# Cybersecurity Experts

## 📞 Contact Details

Cyber Security Experts
📱 Cyber Security Experts
🌐 **Website**: [www.cybersecurity-experts.com]
📧 **Email**: info@cybersecurity-experts.com
📱 **Phone/WhatsApp**: +91 7893512634 (All locations) | +1 6478632478 (Canada)

LinkedIn: https://www.linkedin.com/in/cybersecurity-experts-2b255515a/

**Join our WhatsApp group:** https://chat.whatsapp.com/JbtAsqO9U2T1AXIX2yJ68j

# About Cyber Security Experts

**Cyber Security Experts** is a premier provider of cutting-edge **cybersecurity training and job assistance**, empowering individuals and organizations to stay ahead in an ever-evolving digital threat landscape.

With a strong global presence, we offer world-class training programs that cover essential areas such as **Security Operations (SOC), Threat Hunting, SIEM tools, Cloud Security, Email Security, Vulnerability Management, Incident Response, EDR etc.**

## 🌍 Our Global Reach

We proudly operate across the following countries:

- 🇺🇸 United States
- 🇨🇦 Canada
- 🇬🇧 United Kingdom
- 🇦🇪 United Arab Emirates
- 🇮🇳 India
- 🇦🇺 Australia

## 🎓 What We Offer

- Beginner to Advanced Cybersecurity Trainings
- Customized Corporate Training Solutions
- Hands-on Labs & Real-world Scenarios
- Resume and cover letter preparation
- LinkedIn Profile Optimization
- Interview Preparation & Mock Interviews
- Certifications Guidance (CEH, CompTIA, AZ-500, etc.)
- Job-Oriented Mentorship & Placement Support
- Private support Channel & Community Access

# Cyber Security Training Curriculum

A comprehensive training program covering the foundations of cybersecurity operations, security tools, and practical skills needed for Security Operations Center (SOC) analysts.

## **Module 1:** Foundations of Cybersecurity & SOC Operations

### Cybersecurity Basics

- Definition of cybersecurity and importance
- Basic Network fundamentals
- Threats: malware, phishing, insider threats
- Vulnerabilities: software flaws, misconfigurations
- Risk = Threat x Vulnerability x Impact
- CIA Triad: Confidentiality, Integrity, Availability

### Security Frameworks & Models

- NIST Cybersecurity Framework
- MITRE ATT&CK: tactics, techniques, procedures (TTPs)
- Lockheed Martin Cyber Kill Chain

### SOC Structure

Overview of Tier 1, Tier 2, Tier 3 responsibilities

Typical SOC shift structure and handovers

Incident escalation procedures

Roles: SOC Manager, IR Lead, Threat Hunter, Analyst

### Common SOC Tools

SIEM (Sentinel)

SOAR (Logic Apps)

EDR (Defender for Endpoint)

MDO (Microsoft Defender for Office)

TIP (Threat Intelligence Platforms)

Vulnerability scanners (, Nessus)

IDS/IPS

### Incident Response Lifecycle

Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned

Documentation and evidence handling

### SOC Metrics

SOC Metrics: MTTD, MTTR, Incident Volume, Use Case Effectiveness, False Positive Rate

