Splunk Detection and Incident Response

SEC405

Detect and investigate attacks in Splunk with SPL: scope and shape searches, accelerate detections with tstats over CIM data models, hunt across identity, endpoint, network, and cloud, and run an incident end to end against a runnable corpus, with no Splunk license required.

Modules	21
Lessons	155
Phases	6
Free preview	Course Orientation (7 lessons)

The method

Splunk rewards knowing where the data model ends and raw search begins. This course runs the same loop for every detection and every investigation it works.

1. Search the model, not the index, where you can. tstats against an accelerated data model is orders of magnitude faster than the equivalent raw search, and the difference decides whether a detection runs at all.

2. Normalize before you correlate. CIM exists so a detection written once works across sourcetypes. A search built on raw field names works until somebody onboards a new log source.

3. Write the detection against the behavior. The technique's requirement rather than the tool's name, the same discipline that survives an attacker changing their kit.

4. Scope before you conclude. A hit is one entity. The investigation is the others, and Splunk's job in an incident is turning one alert into a bounded population.

5. Reconstruct the timeline from the events you can defend. With the source and the search that produced each one recorded alongside it.

The course closes on a full-chain incident worked entirely in Splunk.

What this course assumes

No minimum experience and no prerequisite course. SPL, data models, CIM and the search head model are built up from the first search.

What makes it go faster: a Splunk instance with data in it. Not required, because every search in the course runs against a corpus the course provides.

What this course does not cover: Splunk administration, index design and infrastructure. This is detection and incident response by somebody who searches Splunk rather than runs it.

Full syllabus

Phase 1: Foundations

Course Orientation FREE PREVIEW

What Splunk Detection and Incident Response teaches: write tstats-accelerated detections over CIM data models, hunt across identity, endpoint, network, and cloud, and run an incident end to end from the search bar.

1. SPL0.1 Purpose and Scope
2. SPL0.2 Getting the Most From This Course
3. SPL0.3 The SIEM Is the Whole Estate in One Place
4. SPL0.4 An Attack Is a Trail Across Sources
5. SPL0.5 Detection Is Signal Against Noise
6. SPL0.6 The NE Environment and Its Evidence
7. SPL0.7 The On-Page Toolkit and Setup

The Splunk Detection and IR Landscape

How Splunk stores and retrieves data, search-time versus index-time, the Common Information Model, where NE's evidence lives, and your first detection-grade searches against the corpus.

1. SPL1.1 Indexes and Search Scoping
2. SPL1.2 Sourcetypes and Fields
3. SPL1.3 The Search Pipeline
4. SPL1.4 Search-Time versus Index-Time
5. SPL1.5 Shaping Results
6. SPL1.6 The Common Information Model
7. SPL1.7 Data Models
8. SPL1.8 Knowing NE's Data
9. SPL1.9 Your First Detection-Grade Searches
10. SPL1.10 Module Summary

Phase 2: The Splunk Analysis Surface

Data Models, CIM, and tstats

The accelerated-search backbone: how CIM data models normalize NE's sources, how tstats reads the acceleration summary to search millions of events in moments, and how to point it at the Authentication, Endpoint, Network, Change, and Email models that the detection modules build on.

1. SPL2.1 Why Raw Search Doesn't Scale
2. SPL2.2 The Anatomy of tstats
3. SPL2.3 The CIM Data Models in NE
4. SPL2.4 tstats over Authentication
5. SPL2.5 tstats over Endpoint
6. SPL2.6 tstats over the Network and Web Models
7. SPL2.7 tstats over Change and Email
8. SPL2.8 From Acceleration to Detection
9. SPL2.9 When tstats Can't See It
10. SPL2.10 Module Summary

Advanced SPL for Detection

The compute layer: eventstats and streamstats for baselining, bin for time shape, transaction for session reconstruction, subsearch and join for correlation, lookup for enrichment and allowlisting, and rex for extraction, the commands that turn a count into a judgment.

1. SPL3.1 eventstats: Comparing to a Baseline
2. SPL3.2 streamstats and bin: Detection Over Time
3. SPL3.3 transaction: Reconstructing a Session
4. SPL3.4 subsearch and join: One Search Feeding Another
5. SPL3.5 lookup: Enrichment
6. SPL3.6 lookup: Threat Intel and Allowlisting
7. SPL3.7 rex and spath: Extracting What the Model Doesn't Give
8. SPL3.8 Composing the Compute Layer
9. SPL3.9 Module Summary

Phase 3: Detection Engineering

Detection Engineering in Splunk

The lifecycle and discipline that turns a search into a production detection: hypothesis to correlation search, calibrating thresholds from data, false-positive reduction, suppression and scheduling, testing, and detection-as-code.

