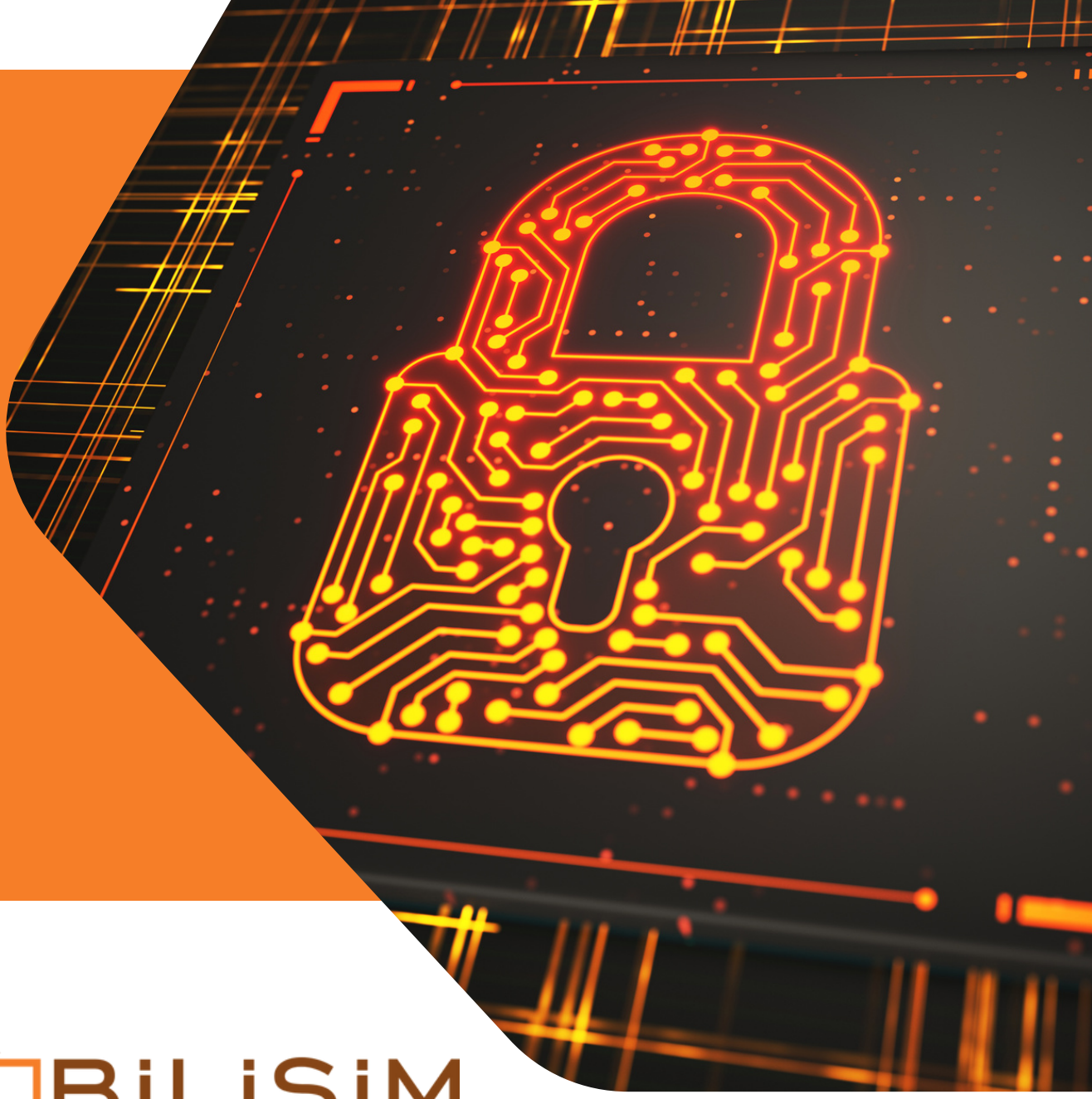

BİLİŞİM ACADEMY

SOC LEVEL-2 INCIDENT RESPONDER

KURS İÇERİĞİ

KURS AÇIKLAMASI

SOC-L2 (Incident Responder) ekipleri güvenlik tehditlerini önleyerek ve hafifleterek kurumsal güvenliği korur ve geliştirir. Bu profesyoneller, olayların derinlemesine araştırılmasından sorumludur. Ayrıca iyileştirme ve önlemler konusunda tavsiyelerde bulunur. SOC-L1 takımlarından iletilen alert'leri derinlemesine inceleyerek gerekli aksiyonları alır. Kursumuzda bir SOC-L2 analistinin ihtiyaç duyacağı tüm yetenekleri uygulamalı olarak öğreneceksiniz.

