Training Catalog

SecureFlag

Lab Technologies

- Java
- Java / Spring Boot
- Java / Spring Boot 3
- C#
- .NET
- .NET / ASP.NET
- Python
- Python / Flask
- Python / FastAPI
- Python / Django
- NodeJS
- NodeJS / JavaScript
- NodeJS / TypeScript
- PHP
- PHP / Symfony
- PHP / Laravel
- Frontend
- Frontend / Angular
- Frontend / React
- Frontend / Vue.js
- Kotlin
- Kotlin / Spring Boot
- Pseudocode
- Scala
- Scala / Play
- Ruby
- Ruby / Rails
- Ruby / Sinatra
- Android
- Android / React Native
- Android / Kotlin
- Android / Java
- Android / Flutter
- C
- C++
- iOS
- iOS / Swift
- iOS / Objective-C
- AI/LLM
- Docker
- Kubernetes
- Kubernetes / Gatekeeper
- Kubernetes / Prometheus
- AWS
- AWS / Terraform
- AWS / CloudFormation
- Azure / Terraform
- Azure / Bicep
- Azure / Resource Manager
- COBOL
- Threat Modeling
- QA Security Testing
- QA Security Testing / Selenium
- QA Security Testing / Python
- QA Security Testing / Postman
- GoLang
- Smart Contracts
- Smart Contracts / Solidity
- Exploitation for Developers
- CI/CD
- CI/CD / Jenkins
- CI/CD / GitLab
- SQL
- SQL / MySQL
- SQL / PL/SQL
- SQL / T-SQL
- SQL / PostgreSQL
- Server Hardening
- Server Hardening / Linux
- Server Hardening / Web
- Server Hardening / Database
- Server Hardening / Java
- Rust
- Haskell
- ABAP
- Apex
- Security Awareness
- Automotive

- AI/LLM / Prompt Injection
- AI/LLM / Langchain
- Log Analysis for SOC Analysts*
- OT / SCADA
- OT / SCADA / C++
- Embedded Linux
- Embedded Linux / Yocto
- Automotive / Yocto
- Automotive / C++
- Automotive / Python
- Automotive / CAN
- Automotive / OTA Updates

Learning Paths

- Java / OWASP Top 10
- Java / OWASP API Security Top 10
- Java / PCI DSS
- Java / OWASP Application Security Verification Standard (ASVS)
- Java / Intermediate and Advanced Secure Coding
- Java / Cryptography
- Java / Secure Authentication
- Java / Injections
- .NET with C# / OWASP Top 10
- .NET with C# / OWASP API Security Top 10
- .NET with C# / PCI DSS
- .NET with C# / OWASP Application Security Verification Standard (ASVS)
- .NET with C# / Cryptography
- .NET with C# / Secure Authentication
- .NET with C# / Intermediate and Advanced Secure Coding
- Python / OWASP Top 10
- Python / OWASP API Security Top 10
- Python / PCI DSS
- Python / OWASP Application Security Verification Standard (ASVS)
- Python / Intermediate and Advanced Secure Coding
- Python / Cryptography
- Python / Injections
- PHP / OWASP Top 10
- PHP / OWASP API Security Top 10
- PHP / PCI DSS
- PHP / Secure Authentication
- PHP / Intermediate and Advanced Secure Coding
- NodeJS with JavaScript / OWASP Top 10
- NodeJS with JavaScript / OWASP API Security Top 10
- NodeJS with JavaScript / PCI DSS
- NodeJS with JavaScript / Intermediate and Advanced Secure Coding
- NodeJS with JavaScript / Injections
- NodeJS with TypeScript / OWASP Top 10
- NodeJS with TypeScript / PCI DSS
- Frontend / Beginner, Intermediate, and Advanced Secure Coding
- Frontend / Implementing Content Security Policy (CSP) Mitigation
- Kotlin / OWASP Top 10
- Kotlin / OWASP API Security Top 10
- Kotlin / PCI DSS
- Kotlin / Intermediate and Advanced Secure Coding
- Pseudocode / Introductory and Intermediate Secure Coding
- Pseudocode / Injections
- Scala / OWASP Top 10
- Scala / PCI DSS
- Scala / Intermediate and Advanced Secure Coding
- Scala / Injections
- Ruby / OWASP Top 10
- Ruby / OWASP API Security Top 10
- Ruby / PCI DSS
- Ruby / Intermediate and Advanced
- Android / OWASP Mobile Top 10
- Android / PCI DSS
- Android / Intermediate Secure Coding
- C / Introductory, Beginner, and Advanced Secure Coding
- C++ / Introductory, Beginner, and Advanced Secure Coding
- SDLC Security / Core Concepts
- SDLC Security / Secure Software Requirements
- SDLC Security / Secure Software Design

