



# Presale1 2025 Courses Syllabuses



# Presale1 2025 Courses Syllabuses

Linux / Mac OS Forensic Investigations ..... 3

Forensic Cloud Investigations ..... 6

Cell Phone Investigations (Android, iOS) ..... 9

Reverse Engineering ..... 12

Strategic Cyber Threat Intelligence (CTI) ..... 15

Threat Hunting ..... 18

Red Team, Pentest - Offensive Security ..... 21

Pentesting for Connected Objects & Supply Chains ..... 24

Cloud Security and DevSecOps Automation ..... 27

Defensible Security Architecture and Engineering ..... 30

Security for Industrial Control Systems (SCADA) ..... 33

CISSP Official course ..... 36

ISO 27001 Lead Auditor ..... 40

Incident response and crisis management ..... 46

Zero Trust Architecture and Implementation Strategies ..... 49

Advanced Malware Analysis and Reverse Engineering ..... 53

Cybersecurity Risk Management and Compliance Essentials ..... 57

Behavioural Analytics and Insider Threat Detection ..... 61

WEBINT Tools, Techniques, and Methodologies ..... 64

Advanced OSINT Course for Identity and Infrastructure Exposure in the SOC World..... 68

SOCAnalyst..... 73

Incident Response..... 77

Osint level 1+2..... 80

Malware Analysis..... 83

Forensics Introduction..... 86

Cybersecurity Risk Management and Compliance Essentials..... 90

Behavioural Analytics and Insider Threat Detection..... 94

WEBINT Tools, Techniques, and Methodologies..... 97





# Presale1 2025 Courses Syllabuses

## Linux / Mac OS Forensic Investigations

### Course Overview

This course provides in-depth knowledge and hands-on experience in conducting forensic investigations on Linux and Mac OS environments. Participants will learn forensic methodologies, tools, and techniques used in cybercrime investigations involving Unix-based systems.

### Duration

24–40 hours

### Pre-requisites

- Basic knowledge of OS architecture

### Target Audience

- Cybersecurity professionals
- Forensic analysts

### Course Modules & Topics

#### Module 1: Introduction to Forensics & OS Fundamentals

- Introduction to Digital Forensics
- Role of forensic investigations in cybersecurity
- Fundamentals of Linux & Mac OS architectures
- File systems overview (Ext4, HFS+, APFS, etc.)
- Boot process & system startup in Unix-based systems



Google Cloud  
Partner







## Module 2: Evidence Acquisition & Chain of Custody

- Legal considerations and forensic best practices
- Chain of custody and evidence preservation
- Imaging and cloning Linux/Mac disks using forensic tools (dd, FTK Imager, Autopsy)
- Live vs. dead box forensics

## Module 3: File System Analysis

- Understanding file metadata and timestamps
- Deleted file recovery and journaling
- Identifying and analyzing hidden files and directories
- Log file forensics (syslog, auth.log, bash history, etc.)

## Module 4: Memory & Process Forensics

- Live memory acquisition (LiME, Volatility)
- Process enumeration and active user analysis
- Detecting malicious processes and rootkits
- Understanding and analyzing memory dumps

## Module 5: User Activity & Artifacts Analysis

- Investigating user accounts and permissions
- Tracking user login history and session data
- Browser forensics: Chrome, Safari, Firefox artifacts
- Analyzing bash history and shell command execution



Google Cloud  
Partner





## Module 6: Network & Log Analysis

- Investigating network logs (iptables, pfSense logs)
- Capturing and analyzing network traffic (Wireshark, tcpdump)
- Identifying remote access and SSH artifacts
- Detecting unauthorized file transfers

## Module 7: Malware & Threat Hunting

- Detecting malware in Linux and Mac OS environments
- Analyzing suspicious binaries using reverse engineering
- Static vs. dynamic malware analysis
- Introduction to YARA rules and forensic scanning

## Module 8: Case Study & Practical Labs

- Hands-on forensic investigation of a compromised Linux/Mac system
- Step-by-step forensic report writing
- Presenting forensic findings and recommendations



Google Cloud  
Partner





# Forensic Cloud Investigations

## Course Overview

This course provides participants with the knowledge and practical skills to conduct forensic investigations in cloud environments. It covers cloud service models, evidence collection techniques, forensic tools, and legal considerations for cloud investigations.

## Duration

8–16 hours

## Pre-requisites

- Familiarity with cloud environments

## Target Audience

- Security analysts
- Cloud administrators
- IT personnel

## Course Modules & Topics

### Module 1: Introduction to Cloud Forensics

- Understanding cloud computing models (IaaS, PaaS, SaaS)
- Cloud service providers (AWS, Azure, Google Cloud)
- Cloud architecture and shared responsibility model
- Challenges in cloud forensic investigations



Google Cloud  
Partner





## Module 2: Legal and Compliance Considerations

- Jurisdiction and data ownership issues
- Cloud provider policies on digital evidence
- GDPR, HIPAA, and other regulatory requirements
- Chain of custody in cloud environments

## Module 3: Data Collection Techniques

- Identifying forensic data sources in the cloud
- Capturing logs and metadata (AWS CloudTrail, Azure Log Analytics, Google Cloud Logging)
- Snapshot and image acquisition (EC2 snapshots, virtual disk imaging)
- API-based forensic evidence extraction

## Module 4: Cloud Log Analysis

- Investigating cloud audit logs for unauthorized access
- Analyzing user activity and privilege escalation attempts
- SIEM integration for cloud security monitoring
- Log correlation and anomaly detection

## Module 5: Network and Storage Forensics

- Capturing and analyzing cloud network traffic
- Investigating S3/GCS/Azure Blob Storage for forensic artifacts
- Identifying unauthorized data exfiltration attempts
- Detecting cloud-based malware and persistence mechanisms



Google Cloud  
Partner





## Module 6: Incident Response in Cloud Environments

- Cloud breach detection and response workflows
- Forensic acquisition of compromised virtual machines
- Analyzing cloud identity and access management (IAM) logs
- Digital evidence preservation best practices

## Module 7: Practical Case Study & Labs

- Investigating a cloud security breach scenario
- Hands-on forensic analysis using AWS, Azure, or GCP tools
- Step-by-step forensic reporting and recommendations



Google Cloud  
Partner







# Cell Phone Investigations (Android, iOS)

## Course Overview

This course focuses on mobile device forensic investigations, covering Android and iOS platforms. Participants will learn methodologies, forensic tools, and best practices to extract, analyze, and interpret digital evidence from mobile devices.

## Duration

8–16 hours

## Pre-requisites

- Understanding of mobile operating systems

## Target Audience

- Forensic analysts
- Digital investigators

## Course Modules & Topics

### Module 1: Introduction to Mobile Forensics

- Overview of mobile forensic investigation processes
- Differences between Android and iOS forensic techniques
- Legal and ethical considerations in mobile forensics
- Understanding data storage and encryption in mobile devices

### Module 2: Mobile Device Acquisition Methods

- Live vs. dead box acquisition
- Logical, physical, and file system extractions



Google Cloud  
Partner





- Imaging techniques for Android & iOS devices
- Data extraction from locked/encrypted devices

### **Module 3: Android Forensic Investigations**

- Android OS architecture and file system structure
- Extracting data from internal storage, SD cards, and cloud backups
- Recovering deleted files, messages, and call logs
- Analyzing SQLite databases and system logs
- Investigating mobile applications (WhatsApp, Telegram, Signal)

### **Module 4: iOS Forensic Investigations**

- iOS security and file system structure (APFS)
- Extracting data from iCloud backups
- Analyzing key iOS artifacts (SMS, contacts, photos, GPS data)
- Investigating Apple Keychain and encrypted databases
- Application analysis (iMessage, FaceTime, social media apps)

### **Module 5: Cloud & Third-Party Data Acquisition**

- Cloud-based forensic acquisition techniques
- Extracting data from Google Drive, iCloud, OneDrive, and other cloud services
- Mobile device sync artifacts and data recovery
- Cross-device evidence correlation

### **Module 6: Malware and Spyware Detection**

- Identifying and analyzing mobile malware
- Investigating spyware and tracking apps



Google Cloud  
Partner





- Detecting unauthorized remote access and exploits
- Sandboxing and behavioral analysis of malicious apps

## **Module 7: Network and Communication Forensics**

- Analyzing mobile network traffic (Wi-Fi, Bluetooth, NFC)
- Investigating VoIP calls and messaging applications
- Recovering deleted chat messages and call logs
- Identifying exfiltration attempts and social engineering attacks

## **Module 8: Case Study & Practical Labs**

- Hands-on forensic investigation of an Android/iOS device
- Step-by-step forensic reporting and evidence presentation
- Best practices in forensic documentation



Google Cloud  
Partner





# Reverse Engineering

## Course Overview

This course covers the fundamental and advanced techniques of reverse engineering software, including malware analysis, software decompilation, and binary exploitation. Participants will learn to analyze software internals, identify vulnerabilities, and dissect malicious code to understand attacker tactics.

## Duration

24–40 hours

## Pre-requisites

- Programming knowledge (C/C++, Assembly)
- Basic malware analysis concepts

## Target Audience

- Cybersecurity engineers
- Malware analysts

## Course Modules & Topics

### Module 1: Introduction to Reverse Engineering

- What is reverse engineering?
- Legal and ethical considerations
- Reverse engineering tools and environments
- Understanding binaries: ELF, PE, Mach-O

### Module 2: Assembly Language Fundamentals



Google Cloud  
Partner







- Basics of x86/x64 architecture
- ARM and RISC-V overview
- Understanding registers, stacks, and memory management
- Disassembling basic programs

### **Module 3: Static Analysis of Executables**

- Using IDA Pro, Ghidra, and Radare2
- Extracting strings and function signatures
- Understanding symbol tables and imports/exports
- Identifying packed and obfuscated binaries

### **Module 4: Dynamic Analysis & Debugging**

- Using GDB, x64dbg, and WinDbg
- Setting breakpoints and stepping through code
- Monitoring process behavior with Sysmon and Process Monitor
- Debugging techniques for malware and software

### **Module 5: Binary Exploitation & Software Cracking**

- Identifying security vulnerabilities in binaries
- Buffer overflows, format string vulnerabilities, and heap exploits
- Bypassing software protections (anti-debugging, anti-reversing)
- Cracking simple software protections (license key bypassing, patching)

### **Module 6: Malware Reverse Engineering**

- Unpacking and de-obfuscating malware
- Analyzing Windows and Linux malware behavior



Google Cloud  
Partner





- Identifying persistence mechanisms and C2 communications
- Case study: Reverse engineering a real-world malware sample

## **Module 7: Network and API Monitoring**

- Monitoring API calls with API Monitor and Process Hacker
- Analyzing network activity of suspicious binaries
- Investigating C2 infrastructure and domain correlations
- Extracting malware configurations from network traffic

## **Module 8: Advanced Reverse Engineering Techniques**

- Automated decompilation and deobfuscation
- Advanced obfuscation and packing techniques
- Understanding firmware and IoT reverse engineering
- Hands-on case studies of advanced reverse engineering challenges

## **Module 9: Case Study & Practical Labs**

- Reverse engineering a ransomware sample
- Identifying vulnerabilities in proprietary software
- Writing custom signatures for detected threats
- Creating detailed forensic reports based on findings



Google Cloud  
Partner





# Strategic Cyber Threat Intelligence (CTI)

## Course Overview

This course provides an in-depth understanding of Cyber Threat Intelligence (CTI) at a strategic level. Participants will learn how to collect, analyze, and operationalize intelligence to improve an organization's security posture, anticipate cyber threats, and enhance decision-making. The course covers intelligence frameworks, adversary profiling, and intelligence-driven defense strategies.

