

Incident Triage and First Response

FOR301

Make the first hour's calls from the records, not the alert. Confirm what fired, capture what expires, scope and score the incident, contain it in an order that removes the access, and hand it off with a report the next team can act on.

Modules	22
Lessons	143
Phases	4
Free preview	Course Orientation (6 lessons)

The method

Every incident type in the course is triaged with the same six calls, practiced against the Northgate Engineering records in Defender KQL, Splunk SPL and PowerShell.

1. Validate the alert. True positive, false positive or benign, decided from the records behind it in five queries.
2. Preserve what expires first. Every source has a clock, and some of your own actions stop it. The capture order comes before the investigation.
3. Scope by what is shared. The alert names one entity. Scope is every account, device and application linked to it by a record, not by resemblance.
4. Score it. Severity and priority on a scorecard, with the overrides that must move a score and the limits of what a score can say.
5. Contain in order. The order that removes the access, what each lever destroys, and when acting alerts the attacker.
6. Escalate and hand off. The escalation path, the regulatory clock, and a Triage Report and package incident response can start from.

Four modules apply the calls to account compromise, phishing and business email compromise, malware and ransomware, and exfiltration and intrusion. A capstone works one incident end to end.

What this course assumes

No minimum experience and no prerequisite course. Every source is introduced from what it records, and every query is explained at first use.

What makes it go faster: exposure to any alert queue, in any tool. Not required. Every triage in the course is worked against records the course provides.

What this course does not cover: deep forensics in any single environment, detection engineering, and the investigation that follows triage. Triage hands off to those, and the handoff is taught.

Full syllabus

Phase 1: Foundations

Course Orientation [FREE PREVIEW](#)

Incident Triage and First Response: the first hour of an incident as five decisions, taught against a month of records from an attacked company.

1. 0.1 Incident Triage and the First Hour
2. 0.2 Triage and Incident Response: The Handoff Point
3. 0.3 The Triage Clock
4. 0.4 Your Lab Environment and Equivalents
5. 0.5 Building the Triage Lab: Steps and Costs
6. 0.6 Triage Tools: Scorecard, Query Pack and Triage Report

Alert Triage and Validation

What an alert claims, how to test the claim against the evidence underneath it, and how to classify the result as a true positive, a false positive, benign activity, or unresolved, across identity, endpoint, email, cloud and network alerts.

1. 1.1 Anatomy of a Security Alert
2. 1.2 True Positives, False Positives and Benign Activity
3. 1.3 Detection Rules Behind an Alert
4. 1.4 The Five-Query Triage Pack
5. 1.5 First Look: Sign-In and Identity Alerts
6. 1.6 First Look: Endpoint Alerts
7. 1.7 First Look: Email and Cloud Alerts
8. 1.8 First Look: Network Alerts
9. Module Summary and Knowledge Check

Evidence Preservation in the First Hour

What evidence an incident leaves, how long each kind lasts, and the capture order that keeps what the investigation will need before time, the attacker or your own containment destroys it.

1. 2.1 Evidence Volatility by Source
2. 2.2 Order of Evidence Capture
3. 2.3 Identity Evidence: Sessions, Tokens and Log Retention
4. 2.4 Endpoint Evidence: Memory, Processes and Connections
5. 2.5 Cloud Evidence: Retention Limits and Audit Gaps
6. 2.6 First-Hour Evidence Capture
7. 2.7 Preservation and Containment Trade-Offs
8. 2.8 Evidence Gaps and Their Documentation
9. Module Summary and Knowledge Check

Incident Scope and Blast Radius

What an incident includes and what it can reach: scope built from links rather than the alert queue, pivots taken to completion, the blast radius of accounts, machines and data, alerts grouped on shared entities, a sourced triage timeline, and every claim graded by the evidence that carries it.

1. 3.1 Incident Scope: Users, Hosts and Time
2. 3.2 Pivoting on Users, Hosts and IP Addresses
3. 3.3 Blast Radius: Accounts and Access
4. 3.4 Blast Radius: Endpoints and Lateral Reach
5. 3.5 Blast Radius: Applications and Data
6. 3.6 Related Alerts and Incident Grouping
7. 3.7 The Triage Timeline
8. 3.8 Scope Confidence and Its Limits
9. Module Summary and Knowledge Check

Incident Severity and Prioritization

How bad an incident is and how fast it must be acted on, scored from evidence on an eight-question card, turned into a priority tier and a response clock, with overrides for the features a total cannot capture and a record for the cases where the card runs out.

