

# WHO WE ARE

America's #1 Builder of Technical Cyber Talent



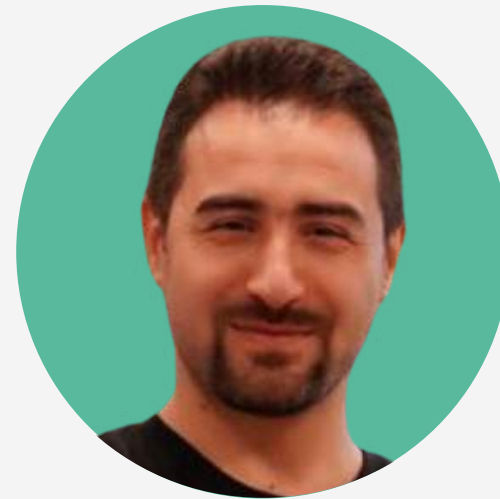
Philip Niedermair

Public-Private



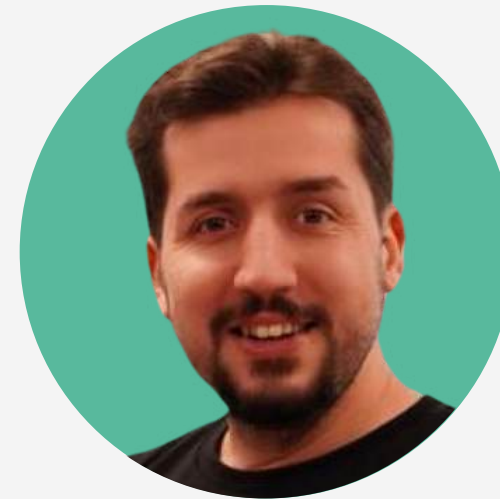
Mike Meyers

IT Training



Omer Arslan

Security Operations Center (SOC)