## Duration

24–40 hours

## Pre-requisites

- Basic threat intelligence knowledge

## Target Audience

- Threat intelligence analysts
- SOC analysts
- Security managers

## Course Modules & Topics

### Module 1: Introduction to Cyber Threat Intelligence

- What is CTI? Importance of strategic intelligence
- Differences between strategic, operational, and tactical intelligence
- Threat Intelligence Lifecycle
- Intelligence sources: Open-source, commercial, dark web, HUMINT



Google Cloud  
Partner





## Module 2: Understanding Adversary Tactics & Frameworks

- MITRE ATT&CK and Cyber Kill Chain
- Diamond Model of Intrusion Analysis
- Tactics, Techniques, and Procedures (TTPs)
- Threat actors: Nation-states, cybercriminals, hacktivists

## Module 3: Cyber Threat Intelligence Collection & Analysis

- Data collection techniques and intelligence sources
- OSINT, HUMINT, SIGINT, and technical intelligence
- Processing and filtering raw intelligence
- Pivoting techniques for intelligence enrichment

## Module 4: Intelligence Analysis & Threat Attribution

- Structured analytic techniques (SATs)
- Analyzing malware and infrastructure for attribution
- Threat actor profiling and behavioral analysis
- Case studies of major cyber threat groups (e.g., APT28, FIN7)

## Module 5: Cyber Threat Intelligence Reporting

- Writing intelligence reports for executives vs. technical teams
- Creating intelligence briefings and strategic advisories
- Effective visualization of intelligence data
- Sharing intelligence with ISACs and industry groups



Google Cloud  
Partner







## Module 6: Threat Intelligence Platforms & Automation

- Threat Intelligence Platforms (TIPs) and SIEM integration
- Automating threat intelligence with STIX, TAXII, and MISP
- Correlating threat intelligence with incident response
- Intelligence-driven security operations

## Module 7: Case Study & Practical Labs

- Hands-on OSINT and pivoting exercises
- Analyzing threat actor infrastructure using passive DNS, WHOIS, and VirusTotal
- Generating a strategic threat intelligence report
- Intelligence-sharing exercises using MISP/STIX



Google Cloud  
Partner





# Threat Hunting

## Course Overview

This course equips participants with advanced skills to proactively detect and mitigate cyber threats within an organization's network. It covers methodologies, frameworks, threat hunting techniques, and real-world case studies to enhance security posture through proactive detection and response.

## Duration

16–24 hours

## Pre-requisites

- SOC experience or basic understanding of SIEM and endpoint security
- Familiarity with networking and security concepts

## Target Audience

- SOC analysts
- Incident responders
- Threat hunters
- Security engineers

## Course Modules & Topics

### Module 1: Introduction to Threat Hunting

- What is threat hunting?
- Difference between threat hunting and incident response
- Proactive vs. reactive security models
- Intelligence-driven threat hunting



Google Cloud  
Partner





## Module 2: Threat Hunting Methodologies & Frameworks

- Cyber Kill Chain and MITRE ATT&CK
- Pyramid of Pain and TTP-based hunting
- Hypothesis-driven threat hunting
- Threat Intelligence in threat hunting

## Module 3: Data Sources for Threat Hunting

- Understanding logs and telemetry sources
- Endpoint telemetry: Sysmon, EDR, AV logs
- Network telemetry: NetFlow, Zeek, PCAP analysis
- SIEM and log aggregation (Splunk, ELK, QRadar)

## Module 4: Hunting for Indicators of Compromise (IOCs)

- Understanding IOCs vs. TTPs
- Extracting indicators from logs and forensic artifacts
- Threat intelligence correlation with hunting
- Using YARA for malware detection

## Module 5: Behavioral Analysis & Anomaly Detection

- Baseline network and endpoint behavior
- Identifying lateral movement and privilege escalation
- Hunting for living-off-the-land attacks (LOLBins)
- Detecting persistence mechanisms



Google Cloud  
Partner





## Module 6: Threat Hunting Tools & Techniques

- Querying logs and threat hunting using:
  - o Splunk SPL queries
  - o KQL in Microsoft Sentinel
  - o ELK Stack
- PowerShell and Python for hunting
- Memory forensics with Volatility

## Module 7: Case Study & Hands-on Threat Hunting Labs

- Hunting APT activities using MITRE ATT&CK
- Investigating ransomware infections
- Detecting C2 (Command & Control) beaconing
- Creating and executing custom hunting queries



Google Cloud  
Partner







# Red Team, Pentest - Offensive Security

## Course Overview

This course provides an in-depth understanding of Red Team operations and penetration testing techniques. Participants will learn offensive security methodologies, exploitation tactics, and adversary emulation techniques used to assess and challenge an organization's security defenses.

## Duration

40–80 hours

## Pre-requisites

- Basic knowledge of networking and cybersecurity
- Familiarity with Linux and Windows OS
- Experience with command-line tools (PowerShell, Bash)

## Target Audience

- Penetration testers
- Red team operators
- Ethical hackers
- Security engineers

## Course Modules & Topics

### Module 1: Introduction to Offensive Security

- Understanding Red Team vs. Penetration Testing
- Ethical hacking and legal considerations
- Rules of engagement (ROE) and reporting guidelines
- Offensive security frameworks: MITRE ATT&CK, Cyber Kill Chain



Google Cloud  
Partner





## Module 2: Reconnaissance & OSINT

- Passive vs. active reconnaissance techniques
- Gathering intelligence using OSINT tools (Shodan, Maltego, FOCA)
- DNS enumeration and subdomain discovery
- Identifying open ports and exposed services

## Module 3: Scanning & Enumeration

- Network mapping with Nmap & Masscan
- Identifying vulnerabilities using Nessus & OpenVAS
- SMB and Active Directory enumeration
- Web application enumeration (Burp Suite, dirb, Nikto)

## Module 4: Exploitation & Gaining Access

- Exploiting network vulnerabilities
- Web application attacks (SQL injection, XSS, LFI/RFI)
- Exploiting misconfigurations and weak credentials
- Exploiting Active Directory (Kerberoasting, Pass-the-Hash)

## Module 5: Post-Exploitation & Lateral Movement

- Privilege escalation techniques (Windows & Linux)
- Credential dumping and password cracking (Mimikatz, Hashcat)
- Lateral movement using PsExec, WMI, and BloodHound
- Covering tracks: log manipulation and anti-forensics

## Module 6: Red Teaming & Adversary Simulation

- Planning and executing a Red Team engagement



Google Cloud  
Partner





- Simulating APT tactics using Cobalt Strike & Empire
- Weaponizing payloads and C2 frameworks
- Conducting social engineering and phishing attacks

## **Module 7: Persistence & Evasion Techniques**

- Establishing persistence in compromised systems
- Evasion techniques against EDR & SIEM solutions
- Fileless malware and Living-off-the-Land attacks (LOLBins)
- Anti-virus and firewall bypass techniques

## **Module 8: Reporting & Debriefing**

- Writing effective penetration testing reports
- Communicating findings to technical & executive teams
- Providing remediation recommendations
- Post-engagement debriefing & lessons learned

## **Module 9: Hands-on Labs & Real-World Scenarios**

- Red Team vs. Blue Team engagement in a simulated environment
- Exploiting an Active Directory environment
- Attacking and defending a simulated corporate network
- Web application penetration testing practical labs



Google Cloud  
Partner





# Pentesting for Connected Objects & Supply Chains

## Course Overview

This course provides participants with hands-on experience in penetration testing and security assessment of connected devices (IoT, OT, embedded systems) and supply chain infrastructures. Participants will learn how to identify, exploit, and mitigate vulnerabilities in interconnected systems, firmware, and third-party supply chain dependencies.

## Duration

16-24 hours

## Pre-requisites

- Basic knowledge of networking, cybersecurity, and penetration testing
- Familiarity with IoT/OT security concepts
- Experience with Linux command-line tools

## Target Audience

- Penetration testers
- Red team operators
- Security engineers
- IoT security specialists
- Supply chain risk analysts

## Course Modules & Topics

### Module 1: Introduction to IoT & Supply Chain Security

- Overview of connected objects and IoT ecosystems
- Understanding the attack surface of IoT and supply chain infrastructures



Google Cloud  
Partner







- Security risks in hardware, firmware, software, and communication protocols
- Common vulnerabilities in connected objects and supply chains (OWASP IoT Top 10)

## Module 2: Reconnaissance & Target Enumeration

- Passive vs. active reconnaissance in IoT environments
- Identifying connected devices using Shodan, Censys, and Google Dorks
- Scanning IoT and industrial control system (ICS) networks
- Supply chain risk assessment and third-party vendor security analysis

## Module 3: Firmware Extraction & Analysis

- Introduction to firmware reverse engineering
- Extracting and analyzing firmware using Binwalk, Firmwalker, and QEMU
- Identifying hardcoded credentials and backdoors
- Understanding U-Boot, JTAG, and UART debugging

## Module 4: Exploiting IoT & Embedded Systems

- Common IoT vulnerabilities (default credentials, insecure APIs, weak encryption)
- Exploiting IoT web interfaces and cloud APIs
- Attacking insecure MQTT, CoAP, and Bluetooth Low Energy (BLE) protocols
- Bypassing secure boot and hardware tampering techniques

## Module 5: Wireless & Network Attacks on IoT

- Hacking wireless communication protocols (Wi-Fi, Zigbee, RFID, NFC, LoRaWAN)
- Sniffing and replaying IoT traffic using Wireshark and SDR
- Bluetooth security testing and exploitation (GATT, MITM attacks)
- IoT botnets and Distributed Denial of Service (DDoS) attacks



Google Cloud  
Partner





## Module 6: Supply Chain Attack Vectors

- Understanding software supply chain risks (SolarWinds, Log4j case studies)
- Assessing risks in third-party software and hardware components
- Compromising package managers and code repositories (NPM, PyPI, GitHub)
- Attacking CI/CD pipelines and cloud-based deployments

## Module 7: Red Teaming IoT & Supply Chains

- Simulating attacks on smart cities, healthcare, and industrial environments
- Compromising supply chain dependencies to infiltrate enterprises
- Using C2 frameworks (Cobalt Strike, Empire) for advanced persistence
- Bypassing SIEM and endpoint security detection

## Module 8: Reporting & Mitigation Strategies

- Writing effective security assessment reports
- Supply chain security best practices and frameworks (NIST, ENISA, MITRE)
- Securing connected objects through threat modeling and Zero Trust principles
- Implementing firmware hardening, network segmentation, and monitoring strategies

## Module 9: Hands-on Labs & Real-World Scenarios

- Exploiting a vulnerable IoT ecosystem in a simulated environment
- Reverse engineering and modifying IoT firmware
- Conducting a penetration test on an ICS network
- Performing a Red Team exercise on a supply chain infrastructure



Google Cloud  
Partner





# Cloud Security and DevSecOps Automation

## Course Overview

This course provides an in-depth understanding of securing cloud environments and implementing DevSecOps automation to integrate security into the CI/CD pipeline. Participants will learn cloud security best practices, infrastructure as code (IaC) security, and automated security testing techniques to enhance cloud-native security.

