# SEC501:™ Applied Cyber Defense™

GCED
Enterprise Defender
giac.org/gced

6 Day Program | 38 CPEs | Laptop Required

## You Will Be Able To

- Correlate records held by different systems, teams, and service providers
- Recover the sequence of suspicious activity from network and host records
- Build and test detections against the traffic they are expected to identify
- Validate which exposed services can extend access before assigning remediation priority
- Establish scope before containment disrupts systems or accounts outside it
- Use malware behavior and program logic to improve detection, scoping, and recovery
- Check AI-assisted analysis and agent actions against primary records

## Business Takeaways

- Reduce the cost of premature escalation by requiring corroborating records
- Limit disruption by matching containment to the systems and accounts in scope
- Give responders timely access to records held by providers and authority to act
- Require tested corrections when controls fail to record or restrict activity
- Identify missing records and short retention periods before they delay an investigation
- Remove persistence and compromised access before systems return to service
- Limit risk from automated actions by verifying authority and the resulting system change

GCED
Enterprise Defender
giac.org/gced

## GIAC Certified Enterprise Defender

TThe GIAC Certified Enterprise Defender (GCED) certification validates a practitioner's knowledge and abilities in the areas of defensive network infrastructure, packet analysis, penetration testing, incident handling, and malware removal, building on the security skills measured by the GIAC Security Essentials certification. GCED certification holders are equipped with more advanced technical skills that are needed to defend the enterprise environment and protect an organization as a whole.

## Defend the Enterprise When the Records Are Incomplete

Cyber defenders must investigate and act across systems and services they do not fully control. A compromised software update can enter through an approved process, while stolen credentials can cross platforms before an investigation establishes scope. AI agents can make authorized changes faster than teams can review the resulting records. SEC501 develops the technical judgment to determine what these records support before escalation or containment creates unnecessary cost or disruption.

SEC501 begins with a persistent anomaly involving network availability, privileged access, and DNS activity. Additional records may narrow the possible explanations without establishing a single cause. You must decide whether they justify escalation, containment, or collection from another system.

You revisit the persistent anomaly by comparing network and identity records with alerts retained elsewhere in the enterprise. Hardening changes, recovered host artifacts, and malware behavior may change which systems or accounts require action.

More than 25 integrated labs require you to decide what the records support. You will trace an alert or exposed service to the record behind it and test a control against observed behavior. You must then decide whether the record justifies escalation, containment, or corrective action. Document any record that remains missing when the decision is made.

Records needed to establish scope may reside with a SaaS provider, cloud management platform, or MSSP. AI systems and agents may also produce analysis or change a system under delegated authority. You will identify which record is missing, verify the authority granted, and compare the automated analysis or system change with records from the affected system before using either to make an incident decision.

Management gains cyber defenders who reduce the cost of premature escalation, match containment to the systems and accounts in scope, and require a tested correction when a control fails. The same investigation reveals whether contracts, retention periods, or access rights will keep a required record from responders during the next incident.

SEC501 prepares practitioners with SEC401-level knowledge or equivalent experience to investigate activity across systems before deeper specialization in the Cyber Defense curriculum.

## Author Statement

"Cyber defenders rarely receive every record at the moment a decision is required. I have spent my career moving between hands-on technical work and leadership roles where records were held by different systems, teams, and providers, and where an unnecessary response action could disrupt the business it was intended to protect. I designed SEC501 around this reality. The persistent anomaly connects the five technical sections, requiring you to examine what the enterprise recorded, determine which explanations remain supportable, and decide whether the records justify escalation, containment, or further collection. SEC501 develops the breadth needed to follow suspicious activity across the enterprise and the judgment to act before every record is available."

—Ross Bergman

# Section Descriptions

### SECTION 1: Seeing Like a Defender

A persistent anomaly begins with records of network availability, privileged access, and DNS activity that do not establish a common cause. Compare what network devices generate with what receiving systems retain, then test how device time, administrative access, network trust, and decoy activity affect a later investigation.