Hasan Eksi



Gabe Schrade

Industry Partnerships



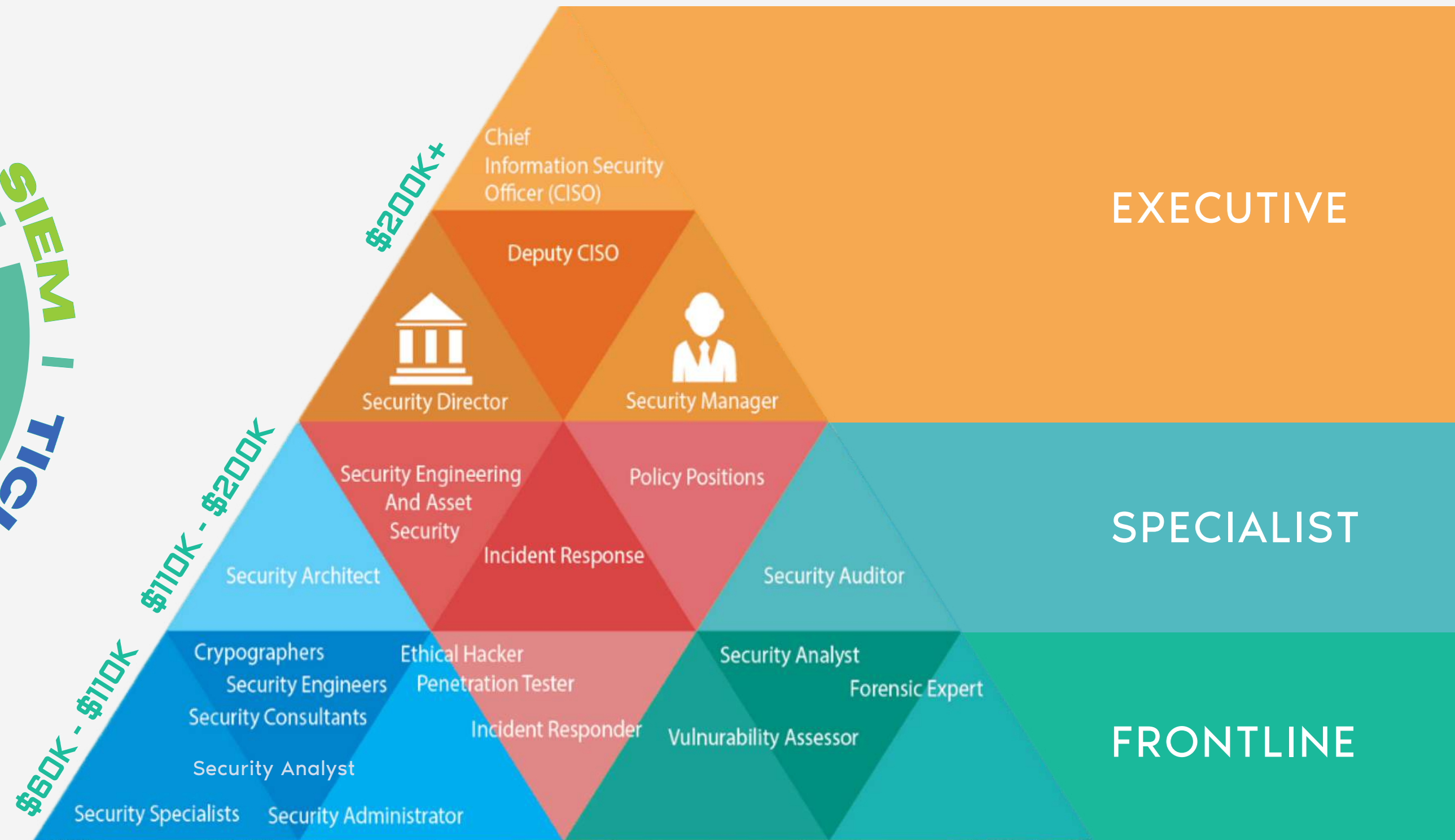
Carly Cavagnoli

**800+** Cybersecurity  
Job Placements

**200+** Companies and  
Agencies Hired

# THE SOC GAP

Most cyber jobs require SOC experience no one can get



# OUR SOC SOLUTION

Your turnkey IT/Cyber Talent Provider



**RECRUITING**

**TRAINING**

**PLACEMENT**

**IT PROS**

**VETERANS**

**CLEARANCE**

**SALES PROS**

**DIVERSITY**



- **DIRECT HIRE (NO FEES)**
- **DOD SKILL-BRIDGE**
- **DOL APPRENTICESHIP**
- **TUITION REIMBURSEMENT**
- **L&D INITIATIVES**



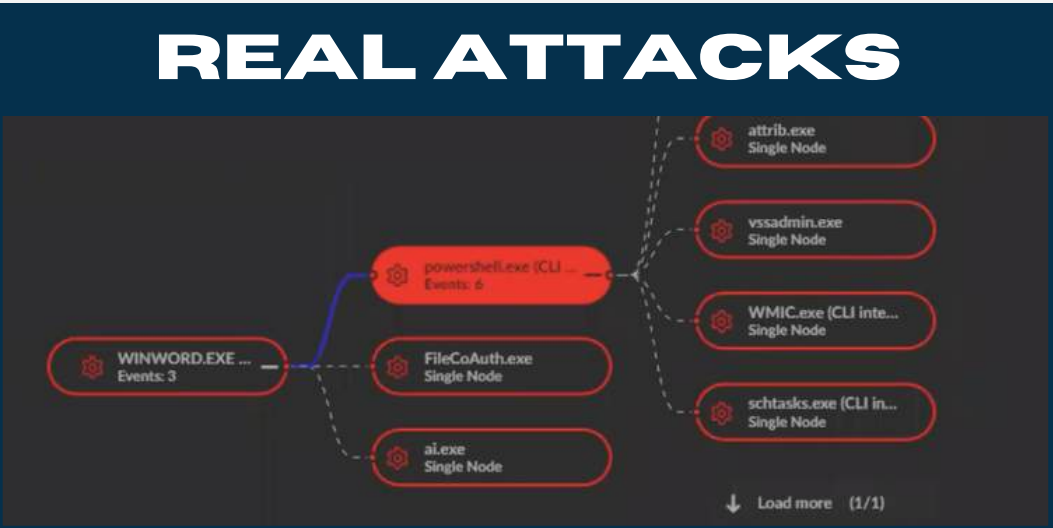
# SOC EXPERIENCE



3-month instructor-led online training (Mon - Thur 7 - 9:30pm ET)