# **Module 2:** SIEM – Microsoft Sentinel

## Introduction to Microsoft Sentinel

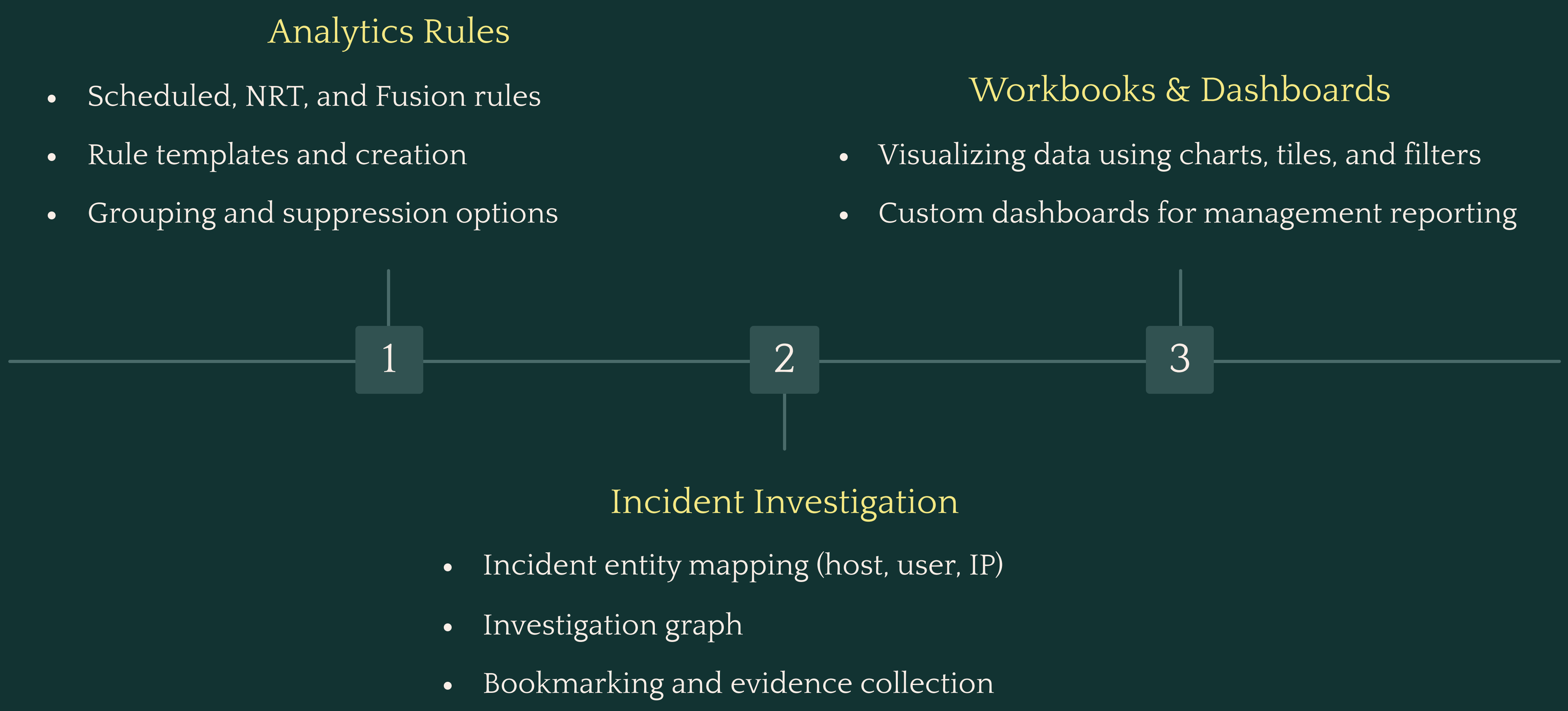
- Cloud-native SIEM benefits
- Sentinel architecture and components
- Comparison with traditional SIEMs

## Data Collection & Connectors

- Built-in connectors: Azure AD, Defender, Office 365, etc.
- Syslog, CEF connectors for third-party tools
- Workspace configuration and data retention

## Log Analytics & KQL

- Tables, columns, and schema understanding
- Filtering, sorting, joins, summarization
- Advanced KQL operators (parse, regex, mv-expand)



### 1 Analytics Rules

- Scheduled, NRT, and Fusion rules
- Rule templates and creation
- Grouping and suppression options

### 2 Incident Investigation

- Incident entity mapping (host, user, IP)
- Investigation graph
- Bookmarking and evidence collection

### 3 Workbooks & Dashboards

- Visualizing data using charts, tiles, and filters
- Custom dashboards for management reporting

## Automation with Playbooks

- Introduction to Logic Apps
- Automating response actions (e.g., disable user, isolate endpoint)
- Using templates and custom connectors

## Threat Intelligence Integration

- Manual and TAXII feed ingestion
- Indicator types (IP, domain, file hash)
- TI matching and alert enrichment