**TOPICS:** Persistent Anomaly and Enterprise Records; Network Device Baselines and Audit Evidence; Syslog, Time Integrity, and Record Retention; Authentication, Authorization, and Accounting (AAA); Domain Name System Decoys and Active Defense

### SECTION 2: Detecting Like a Defender

Trace an alert to the packet, protocol record, flow data, or host event that produced it. Reconstruct suspicious activity, test detection logic against captured traffic, and determine whether the combined records justify escalation or a change in incident scope.

**TOPICS:** Security Operations and Alert Triage; Packet Analysis and Network Forensics; Zeek, Flow Data, and Network Visibility; Suricata Detection Development; SIEM Correlation and Security Analytics

### SECTION 3: Hardening Like a Defender

Find the systems and services that respond now, compare them with the inventory, and validate which exposures can extend access. Test how credentials and command-and-control channels cross expected boundaries, then verify a controlled configuration change against each managed system.

**TOPICS:** Asset, Service, and Identity Discovery; Vulnerability Assessment and Exploit Validation; Credential Exposure and Remote Administrative Access; Command and Control, Segmentation, and Reachability; Configuration Drift and Controlled Automation

### SECTION 4: Responding Like a Defender

Incident response begins before every record is available and often before scope is established. Recover host artifacts, test the claims in a handoff, reconstruct ransomware activity, and decide which systems or accounts require collection, containment, or recovery.

**TOPICS:** Incident Response Thresholds and Authority; Filesystem Recovery and Windows Artifacts; AI-Assisted Handoff Teview; Timeline Analysis and Incident Scoping; Containment, Eradication, and Recovery

### SECTION 5: Understanding Malware Like a Defender

Connect a suspicious file with the incident around it. Use file properties, host changes, network requests, and program logic to refine detection and scope, identify failed controls, and make containment and recovery decisions that the available records support across the enterprise.

**TOPICS:** Malware Triage and Static properties Analysis; Host Behavior and Persistence; Network Dependencies and Controlled Interaction; Code Review and Manual Reversing; Enterprise Detection and Response Implications

### SECTION 6: Operating Like a Defender

The final Applied Cyber Defense capstone draws on all five technical sections through independent challenges. Working individually or with a team, you must recover exact answers from the available artifacts and decide which challenge warrants the next block of time.

**TOPICS:** Malware Triage and Static properties Analysis; Host Behavior and Persistence; Network Dependencies and Controlled Interaction; Code Review and Manual Reversing; Enterprise Detection and Response Implications

**"This course has been valuable to me because it helped connect the risk and remediation work I do with the technical testing activities that often produce those findings. I work in IT risk, so I am often looking at vulnerabilities, controls, remediation plans and business impact.**

—Shanna Cox, **The Church of Jesus Christ of Latter-day Saints**

**"If you want to take a deep-dive into enterprise security, then you must take SEC501."**

—Nikolai Vinogradov, **JSC Severstal Management**

### Who Should Attend

SEC501 is designed for experienced technologists whose defensive responsibilities cross systems, platforms, and teams. It is an intermediate course for practitioners with SEC401-level knowledge or equivalent experience who must connect records and decisions across the enterprise before deeper specialization.

- Security operations center (SOC) analysts moving into incident handling and scoping
- Security engineers responsible for detection, hardening, and response
- Network or system administrators taking on broader cyber defense duties
- Digital forensics and incident response (DFIR) practitioners who connect host artifacts with records held elsewhere
- Computer emergency response team (CERT) and computer security incident response team (CSIRT) members responsible for incidents that cross systems and teams
- Technical leads and managers responsible for access, authority, and corrective action

### NICE Framework Work Roles

- Network Operations Specialist (OPM 441)
- Cyber Instructor (OPM 712)
- Cyber Defense Analyst (OPM 511)
- Cyber Defense Infrastructure Support Specialist (OPM 521)