## Duration

24–32 hours

## Pre-requisites

- Basic knowledge of cloud computing (AWS, Azure, or GCP)
- Familiarity with DevOps processes and CI/CD pipelines
- Understanding of networking and security fundamentals

## Target Audience

- Cloud security engineers
- DevSecOps professionals
- Security architects
- DevOps engineers
- IT administrators

## Course Modules & Topics

### Module 1: Introduction to Cloud Security & DevSecOps

- Understanding cloud computing models (IaaS, PaaS, SaaS, FaaS)
- Shared responsibility model in cloud security



Google Cloud  
Partner





- Introduction to DevSecOps: shifting security left
- Key security challenges in cloud-native environments

## **Module 2: Identity & Access Management (IAM) Security**

- Implementing least privilege access in cloud environments
- IAM security best practices for AWS, Azure, and GCP
- Multi-Factor Authentication (MFA) and Just-In-Time (JIT) access controls
- Detecting and mitigating privilege escalation attacks

## **Module 3: Cloud Security Monitoring & Threat Detection**

- Cloud logging and monitoring best practices
- SIEM and threat detection in cloud environments
- Implementing security monitoring using AWS GuardDuty, Azure Security Center, and GCP Security Command Center
- Incident response in cloud environments

## **Module 4: Infrastructure as Code (IaC) Security**

- Introduction to Terraform, CloudFormation, and Ansible
- Secure coding practices for IaC
- Detecting misconfigurations using Checkov and Tfsec
- Automating security compliance in cloud deployments

## **Module 5: Cloud Networking & Security Controls**

- Implementing secure VPC architectures and network segmentation
- Securing cloud APIs and web applications
- Firewalls, security groups, and Zero Trust networking
- Detecting and mitigating DDoS attacks in cloud environments



Google Cloud  
Partner







## Module 6: Container Security & Kubernetes Hardening

- Container security fundamentals: Docker, Kubernetes, OpenShift
- Securing container images and registries (Docker Bench, Clair, Trivy)
- Kubernetes security best practices (RBAC, Pod Security Policies, Network Policies)
- Monitoring and threat detection in Kubernetes environments

## Module 7: CI/CD Security & DevSecOps Automation

- Security integration in the CI/CD pipeline
- Automating security testing with SAST, DAST, and IAST
- Implementing automated security scans using SonarQube, OWASP ZAP, and Snyk
- Enforcing compliance using Open Policy Agent (OPA)

## Module 8: Serverless Security & Cloud Workload Protection

- Securing serverless applications (AWS Lambda, Azure Functions, Google Cloud Functions)
- Detecting and preventing function abuse (event injection, excessive permissions)
- Implementing security monitoring for serverless architectures
- Serverless security tools and best practices

## Module 9: Hands-on Labs & Real-World Scenarios

- Setting up a secure cloud infrastructure using Terraform
- Implementing automated security testing in a CI/CD pipeline
- Detecting and mitigating real-world cloud security threats
- Threat hunting in a Kubernetes environment





# Defensible Security Architecture and Engineering

## Course Overview

This course provides a deep dive into designing and implementing defensible security architectures to protect modern IT infrastructures against cyber threats. It focuses on security engineering principles, Zero Trust architectures, layered defense strategies, and best practices for securing enterprise networks, applications, and cloud environments.

## Duration

32–40 hours

## Pre-requisites

- Basic understanding of networking and cybersecurity concepts
- Familiarity with cloud environments and enterprise security tools
- Experience with security operations or IT infrastructure

## Target Audience

- Security architects
- Security engineers
- SOC analysts
- IT administrators
- CISOs and security managers

## Course Modules & Topics

### Module 1: Foundations of Security Architecture

- Principles of security architecture & engineering
- Designing for security vs. designing for compliance



Google Cloud  
Partner





- Zero Trust security model overview
- Risk-based approach to security design

## **Module 2: Threat Modeling & Attack Surface Reduction**

- Understanding attack surfaces in enterprise environments
- Threat modeling methodologies (STRIDE, PASTA, DREAD)
- Identifying security gaps and attack paths
- Defensible security controls to mitigate common threats

## **Module 3: Network Security Architecture & Segmentation**

- Secure network design principles
- Defense-in-depth & layered security strategies
- Implementing network segmentation (microsegmentation, VLANs, SDP)
- Network security controls (firewalls, IDS/IPS, NAC)

## **Module 4: Endpoint & Identity Security Architecture**

- Endpoint security best practices (EDR, XDR, AV)
- Identity & Access Management (IAM) in security architecture
- Zero Trust Identity (JIT, MFA, Role-Based Access Control)
- Implementing security controls for privileged accounts

## **Module 5: Cloud Security Architecture**

- Designing security in cloud environments (AWS, Azure, GCP)
- Cloud-native security services (CSPM, CIEM, CWPP)
- Hybrid cloud security challenges and solutions
- Implementing Zero Trust in cloud environments



Google Cloud  
Partner





## Module 6: Application Security & Secure Software Architecture

- Secure software development lifecycle (SSDLC)
- Implementing DevSecOps for secure application pipelines
- Web application security principles (OWASP Top 10)
- API security design (OAuth, JWT, API Gateway)

## Module 7: Security Automation & Orchestration

- Implementing Security Orchestration, Automation, and Response (SOAR)
- Automated threat detection and response workflows
- AI/ML in security engineering
- Automating compliance and security baselines

## Module 8: Resilient Security Operations & Monitoring

- Designing a defensible SOC (Security Operations Center)
- Log management and SIEM integration
- Threat intelligence-driven security engineering
- Implementing proactive threat hunting strategies

## Module 9: Case Study & Hands-on Labs

- Designing a secure enterprise architecture for a financial institution
- Implementing a Zero Trust model for a hybrid cloud environment
- Analyzing real-world security breaches and mitigation strategies
- Practical lab exercises using Splunk, Palo Alto, Azure Sentinel, and AWS Security Hub



Google Cloud  
Partner





# Security for Industrial Control Systems (SCADA)

## Course Overview

This course provides participants with an in-depth understanding of Industrial Control System (ICS) and SCADA security, covering risks, attack vectors, and defense strategies. It focuses on protecting critical infrastructure, securing Operational Technology (OT) networks, and responding to cyber threats in industrial environments.

## Duration

16–24 hours

## Pre-requisites

- Basic knowledge of networking and cybersecurity
- Familiarity with industrial control systems or OT environments
- Understanding of risk management in critical infrastructure

## Target Audience

- ICS/SCADA security professionals
- SOC analysts for critical infrastructure
- Industrial automation engineers
- IT/OT security architects
- Incident responders in industrial sectors

## Course Modules & Topics

### Module 1: Introduction to ICS & SCADA Security

- Overview of Industrial Control Systems (ICS) and SCADA
- Differences between IT and OT security



Google Cloud  
Partner







- Common ICS protocols (Modbus, DNP3, OPC, BACnet, Profinet)
- Key ICS threats and vulnerabilities

## **Module 2: ICS/SCADA Risk Assessment & Threat Landscape**

- Top ICS security risks (insider threats, ransomware, nation-state attacks)
- MITRE ATT&CK for ICS and ICS-specific attack techniques
- Real-world case studies (Stuxnet, Triton, Industroyer)
- Identifying threat actors targeting ICS/SCADA

## **Module 3: ICS Network Architecture & Segmentation**

- Designing a secure ICS/SCADA network
- Implementing ISA/IEC 62443 security architecture
- ICS network segmentation using Purdue Model
- Best practices for securing ICS perimeters

## **Module 4: Industrial Protocol Security & Monitoring**

- Securing legacy ICS/SCADA protocols
- Understanding network traffic anomalies in ICS environments
- Threat detection techniques for Modbus, DNP3, OPC-UA
- Implementing ICS-specific IDS/IPS solutions

## **Module 5: Securing Remote Access & ICS Authentication**

- Risks of remote access in ICS environments
- Secure VPN and jump host implementations
- Multi-Factor Authentication (MFA) for ICS operators
- Privileged Access Management (PAM) for SCADA systems



Google Cloud  
Partner





## **Module 6: ICS/SCADA Incident Response & Threat Hunting**

- Developing an ICS-specific incident response plan
- Forensic investigation techniques for SCADA breaches
- Using SIEM & threat intelligence in ICS/OT environments
- Threat hunting methodologies for ICS networks

## **Module 7: Malware & Ransomware in Industrial Environments**

- Understanding ICS-specific malware (Stuxnet, BlackEnergy, Industroyer)
- Detecting and preventing ICS ransomware attacks
- Hardening ICS endpoints & Human-Machine Interfaces (HMIs)
- ICS honeypots and deception techniques

## **Module 8: Compliance & Regulatory Frameworks for ICS**

- Overview of ISA/IEC 62443, NIST 800-82, NERC CIP
- Regulatory requirements for critical infrastructure protection
- Implementing security controls for compliance readiness
- Best practices for ICS governance & risk management

## **Module 9: Case Study & Hands-on Labs**

- Simulating an ICS/SCADA cyber attack & response
- Configuring an ICS honeypot for threat intelligence
- Live packet analysis of SCADA traffic using Wireshark
- Developing an ICS cyber resilience strategy



Google Cloud  
Partner





## CISSP Official course

### Course Overview

The CISSP Official Course prepares participants for the Certified Information Systems Security Professional (CISSP) certification, one of the most recognized cybersecurity certifications worldwide. The course covers the eight domains of the ISC2 Common Body of Knowledge (CBK) and provides hands-on learning, exam strategies, and real-world security applications.