- SDLC Security / Secure Software Implementation
- SDLC Security / Secure Software Testing
- SDLC Security / Secure Software Acceptance
- Security Awareness / Securing Your Organization
- Security Awareness / Staying Safe Online
- Security Awareness / Team Manager's Guide
- iOS / OWASP Mobile Top 10
- iOS / Intermediate and Advanced Secure Coding
- SOC Analyst / Introduction to Binary Analysis*
- SOC Analyst / Introduction to Container Threat Detection*
- SOC Analyst / Introduction to Malware Analysis*
- SOC Analyst / Introduction to security prevention and response fundamentals*
- SOC Analyst / Detection of MITRE ATT&CK most used techniques*
- SOC Analyst / Improve Base Detection Capabilities on SIEM and Endpoints
- SOC Analyst / Introduction to Cyber Threat Intelligence*
- Docker / Introductory and Intermediate Secure DevOps
- Kubernetes / Introductory, Intermediate, and Advanced Secure DevOps
- AWS / Introductory, Intermediate, and Advanced Security
- AWS / PCI DSS
- Azure / Introductory, Intermediate, and Advanced Security
- Azure / PCI DSS
- COBOL / Introductory, Intermediate, and Advanced Secure Coding
- Threat Modeling / Introductory, Intermediate, and Advanced Modeling
- Threat Modeling / PCI DSS
- Threat Modeling / Cloud Modeling
- QA Security Testing / Introductory, Intermediate, and Advanced Regression Test Writing
- SDLC Security / Secure Software Operations
- SDLC Security / Supply Chain and Software Acquisition
- SDLC Security / Secure SDLC Essentials
- Go Lang / OWASP Top 10
- Go Lang / OWASP Top 10
- Go Lang / OWASP API Security Top 10
- Go Lang / PCI DSS
- Go Lang / Intermediate and Advanced
- AI LLM / OWASP Top 10 for Large Language Model Applications
- AI LLM / Prompt Injection Attacks
- Smart Contracts / Introductory, Intermediate, and Advanced Secure Coding
- Exploitation / Introductory, Intermediate, and Advanced Offensive Web Security for Developers
- CI/CD / OWASP TOP 10 CI/CD Security Risks
- CI/CD / Introductory and Intermediate Secure Configuration
- SQL / Introductory, Intermediate, and Advanced Secure Coding
- Server Hardening / Introductory, Intermediate, and Advanced Server Hardening for Sysadmins
- Server Hardening / Protecting Network Services
- Server Hardening / Securing Servers From Privilege Escalation
- Haskell / OWASP Top 10

- ABAP / Introductory, Beginner, and Advanced Secure Coding
- ABAP / Injections
- ABAP / Secure Authorization
- Apex / Introductory and Intermediate Secure Coding
- Security Awareness / Program Manager's Guide
- Security Awareness / Protecting Your Corporate Assets
- Security Awareness / Uncovering Digital Frauds
- Security Awareness / Web Security with OWASP Top 10

Secure Coding Labs Topics

Audience: Frontend Developers, Backend Developers, API Developers, and QA Engineers.