1. 4.1 Severity and Urgency
2. 4.2 The Triage Scorecard: Eight Questions
3. 4.3 The Triage Scorecard: Scoring From Evidence
4. 4.4 The Triage Scorecard: Unanswered Questions
5. 4.5 Priority Tiers and Response Timelines
6. 4.6 Severity Overrides
7. 4.7 Prioritization With Conflicting Evidence
8. 4.8 Scorecard Limits and Analyst Judgment
9. Module Summary and Knowledge Check

Phase 2: Incident Triage

Account Compromise Triage

Triaging a compromised account from its evidence: suspicious sign-ins, stolen sessions, MFA fatigue, password spray and brute force, service accounts, the changes attackers make to keep access, and hybrid pivots, each ending in a call, a severity and a next move.

1. 5.1 Suspicious Sign-Ins: Location, Device and Risk
2. 5.2 Session and Token Theft
3. 5.3 MFA Fatigue and Push Abuse
4. 5.4 Password Spray and Credential Stuffing
5. 5.5 Service Account Compromise
6. 5.6 Attacker Changes: MFA Methods, Roles and Credentials
7. 5.7 Hybrid Pivots: On-Premises to Cloud
8. 5.8 Account Compromise: Severity and Next Moves
9. Module Summary and Knowledge Check

Phishing and Business Email Compromise Triage

Triaging reported phishing and business email compromise from the message, its delivery evidence and what recipients did with it: clicks and relayed sessions, attachments that run, consent grants, inbox rules and forwarding, the campaign scope and purge, each ending in a call, a severity and a...

1. 6.1 Reported Phishing: The First Read
2. 6.2 Email Headers and Delivery Evidence
3. 6.3 Clicks and Credential Submission
4. 6.4 Malicious Attachments: Delivery to Execution
5. 6.5 Consent Phishing and Malicious App Grants
6. 6.6 Business Email Compromise: Inbox Rules and Forwarding
7. 6.7 Campaign Scope: Recipients, Clicks and Purge
8. 6.8 Phishing and BEC: Severity and Next Moves
9. Module Summary and Knowledge Check

Malware and Ransomware Triage

Triaging malware and ransomware from the endpoint evidence: process trees and command lines, borrowed Windows binaries, credential dumping, persistence, lateral movement, Linux hosts, and the precursors that come before encryption, each ending in a call, a severity and a next move.

1. 7.1 Endpoint Alerts: Process Trees and Command Lines
2. 7.2 Malicious Documents, Scripts and LOLBins
3. 7.3 Credential Dumping on the Endpoint
4. 7.4 Persistence Mechanisms
5. 7.5 Lateral Movement From a Compromised Host
6. 7.6 Linux Host Compromise: SSH, Cron and Web Shells
7. 7.7 Ransomware Precursors: Staging, Backups and Shadow Copies
8. 7.8 Malware and Ransomware: Severity and Next Moves
9. Module Summary and Knowledge Check

Data Exfiltration and Network Intrusion Triage

Triaging intrusions that cross the network edge, hosts, the identity layer and cloud applications: data leaving, cloud downloads, persistence in applications, perimeter alerts, VPN compromise and command-and-control, scoped across domains and scored as one incident.

1. 8.1 Data Exfiltration: Volume, Destination and Timing
2. 8.2 Cloud Storage and SaaS Data Access
3. 8.3 Cloud Persistence: App Credentials and Federation
4. 8.4 Perimeter Alerts: Firewall and Proxy Evidence
5. 8.5 Edge Device and VPN Compromise
6. 8.6 Command-and-Control Beaconing
7. 8.7 Exfiltration and Intrusion: Scope Across Domains
8. 8.8 Exfiltration and Intrusion: Severity and Next Moves
9. Module Summary and Knowledge Check

Phase 3: Response

Incident Containment

Stopping attackers while the investigation continues: account, host, application and mailbox levers, each pulled in the system that holds it, in an order and at a time that leave no way back and give no warning, with the business cost measured and planned.

1. 9.1 Containment Options: Accounts, Hosts, Apps and Network
2. 9.2 Session and Token Revocation
3. 9.3 Password and MFA Reset Sequencing
4. 9.4 Host Isolation and Evidence Preservation
5. 9.5 App and Consent Removal
6. 9.6 Containment Order Under Time Pressure
7. 9.7 Containment Timing and Attacker Awareness
8. 9.8 Containment Side Effects and Business Impact
9. Module Summary and Knowledge Check

Escalation, Reporting and Handoff

Moving a triaged incident to the people who act on it: escalation by threshold and clock, communication on channels the attacker cannot read, the notification trigger, the fifteen-minute Triage Report at the right confidence, and handoffs to the response team and the next shift.