### Duration

50 hours

### Pre-requisites

- Minimum of 5 years of work experience in two or more CISSP domains
- One year can be waived with an approved security certification (Security+, CEH, CISM, etc.)
- No experience requirement for the Associate of (ISC)<sup>2</sup> path

### Target Audience

- Security consultants & managers
- Security auditors & analysts
- Security architects & engineers
- Network architects
- IT/IS directors

### Course Modules & Topics

#### Module 1: Security & Risk Management

- CIA Triad: Confidentiality, Integrity, Availability
- Security governance & compliance frameworks (ISO 27001, NIST, GDPR, HIPAA)



Google Cloud  
Partner





- Legal & regulatory issues in cybersecurity
- Security policies, risk management, and risk assessment
- Professional ethics: (ISC)<sup>2</sup> Code of Ethics
- Security awareness training and security culture

## Module 2: Asset Security

- Data classification & protection (PII, PHI, FCI)
- Data lifecycle management
- Data retention & secure disposal
- Data security controls (encryption, masking, tokenization)
- Cloud security challenges & secure data handling

## Module 3: Security Architecture & Engineering

- Security models & principles (Bell-LaPadula, Biba, Clark-Wilson)
- System security controls & design principles
- Cryptography fundamentals (symmetric vs. asymmetric, hashing, PKI)
- Application security best practices
- Cloud security architecture & virtualization security
- IoT, ICS, and embedded system security

## Module 4: Communication & Network Security

- Network protocols & security mechanisms (TCP/IP, VPNs, TLS, IPSec)
- Wireless security best practices
- Firewall & intrusion detection/prevention systems (IDS/IPS)
- Secure network design (Zero Trust, microsegmentation, SDN security)
- VoIP & telecommunication security



Google Cloud  
Partner







## Module 5: Identity & Access Management (IAM)

- Identification, authentication & authorization mechanisms
- Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Federated Identity Management
- Role-Based Access Control (RBAC) vs. Attribute-Based Access Control (ABAC)
- Biometric authentication & password security best practices
- Privileged Access Management (PAM) & identity governance

## Module 6: Security Assessment & Testing

- Security testing methodologies (pen testing, vulnerability scanning, risk assessments)
- Application security testing (static, dynamic, interactive, fuzz testing)
- Third-party security audits & security control validation
- Log management, SIEM, and continuous monitoring strategies
- SOC & Threat Hunting techniques

## Module 7: Security Operations

- Security operations center (SOC) functions & processes
- Incident response lifecycle & disaster recovery planning
- Forensics investigation techniques & chain of custody
- Patch management, endpoint security, and hardening
- Malware analysis & security automation

## Module 8: Software Development Security

- Secure coding principles (OWASP Top 10, secure SDLC)
- Application threat modeling & secure software design
- CI/CD pipeline security & DevSecOps best practices
- API security & cloud-native application security





- Security testing in Agile & DevOps environments

## **Module 9: Putting it all together**

- How cybersecurity really works
- Implementing the domains together
- CISSP Exam tricks and Tips
- Exam Prep Mastermind
- CISSP Flashcards and quizzes



Google Cloud  
Partner





# Presale1 2025 Courses Syllabuses



## ISO 27001 Lead Auditor

ISO/IEC 27001 Lead Auditor training enables you to develop the necessary expertise to perform an Information Security Management System (ISMS) audit by applying widely recognized audit principles, procedures and techniques.

including the official test costs

40 Hours by Official MASTER Trainer

### Learning objectives

By the end of this training course, the participants will be able to:

Explain the fundamental concepts and principles of an information security management system (ISMS) based on ISO/IEC 27001

Interpret the ISO/IEC 27001 requirements for an ISMS from the perspective of an auditor

Evaluate the ISMS conformity to ISO/IEC 27001 requirements, in accordance with the fundamental audit concepts and principles

Plan, conduct, and close an ISO/IEC 27001 compliance audit, in accordance with ISO/IEC 17021-1 requirements, ISO 19011 guidelines, and other best practices of auditing

Manage an ISO/IEC 27001 audit program

**Domain 1** Fundamental principles and concepts of Information Security Management System (ISMS)

**Domain 2** Information Security Management System (ISMS)

**Domain 3** Fundamental audit concepts and principles



Google Cloud  
Partner



Lead  
Auditor







**Domain 4** Preparation of an ISO/IEC 27001 audit

**Domain 5** Conducting an ISO/IEC 27001 audit

**Domain 6** Closing an ISO/IEC 27001 audit

**Domain 7** Managing an ISO/IEC 27001 audit program

### **Course Description:**

#### **ISO27001 Lead Auditor**

#### **Who should attend?**

- Auditors wishing to carry out and lead information security management system (ISMS) certification audits
- Managers or consultants wishing to master the information security management system audit process
- Individuals responsible for maintaining compliance with information security management system requirements.
- Technical experts wishing to prepare for an information security management system audit.
- Expert consultants in information security management.

#### **Training program Duration: 5 days**

#### **Day 1 Introduction to the Information Security Management System (ISMS) and to ISO/IEC 27001**

- Training objectives and structure
- Standards and regulatory frameworks



Google Cloud  
Partner



Lead  
Auditor





- Certification processes
- Fundamental concepts and principles of information security
- Information security management system (ISMS)

## **Day 2 Audit principles, audit preparation and initiation**

- Audit concepts and fundamentals
- Impact of trends and technology on auditing
- Evidence-based auditing
- Risk-based auditing
- Initiating the audit process
- Stage 1 of the audit

## **Day 3 On-site audit activities**

- Preparing for stage 2 of the audit
- Stage 2 of the audit
- Communication during the audit
- Audit procedures
- Creation of audit test plans

## **Day 4 Closing the audit**

- Drafting of audit findings and non-conformance reports
- Audit documentation and quality review
- Closing the audit
- Auditor's evaluation of action plans
- After the initial audit
- Managing an internal audit program



Google Cloud  
Partner



Lead  
Auditor





- End of training

## Day 5 Certification exam

### Training objectives

On completion of this course, participants will be able to:

- Explain the basic concepts and principles of an information security management system (ISMS) based on ISO 27001
- Interpret ISO 27001 requirements for an ISMS from an auditor's point of view
- Assess the conformity of the ISMS to ISO 27001 requirements, in accordance with fundamental auditing concepts and principles.
- Plan, conduct and close an ISO 27001 compliance audit, in accordance with the requirements of ISO/IEC 17021-1, ISO 19011 guidelines and other good auditing practices.
- Manage an ISO/IEC 27001 audit program

## Exam Duration: 3 hours

The PECB Certified ISO/IEC 27001 Lead Auditor exam fully meets the requirements of the PECB Examination and Certification Program (ECP). The exam covers the following areas of competence:

- Area 1 Fundamental principles and concepts of an information security management system (ISMS)
- Area 2 Information Security Management System (ISMS)
- Area 3 Audit concepts and fundamentals
- Area 4 Preparing for an ISO/IEC 27001 audit
- Area 5 Performing an ISO/IEC 27001 audit
- Area 6 Closing an ISO/IEC 27001 audit
- Area 7 Managing an ISO/IEC 27001 audit program



Google Cloud  
Partner



Lead  
Auditor





## Duration

40 hours

## Prerequisites

A fundamental understanding of ISO/IEC 27001 and comprehensive knowledge of audit principles.

Incident Response and Crisis Management

**REGISTER NOW >>**



Google Cloud  
Partner



Lead  
Auditor







# Incident response and crisis management

## Course Overview

This course provides a comprehensive understanding of incident response (IR) and crisis management, focusing on how to detect, contain, respond to, and recover from cyber incidents. Participants will learn how to build an effective Incident Response Plan (IRP), manage security breaches, and coordinate responses with legal, executive, and technical teams.

## Duration

16–24 hours

## Pre-requisites

- Basic knowledge of cybersecurity fundamentals
- Familiarity with security operations and risk management
- Understanding of compliance and legal aspects of cybersecurity

## Target Audience

- Incident responders
- SOC analysts
- Security managers & CISOs
- IT administrators & security engineers
- Business continuity & crisis management teams

## Course Modules & Topics

### Module 1: Introduction to Incident Response & Crisis Management

- What is Incident Response (IR) and why is it critical?
- The difference between Incident Response vs. Crisis Management



Google Cloud  
Partner





- The impact of cybersecurity incidents on business continuity
- Key stakeholders in crisis management (Legal, PR, IT, Executives)

## **Module 2: Incident Response Lifecycle & Frameworks**

- Understanding the NIST 800-61 Incident Response Lifecycle
- SANS 6-Step Incident Response Model
- Aligning Incident Response with MITRE ATT&CK framework
- IR frameworks used in critical infrastructure & enterprise security

## **Module 3: Incident Detection & Threat Intelligence**

- Identifying indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs)
- Threat intelligence gathering (internal & external sources)
- Using SIEM & EDR/XDR solutions for real-time incident detection
- Threat hunting strategies for proactive incident identification

## **Module 4: Incident Containment & Eradication**

- Steps for containing an active breach (e.g., ransomware, insider threats)
- Isolating infected systems and mitigating lateral movement
- Cloud & network segmentation strategies
- Root cause analysis for long-term remediation

## **Module 5: Digital Forensics & Evidence Collection**

- Chain of custody & legal considerations in forensics
- Collecting and analyzing log data, memory dumps, and network traffic
- Using Volatility, Wireshark, and ELK Stack for forensic analysis
- Reporting forensic findings to executive teams & law enforcement





## **Module 6: Crisis Management & Communication Strategies**

- Creating a Cyber Crisis Communication Plan (CCCP)
- Managing executive & board expectations during a crisis
- Legal & regulatory compliance (GDPR, HIPAA, NIST, PCI-DSS)
- Handling public relations & media response for cybersecurity incidents

## **Module 7: Ransomware & Data Breach Response**

- Best practices for ransomware detection, containment, and recovery
- Handling data exfiltration and data breach disclosures
- Evaluating whether to pay the ransom or not
- Real-world case studies on major ransomware attacks

## **Module 8: Business Continuity & Disaster Recovery (BC/DR)**

- Developing an Incident Response Plan (IRP)
- Disaster Recovery (DR) and Business Continuity Planning (BCP)
- Conducting Tabletop Exercises & War Gaming Scenarios
- Running post-incident reviews & lessons learned sessions

## **Module 9: Hands-On Labs & Simulations**

- Simulated cyber incident response exercise
- Incident handling and escalation simulation
- SIEM-based threat detection & forensic analysis exercise
- Cyber Crisis Management Tabletop Scenario (Red Team vs. Blue Team)



Google Cloud  
Partner





# Zero Trust Architecture and Implementation Strategies

## Course Overview

This course provides participants with a deep understanding of Zero Trust Architecture (ZTA), its guiding principles, and practical implementation strategies for securing enterprise networks, applications, cloud environments, and critical infrastructure. Participants will learn how to design, implement, and operate a Zero Trust Security Model, ensuring continuous verification, least privilege access, and microsegmentation.