- Abrupt Termination
- Arbitrary File Access
- Arbitrary File Deletion
- Arbitrary File Download
- Arbitrary File Upload
- Archive Upload Allows Arbitrary File Overwrite
- Argument Injection
- Authentication Bypass
- Authorization Bypass
- Blind SQL Injection
- Broken Authentication
- Broken Authorization
- Broken Input Validation
- Broken JSON Web Token
- Broken Memory Management
- Broken OAuth
- Broken Regular Expression Results
- Broken Session Management
- Buffer Overflow
- Business Logic Bypass
- Bypass IP-Based Access Control
- Clickjacking
- Code Injection
- Compromised Passwords Permitted
- Credentials in GET Request
- Cross-Site Request Forgery
- Cross-Site Scripting
- Cross-Site WebSocket Hijacking
- CSS Injection
- Dangerous Open Redirect
- Directory Traversal
- Document Upload
- DOM Cross-Site Scripting
- Double Free
- Double Free
- Excessive Data Exposure
- Exposed Elasticsearch
- Exposed H2 Console
- Exposed JWT Generation
- Exposed Padding Validation
- Exposed Sensitive Folder
- Exposed Spring Boot Actuators
- File Inclusion
- Format String Injection
- Hardcoded Cloud Credentials
- Hardcoded JWT Secret
- Heap Overflow
- HTTP Response Splitting
- Inadequate Content Security Policy for CSS
- Inadequate Content Security Policy for HTML Objects
- Inadequate Reporting for Content Security Policy Violations
- Incomplete Admin Authorization Control
- Incorrect Access-Control Headers
- Incorrect Content Security Policy
- Incorrect CORS Headers
- Incorrect Referrer Policy
- Insecure Debug Functionality Exposed
- Insecure Design
- Insecure Direct Object Reference
- Insecure Functionality Exposed
- Insecure Password Hashing Storage
- Insufficient Input Validation
- Insufficient Logging
- Insufficient postMessage Origin Check
- Insufficient Protection Against Denial of Service (DoS) Attacks
- Insufficient Transport Layer Security
- Integer Overflow
- Invalidated Iterator
- JWT "None" Algorithm Permitted
- JWT Expiry Not Checked

- JWT Signature Not Verified
- Lack of Cloud-based Logging
- Lack of Content-Type Headers
- Lack of HTML Link Security Attributes
- Lack of Jailbreak/Root Check
- Lack of Resources and Rate Limiting
- Lack of Sanitization
- Lack of Secret Management Service
- Lack of Server-side Checks
- Lack of Subresource Integrity Check
- Lack of Transport Layer Security (TLS/SSL)
- Leftover Debug Functionality Exposed
- Local File Inclusion
- Log Injection
- Mass Assignment
- Memory Leak
- Mismatched Deallocation
- Missing Anti-Brute Force Protection
- Missing Cloud-based Authentication
- Missing Common Passwords Check
- Missing Server Side Encryption
- Missing Weak Passwords Check
- Non-const String Literals
- NoSQL Injection On DynamoDB
- NoSQL Injection On ElasticSearch
- NoSQL Injection On MongoDB
- NULL Pointer Dereference
- OAuth Account Impersonation
- OAuth Client Secret Disclosure
- OAuth Cookie Stealing
- OAuth Phishing
- Open Redirect
- ORM Leak
- OS Command Injection
- Outdated Dependency Package
- Padding Oracle
- Parameter Tampering
- Parameter Tampering
- Password Hash Disclosure
- Path Traversal
- Path Traversal Attack On Cloud Bucket
- PCI Compliance Violation
- PII Exposure
- Privilege Escalation
- Prototype Pollution
- Race Condition
- Reflected Cross-Site Scripting
- Remote Code Execution
- Remote File Inclusion
- Reused IV-Key Pair
- Reused JWT Secret
- Reused Secret
- Security Misconfiguration
- Sensitive Information Disclosure
- Server Side Template Injection
- Server-Side Request Forgery
- Server-Side Request Forgery
- Server-Side Template Injection
- Session Fixation
- Session Not Invalidated
- SQL Injection
- Stack Overflow Using gets
- Stack Overflow Using Sprintf
- Stack Overflow When Reading Into a Char Array
- Stack Trace Disclosure upon Server Error
- Stored Cross-Site Scripting
- String Truncation
- Supply Chain Attack
- Type Juggling
- UI Redressing
- Unauthenticated Account Enumeration
- Unauthorized Access to Admin Panel
- Unchecked Origin in postMessage
- Unchecked postMessage Origin
- Unfinished Account Lockout
- Unprotected Access to Message Board
- Unrestricted File Download
- Unrestricted File Read
- Unrestricted File Upload
- Unsafe Deserialization
- Use After Free
- Use of Dangerous Functionality