# Module 3:EDR – Microsoft Defender for Endpoint

## Introduction & Architecture

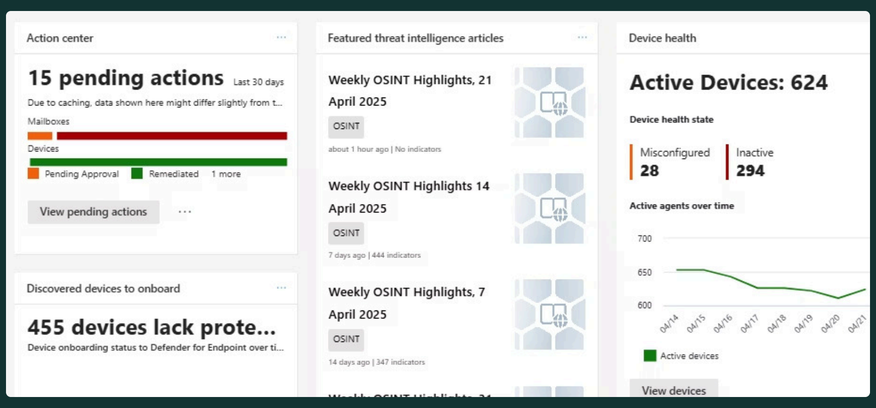
- Defender Sensor overview
- Licensing and integration options

## Device Onboarding

- Onboarding Windows, macOS, Linux systems
- Policy enforcement via Intune or GPO

## Alerts and Incidents

- Alert severity levels
- Alert to incident correlation
- Incident evidence review



Action center

**15 pending actions** Last 30 days

Due to caching, data shown here might differ slightly from t...

Discovered devices to onboard

**455 devices lack prote...**

Device onboarding status to Defender for Endpoint over ti...