1. SPL4.1 Search, Alert, Detection
2. SPL4.2 From Hypothesis to Correlation Search
3. SPL4.3 Calibrating Thresholds From Data
4. SPL4.4 Precision and False-Positive Reduction
5. SPL4.5 Suppression, Throttling, and Scheduling
6. SPL4.6 Testing a Detection
7. SPL4.7 Detection-as-Code and the Lifecycle
8. SPL4.8 Module Summary

Identity Attack Detection

Detecting the identity attacks that dominate cloud intrusions, on the Authentication model: password spray, MFA gaps, risky sign-ins, impossible travel, adversary-in-the-middle token replay, and OAuth persistence, engineered against NE's real spray-and-AiTM intrusion.

1. SPL5.1 The Identity Attack Surface
2. SPL5.2 Baselining an Identity
3. SPL5.3 Detecting Password Spray
4. SPL5.4 MFA Gaps and Weak Authentication
5. SPL5.5 Risky Sign-Ins and the Risk Signal
6. SPL5.6 Impossible Travel
7. SPL5.7 Adversary-in-the-Middle Token Replay
8. SPL5.8 Token Replay in the Non-Interactive Logs
9. SPL5.9 Anomalous Service Principals and OAuth Persistence
10. SPL5.10 Correlating the Identity Kill Chain
11. SPL5.11 Module Summary

Endpoint Attack Detection

Detecting the endpoint-compromise chain on the Endpoint data model and Sysmon: process ancestry, encoded execution, LOLBins, credential theft, persistence, lateral movement, and host-based C2, engineered against NE's real macro-to-foothold intrusion on a single laptop.

1. SPL6.1 The Endpoint Attack Surface
2. SPL6.2 Baselining Endpoint Activity
3. SPL6.3 Process Ancestry: the Anomalous Parent
4. SPL6.4 Command-Line Analysis
5. SPL6.5 LOLBins and Living Off the Land
6. SPL6.6 Credential Theft
7. SPL6.7 Persistence
8. SPL6.8 Lateral Movement
9. SPL6.9 Endpoint C2 and Network Activity
10. SPL6.10 Correlating the Endpoint Kill Chain
11. SPL6.11 Module Summary

Phase 4: Hunting and Correlation

Network, Web, and DNS Detection

Detecting an intrusion in the traffic that leaves the estate: beacon cadence and shape in proxy logs, exfiltration by volume, DNS as a covert channel, threat-intel and CIDR matching at the egress, and the perimeter firewall's own verdicts, engineered against NE's real C2, exfiltration, and...

1. SPL7.1 The Network, Web, and DNS Attack Surface
2. SPL7.2 Baselining Egress Traffic
3. SPL7.3 Detecting Beaconing
4. SPL7.4 C2 Over Web: Shape Beyond Cadence
5. SPL7.5 Exfiltration by Volume
6. SPL7.6 DNS as a Covert Channel
7. SPL7.7 Threat Intelligence at the Egress
8. SPL7.8 The Perimeter View: Firewall and Denied Traffic
9. SPL7.9 Correlating the Network View into the Kill Chain
10. SPL7.10 Module Summary

Threat Hunting

The proactive search for the intrusion no rule caught: hypothesis-driven hunting, tstats over accelerated data models for whole-estate speed, and the cloud as a hunting surface, working a real AWS account compromise from reconnaissance through credential access and defense evasion to a...

1. SPL8.1 What Threat Hunting Is
2. SPL8.2 Hunting at Scale with tstats
3. SPL8.3 The Cloud Attack Surface
4. SPL8.4 Hunting Cloud Reconnaissance
5. SPL8.5 Hunting Credential Access and Defense Evasion
6. SPL8.6 Following an Actor Across Sources
7. SPL8.7 From a Hunt to a Detection
8. SPL8.8 Module Summary

Phase 5: Incident Response

Triage and Scoping

The incident-response entry point in Splunk: triage a queue to the one lead that matters, validate it against independent telemetry, scope the blast radius across identity, endpoint, network, and cloud, reconstruct sessions with transaction, and build the incident timeline, working a real...

1. SPL9.1 The Incident Response Entry Point
2. SPL9.2 Triaging the Queue
3. SPL9.3 Validating the Lead
4. SPL9.4 Scoping the Blast Radius
5. SPL9.5 Session Reconstruction with transaction
6. SPL9.6 Building the Incident Timeline
7. SPL9.7 From a Lead to a Scoped Incident
8. SPL9.8 Module Summary

Investigation and Timeline Reconstruction

Full multi-source incident reconstruction in Splunk: work backward to initial access, reconstruct the identity, endpoint, network, and cloud stages each in depth, correlate them into one chain, and assemble a defensible timeline of a real multi-stage NE intrusion from the edge through identity...