### REAL TRAFFIC

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
DNS Query	DNSServer	4	May 19, 2024, 12:30	DNS In Progress	10.201.152.14	0	0.0.0.0	0	N/A	
Firewall Deny	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Deny	10.1.1.254	40829	10.210.206.61	4447	N/A	
Firewall Deny	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Deny	70.110.62.81	42714	10.210.206.60	32712	N/A	
Firewall Permit	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Permit	10.1.1.88	63432	142.250.190.135	443	N/A	
DNS Query	DNSServer	40	May 19, 2024, 12:30	DNS In Progress	10.201.152.12	0	54.69.251.5	0	N/A	
DNS Query	DNSServer	3,672	May 19, 2024, 12:30	DNS In Progress	10.1.1.86	0	0.0.0.0	0	N/A	
Firewall Permit	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Permit	10.1.1.44	195	10.1.1.254	N/A	N/A	
Firewall Permit	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Permit	10.1.1.46	63437	142.250.190.135	443	N/A	
Firewall Deny	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Deny	10.150.1.79	56425	1.44.224.217	389	N/A	
Allow Action	FortiGate @ 10.1.1.254	2	May 19, 2024, 12:30	Firewall Permit	10.1.1.10	92209	189.253.249.63	60	N/A	
Firewall Deny	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Deny	70.110.62.81	42714	10.210.206.60	32681	N/A	
Firewall Deny	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Deny	10.160.1.71	52659	175.160.175.68	7080	N/A	
Firewall Deny	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Deny	10.1.1.254	93647	10.210.206.60	5330	N/A	
Firewall Deny	FortiGate @ 10.1.1.254	2	May 19, 2024, 12:30	Firewall Deny	10.160.1.130	52961	75.274.87.190	7080	N/A	
Information Message	System Notification 2 - gmsd	1	May 19, 2024, 12:30	Information	10.1.1.120	0	127.0.0.1	0	N/A	
Information Message	System Notification 2 - gmsd	1	May 19, 2024, 12:30	Information	10.1.1.120	0	127.0.0.1	0	N/A	
Allow Action	FortiGate @ 10.1.1.254	3	May 19, 2024, 12:30	Firewall Permit	10.1.1.10	99677	189.86.116.5	60	N/A	
Allow Action	FortiGate @ 10.1.1.254	3	May 19, 2024, 12:30	Firewall Permit	10.1.1.10	58977	81.198.76.5	60	N/A	
Firewall Permit	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Permit	10.160.1.130	91862	25.196.130.88	443	N/A	
Blocked Action	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Deny	10.85.210.00	59529	10.210.206.60	20	N/A	
Information Message	System Notification 2 - gmsd	1	May 19, 2024, 12:30	Information	10.1.1.120	0	127.0.0.1	0	N/A	
Information Message	System Notification 2 - gmsd	1	May 19, 2024, 12:30	Information	10.1.1.120	0	127.0.0.1	0	N/A	
Firewall Deny	FortiGate @ 10.1.1.254	1	May 19, 2024, 12:30	Firewall Deny	141.80.7.167	34822	10.210.206.60	8728	N/A	
User Logout	SSM Audit 2 - gmsd	1	May 19, 2024, 12:30	SSM User Authentication	10.1.1.120	0	10.1.1.120	0	not	
User Login	SSM Audit 2 - gmsd	1	May 19, 2024, 12:30	SSM User Authentication	10.1.1.120	0	10.1.1.120	0	not	
User Logout	SSM Audit 2 - gmsd	1	May 19, 2024, 12:30	SSM User Authentication	10.1.1.120	0	10.1.1.120	0	not	