Featured threat intelligence articles

Weekly OSINT Highlights, 21 April 2025
OSINT
about 1 hour ago | No indicators

Weekly OSINT Highlights 14 April 2025
OSINT
7 days ago | 444 indicators

Weekly OSINT Highlights, 7 April 2025
OSINT
14 days ago | 347 indicators

Device health

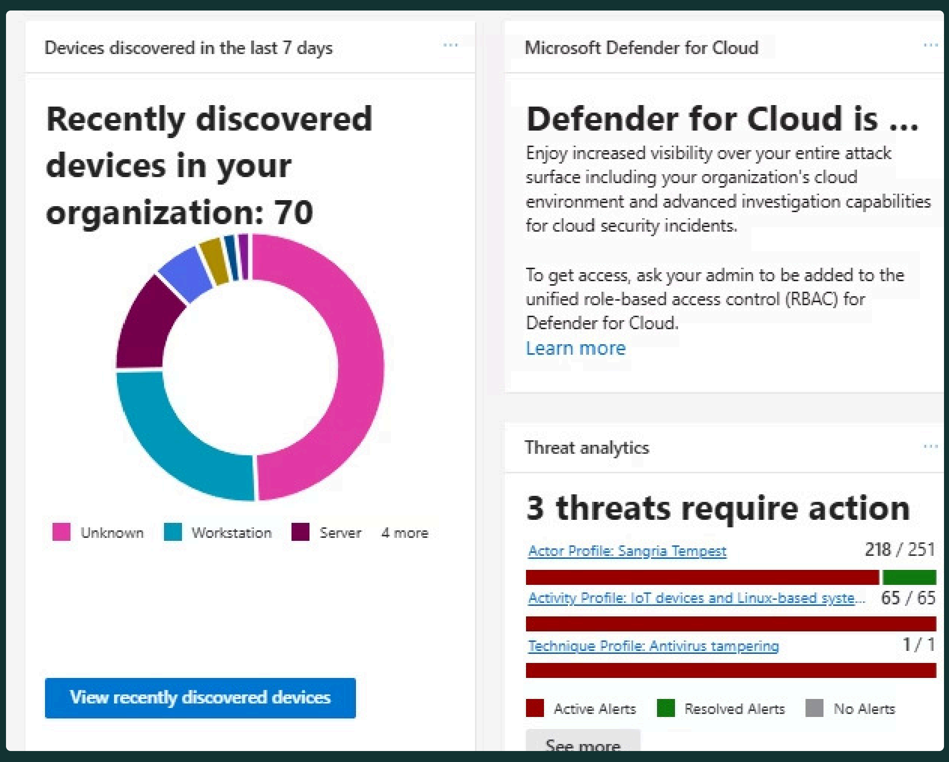
**Active Devices: 624**

Device health state

Misconfigured 28

Inactive 294

Active agents over time



Devices discovered in the last 7 days

**Recently discovered devices in your organization: 70**

Microsoft Defender for Cloud

**Defender for Cloud is ...**

Enjoy increased visibility over your entire attack surface including your organization's cloud environment and advanced investigation capabilities for cloud security incidents.

To get access, ask your admin to be added to the unified role-based access control (RBAC) for Defender for Cloud.

Learn more

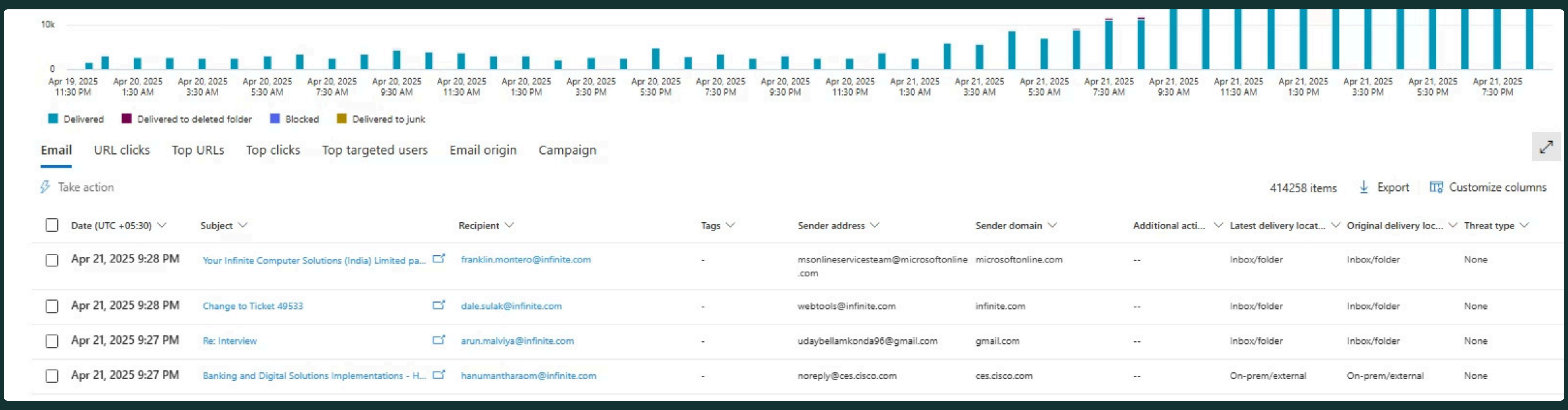
Threat analytics

**3 threats require action**

| | |
|---|---|
| Actor Profile: Sangria Tempest | 218 / 251 |
| Activity Profile: IoT devices and Linux-based syste... | 65 / 65 |
| Technique Profile: Antivirus tampering | 1 / 1 |

| Device Investigation | Response Actions | Advanced Features |
|---|---|---|
| • Timeline analysis<br>• Alert storyline and MITRE mapping<br>• Threat analytics dashboard | • Live Response Shell<br>• File collection, process kill, device isolation | • Attack Surface Reduction (ASR)<br>• Threat & Vulnerability Management (TVM)<br>• Endpoint indicators and exclusions |