## Duration

24–32 hours

## Pre-requisites

- Basic knowledge of networking and cybersecurity
- Familiarity with IAM, cloud security, and endpoint security
- Understanding of risk management & security frameworks

## Target Audience

- Security architects
- Security engineers
- CISOs & IT leaders
- Cloud security professionals







- SOC analysts & identity security specialists

## Course Modules & Topics

### Module 1: Introduction to Zero Trust Architecture

- What is Zero Trust Security, and why does it matter?
- Evolution from perimeter-based security to Zero Trust
- Zero Trust guiding principles:
  - o Never trust, always verify
  - o Least privilege access
  - o Microsegmentation
  - o Assume breach
  - o Continuous monitoring & adaptive security
- Compliance and regulatory frameworks supporting Zero Trust (NIST 800-207, CISA, ISO, PCI-DSS)

### Module 2: Zero Trust Architecture Frameworks

- NIST Zero Trust Architecture (ZTA) model
- Forrester's Zero Trust eXtended (ZTX) framework
- Google's BeyondCorp model
- CISA's Zero Trust Maturity Model
- Core Zero Trust components (Identity, Devices, Networks, Applications, Workloads, Data)

### Module 3: Identity & Access Management (IAM) in Zero Trust

- Zero Trust Identity principles (Strong Authentication, Continuous Verification)
- Implementing Multi-Factor Authentication (MFA) & Adaptive Authentication
- Just-In-Time (JIT) & Just-Enough-Access (JEA) permissions
- Role-Based Access Control (RBAC) vs. Attribute-Based Access Control (ABAC)



Google Cloud  
Partner





- Implementing Privileged Access Management (PAM) in Zero Trust

## **Module 4: Network Security & Microsegmentation**

- Redesigning networks for Zero Trust
- Implementing Software-Defined Perimeter (SDP)
- Microsegmentation & lateral movement prevention
- Network Access Control (NAC) & Zero Trust Network Access (ZTNA)
- Zero Trust in cloud & hybrid environments (AWS, Azure, GCP)

## **Module 5: Endpoint Security & Device Trust**

- Implementing Zero Trust for endpoints (EDR, XDR, MDM)
- Device identity & health verification
- Zero Trust security for remote workforces (VPN alternatives, ZTNA, SASE)
- Securing IoT & OT devices in Zero Trust environments
- Adaptive security policies based on device risk levels

## **Module 6: Application & API Security in Zero Trust**

- Securing cloud-native & on-prem applications
- Zero Trust API security best practices
- Implementing secure software development lifecycle (SSDLC) & DevSecOps in Zero Trust
- Threat modeling for Zero Trust applications
- Case study: Google BeyondProd & securing microservices

## **Module 7: Data Security & Zero Trust Access to Information**

- Data-centric security & Zero Trust data policies
- Implementing data encryption, tokenization, and DLP



Google Cloud  
Partner





- Zero Trust Data Access (ZTDA) strategies
- Behavioral analytics & anomaly detection for data exfiltration
- Insider threat prevention in a Zero Trust environment

## **Module 8: Zero Trust Security Operations & Threat Detection**

- Monitoring & continuous verification
- SOC integration with Zero Trust Security
- Implementing SIEM, SOAR, and UEBA for Zero Trust threat detection
- Zero Trust attack surface reduction strategies
- Incident response in a Zero Trust model

## **Module 9: Zero Trust Implementation Roadmap**

- Step-by-step implementation plan for Zero Trust
- Common challenges & roadblocks in Zero Trust adoption
- Zero Trust maturity model & progress assessment
- Automating Zero Trust security policies
- Best tools & technologies for Zero Trust implementation (Microsoft, Cisco, Palo Alto, Zscaler, CrowdStrike, etc.)

## **Module 10: Hands-On Labs & Real-World Scenarios**

- Designing a Zero Trust architecture for an enterprise
- Microsegmentation & ZTNA deployment in a hybrid cloud
- Configuring identity-based access control in Zero Trust
- Implementing Zero Trust endpoint security & network monitoring
- Simulated Red Team vs. Blue Team Zero Trust attack/defense scenario



Google Cloud  
Partner





# Advanced Malware Analysis and Reverse Engineering

## Course Overview

This course provides an advanced, hands-on deep dive into malware analysis and reverse engineering, focusing on dissecting malicious code, identifying attack techniques, and developing countermeasures. Participants will work with real-world malware samples to enhance their skills in static and dynamic analysis, memory forensics, code deobfuscation, and exploit research.

## Duration

24–40 hours

## Pre-requisites

- Basic understanding of assembly language (x86/x64, ARM)
- Programming skills in C, C++, Python, or scripting
- Experience with Windows/Linux internals and debugging tools
- Familiarity with malware analysis concepts

## Target Audience

- Malware analysts
- Threat intelligence professionals
- Incident responders & forensic analysts
- Reverse engineers & exploit developers
- SOC analysts & cybersecurity engineers

## Course Modules & Topics

### Module 1: Introduction to Malware Analysis & Reverse Engineering

- Types of malware: Trojans, Ransomware, Rootkits, Loaders, Keyloggers



Google Cloud  
Partner







- Understanding the Malware Analysis Lifecycle
- Malware delivery mechanisms (Phishing, Exploit Kits, Drive-by Downloads)
- Setting up a secure analysis lab (VM, Snapshots, Sandboxing)

## Module 2: Static Malware Analysis

- Analyzing PE (Portable Executable) and ELF file structures
- Extracting metadata, headers, and dependencies
- Using strings, imports, and function calls for quick triage
- Identifying packing and obfuscation techniques
- Hands-on Labs:
  - Extracting IOCs from a static malware sample
  - Analyzing PE file structure using PESTudio, CFF Explorer

## Module 3: Dynamic Malware Analysis

- Setting up malware sandboxes (Cuckoo, Any.Run, Hybrid Analysis)
- Monitoring API calls, registry modifications, file system activities
- Debugging malware in Windows/Linux/macOS environments
- Behavior-based detection vs. Signature-based detection
- Hands-on Labs:
  - Running a malware sample in Cuckoo Sandbox
  - Analyzing malware API calls using ProcMon & Process Hacker

## Module 4: Code Reverse Engineering & Disassembly

- Introduction to Assembly Language (x86/x64, ARM)
- Disassembling malware with IDA Pro, Ghidra, Radare2
- Identifying control flow, function calls, and reconstructing logic



Google Cloud  
Partner





- Extracting decryption algorithms, C2 URLs, embedded payloads
- Reverse-engineering a Windows Trojan using IDA Pro
- Extracting encoded strings & C2 communications from malware

## Module 5: Unpacking & Deobfuscation

- Common packers and obfuscation techniques (UPX, Themida, VMProtect)
- Manual unpacking with OllyDbg, x64dbg, PE Explorer
- Extracting shellcode and reconstructing malicious payloads
- Defeating anti-debugging & anti-analysis tricks
- Manually unpacking a packed malware binary
- Bypassing anti-analysis techniques in real malware samples

## Module 6: Advanced Memory Forensics & Rootkit Analysis

- Analyzing malware in memory (Volatility, Rekall, RAM captures)
- Extracting malicious code from process injection & DLL hijacking
- Reverse engineering Rootkits & Bootkits
- Identifying User-mode vs. Kernel-mode malware
- Memory forensics using Volatility
- Dumping malware-injected processes from memory

## Module 7: Malware Communication & Command & Control (C2) Analysis

- Analyzing malware network behavior (HTTP, HTTPS, DNS, SMB)
- Extracting malware configurations from C2 traffic
- Analyzing malicious PowerShell & Macro-based malware
- Bypassing Domain Generation Algorithms (DGA) & encryption
- Intercepting malware traffic with Wireshark & Fiddler
- Analyzing a botnet's C2 infrastructure using passive DNS & VirusTotal



Google Cloud  
Partner





## Module 8: Reverse Engineering Exploits & APT Malware

- Reversing APT malware samples (Lazarus, Sandworm, FIN7)
- Identifying exploit techniques in malware samples
- Dissecting buffer overflow, heap spraying, and ROP chain attacks
- Building and testing custom exploit payloads
- Reversing an APT backdoor using IDA Pro & Ghidra
- Debugging a real-world exploit using x64dbg

## Module 9: Threat Intelligence & Malware Attribution

- Tracking Threat Actor TTPs using MITRE ATT&CK
- Malware family classification & clustering techniques
- Automating malware analysis with YARA, FLARE-VM, and Python scripts
- Writing threat intelligence reports for enterprise security teams
- Creating YARA rules for malware detection
- Classifying malware samples based on TTPs

## Module 10: Hands-on Labs & Real-World Case Studies

- Analyzing a live Ransomware strain (Conti, LockBit, BlackCat)
- Reverse-engineering a Windows Trojan & banking malware sample
- Extracting and decrypting C2 configurations from a RAT sample
- Manually unpacking an obfuscated malware binary
- Simulating real-world malware infection scenarios



Google Cloud  
Partner





# Cybersecurity Risk Management and Compliance Essentials

## Course Overview

This course provides an in-depth understanding of cybersecurity risk management, governance, and compliance, focusing on industry standards, regulatory frameworks, and best practices for securing enterprise environments. Participants will learn how to assess, mitigate, and manage cybersecurity risks while ensuring compliance with legal and regulatory requirements.

## Duration

16–24 hours

## Pre-requisites

- Basic understanding of cybersecurity concepts
- Familiarity with IT governance and risk management principles
- Experience with security frameworks is helpful but not required

## Target Audience

- Security analysts
- Risk managers
- IT compliance officers
- Security consultants
- CISO and IT leadership

## Course Modules & Topics

### Module 1: Introduction to Cybersecurity Risk Management

- What is risk management in cybersecurity?
- Understanding threats, vulnerabilities, and impacts



Google Cloud  
Partner







- Key risk management concepts (risk appetite, risk tolerance, risk mitigation)
- Risk management vs. compliance
- Mapping security controls to business objectives

## Module 2: Cybersecurity Governance & Frameworks

- Overview of governance, risk, and compliance (GRC)
- Key cybersecurity frameworks:
  - NIST Cybersecurity Framework (CSF)
  - ISO/IEC 27001
  - CIS Controls
  - COBIT 5 & 2019
- Aligning cybersecurity with business objectives
- Conducting a cybersecurity governance assessment

## Module 3: Risk Assessment Methodologies

- Risk identification, analysis, and evaluation
- Qualitative vs. quantitative risk assessments
- Conducting Business Impact Analysis (BIA)
- Applying the FAIR (Factor Analysis of Information Risk) model
- Performing a risk assessment on a business system
- Developing risk scenarios and mitigation strategies

## Module 4: Regulatory & Compliance Requirements

- Understanding global compliance regulations:
  - GDPR (General Data Protection Regulation)
  - HIPAA (Health Insurance Portability and Accountability Act)



Google Cloud  
Partner





- o PCI-DSS (Payment Card Industry Data Security Standard)
- o SOX (Sarbanes-Oxley Act)
- o CMMC (Cybersecurity Maturity Model Certification)
- o FISMA (Federal Information Security Management Act)
- Industry-specific cybersecurity compliance
- Mapping compliance frameworks to security controls
- Preparing compliance audit documentation

## **Module 5: Third-Party & Supply Chain Risk Management**

- Identifying and managing third-party risks
- Vendor security assessments and contract requirements
- Supply chain cybersecurity best practices
- Case study: NotPetya attack and supply chain compromise
- Conducting a third-party risk assessment
- Developing vendor security policies

## **Module 6: Cyber Risk Mitigation & Incident Response Planning**

- Risk mitigation strategies and security control selection
- Implementing layered defense strategies
- Cyber incident response planning
- Business Continuity Planning (BCP) and Disaster Recovery (DR)
- Building an incident response plan
- Developing a risk mitigation roadmap

## **Module 7: Security Metrics, Reporting & Risk Communication**

- Cyber risk metrics and Key Performance Indicators (KPIs)





- Creating effective risk reports for executives
- Risk communication strategies for boardrooms
- Case study: Communicating risk in real-world cyber incidents
- Developing a cybersecurity risk dashboard
- Presenting risk findings to executive leadership

### **Module 8: Case Studies & Compliance Simulations**

- Conducting a risk assessment for a financial institution
- Implementing security controls in a healthcare environment
- Preparing a compliance audit report
- Simulating a regulatory compliance audit



# Behavioural Analytics and Insider Threat Detection

## Course Overview

This course provides an in-depth understanding of behavioral analytics and insider threat detection, focusing on user and entity behavior analytics (UEBA), anomaly detection, and techniques for identifying malicious insiders. Participants will learn how to detect early warning signs, prevent insider threats, and develop response strategies using behavioral analysis models and security tools.