BU KURSU KİMLER ALMALI?

- Siber güvenlik sektöründe yer almak isteyen öğrenci veya IT Personeli,
- Kariyerini siber güvenlik alanında ilerletmeyi düşünenler,
- Siber güvenlik alanında kariyer yapmak isteyenler,
- Siber Güvenlik Analistleri (SOC Analyst),
- Olay Yanıtlayıcılar (Incident Responder)
- Tehdit istihbaratı Analistleri (Threat Intelligence Analyst)
- Adli Bilişim Uzmanları (Forensics Analyst)

1.FORTIGATE FIREWALL

1.1. Firewall

1.1.1. What is Firewall?

1.1.2. Types of Firewall (NGFW, WAF)

1.1.3. What is Firewall Rules?

1.1.4. What is 5-Tuple?

1.2. EVE-NG (Emulated Virtual Environment)

1.2.1. Installation Eve-Ng

1.2.2. Intro to Eve-Ng GUI

1.2.3. Creating a Topology in Eve-ng

1.2.4. Connecting to the Fortigate Web GUI

1.2.5. Configuring Interfaces

1.2.6. Write a Rule in Fortigate

1.2.7. Security Profiles

2.IBM QRADAR

2.1. Intro to IBM QRADAR

2.2. Log Activity

2.3. Network Activity

2.4. Assests and Offenses

2.5. Reports

2.6. Data Collection

2.7. Qradar Rules and Configuring Rules

2.8. Searching Events

2.9. Saving Event Search Criteria

2.10. Configuring Time Series Chart

2.11. Offense Investigation

- 2.11.1. AWS Cloud Attack
- 2.11.2. GDPR Attack
- 2.11.3. Phising Attack
- 2.11.4. Cyrptojacking Attack
- 2.11.5. DDos Attack

2.12. Offense Reporting

3.LOG INVESTIGATION WITH SPLUNK

3.1. Installation Botsv1

3.2. Incident Handling With Splunk

3.3. Investigating With Splunk

4.ADVANCE ENDPOINT SECURITY

4.1. Sysmon

4.2. Syslog

4.3. Osquery

4.4. Investigation CrowdStrike Detections

- 4.4.1. Malware Investigation in CrowdStrike
- 4.4.2. Ransomware Investigation in CrowdStrike
- 4.4.3. Lsas.exe Credential Dumping
- 4.4.4. Follina

5.PYTHON FOR CYBER SECURITY

5.1. Python Essentials-1

5.1.1. Introduction to Python and Computer Programming.

5.1.2. Python Data Types, Variables, Operators, and Basic I/O Operations.

5.1.3. Boolean Values, Conditional Execution, Loops, Lists and List Processing, Logical and Bitwise Operations.

5.1.4.Functions, Tuples, Dictionaries, Exceptions, and Data Processing

5.2. Python Essentials-2

5.2.1. Modules, Packages, and PIP

5.2.2. Strings, String and List Methods, Exceptions Types of Endpoint Threats?

5.3. Bash Scripting

6.ADVANCED MALWARE ANALYSIS

6.1 Static Malware Analysis

6.1.1. What is Static Malware Analysis?

6.1.2. Malware Static Analysis Techniques

6.1.3. Static Malware Analysis Example

6.2. Dynamic Malware Analysis

6.2.1. What is Dynamic Malware Analysis?

6.2.2. Which Tools and Software do We Need?

6.2.3. Flare-VM Installation

6.2.4. Dynamic Malware Analysis Example - 1

6.3 Malware Traffic Analysis with WIRESHARK

6.3.1. Configuring the Wireshark for Malware Traffic Analysis

6.3.2. Malware Traffic Analysis With Wireshark – 1

7.DIGITAL FORENSICS

7.1. Introduction to Forensic

7.2. Forensic Fundamentals

7.3. Digital Evidence

7.4. Windows Forensics