# Module 4: Email Security – Microsoft Defender for Office 365



414258 items

| ☐ | Date (UTC +05:30) | Subject | Recipient | Tags | Sender address | Sender domain | Additional acti... | Latest delivery locat... | Original delivery loc... | Threat type |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | Apr 21, 2025 9:28 PM | Your Infinite Computer Solutions (India) Limited pa... | franklin.montero@infinite.com | - | msonlineservicesteam@microsoftonline.com | microsoftonline.com | -- | Inbox/folder | Inbox/folder | None |
| ☐ | Apr 21, 2025 9:28 PM | Change to Ticket 49533 | dale.sulak@infinite.com | - | webtools@infinite.com | infinite.com | -- | Inbox/folder | Inbox/folder | None |
| ☐ | Apr 21, 2025 9:27 PM | Re: Interview | arun.malviya@infinite.com | - | udaybellamkonda96@gmail.com | gmail.com | -- | Inbox/folder | Inbox/folder | None |
| ☐ | Apr 21, 2025 9:27 PM | Banking and Digital Solutions Implementations - H... | hanumantharaom@infinite.com | - | noreply@ces.cisco.com | ces.cisco.com | -- | On-prem/external | On-prem/external | None |

## Email Threat Landscape

- Email-based attacks: phishing, malware, spoofing
- Understanding attack vectors

## Defender for O365 Overview

- Plan 1 vs Plan 2 features
- Architecture and mail flow

## Policy Configuration

- Anti-spam, anti-malware, anti-phishing policies
- Safe Attachments and Safe Links

## Threat Explorer

- Real-time investigation of email threats
- Campaign view and attack patterns

## Attack Simulation Training

- Creating phishing simulations
- Reporting user awareness metrics

# **Module 5:** Identity Protection and Management

## Identity Basics

- Entra ID overview
- Identity lifecycle and management

## Identity Protection Features

- Risky sign-ins, risky users
- Sign-in risk policies

## Conditional Access & MFA

- MFA enforcement
- Blocking high-risk sign-ins
- Policy creation and testing

## Privileged Identity Management

- Just-in-time access
- Role activation and auditing

## Monitoring & Logs

- Sign-in and audit logs
- Integration with Microsoft Sentinel

# Module 6: Vulnerability Management – Nessus

### VM Basics

- Understanding vulnerabilities
- CVSS scoring, CVE references

### Nessus Overview

- Nessus Essentials vs Pro
- Deployment and architecture

### Scan Configuration

- Discovery, full scans, credentialed scans
- Target groups and exclusions

### Report Analysis

- Viewing and exporting scan results
- Prioritization and remediation suggestions