## Duration

16–24 hours

## Pre-requisites

- Basic knowledge of cybersecurity fundamentals
- Familiarity with SIEM, logging, and threat intelligence concepts
- Understanding of risk management and user access controls

## Target Audience

- Security analysts
- SOC teams
- Threat intelligence professionals
- Incident responders
- Risk managers & security architects

## Course Modules & Topics

Module 1: Introduction to Behavioral Analytics in Cybersecurity

- Understanding behavioral analytics and anomaly detection
- Differences between signature-based vs. behavior-based detection



Google Cloud  
Partner







- Introduction to User and Entity Behavior Analytics (UEBA)
- Common insider threats: accidental, negligent, and malicious insiders
- Case study: High-profile insider threat incidents

## **Module 2: Insider Threat Landscape & Risk Indicators**

- Categories of insider threats (disgruntled employees, espionage, third-party risks)
- Key risk indicators (KRIs) for insider threats
- Psychological and behavioral triggers for insider activity
- Understanding Data Loss Prevention (DLP) and exfiltration tactics
- Mapping insider threat behaviors to MITRE ATT&CK framework

## **Module 3: UEBA & Machine Learning for Threat Detection**

- How User and Entity Behavior Analytics (UEBA) works
- Machine Learning & AI in insider threat detection
- Identifying anomalies in user behavior (time-based, role-based, device-based)
- Correlating user actions with security events
- Implementing UEBA in SIEM platforms (Splunk, Microsoft Sentinel, IBM QRadar)

## **Module 4: Insider Threat Detection & Prevention Techniques**

- Establishing baselines for normal behavior
- Identifying privilege abuse and unauthorized access attempts
- Monitoring unusual data transfers, file access, and privilege escalation
- Detecting shadow IT, unauthorized software, and rogue devices
- Implementing access control policies & Zero Trust for insider mitigation



Google Cloud  
Partner





## **Module 5: Behavioral Analytics in Cloud & Hybrid Environments**

- Insider threat risks in cloud environments (AWS, Azure, Google Cloud)
- Monitoring SaaS applications & remote work risks
- Detecting malicious behavior in Office 365, Google Workspace, Slack, and Teams
- Investigating insider threats in hybrid and multi-cloud setups

## **Module 6: Investigating & Responding to Insider Threats**

- Developing an Insider Threat Detection Playbook
- Using SIEM, SOAR, and forensic tools for investigations
- Collecting digital evidence and maintaining chain of custody
- Coordinating HR, legal, and executive teams in an insider threat investigation
- Case study: Investigating a data exfiltration incident

## **Module 7: Risk-Based Access Controls & Insider Threat Mitigation**

- Implementing Risk-Based Authentication (RBA) and Adaptive Access Controls
- Least privilege enforcement and Just-in-Time (JIT) access
- Automating alerts for insider threat behaviors in SIEM
- Threat modeling and Red Team vs. Blue Team exercises for insider threat simulations

## **Module 8: Case Studies & Real-World Insider Threat Scenarios**

- Investigating malicious employee activity in a financial institution
- Detecting intellectual property theft in a technology firm
- Monitoring suspicious privileged user behavior in a government agency
- Simulating an insider threat investigation from detection to response



Google Cloud  
Partner





# WEBINT Tools, Techniques, and Methodologies

## Course Overview

This course provides an in-depth exploration of Web Intelligence (WEBINT), focusing on OSINT (Open-Source Intelligence) techniques, online footprint analysis, social media intelligence (SOCMINT), and data extraction methodologies. Participants will learn how to leverage automated tools, scripting, and advanced search techniques to gather actionable intelligence from web sources while maintaining operational security.

## Duration

16–40 hours

## Pre-requisites

- Basic knowledge of internet technologies and cybersecurity
- Familiarity with search engines and social media platforms
- Understanding of data privacy, ethics, and compliance

## Target Audience

- Cyber intelligence analysts
- Investigators & law enforcement professionals
- Red & Blue team members
- Security researchers
- Journalists & ethical hackers

## Course Modules & Topics

### Module 1: Introduction to WEBINT & OSINT

- Definition and importance of Web Intelligence (WEBINT) & OSINT





- Difference between OSINT, SIGINT, HUMINT, and TECHINT
- Legal and ethical considerations in WEBINT investigations
- Understanding the deep web, dark web, and surface web
- Case studies of successful WEBINT operations

## **Module 2: Search Engine Techniques & Online Footprint Analysis**

- Advanced Google Dorking & Boolean search queries
- Extracting intelligence from Bing, Yandex, and other search engines
- Investigating digital footprints & metadata analysis
- Identifying compromised credentials on data breach sites
- Using archive tools (Wayback Machine, Cached Pages) for intelligence gathering

## **Module 3: Social Media Intelligence (SOCMINT)**

- Harvesting data from social media platforms (Facebook, Twitter, Instagram, LinkedIn, TikTok)
- Tracking user behavior, location history, and metadata
- Identifying fake accounts, sock puppets, and bot networks
- Extracting intelligence from Telegram, Discord, and WhatsApp
- Automating social media collection with OSINT tools and Python scripts

## **Module 4: Website & Domain Intelligence Gathering**

- Investigating websites, subdomains, and DNS records
- Using WHOIS, Reverse WHOIS, and passive DNS analysis
- Tracking website hosting, CMS, and technology fingerprints
- Discovering leaked documents and unsecured web resources
- Analyzing robots.txt, sitemap.xml, and web application vulnerabilities



Google Cloud  
Partner







## Module 5: Dark Web & Deep Web Intelligence

- Navigating the dark web using Tor and I2P
- Investigating dark web marketplaces and forums
- Extracting intelligence from onion sites and underground communities
- Identifying dark web threats to organizations
- Monitoring dark web threat actors and leaked credentials

## Module 6: Image & Video Intelligence (IMINT/VidINT)

- Performing reverse image searches (Google, Yandex, TinEye)
- Extracting metadata from images and videos (ExifTool, OSINT Combine, Forensically)
- Identifying geolocation data from images & satellite imagery analysis
- Tracking deepfake content & manipulated media
- Case study: Analyzing a leaked video for source identification

## Module 7: WEBINT Automation & Toolkits

- Overview of OSINT tools and frameworks (SpiderFoot, Maltego, Recon-ng)
- Automating intelligence collection with Python (BeautifulSoup, Scrapy, Tweepy)
- Using Google Colab and Jupyter Notebooks for OSINT automation
- API-based data collection from Shodan, HavelBeenPwned, VirusTotal
- Building custom intelligence dashboards and reporting tools

## Module 8: WEBINT Operational Security (OPSEC) & Counter-OSINT

- Maintaining anonymity while conducting WEBINT investigations
- Using VPNs, proxies, and Tor for operational security
- Identifying tracking techniques used against investigators
- Understanding counter-OSINT techniques used by adversaries



Google Cloud  
Partner





- Practicing safe intelligence gathering techniques in real-world scenarios

## **Module 9: Hands-on Investigations & Case Studies**

- Investigating a target using only open-source intelligence
- Tracking a threat actor across social media & web platforms
- Identifying leaked credentials and compromised business accounts
- Conducting an intelligence assessment on a dark web entity





# Advanced OSINT Course for Identity and Infrastructure Exposure in the SOC World

## OSINT for SOC - Investigating Anonymity and Websites for Threat and Malicious Actor Identification

### Introduction

- Course overview and introduction to the world of intelligence
- Technical collection
- Dorking + examples including an exercise: site: iswnews.com IDF
- Unmasking anonymous users
- Connections between individuals
- Identifying people in organizations (LinkedIn and additional tools)
- Phishing (learning from both attacker and victim perspectives)
- Profiling (intelligence explanation and creating a "Socket Puppet")
- Reports
- Live demonstration of deep investigation
- Summary + bonus

## 1. Introduction to OSINT + Intelligence Collection Cycle

### What is OSINT

- Explanation and reference to basic OSINT course
- Why OSINT is a critical component in SOC
- Legal and ethical principles (what's allowed and what's not)

### Intelligence Collection Cycle

- Planning: setting collection goals
- Collection: resources, tools, and methods
- Processing: filtering and organizing data





- Analysis: understanding patterns and connections
- Dissemination: creating a final report
- Feedback: corrections and continued investigation

### Collection from Open Sources

- OSINT tools like Webmii, dog registry, gov.il databases, certified accountants, lawyers, doctors, and more
- Webmii
- GoogleSearchSocial
- Epieos (Google ID + Maps + Photos)
- GHunt (Google ID + Reviews + Photos + YouTube)
- <https://whatsmyname.app/#>

**Exercise 1 + Bonus:** Accessing darknet leaks with demonstration (usage warning)

## 2. Google Dorking + Image Search

- What is Google Dorking
- Finding sensitive info and hidden pages
- Image-based search

### Tools:

- DorkSearch
- Google, Yandex, TinEye
- ExifTool (metadata checking)

### Examples:

- `site:example.com filetype:pdf`
- `site:example.com inurl:admin`
- `site:iswnnews.com IDF`
- `intitle:"index of"`



Google Cloud  
Partner







### Exercise 2:

- Finding hidden site information using queries
- Dorking + examples including site:iswnnews.com IDF

## 3. Technical Website Information Gathering

- WHOIS and Domains (DomainTools, SecurityTrails, Reverse Whois, CRT.sh)
- DNS and IP checks (nslookup, dig)
- Reverse IP Lookup

### Exercise 3 (Long WhatsApp Exercise)

#### Locating Exposed Files

- Sitemap.xml
- Robots.txt
- ?author=1
- /wp-json/wp/v2/users
- Hidden files (.git, .bak)
- Reference: <https://hacktricks.boititech.com.br/pentesting/pentesting-web/wordpress>

### Exercise 4:

- WordPress site investigation

## 4. Organization Info Gathering and Mapping

- RocketReach
- Hunter.io
- Emailchaser
- TheHarvester
- LinkedIn
- theorg.com



Google Cloud  
Partner





- Maltego (relationship graphs between IPs, emails, names)

### Exercise 5:

- Organization structure and detail completion

## 5. Offensive OSINT

### From the Attacker's Perspective

- Gophish
- SET Toolkit
- Grabify
- IPLogger
- CanaryTokens
- Creating phishing campaigns

### From the Victim's Perspective

- Using Sandbox to avoid infection
- How not to get infected and how to avoid opening phishing links
- Link recognition
- Telegram tools for data extraction

### Exercise 6:

- Creating an IP Grabber
- Unmasking phishing sites and stolen data

## 6. Telegram OSINT + Leaks

- FunStatBot
- Universal Search
- Me Bot / Caller True



Google Cloud  
Partner





- Dehashed, LeakCheck, Pastebin
- That'sThem / PeekYou
- Have I Been Pwned?