1. SPL10.1 From Skeleton to Defensible Timeline
2. SPL10.2 Working Backward to Initial Access
3. SPL10.3 The Identity Foothold and Its Expansion
4. SPL10.4 Reconstructing the Endpoint Stage
5. SPL10.5 Correlating Endpoint to Network
6. SPL10.6 Reconstructing the Cloud Stage
7. SPL10.7 Correlating the Chain Across Planes
8. SPL10.8 Building the Master Timeline
9. SPL10.9 The Objective and the Narrative
10. SPL10.10 Module Summary

Incident Response, Evidence, and Reporting

The Splunk-driven incident response workflow after the investigation: preserve search-derived evidence, derive the remediation picture, contain and evict the attacker across identity, endpoint, network, and cloud, validate the eviction, write the incident report, and version-control the...

1. SPL11.1 From Timeline to Response
2. SPL11.2 Preserving Evidence From Search
3. SPL11.3 Deriving the Remediation Picture
4. SPL11.4 Containing and Evicting Identity
5. SPL11.5 Containing and Evicting Endpoint and Network
6. SPL11.6 Validating the Eviction
7. SPL11.7 Writing the Incident Report
8. SPL11.8 Detection as Code
9. SPL11.9 Module Summary

Phase 6: Capstone

Capstone: Full-Chain Incident in Splunk

The capstone: applying the whole course method to a fresh edge-to-identity intrusion, from a single alert on an internet-facing host through triage, reconstruction of the entry and the pivot inward, correlation and a master timeline, the objective and the response, to a defensible final report.

1. SPL12.1 The Capstone Brief
2. SPL12.2 Triage and Scope the Lead
3. SPL12.3 Reconstructing the Entry
4. SPL12.4 Reconstructing the Pivot Inward
5. SPL12.5 Correlating and the Master Timeline
6. SPL12.6 The Objective and the Response
7. SPL12.7 The Capstone Report and Debrief
8. SPL12.8 Module Summary

Phase 0: Course Resources

Cheatsheets

SPL by investigation area, each search with the fields that carry the decision and what the result does not establish.

1. Search Patterns
2. Data Models and CIM
3. The Compute Layer
4. Identity Detections
5. Endpoint Detections
6. Network, Web and DNS
7. Threat Hunting
8. Triage and Scoping
9. Response and Reporting
10. The Engine and the Estate

Cookbooks

Ordered procedures for the situations that recur: validating a lead, scoping an identity, building a timeline, tuning a noisy detection and proving an eviction.

1. Validating a Password Spray Lead
2. Scoping a Compromised Identity
3. Confirming a Beacon
4. Tuning a Detection That Fires Too Often
5. Investigating a Suspicious Execution
6. Building a Cross-Source Timeline
7. Proving an Eviction Held

Lab Setup

Building a Splunk instance that runs this course's searches, with the license decision that determines which modules you can actually practice in it.

1. The License Decision, and Why It Comes First
2. Installing, and the First Ten Minutes
3. Getting Data In
4. CIM and Data Model Acceleration
5. Verify It Works, and What It Cannot Show You

Walkthroughs

Six worked investigations against the course corpus, each ending in a written finding with its confidence stated and its gaps named.

1. The Nineteen That Were Really One
2. The Host That Resolved Everything
3. The Host We Could Not Put on the Network
4. The Account That Stopped Being the Subject
5. Twenty-Four Minutes on One Laptop
6. Four Events and a Month

Playbooks

Seven playbooks keyed to what actually fires, each with a pre-flight, a sequence, escalation tiers and the false positives that live in that domain.

1. A Surge of Failed Authentications
2. A Host Talking on a Schedule
3. A Process That Should Not Have Run
4. An Identity Gained Rights It Did Not Have
5. A Large Amount of Data Left
6. A Source Stopped Reporting
7. A Detection Nobody Can Work

Playground

Where to practice SPL and use it at work: the drills, the corpus, your own instance, the detection library, and the reference pages worth keeping open.

References & Further Reading

Splunk documentation, the Common Information Model, MITRE ATT&CK, Splunk Security Content, NIST SP 800-61 Rev 3, and the threat-intelligence and methodology sources used throughout the Splunk Detection and Incident Response course.

Course Completion

Course Exam

Splunk Detection and Incident Response end-of-course exam: a simulation-based assessment testing your ability to triage, investigate, and respond to a Splunk-detected intrusion you have not seen before, using the evidence and the method built across all thirteen modules.

1. Course Completion. Splunk Detection and Incident Response

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/splunk-detection-and-response/