1. 10.1 Escalation Paths and Thresholds
2. 10.2 Escalation Timing by Priority
3. 10.3 Stakeholder Communication During Triage
4. 10.4 Regulatory Notification Triggers
5. 10.5 The Fifteen-Minute Triage Report
6. 10.6 Triage Report: Findings, Confidence and Gaps
7. 10.7 Handoff to Incident Response
8. 10.8 Shift Handover for Open Incidents
9. Module Summary and Knowledge Check

Automation and AI in Triage

Consuming what automation and AI hand the analyst: outputs read as inputs, enrichment whose silence is not clean, verdicts read for what they are about and overridden with a reason, automated containment reviewed for result, reach and aim, AI summaries checked claim by claim, and the narrow...

1. 11.1 Automation in the Triage Workflow
2. 11.2 Automated Enrichment and Its Verification
3. 11.3 Automated Verdicts and Analyst Override
4. 11.4 Automated Containment: Review and Reversal
5. 11.5 AI-Assisted Triage: Summaries and Verification
6. 11.6 Fast-Moving Attacks and the Triage Clock
7. Module Summary and Knowledge Check

Phase 4: Capstone

Capstone: A Full Incident Triage

One incident triaged end to end, one decision per section: an intrusion from a public web server to a tenant-wide mail grant in eight minutes, left unopened for a day, then validated, preserved, scoped, scored, contained, escalated and reported in one afternoon.

1. 12.1 Capstone Case: The Alert
2. 12.2 Capstone Case: Alert Validation
3. 12.3 Capstone Case: Evidence Preservation
4. 12.4 Capstone Case: Scope and Blast Radius
5. 12.5 Capstone Case: Severity and Priority
6. 12.6 Capstone Case: Containment Plan
7. 12.7 Capstone Case: Escalation and Notification
8. 12.8 Capstone Case: The Triage Report

Phase 0: Course Resources

Cheatsheets

The instruments you should know from memory, the artifact-type vocabulary that makes a question transfer between stacks, and the four query pages covering every sub in the course.

1. Evidence and Preservation
2. Identity
3. Applications and Consent
4. Endpoint
5. Cloud and Hybrid
6. Network and Perimeter
7. Correlation
8. Severity, Containment and Automation
9. Codes, Types and What They Prove

Cookbooks

Seven step-by-step triage procedures, one per subject area.

1. The Sixty-Minute Timeline
2. Preserving Evidence Before You Change Anything
3. Triageing an Identity Alert
4. Triageing an Application or Consent Alert
5. Triageing an Endpoint Alert
6. Deciding Severity and Escalating
7. Containing an Identity Compromise

Lab Setup

Build the reference environment the course teaches against, at no cost, with a documented swap for every layer you already run.

1. Lab Setup

Walkthroughs

Eight complete triages worked start to finish with the clock running.

1. The Cheap Check That Ends It
2. When the Cheap Check Does Not Clear It
3. The Reset That Contained Nothing
4. A Grant Nobody Noticed
5. The Alert With No Evidence Behind It
6. The Score Was Right and the Call Was Wrong
7. The Sixty Minutes That Went Nowhere

Playbooks

Six playbooks, one per alert type. What the alert asserts, the check that could clear it, what escalates it instead, the containment order, and what the handoff must say.

1. Impossible Travel
2. Token Theft and Replay
3. Consent Granted to an Application
4. Endpoint Execution Alert
5. Suspected Data Egress
6. Three Alerts, One Incident

Playground

Resources for practicing triage and using it at work: guided investigations, response playbooks, the detection library, a query console, and an open-source DFIR toolkit.

References & Further Reading

External sources this course draws on: vendor documentation, frameworks, standards, and research.

Project

Project: Build Your Own Triage Kit

The FOR301 project: a brief for three artifacts you build for your own estate from what the course taught, a five-query first-look pack, a scorecard calibrated to your priority tiers, and a Triage Report template your escalation path accepts.

1. The Brief

Course Completion

Course Exam

Incident Triage and First Response end-of-course exam: a three-phase simulation testing whether you can apply the method to a situation the course did not walk through.

1. Course Completion. Incident Triage and First Response

Generated 2026-09-27 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/incident-triage-first-response/