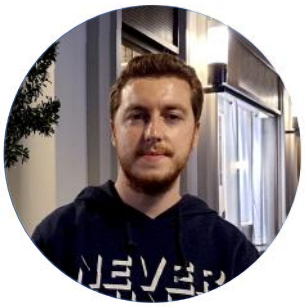

S.Furkan KAYAR

SOC Analyst

PROFILE

"Bir sistemin güvenliğini sağlamak için sistemin nasıl çalıştığını bilmek gerekir" mantığıyla Microsoft System & Network eğitimi aldım.

Aldığım bu eğitimin ardından Siber Güvenlik çözümleri sağlayan bir firmada çalışmaya başladım. Burada Endpoint Security,EDR,Mail Gateway,DLP gibi birçok farklı güvenlik çözümünü inceleme fırsatı buldum.

Bu deneyimimin ardından kendi isteğimle Adeo Bilişim Dan. firması bünyesinde, bir Finans Kurumunda SOC Analyst pozisyonunda çalışmaya başladım. Birçok vakada tehdit tespiti - analiz süreçlerini yürüttüm.

Tier 2 pozisyonuna geçmemle birlikte ek olarak Incident Response süreçlerine dahil olarak threat hunting çalışmaları gerçekleştirdim. Önleyici aksiyonlarda rol aldım.

CONTACT

ADDRESS	Ataşehir, İstanbul
E-MAIL	sfurkankayar@gmail.com
PHONE	534 - 959 - 9038
LINKEDIN	linkedin.com/in/sfurkankayar
WEB SITE	furkankayar.net

ABOUT

MILITARY SITUATION	Ekim 2021 (Bedelli)
DRIVING LICENSE	B Sınıfı
BORN	11.10.1994
MARITAL STATUS	Bekar

LANGUAGE

English

READING

WRITING

SPEAKING

EDUCATION

KÜTAHYA ATATÜRK ANADOLU TEKNİK LİSESİ // 2008 - 2012
Bilişim Teknolojileri - Web Tasarım

İSTANBUL ÜNİVERSİTESİ // 2012 - 2016
Bilgisayar ve Öğretim Teknolojileri Eğitimi

EXPERIENCE

Ziraat Teknoloji (Adeo Consultant) // Şubat 2020 - Şuan
SOC Analyst Tier 2

Ziraat Teknoloji (Adeo Consultant) // Aralık 2018 - Şubat 2020
SOC Analyst Tier 1

Güney Bilişim Bilgi Teknolojileri // Şubat 2018 - Aralık 2018
IT Security Specialist

Kaspersky Endpoint Security,Kaspersky Mail Gateway,Libra Esva Mail Gateway,Cososys DLP ürünleri hakkında teknik destek uzmanlığı. Kasperksy Anti Targeted Attack ve EDR ürünleri hakkında kurulum ve konfigurasyon desteği.

Toki Kayaşehir MTA Lisesi // Ekim 2016 - Haziran 2017
Bilgisayar Öğretmeni

COURSE AND SOCIETY

Wissen Akademie - Microsoft System&Network Eğitimi
10.2017 - 01.2018 / 550 saat | İŞKUR Nitelikli Bilişim Uzmanı Yetiştirme Programı

Hacktrick'17 - Blackbox Sızma Testi Eğitimi

Microsoft Certified Professional (MCP)

Kaspersky Lab Certified Professional: Kaspersky Endpoint Security 11 for Windows Kaspersky Security Center 10

Carbon Black - CB Response Advanced Analyst

Applied Network Defense - Investigation Theory

Active Countermeasures - Network Cyber Threat Hunter Training

Splunk - Splunk 7.x Fundamentals (eLearning)

İsmek - Diksiyon Eğitimi | Sosyal Hayatta İletişim

PROJECT

- **Threat Hunting with SecurityOnion**
- **Siber Sözlük Projesi** - twitter.com/sibersozluk
- **MCSE eğitimi** kapsamında sanal ortam üzerinde Domain, DC, ADC kurulumu, Active Directory,DHCP, DHCP Failover, Local Storage, Print Server, DNS ve Group Policy yapılandırmalarını kapsayan sistem altyapı projesi
- **MCSE eğitimi** kapsamında network altyapı projesi
- **MCSE eğitimi** kapsamında Exchange projesi,

SKILLS

THREAT ANALYSIS

INTRUSION DETECTION

EVENT MONITORING AND INCIDENT IDENTIFICATION

THREAT HUNTING

TECHNICAL SKILLS

PROGRAMS & PLATFORMS

- Splunk Enterprise **(7/10)**
- CB Response **(9/10)**
- Endpoint Security **(9/10)**
- Endpoint Detection & Response **(5/10)**
- Anti Targeted Attack **(4/10)**
- Mail Gateway **(7/10)**
- Endpoint Detection & Response **(8/10)**
- QRadar SIEM **(7/10)**
- Incident Response Platform **(8/10)**
- Threat Intelligence **(8/10)**
- Advanced Threat Analytics **(5/10)**
- Network Forensics tool **(5/10)**
- Mail Gateway **(7/10)**
- Data Loss Prevention **(8/10)**
- Visual Studio **(5/10)**
- Hyper-V **(8/10)**
- Office 365 **(7/10)**
- Cisco Packet Tracer **(7/10)**
- Email Security Appliance **(5/10)**
- Exchange Server **(7/10)**
- Amazon AWS **(3/10)**
- MS-SQL **(3/10)**
- Adobe Photoshop **(8/10)**

OPERATING SYSTEMS

- Windows XP-7-10 **(8/10)**
- Windows Server 2012 **(7/10)**
- Parrot OS Security **(5/10)**
- Kali Linux **(4/10)**

TOOLS

- Sızma Testlerinde Keşif ve Pasif/Aktif Bilgi Toplama(OSINT)
- Metasploit Exploit Kullanımı
- Host/Ağ/Port Arama Teknikleri(Nmap-Hping)
- Kablosuz Ağlara Yönelik Saldırılar
- Web Uygulama Güvenliği(OWASP,XSS,Sql Injection)
- Paket Analizi(Wireshark)
- Vulnerability Assessment(Nessus)

PROGRAMMING LANGUAGE

C Sharp **(6/10)**

Asp.Net **(5/10)**

Html / Css **(5/10)**

Python **(4/10)**

REFERENCE

- **Ahmet Ata Akça**
  Ziraat Teknoloji - Security Monitoring and Incident Response Manager
  0507 138 17 36
- **Caner Ahmet Aydın**
  Kaspersky Lab Turkey - Presales Manager
  0544 337 08 63
- **Yasin Yavuzalp**
  Wissen Akademie - Eğitmen
  0554 348 58 27