- User Not Reauthenticated
- Vulnerable Dependency Package
- Weak Cipher
- Weak Cipher Mode
- Weak Hashing Algorithm
- Weak Password Policy
- XML Entity Expansion
- Zip Slip Attacks
- Logic Bugs

DevOps Labs Topics

Audience: DevOps Engineers, System Administrators, Platform Engineers, Kubernetes Engineers, Docker Engineers, and CI/CD Engineers

Server Hardening

- Argument Injection
- Exposed Database
- Exposed JDWP Debug Server
- Exposed JMX Debug Server
- Exposed MQTT Server
- Exposed Port
- Exposed Redis Database
- Frontjacking
- Implanted Backdoor
- Insecure MySQL Remote Access
- Insecure Path
- Insecure Settings
- Lack of TLS Client Authentication
- Lack of Transport Layer Security
- Logging Setting Leading to Information Disclosure
- Misconfiguration That Allows Password Transmission
- Misconfiguration That Allows Remote Access
- Misconfigured Nginx Root Location
- Off-By-Slash Misconfiguration
- Permissive MySQL Privileges Lead to Arbitrary File Write
- Permissive MySQL Privileges Lead to Password Hash Disclosure
- Permissive MySQL Remote Access
- Poor IP-Based Remote Access Control
- Privilege Escalation
- Race Condition
- Readable Credential File
- Sudo-Enabled Monitoring Tool
- SUID Interpreter
- SUID With Path Manipulation
- Unencrypted File Transfer Service
- Use of Nginx $uri
- Use of Weak Ciphers
- Use of Weak SSL Protocols
- Weak Redis Password
- Weak Users Configuration
- Writable Cron Script
- Writable Home Directory
- Writable System File
- Headers Injection

Kubernetes

- Blocking Wildcard Ingress Using Gatekeeper
- Broken Authentication
- Broken Authorization
- Enforcing Resource Limits
- Etcd's Certificates Disclosure
- Exposed Docker Socket
- Exposed Internal Service
- Exposed Kubelet Read-Only Port
- Exposed Secrets File
- Improper Use of Namespaces
- Insecure Functionality Exposed
- Networks
- Permissive RBAC
- Publicly Exposed Kubectl Proxy
- RBAC Misconfiguration Allows Anonymous Secrets Access
- Sensitive Information Disclosure
- Supply Chain Security
- Unrestricted Access to Kubelet API
- Use of Dangerous Functionality
-

- Using Gatekeeper to Block Untrusted Image Repos
- Writing Basic Ingress Rules With Prometheus

Docker

- Container Breakout
- Exposed Docker Port
- Exposed Service Port
- Hardcoded Secrets at Build Time
- Insecure File Inclusion
- Insecure Functionality Exposed
- Privilege Escalation
- Rogue NTP Server Allows Sandbox Breakout
- Secret Disclosure
- Secrets Disclosure
- Secrets Exposure
- Sensitive Information Disclosure
- Unrestricted User Privileges

CI/CD

- Broken Authentication
- Broken Authorization
- Build on Controller Node
- Build with SYSTEM User
- Exposed Instance
- Group-based Secrets Leak
- Insecure Functionality Exposed
- Insufficiently Scoped Secrets
- Lack of 2FA
- Lack of Artifact Validation
- Lack of Integration with SSO
- Lack of Monitoring
- Open Sign Up
- Outdated Plugin
- Permissive Read Access
- Pipeline Poisoning
- Plaintext Secrets in Pipeline
- Secret Credentials Revealed to Authenticated Users
- Sensitive Information Disclosure
- Unmasked Secrets
- Unprivileged Users May Execute Commands
- Unprotected Master Branch
- Unrestricted Access
- Unrestricted Container Repository
- Use of 3rd-party CI Script
- Users Can Make Public Repos

More topics on the roadmap...