### Integration & Mapping

- Exporting data to SIEM
- Mapping vulnerabilities to MITRE ATT&CK

# **Module 7:** Threat Intelligence & Threat Hunting

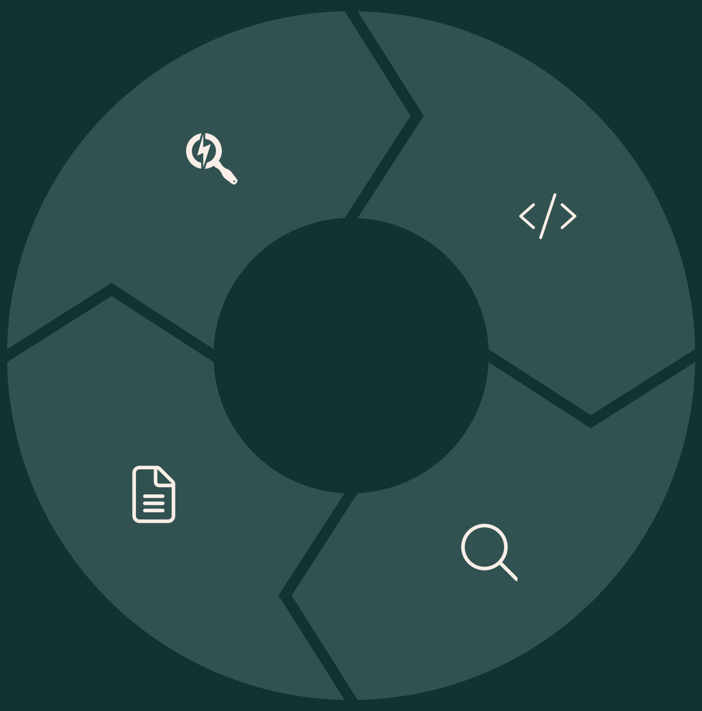
### Threat Intelligence Basics

Strategic, Tactical, Operational, Technical

Types of IoCs

### Sources and Platforms

- OTX, MISP, VirusTotal, MS Defender TI
- STIX/TAXII protocols



### Hypothesis Formation

Develop hunting theories based on threat intelligence and known TTPs

### Query Development

Build custom KQL queries to test hypotheses in Sentinel

### Investigation

Analyze results and perform deeper investigation of findings

### Documentation

Document findings and create hunting playbooks for future use

### Hunting in Sentinel

- Using built-in hunting queries
- Building custom KQL queries
- Bookmarking and investigation chaining

### Dashboard and Documentation

- Creating hunting workbooks
- Reporting and playbook creation

# Module 8: Capstone Project

## Objectives:

- Analyze a simulated incident (Letsdefend.io)
- Use Microsoft Sentinel for detection
- Investigate via Defender for Endpoint and Defender for O365
- Correlate identity logs from Entra ID
- Reference vulnerability data from Nessus
- Perform threat hunting and document findings

## Deliverables:

- Incident timeline
- Technical investigation report
- Remediation plan
- Executive summary

The capstone project brings together all the skills learned throughout the course, allowing students to demonstrate their ability to detect, investigate, and respond to security incidents using the Microsoft security stack and other tools covered in the curriculum.

# Career Opportunities After Completing This SOC Course

### SOC Analyst (Level 1 / Level 2 / Level 3)

**Typical Titles:**

- SOC Analyst – L1 / L2 / L3,
- Cybersecurity Analyst,
- Security Analyst (SOC),
- Security Monitoring Analyst

**Key Skills Covered:**

- Alert triage and investigation (Microsoft Sentinel)
- Endpoint and email threat analysis (Defender suite)
- KQL queries, playbooks, use cases

### Incident Responder

**Typical Titles:**

- Incident Response Analyst,
- Cyber Incident Responder,
- Digital Forensics & IR Analyst (DFIR)

**Key Skills Covered:**

- End-to-end IR lifecycle
- Investigation using Defender for Endpoint and Entra ID,
- Threat intel enrichment and reporting

### Threat Hunter

**Typical Titles:**

- Cyber Threat Hunter
- Threat Detection Engineer
- Threat Research Analyst

**Key Skills Covered:**

- Hypothesis-based threat hunting
- Using KQL in Sentinel
- MITRE ATT&CK mapping
- TI integration

### Email Security Analyst

**Typical Titles:**

- Email Security Analyst
- Messaging Security Analyst
- Microsoft Defender for O365 Specialist

**Key Skills Covered:**

- Phishing detection
- Safe Link/Safe Attachment policies
- Email header analysis and campaign investigation

### Security Engineer / SIEM Engineer

**Typical Titles:**

- SIEM Engineer (Microsoft Sentinel)
- Security Content Developer
- Security Engineer (EDR/SOAR)

**Key Skills Covered:**

- Data connector onboarding
- Analytics rule tuning & dashboarding
- SOAR playbook creation (Logic Apps)

### Identity & Access Analyst

**Typical Titles:**

- IAM Analyst
- Azure AD/Entra Security Analyst
- Identity Protection Specialist

**Key Skills Covered:**

- Risk-based sign-in analysis
- Conditional Access
- MFA
- Entra ID integration and monitoring

### Vulnerability Management Analyst

**Typical Titles:**

- Vulnerability Analyst
- VM & Patch Management Analyst
- Nessus Analyst

**Key Skills Covered:**

- Vulnerability scanning and interpretation
- CVSS scoring, prioritization
- Mapping to SOC incidents and reports

### Cybersecurity Consultant / MSSP Analyst

**Typical Titles:**

- Cybersecurity Consultant
- SOC Analyst – MSSP
- Security Consultant (SIEM/EDR/TI)

**Key Skills Covered:**

- End-to-end SOC service knowledge
- Reporting
- client communication
- Integrating multi-tenant environments