## 7. Writing a Professional Intelligence Report

- Report structure
- Key considerations
- Proper data presentation

## 8. Live Demo Work Methodology

- Performing all steps from beginning to final report
- Summary exercise combining everything

## 9. Summary and Bonus

- OSINT investigator golden rules
- Bonus AI websites for OSINT

### Relevant Links:

- <https://whatsmyname.app/#>
- <https://github.com/0x6rss/matkap>
- <https://github.com/mxrch/GHunt>



Google Cloud  
Partner





## SOC Analyst

### 1. Introduction to Windows Environments

- Introduction to virtualization
- VirtualBox Installation
- Virtualization Networking
- Deploy a virtual machine
- Windows Server2016 installation
- Domain Controller
- DC Pre configurations
- AD DS installation on DC
- Windows 10 Client installation
- Virtualization and Windows10 client
- Client domain join
- DHCP Service
- DHCP deployment
- IP ranges
- IP Reservations
- DNS record types
- DNS Zones
- Creating and managing domain users
- Creatubg and managing domain groups
- Creating and managing GPO's

### 2. Fundamentals of Defense

- CIA Triad
- Risk Consideration



Google Cloud  
Partner







- Identity Threats
- Risk Assessment
- Risk Control
- AAA Security
- Hashing
- Cryptography And Encryption
- Web Security
- Malwares

### **3. Introduction to the Attacker's Perspective**

- Layer II cyber attacks
- Layer III cyber attacks
- Various cyber attacks types
- Cyber Kill Chain
- IOC's

### **4. SIEM/SOC Fundamentals**

- Organization Monitoring
- SOC Fundamentals
- The Adaptive Security Architectures
- Cyber Security Components And Vendors
- SIEM Introduction
- Qradar SIEM Introduction
- WinCollect Installation
- Windows Audit





## 5. Qradar SIEM Hands-on

- Qradar Log Activity
- Qradar Log Source
- Qradar Console
- Qradar DSM&Parsing
- Qradar Building Block
- Qradar Rules
- Qradar Reference Lists

## 6. Forensics, Threat intelligence & SOAR

- Qradar Log Activity
- Windows sysinternals
- Windows Sysmon
- Cyber Attack Summary
- Log Analysis
- Threat Intelligence
- SOAR Concept

## 7. SOC Analyst - Labs

- Lab 1:
  - IBM Wincollect Installation On Dedicated Server
- Lab 2:
  - Qradar - Custom Log Activity
- Lab 3:
  - Qradar - Parsing Fields From Payload
- Lab 4:



Google Cloud  
Partner





- o Qradar - Custom Building Block
- Lab 5:
  - o Qradar - Custom Rules
- Lab 6:
  - o Qradar - Reference Lists
- Lab 7:
  - o Sysmon
- Lab 8:
  - o Find The Suspicious Log
- Lab 9:
  - o Threat intelligence With Qradar



Google Cloud  
Partner





# Incident Response

## 1. Attack & Defense Methodolgy

- Introduction
- MITRE ATT&CK
- Cyber Kill Chain
- TACTICS,TECHNIQUES & PROCEDURES
- Incident Response Methodolgy
- Proactive Hunt
- Live Analysis
- IOC's Vs IOA's
- Know Your Process
- Virtualization And Windows10 Lab

## 2. Threats And Scoping

- Host & Network Based Incidents
- Threats Types
- Threat Triage
- Operation System Visibility
- PS Transcription And User SID

## 3. Endpoint Threat Artifacts

- The Sysinternals Suite
- Process Explorer DeepDive
- Persistnce With Autoruns
- Autoruns CommandLine
- Exercise Scenario - Red Line Malware



Google Cloud  
Partner





- Unsigned Binary Detection
- Operation Detection Procmon
- Procmon Beautifier
- Exercise - Njrat
- Network Activity views
- Detect Source Zone Identifier
- System Resource Utilization Monitor
- RDP Cacheing
- ActivitiesCache

#### **4. Windows Logs Analysis**

- Windows Event Logs
- Event Logon Types
- Event Id's
- Event Log's Capabilities Demo
- Investigation Scenario Exercise
- Evtx Over TimeLine Explorer
- Sysmon
- Event Hunting

#### **5. Registry Threat Artifacts**

- Qradar Log Activity
- Registry Structure
- Registry File Acquisition
- Registry Explorer
- Registry Point Of Interest



Google Cloud  
Partner







- Registry ASEPS
- UserAssist
- ShellBags
- SetupApi

## 6. Networking Threat Analysis

- Introduction To Wireshark
- Wireshark Statistics
- DNS Analysis
- DHCP Analysis
- HTTP Analysis
- Attack Scenarios Exercises
- SMB & MS-RPC Analysis
- Attack Scenario Exam

## 7. Evidence Of Execution

- JumpLists
- ShimCache
- AmCache



## Osint level 1+2

### 1. Introduction & Sock Puppets

- OSINT introduction
- Introduction to Sock Puppets
- Sock Puppets
- Creation of a sock puppets

### 2. Different OSINT Artifacts

- Different Artifacts OSINT
- Search Engine OSINT
- Search engines advanced search
- Image OSINT
- Reverse Image Searching
- Viewing EXIF Data
- Physical Location OSINT
- Identifying Geographical Location
- Email OSINT
- Discovering Email Addresses
- Password OSINT
- Hunting Breached Passwords
- Username OSINT
- Hunting Usernames
- Locating social accounts
- People OSINT
- Searching for People
- Hunting Phone Numbers



Google Cloud  
Partner





### 3. Social Media OSINT

- Twitter (X)
- Facebook
- Github
- Instagram
- LinkedIn

### 4. Tech OSINT

- Website OSINT
- Exploring domains
- Business OSINT
- Hunting Business Information
- Wireless OSINT
- Hunting Wifi
- Access points and passwords

### 5. Different OSINT Artifacts

- Working with OSINT Tools
- Image and Location OSINT
- Hunting Emails
- Breached Data
- Username & Account OSINT
- Phone Number OSINT
- OSINT Frameworks
- Writing an OSINT Report



Google Cloud  
Partner





## 6. OSINT Level 2 - Location Detection

- Image Techniques
- Visual Clues
- Video Analysis
- Smart Tools I
- Smart Tools II
- Overview



# Malware Analysis

## 1. Malware Research Introduction

- Course goals
- What is a malware
- What is a malware research
- Importance of research
- Malware types in the wild
- Malware triage

## 2. Malware Lab Environment

- Lab network scope
- Windows 10 lab setup
- Kali Linux lab setup
- Lab optimization
- Flare
- Snapshot Management

## 3. Anatomy of a process

- What is a process
- Virtual Address
- Physical Address
- OS Loader
- Page table
- Las & Pas
- MMU
- PE Structure



Google Cloud  
Partner







- DOS Header
- NT Header
- File Header
- Optional Header
- Sections
- Exe vs DLL
- Export Address table
- Import Address table
- Must know DLL's
- Functions Fuzzing
- Packers
- Hashing & Fingerprinting
- Host based IOC's
- Network Based IOC's
- Sections
- Textual analysis
- Malware Research Demo
- Hands-on Lab

#### 4. Behavior Analysis

- What is dynamic analysis
- Static Analysis
- Network based analysis - DNS
- Wide Protocols
- Data extraction
- Sysinternals



Google Cloud  
Partner





- Registry monitoring
- Persistence hunting
- File system monitoring
- Process operation breakdown
- Process operation post extract
- Hands-on Lab

## 5. Signature based detection

- Introduction to Yara rules
- Yara Rules formats
- Yara rules conditions
- Case sensitive strings
- Yara rules automation
- SSMA
- Hands-on Lab

## 6. Malware Research Project

- Malware Research Reporting
- Malware Labs Project



Google Cloud  
Partner





## Forensics Introduction

### 1. Introduction to Windows Server Environments

- What is virtualization?
- Installing a virtual environment with VBox
- Defining networks in virtualization
- Creating a virtual machine
- Installing Windows Server 2016
- What is a Domain Controller?
- Initial configuration for a DC
- Installing AD DS on a DC
- Installing a Windows 10 client
- Connecting a client to a domain
- Managing and defining GPO
- Creating and managing groups
- Creating and managing users in a domain
- DNS Record Types
- DNS Zones
- Backup policies
- Defining shared folders
- Installing DHCP service
- What is the DHCP service?

### 2. Data and File Storage

- Memory management methods
- Types of memory
- Methods of file storage in the system



Google Cloud  
Partner





- File deletion process
- Files and their uses
- File signatures (Fingerprints)
- File permissions and uses

### **3. ProDiscover - Windows**

- NAT
- SYSLOG
- SSH
- Attacks on files
- Attacks on network services
- Using Access Lists
- Working with Port Security
- How to secure the network

### **4. AutoPsy - Linux**

- Kali Linux Forensics
- Opening a project and case files
- Extracting data from images
- AutoPsy definitions
- AutoPsy results
- Generating a forensic report
- Practice lab



Google Cloud  
Partner





## 5. Memory Forensics - Volatility

- Volatility Intro
- Volatility over Windows
- Volatility over Linux
- Memory analysis
- Practice lab

## 6. Forensics Capabilities

- Email analysis
- File tracking
- Printer forensics
- WiFi profile extraction
- WiFi signal extraction
- Printer signal extraction
- Identifying suspicious files
- Practice lab

## 7. Sysinternals Suite

- Autorun
- Process Monitor
- ProcDump
- PsServices
- RamMap
- RegDelNull
- TCPView
- ProcMon



Google Cloud  
Partner







- PsLoggedOn
- PsList

## 8. OSINT (Open Source Intelligence)

- Maltego
- Shodan
- Google Dorks
- The Harvester
- Whois
- Open Source tools for OSINT



# Cybersecurity Risk Management and Compliance Essentials

## Course Overview

This course provides an in-depth understanding of cybersecurity risk management, governance, and compliance, focusing on industry standards, regulatory frameworks, and best practices for securing enterprise environments. Participants will learn how to assess, mitigate, and manage cybersecurity risks while ensuring compliance with legal and regulatory requirements.