Cloud Labs Topics

Audience: Cloud Engineers, AWS Engineers, Azure Engineers, and DevOps Engineers.

AWS

- Broken Authentication
- Broken Authorization
- CloudFormation Security
- IMDSv1
- Incorrect S3 Grants Lead to Web Assets Compromise
- Insecure Functionality Exposed
- Insufficient Logging
- Lack of KMS Encryption
- Lack of KMS Key Usage
- Lack of KMS Usage
- Lack of Logging
- Lack of Password Policy
- Lambda Admin Has Full AWS Permissions
- Lambda Secrets Stored
- Load Balancer Running Over HTTP
- Misconfigured IP-Based SQS Access Policy
- Missing Deny
- Missing Encryption
- Missing Group Level Access Control
- Missing Server Side Encryption
- Missing SQS Server-Side Encryption
- No Logging of Events
- Over Privileged Lambda IAM Admin
- Permissive Action
- Permissive S3 ACL Leaks Vendor Names
- Plaintext Secrets Stored
- Publicly Accessible Lambda Function
- Publicly Callable Lambda
- Publicly Writable SQS Queue
- Restricted IAM User Has Full Lambda Access
- S3 Security
- Sensitive Information Disclosure
- SNS Security
- SQS Missing Encryption
- SQS Security
- Unrestricted AMI Allows Public Access
- Unrestricted S3 Public Access
- Using KMS to Store Plaintext Secrets
- Writable SQS Queue
- Wrong User Policy

Azure

- Broken Authentication
- Broken Authorization
- Disabled Secure Transfer in Storage
- Exposed NetBIOS Access
- Exposed RDP Access
- Exposed UDP Ports
- Insufficient Certificate Key Size
- Lack of Alerts
- Lack of In-Transit Encryption in Flexible Database Server
- Lack of Resource Lock
- Lack of Soft Delete in Storage
- Misconfigured Immutable Storage
- Misconfigured TLS in Flexible Database Server
- Missing HTTP Logging in App Service

- Missing Key Vault Encryption Key Expiration
- Missing Key Vault Secret Key Expiration
- Missing redirection to HTTPS in Web Apps
- Missing Storage Double Encryption
- Outdated Framework Version in App Service
- Outdated Transport Security Settings
- Over-Privileged Monitoring Role
- Permissive Action
- Publicly Accessible Certificates Storage
- Weak Network Security Group

More topics on the roadmap...

Mobile Labs Topics

Audience: Mobile Developers, Android Developers, and iOS Developers.

- API Key Leak
- Application Allows Backup of Sensitive Data
- Authentication Bypass
- Authorization Bypass
- Authorization Header Sent Over Insecure HTTP Connection
- Broken Authentication
- Broken Authorization
- Directory Traversal
- Exported Components
- Exposed Backend URL
- Extraneous Functionality
- Hardcoded Credentials
- Hardcoded Encryption Key
- HTML Manipulation
- Information Leakage
- Insecure Authentication
- Insecure Broadcast Receiver
- Insecure Communication
- Insecure File Paths
- Insecure Functionality Exposed
- Insecure Token Storage
- Insufficient Cryptography
- Insufficient Transport Layer Security
- Intent Redirection
- Lack of Certificate Pinning
- Lack of Jailbreak/Root Check
- Lack of Root Check
- Missing Emulation Check
- Missing Root Check
- Non-obfuscated APK
- Non-Obfuscated Release APK
- NoSQL Injection
- Secrets Disclosure
- Sensitive Activity Exported
- Sensitive Information Disclosure
- SQL Injection
- Unrestricted File Download
- Unsecured Content Provider
- Unsecured WebView
- Weak Host Validation

More topics on the roadmap...