### REAL TICKETS

Alert ID	Alert Name	Severity	Category	Status	Created At	Resolved At	Owner	Tasks	Observables	TTFS
#1080	S1 Alert - RAT.exe Malware Detection - PLAMA - 04/15/2024	High	Malicious File	Malicious Hash	Malware	Running		10	16	5.05/15/24 21:39
#1070	SP Alert on Remote Desktop Network Brute Force - Short ID Brute - CH18 - PUGH - 5/15/2024 - MAL Reviewed	High	Brute Force	Suspicious Activity	Malware	Login Failure	Malicious File	10	1	5.05/15/24 14:52
#1053	SP Alert-Registry Keys Used For Persistence-Short ID qfjz-CH18 Mowusu 05/14/2024 - MAL Reviewed	High	Brute Force	Suspicious Activity	Malware	Login Failure	Malicious File	10	3	5.05/14/24 14:39
#1029	Splunk - Excessive Failed Logins - Omendex MByrow 05/12/2024 - MAL Reviewed	High	Brute Force	Suspicious Activity	Malware	Login Failure	Malicious File	10	2	5.05/12/24 8:50
#1021	PP Alert - Active Malware Threat through link - 5/11/24 Hsaker - Coh39	High	Malicious Link	Phishing	Scam	Credentia Theft	Malicious Attachment	2	1	5.05/11/24 13:55
#1006	QR Offense 55347-Automated Scan Tools Detected-Ransom-5-10-2024 - MAL Reviewed	High	Malicious Scan	Exploit	Brute Force	Suspicious Activity	Malware	10	0	5.05/10/24 13:38

Best of Breed  
**TOOLS**

**FORTINET**

**proofpoint**  
Jira Software  
**TheHive**

**Acunetix**  
**tenable.io**  
Nessus  
**ARMIS**



**SentinelOne**



**DOMAINS**

**NEXT-GEN  
FIREWALL**

**EMAIL &  
TICKETING**

**ASSET  
MGMT**

**EDR**

**SIEM**

**MONTH #**

**1**

**2**

**3**

# QUALIFICATIONS

For admission into 3-month SOC Training Program



## KNOWLEDGE

CERTS      CompTIA Security+, CySA+, PenTest+  
                  ISC^2 Certified in Cybersecurity (CC)  
                  or      EC-Council Certified Ethical Hacker (CEH)  
DEGREE    AA, BA, or MS Specializing Cybersecurity



## EXPERIENCE

REAL TOOLS      Enterprise EDR, SIEM, ASM, Email  
REAL TRAFFIC    Alert Investigation, Declaration  
REAL TICKETS    Alert Tickets, Summaries + IOCs

## FAQS

- Monthly Starts (1st Monday)
- Mon - Thur 7 - 9:30pm ET (10hrs/wk)
- Certified Defensive Security Analyst (CDSA) Credential at Graduation

### CREDENTIAL REQUIREMENTS

- 75% Attendance (recordings accessible)
- 70% On All Technical Assessments

### OTHER

8-week CompTIA Security+ Instructor-Led Online Training offered as prerequisite

# CYBER PATHWAY

Industry Certification + REAL Hands-On Cyber SOC Experience



Optional for those without  
cyber certification/degree

CompTIA Security+

Hands-On Experience

America's #1 Builder of Technical Cyber Talent

**CAREER  
SECURED**

JAMES CHIU  
**STATE STREET  
SOC ANALYST**

CERTIFICATIONS  
TECHNOLOGIES

COMPTIA SECURITY+  
IBM Guardium splunk> SentinelOne revesetake ThreatMan  
proofpoint Netsparker PORTINET CROWDSTRIKE Linsiderland tavaria

**CyberNow Labs**  
A NATIONAL CYBER GROUP COMPANY

Week # 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Weekday	<u>Monday</u>	<u>Tuesday</u>	<u>Wednesday</u>	<u>Thursday</u>
Times (eastern time)	7 - 9:30 PM	7 - 9:30 PM	7 - 9:30 PM	7 - 9:30 PM
Training Format	Instructor-Led Online	Instructor-Led Online	Instructor-Led Online	Instructor-Led Online





800

**More than**

**CYBERSECURITY PLACEMENTS**

*Congratulations!!*