Pipeline

Pipeline is a Leading Learning Partners Association Member

MILE2 C)CSA: CERTIFIED CYBER SECURITY ANALYST (SELF-STUDY + ESAME)

CORSO IN AUTOAPPRENDIMENTO

Durata	Prezzo	Orari	Calendario
circa 40 ore	1.249,00€ + IVA		

Il corso Mile2 C)CSA Certified Cyber Security Analyst vi aiuta a preparare un'organizzazione a definire una soluzione completa end-to-end per monitorare, prevenire, rilevare e mitigare in modo proattivo le minacce che si presentano in tempo reale.

Non illudetevi, questo corso è molto più avanzato di quanto possiate aspettarvi. Il ritmo è veloce e approfondito, in modo che possiate godere di un'esperienza a tutto tondo. Preparatevi ad approfondire i dettagli dell'analisi della sicurezza per le esigenze di oggi.

Al termine del corso sarete in grado di configurare e distribuire strumenti di analisi all'avanguardia, strumenti di rilevamento delle intrusioni, server syslog, SIEM e di integrarli per l'intera azienda al fine di individuare e in molti casi prevenire gli exploit odierni.

Il presente prodotto è un'ottima soluzione per l'autoapprendimento rivolta a chi ha bisogno di acquisire le conoscenze necessarie per sostenere con competenza l'esame associato.

Contenuti del corso

Chapter 1 – Blue TeamPrinciples

- Network Architectureand how it lays the groundwork
    - Defensive Network
- Security Data Locationsand how they tie together
- SecurityOperationsCenter
    - The People, Processes, and Technology
    - Triage and Analysis
    - Digital Forensics
    - Incident Handling
    - Vulnerability Management
- Automation, Improvement, and Tuning

Chapter 1 Labs – Blue Team Principles

- Analyze Initial Compromise Vector

- Network Forensics
- System Forensics

Chapter 2 – DigitalForensics

- Investigative Theory andProcesses
    - Digital Acquisition
    - Evidence Protocols
    - Evidence Presentation
- Computer ForensicsLaboratory
    - Protocols
    - Processing Techniques
    - SpecializedArtifacts
- Advanced Forensics for Today'sExploitations

Chapter 2 Labs – Digital Forensics

- Analysis of Captured Network Activity
- Analysis of Captured Zip File

Chapter 3 – Malware Analysis

- Creating the Safe Environment
- Static Analysis
- Dynamic Analysis
- Behavior Based Analysis
- What is different aboutRansomware?
- Manual Code Reversing

Chapter 3 Labs – Malware Analysis

- Analysis of an MSFVenom Executable
- Analysis of Locky Ransomware
- Creating YARA Rules based on Analysis Results
- Final Assessment

Chapter 4 – Traffic Analysis

- Manual Analysis Principles
- AutomatedAnalysis Principles
    - Signaturescompared toBehaviors
- Application Protocols Analysis Principles
- Networking Forensics

Chapter 4 Labs – Traffic Analysis

- Traffic Analysis of a Website Defacement Attack
- Traffic Analysis Based on IDS Alerts
- Traffic Analysis of a ZLoader Delivery Attempt
- Bonus: Find the Backdoor!!!

Chapter 5 – Assessing the Current State of Defense with theOrganization

- Network Architecture and Monitoring
- Endpoint Architecture and Monitoring
- Automation, Improvement, and continuousmonitoring

Chapter 5 Labs – Assessing the Current State of Defense within the Organization

- Configuring a Firewall
- Configuring SIEM
- Configuring IPDS
- Upgrading Detection/Protection Capabilities

Chapter 6 – Leveraging SIEM for Advanced Analytics

- Architectural Benefits
- Profiling andBaselining
- Advanced Analytics

Chapter 6 Labs – Leveraging SIEM for Advanced Analytics

- Deploying Agent
- Implementing User Behavior Analytics through Machine Learning
- Simulate an Attack and Analyze Alerts

Chapter 7 – Defeating the Red Team with Purple Team tactics

- Penetration Testingwith full knowledge
    - Reconnaissance
    - Scanning
    - Enumeration
    - Exploitation
    - Lateral Movement

Chapter 7 Labs – Defeating the Red Team with Purple Team Tactics

- Configuring Defensive Systems

- Purple Team Testing
- Mitigation
- Bypass Anti-Virus and LSASS Patch through edited Mimikatz

Partecipanti

Il pubblico principale di questo corso Mile2 C)CSA Certified Cyber Security Analyst è costituito da:

- Professionisti della sicurezza
- Professionisti della gestione degli incident
- Chiunque lavori in un centro operativo di sicurezza
- Esperti forensi
- Analisti di sicurezza informatica

Obiettivi

La certificazione Mile2 C)CSA mira a garantire che il titolare disponga di un'ampia base di conoscenze che coprono una grande varietà di aree necessarie per analizzare i sistemi di cybersecurity, sviluppare report e suggerire miglioramenti per garantire che il sistema sia in grado di rilevare e scoraggiare efficacemente le intrusioni.

Prerequisiti

Per seguire con profitto il corso Mile2 C)CSA Certified Cyber Security Analyst è consigliato aver frequentato almeno uno dei seguenti corsi Mile2 oppure avere competenze equivalenti:

- Certified Security Principles
- Certified Digital Forensics Examiner
- Certified Incident Handling Engineer
- Certified Professional Ethical Hacker
- Certified Penetration Testing Engineer

Lingua

Il materiale didattico è in lingua inglese

Materiali e Bonus

Comprende un libro, un video dove un istruttore vi guida attraverso il libro, la guida di preparazione all'esame, simulazioni illimitate dell'esame e l'esame di certificazione. Tutto il materiale sarà disponibile per 12 mesi nel vostro account Mile2.com. Se non si dispone già di un account Mile2.com, ne verrà creato uno al momento dell'iscrizione.

Pipeline

Pipeline is a Leading Learning Partners Association Member

Vuoi organizzare un corso personalizzato?

Chiamaci: 02/6074791 Scrivici: formazione@pipeline.it

MAIN PARTNERS

Microsoft Solutions Partner

CompTIA Authorized Partner DELIVERY PARTNER

ITIL