# CyberNow Labs Institute

# revelstöker Spluck CROWDSTRIKE Acunetix SentinelOne Acunetix SentinelOne Radar SentinelOne Massage ThreatMoo Massage ThreatMoo Massage SentinelOne Massage SentinelOne Massage ThreatMoo Massage SentinelOne Massage Sente

Hands-On SOC Engineering Training for Professionals

**ONLY 35 SPOTS AVAILABLE** 

## Starts September 5

#### Call Now to Save Your Seat (571) 771-1354 Course Outline & Instructors Next Page ≫



### MEET THE MASTERMINDS

#### Omer Arslan

Over 15 years in cyber and architect of three Security Operation Centers (SOCs). Before co-founding CyberNow Labs, held national positions at IBM and Peraton.

#### Hasan Eksi

More than 10 years of cyber and SOC operations experience. Before co-founding CyberNow Labs, held senior positions at CapitalOne and MasterCard.

## MASTERMIND INSTRUCTORS

Since 2018, CyberNow Labs has delivered innovative and hands-on security training enabled by its <u>live Security Operations Center (SOC)</u>, featuring real network traffic, integrated security tools and workflows, and real security events. All training is delivered live and online by industry professionals within this digital SOC environment.



Aras "Prof. M" Memisyazici **Program Director** 



Dartanian Williams Security Scripting



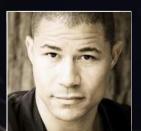
Hallie Shaw EDR/XDR



Allan Kurumlu EDR/XDR



Max Lewis SIM/SIEM



Lyndon Williams SIM/SIEM



Art Norton **SOAR** 



Michael Camp Bentley The Splunk Doctor™

<sup>nisyazici</sup> Dartani e**ctor Securit** 

## **16-WEEK S-O-C LIVE TRAINING**

Live Online <u>Mondays - Thursdays</u> from <u>19:00 - 22:00 EDT</u>

D

| <u>WK</u>   | <b>DATES</b>                          | TRAINING FOCUS  |  |  |
|---|---------------------------------------|---|--|--|
| MODULE 1: SYSTEM & NETWORK SECURITY                           |                                       |   |  |  |
| 1   | 9/5 - 9/7                             | Network Types, Devices, Configuration, Logs, OSI, TCP/IP.   |  |  |
| 2   | 9/11 - 9/14                           | Network Protocols, Services, Traffic Analysis, Virtualization(ESXI)   |  |  |
| з   | 9/18 - 9/21                           | Operating Systems, Authentication, Windows Servers, Linux/Unix Logs   |  |  |
| MODULE 2: Scripting for Security Automation                   |                                       |   |  |  |
| 4   | 9/25 - 9/28                           | Python Scripting for Security Engineers   |  |  |
| 5   | 10/2 - 10/5                           | Powershell Scripting for Security Engineers   |  |  |
| MODULE 3: Attack-Surface Management, Vulnerability Management |                                       |   |  |  |
| 6   | 10/9 - 10/12                          | Threat Intelligence, Attack Surface Management, Dark Web Monitoring,<br>Vulnerability Intelligence, Breaches, Malware, IDCs, Threat Groups,   |  |  |
| 7   | 10/16 - 10/19                         | Vulnerability Management Systems and Scanners (Tenable), Web<br>Application Security Scanners (Acunetix), Asset management  |  |  |
|   | М                                     | ODULE 4: Advanced XDR/EDR Implementation & Management   |  |  |
| 8   | 10/23 - 10/26                         | SentinelOne XDR Solutions, Console Setup, Groups, and Policies Best-<br>Practices, Tuning, Threat Hunting (Deep Visibility) Agent Deployment  |  |  |
| 9   | 10/30 - 11/2                          | CrowdStrike Falcon XDR Solution, Console Setup, Groups, and Policies<br>Best-Practices, Incident Analysis, Threat Hunting, Response Scripting   |  |  |
|   | MODI                                  | ULE 5: Advanced SIM/SIEM Security Monitoring and Log Analysis   |  |  |
| 10  | 11/6 - 11/9                           | SIM/SIEM Deep Dive, Splunk Enterprise Security Configuration,<br>Deployment, User roles, Licensing, Application & Index Management,<br>Forwarding, Dashboard Creation, and Detection Rules Creation |  |  |
| 11  | 11/13 - 11/16                         | Configuring Forwarders, Data & Tuning Inputs, Parsing, Advanced Search,<br>Enrichment, Sub-searches, Monitoring, Troubleshooting, Regex in Splunk   |  |  |
| 12  |                                       | ElkStack Deep Dive, Planning, Deployment, Advanced Searching, Event<br>Analysis, Log & Alert Management   |  |  |
| 13  | 11/27 - 11/30                         | QRadar Deep Dive, Planning, Deployment, Advanced Search, Event<br>Analysis, Log & Offense Management, Rule & Dashboard Creation & Tuning  |  |  |
| 14  | 12/4 - 12/7                           | SOAR Overview, Planning, and Deployment, Integration Configuration,<br>Access Control, Playbook Development, Marketplace Utilization, Content   |  |  |
|   | MODULE 6: Cloud Security Fundamentals |   |  |  |
| 15  | 12/11 - 12/14                         | Cloud Security Monitoring, Logs and Events, AWS CloudTrail, Azure   |  |  |
| 16  | 12/18 - 12/21                         | Cloud Security Monitoring, Logs and Events, AWS CloudTrail, Azure   |  |  |

## **CyberNow** Labs Institute 5-D-C MASTERMIND

Become an S-O-C MASTERMIND in 16 weeks learning from America's Most Exclusive S-O-C Community

|   | Price  | <u>Package</u> |
|---|--------|----------------|
| 16-Week S-O-C MasterMind Live Training            | 16,900 | 16,900         |
| (+) 12 Months' Access to Training Recordings      | 950    | Included       |
| (+) 12 Months' S-O-C Unlimited Access             | 950    | Included       |
| (+) 12 Months' of Monthly MasterMind Calls        | 950    | Included       |
| (+) NEW Python for Security Video Training (7hrs) | 150    | Included       |
| (=) Total Value                                   | 19,900 | 16,900         |
| CyberNow Labs' Hiring Partners 25% OFF            | 14 025 |                |
|   | 14,925 | 12,675         |
| National Security Personnel 25% OFF               | 14,925 | 12,675         |
|   |        | 12,675         |

**APPLY: MASTERMIND.CYBERNOWLABS.COM** 

Call: (571) 771-1354 | Email: Enrollment@CyberNowLabs.com | CyberNowLabs.com