
Read Microsoft's guide to responding to a compromised email account.

Deliverable
Drill 2 submitted within 45 minutes, including the first response action and why.

Instructor note
Exam mode. Time pressure is realistic here.

Week 8: Final incident: ransomware

Objectives
• Run a live ransomware chain through detection, containment, eradication and recovery.

• Write the breach report.

Case
Ransomware Before Coffee. You're the on-call responder. The EDR console lit up at 06:48 with a stack of detections from a finance workstation. Triage the detection feed and the host's own event logs, scope the intrusion from first access to impact, pull the indicators, map it to ATT&CK, and make the containment call fast.

Timed exam, 90 min, with report · Up to 20 questions · Tools: Any JSON viewer, jq, Excel, Event Viewer, EvtxECmd, Timeline Explorer

Reading
SP 800-61r2 sections 3.3 to 3.4 and the #StopRansomware Guide response checklist. ENISA guide on reporting.

Before the lab
Review every week. Read the breach report rubric.

Deliverable
Final incident submitted within 90 minutes; breach report due one week later.

Instructor note
Run as a timed exam with the breach report added. The report is the deliverable a manager would read; grade it on decisions and evidence, not narrative.

8. Report rubric

Applied to the written report that follows the final timed assessment. The report is written from the student's own saved answers for their own variant, so two reports in the same class never describe the same facts.

Criterion	Weight	Full credit looks like
Scope	30%	Initial access, every host and account reached, and the data touched, each with the evidence that proves it.
Decisions	30%	Containment, eradication and recovery actions are specific, ordered, and justified against the evidence.
Indicators	20%	A usable indicator list: hashes, domains, IPs, accounts, with where each was seen.
Timeline	10%	One normalized timezone, in order, mapped to ATT&CK and NIST phases.
Writing	10%	A manager can act on page one; detail follows; no speculation presented as fact.

9. Running the course in Red Herrings

1. Open Courses, pick this course, enter the class size or import the roster CSV, and press Generate the whole course. One job per week is created with the mode and time limit in the schedule.

2. Each week, open that week's job and hand out the student ZIPs or the private portal links. Portal links can be exported as a CSV for the LMS.

3. Timed weeks run in exam mode with integrity logging. Release scores from the job page after the sitting.

4. Grade from the job page or the Grading screen; export to Canvas, Blackboard, Moodle, D2L or QTI, or let LTI pass grades back.

5. Term Analytics shows the whole course at the end of term: scores by week, the questions most often missed, and integrity events.

Syllabus text, policies and the rubric may be copied into institutional templates without attribution.