OT and Automotive Labs Topic

Audience: OT / IoT / SCADA / ICS / Embedded / Automotive Engineers

- Hardcoded Keys in Firmware
- Writable Root Filesystem Enables Attacker Persistence
- Memory Corruption in CAN Message Handling
- Outdated Vulnerable Component
- Downgrade Attack Against OTA Updates
- Privilege Escalation via Root Service
- Double-free In Signal Handling
- Missing Authentication In Critical Endpoint
- XML Expansion Attacks Via MQTT Messages
- Lack of Integration of Cloud IoT Services
- Enabled Debug Mode
- Exposed SSH Service
- Privilege Escalation Via SUID Binary
- Unauthorized Access via UART Serial Port
- Static Key Usage Across Multiple Devices
- Plaintext Transmission of Device Logs
- Binaries Not Compiled with Security Flags
- Weak Random Generation of Authentication Material
- Deserialization Attacks on Config Files Update
- Lack of TLS-based Client-Side Authentication
- Stack Overflow In Sensor
- Kernel Prints Disclosure Via Serial Port
- Lack of Signature Check in OTA Update
- Unnecessary Root Service
- Privilege Escalation via Sudo
- Remote Command Execution via Deserialization
- Memory Corruption Through Malformed Sensor Data
- Plaintext Transmission of Device Logs
- Command Injection in Actuator
- Lack of TLS in MQTT Messaging
- Weak JWT Authentication
- Lack of Password Hashing in Configuration File
- Directory Traversal In Serving Assets
- Failure to Validate HTTPS Certificate

More topics on the roadmap...

SOC Analysts Topics

Audience: SOC Analysts and Threat Hunters.

** SOC Labs are an add-on that can be purchased separately.*

- Access Token Manipulation
- Account Discovery
- Achieving Remote Execution with WMI
- Alan: injection into a legitimate process
- Analyze binary behavior with speakeasy
- Analyze binary with objdump
- Analyzing Malware Network Traffic
- Analyzing malware persistence
- Application Layer Protocol
- Binary format
- Binary's .text section analysis
- Brute Force
- Building an Open Source SOAR
- Calculate hashes of a given file
- CERT versus CSIRT
- Code Injection
- Collecting logs with Sysmon
- Common Persistence Techniques
- Comparing Malware Signatures
- Computer Security Incident Handling
- Containers
- Credential Dumping: DCSync
- Credential Theft
- Cyber Threat Intelligence
- Cyber Threat Intelligence Platforms
- Defensive Technologies
- Detecting a compromised container performing a DOS attack
- Detecting Backdoor in Linux Environment
- Detecting Business Email Compromise
- Detecting Evidence with YARA
- Detecting malicious Cryptominer
- Detecting malicious USB HID attacks
- Detecting phishing with Sigma
- Detecting Remote Access Software installed as a service
- Detecting Remote Access Software network activity
- Detecting Windows Persistence Technique
- Detection Swiss Knife
- Device Code Phishing on Azure
- Diamond Model
- Difference between program and process
- Dynamic Analysis
- ELF format
- Email attachment hash analysis
- Escape to Host
- Event Classification
- Event Log Clearing
- Exfiltration Over Alternative Protocol
- Exfiltration Over Unencrypted/Obfuscated Protocol towards C2
- Exploit Public-Facing Application
- Exploitation for Privilege Escalation
- Exploitation of Remote Services
- Exploiting PetitPotam vulnerability
- Exploiting PrintNightmare Vulnerability
- Exploiting Zerologon vulnerability
- Extract indicators
- Extract Malicious DLL Path
- Extract strings with strings command
- Extracting TTPs
- Extracting TTPs from a CTI report
- Extracting TTPs from raw data
- Extracting Ursnif configuration
- File Identification
- File type identification
- Gaining initial access within a network
- Hardware Additions