## Duration

24 hours

## Pre-requisites

- Basic understanding of cybersecurity concepts
- Familiarity with IT governance and risk management principles
- Experience with security frameworks is helpful but not required

## Target Audience

- Security analysts
- Risk managers
- IT compliance officers
- Security consultants
- CISO and IT leadership

## Course Modules & Topics

### Module 1: Introduction to Cybersecurity Risk Management

- What is risk management in cybersecurity?
- Understanding threats, vulnerabilities, and impacts



Google Cloud  
Partner





- Key risk management concepts (risk appetite, risk tolerance, risk mitigation)
- Risk management vs. compliance
- Mapping security controls to business objectives

## Module 2: Cybersecurity Governance & Frameworks

- Overview of governance, risk, and compliance (GRC)
- Key cybersecurity frameworks:
  - NIST Cybersecurity Framework (CSF)
  - ISO/IEC 27001
  - CIS Controls
  - COBIT 5 & 2019
- Aligning cybersecurity with business objectives
- Conducting a cybersecurity governance assessment

## Module 3: Risk Assessment Methodologies

- Risk identification, analysis, and evaluation
- Qualitative vs. quantitative risk assessments
- Conducting Business Impact Analysis (BIA)
- Applying the FAIR (Factor Analysis of Information Risk) model
- Performing a risk assessment on a business system
- Developing risk scenarios and mitigation strategies

## Module 4: Regulatory & Compliance Requirements

- Understanding global compliance regulations:
  - GDPR (General Data Protection Regulation)
  - HIPAA (Health Insurance Portability and Accountability Act)



Google Cloud  
Partner





- o PCI-DSS (Payment Card Industry Data Security Standard)
- o SOX (Sarbanes-Oxley Act)
- o CMMC (Cybersecurity Maturity Model Certification)
- o FISMA (Federal Information Security Management Act)
- Industry-specific cybersecurity compliance
- Mapping compliance frameworks to security controls
- Preparing compliance audit documentation

## **Module 5: Third-Party & Supply Chain Risk Management**

- Identifying and managing third-party risks
- Vendor security assessments and contract requirements
- Supply chain cybersecurity best practices
- Case study: NotPetya attack and supply chain compromise
- Conducting a third-party risk assessment
- Developing vendor security policies

## **Module 6: Cyber Risk Mitigation & Incident Response Planning**

- Risk mitigation strategies and security control selection
- Implementing layered defense strategies
- Cyber incident response planning
- Business Continuity Planning (BCP) and Disaster Recovery (DR)
- Building an incident response plan
- Developing a risk mitigation roadmap

## **Module 7: Security Metrics, Reporting & Risk Communication**

- Cyber risk metrics and Key Performance Indicators (KPIs)





- Creating effective risk reports for executives
- Risk communication strategies for boardrooms
- Case study: Communicating risk in real-world cyber incidents
- Developing a cybersecurity risk dashboard
- Presenting risk findings to executive leadership

### **Module 8: Case Studies & Compliance Simulations**

- Conducting a risk assessment for a financial institution
- Implementing security controls in a healthcare environment
- Preparing a compliance audit report
- Simulating a regulatory compliance audit





# Behavioural Analytics and Insider Threat Detection

## Course Overview

This course provides an in-depth understanding of behavioral analytics and insider threat detection, focusing on user and entity behavior analytics (UEBA), anomaly detection, and techniques for identifying malicious insiders. Participants will learn how to detect early warning signs, prevent insider threats, and develop response strategies using behavioral analysis models and security tools.

## Duration

16–24 hours

## Pre-requisites

- Basic knowledge of cybersecurity fundamentals
- Familiarity with SIEM, logging, and threat intelligence concepts
- Understanding of risk management and user access controls

## Target Audience

- Security analysts
- SOC teams
- Threat intelligence professionals
- Incident responders
- Risk managers & security architects

## Course Modules & Topics

### Module 1: Introduction to Behavioral Analytics in Cybersecurity

- Understanding behavioral analytics and anomaly detection
- Differences between signature-based vs. behavior-based detection



Google Cloud  
Partner





- Introduction to User and Entity Behavior Analytics (UEBA)
- Common insider threats: accidental, negligent, and malicious insiders
- Case study: High-profile insider threat incidents

## **Module 2: Insider Threat Landscape & Risk Indicators**

- Categories of insider threats (disgruntled employees, espionage, third-party risks)
- Key risk indicators (KRIs) for insider threats
- Psychological and behavioral triggers for insider activity
- Understanding Data Loss Prevention (DLP) and exfiltration tactics
- Mapping insider threat behaviors to MITRE ATT&CK framework

## **Module 3: UEBA & Machine Learning for Threat Detection**

- How User and Entity Behavior Analytics (UEBA) works
- Machine Learning & AI in insider threat detection
- Identifying anomalies in user behavior (time-based, role-based, device-based)
- Correlating user actions with security events
- Implementing UEBA in SIEM platforms (Splunk, Microsoft Sentinel, IBM QRadar)

## **Module 4: Insider Threat Detection & Prevention Techniques**

- Establishing baselines for normal behavior
- Identifying privilege abuse and unauthorized access attempts
- Monitoring unusual data transfers, file access, and privilege escalation
- Detecting shadow IT, unauthorized software, and rogue devices
- Implementing access control policies & Zero Trust for insider mitigation



Google Cloud  
Partner





## **Module 5: Behavioral Analytics in Cloud & Hybrid Environments**

- Insider threat risks in cloud environments (AWS, Azure, Google Cloud)
- Monitoring SaaS applications & remote work risks
- Detecting malicious behavior in Office 365, Google Workspace, Slack, and Teams
- Investigating insider threats in hybrid and multi-cloud setups

## **Module 6: Investigating & Responding to Insider Threats**

- Developing an Insider Threat Detection Playbook
- Using SIEM, SOAR, and forensic tools for investigations
- Collecting digital evidence and maintaining chain of custody
- Coordinating HR, legal, and executive teams in an insider threat investigation
- Case study: Investigating a data exfiltration incident

## **Module 7: Risk-Based Access Controls & Insider Threat Mitigation**

- Implementing Risk-Based Authentication (RBA) and Adaptive Access Controls
- Least privilege enforcement and Just-in-Time (JIT) access
- Automating alerts for insider threat behaviors in SIEM
- Threat modeling and Red Team vs. Blue Team exercises for insider threat simulations

## **Module 8: Case Studies & Real-World Insider Threat Scenarios**

- Investigating malicious employee activity in a financial institution
- Detecting intellectual property theft in a technology firm
- Monitoring suspicious privileged user behavior in a government agency
- Simulating an insider threat investigation from detection to response



Google Cloud  
Partner





# WEBINT Tools, Techniques, and Methodologies

## Course Overview

This course provides an in-depth exploration of Web Intelligence (WEBINT), focusing on OSINT (Open-Source Intelligence) techniques, online footprint analysis, social media intelligence (SOCMINT), and data extraction methodologies. Participants will learn how to leverage automated tools, scripting, and advanced search techniques to gather actionable intelligence from web sources while maintaining operational security.

## Duration

16–40 hours

## Pre-requisites

- Basic knowledge of internet technologies and cybersecurity
- Familiarity with search engines and social media platforms
- Understanding of data privacy, ethics, and compliance

## Target Audience

- Cyber intelligence analysts
- Investigators & law enforcement professionals
- Red & Blue team members
- Security researchers
- Journalists & ethical hackers

## Course Modules & Topics

Module 1: Introduction to WEBINT & OSINT

- Definition and importance of Web Intelligence (WEBINT) & OSINT



Google Cloud  
Partner







- Difference between OSINT, SIGINT, HUMINT, and TECHINT
- Legal and ethical considerations in WEBINT investigations
- Understanding the deep web, dark web, and surface web
- Case studies of successful WEBINT operations

## **Module 2: Search Engine Techniques & Online Footprint Analysis**

- Advanced Google Dorking & Boolean search queries
- Extracting intelligence from Bing, Yandex, and other search engines
- Investigating digital footprints & metadata analysis
- Identifying compromised credentials on data breach sites
- Using archive tools (Wayback Machine, Cached Pages) for intelligence gathering

## **Module 3: Social Media Intelligence (SOCMINT)**

- Harvesting data from social media platforms (Facebook, Twitter, Instagram, LinkedIn, TikTok)
- Tracking user behavior, location history, and metadata
- Identifying fake accounts, sock puppets, and bot networks
- Extracting intelligence from Telegram, Discord, and WhatsApp
- Automating social media collection with OSINT tools and Python scripts

## **Module 4: Website & Domain Intelligence Gathering**

- Investigating websites, subdomains, and DNS records
- Using WHOIS, Reverse WHOIS, and passive DNS analysis
- Tracking website hosting, CMS, and technology fingerprints
- Discovering leaked documents and unsecured web resources
- Analyzing robots.txt, sitemap.xml, and web application vulnerabilities



Google Cloud  
Partner







## Module 5: Dark Web & Deep Web Intelligence

- Navigating the dark web using Tor and I2P
- Investigating dark web marketplaces and forums
- Extracting intelligence from onion sites and underground communities
- Identifying dark web threats to organizations
- Monitoring dark web threat actors and leaked credentials

## Module 6: Image & Video Intelligence (IMINT/VidINT)

- Performing reverse image searches (Google, Yandex, TinEye)
- Extracting metadata from images and videos (ExifTool, OSINT Combine, Forensically)
- Identifying geolocation data from images & satellite imagery analysis
- Tracking deepfake content & manipulated media
- Case study: Analyzing a leaked video for source identification

## Module 7: WEBINT Automation & Toolkits

- Overview of OSINT tools and frameworks (SpiderFoot, Maltego, Recon-ng)
- Automating intelligence collection with Python (BeautifulSoup, Scrapy, Tweepy)
- Using Google Colab and Jupyter Notebooks for OSINT automation
- API-based data collection from Shodan, HavelBeenPwned, VirusTotal
- Building custom intelligence dashboards and reporting tools

## Module 8: WEBINT Operational Security (OPSEC) & Counter-OSINT

- Maintaining anonymity while conducting WEBINT investigations
- Using VPNs, proxies, and Tor for operational security
- Identifying tracking techniques used against investigators
- Understanding counter-OSINT techniques used by adversaries



Google Cloud  
Partner





- Practicing safe intelligence gathering techniques in real-world scenarios

## Module 9: Hands-on Investigations & Case Studies

- Investigating a target using only open-source intelligence
- Tracking a threat actor across social media & web platforms
- Identifying leaked credentials and compromised business accounts
- Conducting an intelligence assessment on a dark web entity

### Regards,

Eyal Weintraub - Founder C.E.O.

Eyalw@presale1.com

Mobile: +972-54-7772373 - Office: +972-3-6989371

Main Office: Tel Aviv, Israel | Florida, USA



Google Cloud  
Partner