- Hashing Functions
- Identification of known malware
- Identifying backdoor
- Identifying Compressed Malware
- Identifying known malware with YARA
- Identifying obfuscated malware
- Incident Management
- Indicator Removal on Host
- Intelligence
- Introduction to Malware Analysis
- Introduction to the Elastic Stack
- Kerberoasting and Silver Ticket
- Kill-Chain Model
- Kill-Chain Model & Diamond Model Comparison
- LDAP Domain Discovery
- LOLBAS: AppLocker Bypass
- Maintain access through Golden Ticket
- Malicious email extensions analysis
- Malware Behaviours
- Malware Functionalities
- Man
- Man-in-the-Middle
- Management Plan
- Masquerading
- Memory dump importance for IoC auditing
- Metrics for team evaluation
- MITRE ATT&CK Containers Matrix
- Models Comparison
- Modern SOC
- Monitoring logs with Sigma
- Network Communication
- Obfuscation
- Operating Procedures
- Orchestrators
- OS Credential Dumping
- OS Exhaustion Flood
- Packers
- Parse Executable Header with readelf command
- Password Spraying against LDAP
- Password Spraying against Kerberos
- Password Spraying against SMTP
- Password Spraying on Azure
- PE format
- Phishing
- Playbook - Phishing
- Privilege Escalation
- Privilege Escalation inside a container with Dirty Pipe vulnerability
- Process Injection
- Remote Access Software
- Remote Code Execution
- Resource Hijacking
- Retrieve DLL
- Retrieve information
- Retrieving STIX data with Python
- Sandboxes
- Scheduled Task/Job
- Security Incident Management Process
- Security Incident Reporting
- Security Orchestration, Automation, and Response
- Service Principal Abuse on Azure
- Sharing Cyber Threat Intelligence
- Sigma
- Signed Binary Proxy Execution
- SOC versus MDR versus MSSP
- SOC, CSIRT & CERT teams
- Static Analysis
- Steal or Forge Kerberos Tickets
- Suspicious mail header
- Technologies
- The Computer Security Incident Response Team
- The Elastic Stack
- The MITRE ATT&CK Framework
- The Security Operations Centre
- Threat Actors, Thread Impacts, and how to map them
- Types of Binary Analysis
- Using containers with Docker
- Using TTPs in Cyber Threat Intelligence

- Windows Management Instrumentation
- YARA
- Privilege Escalation in Azure
- Service Principal Abuse
- Device Code Phishing

More topics on the roadmap...

Security Awareness Topics

Audience: Technical Managers, Program Managers, Project Managers, and Information Security Managers.

- Safe Home Working (Video + Knowledge Base Article)
- Safe Internet (Video + Knowledge Base Article)
- Mobile Device Security (Video + Knowledge Base Article)
- Physical Devices Security (Video + Knowledge Base Article)
- Malware (Video + Knowledge Base Article)
- Phishing (Video + Knowledge Base Article)
- Cyber Fundamentals (Video + Knowledge Base Article)
- Account Takeover (Video + Knowledge Base Article)
- Data Breach (Video + Knowledge Base Article)
- Ransomware (Video + Knowledge Base Article)
- CEO Impersonation Fraud (Video + Knowledge Base Article)
- Data Protection and GDPR (Video + Knowledge Base Article)
- Online Self Defence (Video + Knowledge Base Article)
- Password Security (Video + Knowledge Base Article)
- Identity Theft (Video + Knowledge base Article)
- Credit Card Fraud (Video + Knowledge Base Article)
- Online Shopping (Video + Knowledge Base Article)
- Social Media Security (Video + Knowledge Base Article)
- Social Engineering (Video + Knowledge Base Article)
- Passphrases (Video + Knowledge Base Article)
- Spear Phishing (Video + Knowledge Base Article)

More topics on the roadmap...

SecureFlag

Contact us to get started

www.secureflag.com