Ferdi Sönmez

COMPUTER ENGINEER

Phone
05443785574

Address
Üsküdar,Türkiye

Email
ferdi.17810@gmail.com

LinkedIn
ferdi-s%C3%B6nmez-43a472165

Site
https://ferdisonmez.github.io

Detail-oriented security analyst with 3 years of experience in identifying vulnerabilities, implementing security measures, and ensuring the integrity of IT systems. Proficient in conducting risk assessments, monitoring network traffic, and responding to security incidents. Experienced in utilizing security tools and protocols to protect sensitive data and prevent cyber threats. Strong problem-solving skills and a proactive approach to safeguarding organizational assets.

WORK EXPERIENCE

Cyber Security Engineer (2022-present)
VakıfBank

Cortex Soar:

I have been working with the Palo Alto Cortex XSOAR platform for over 3 years, gaining experience in automating security operations, optimizing incident response processes, and integrating threat intelligence.

- Designing and developing SOAR Playbooks
- Integrations with SIEM solutions (Splunk, QRadar, etc.)
- API and automation scripts (Python, PowerShell)
- Incident management, threat hunting, and log analysis
- Custom XSOAR integrations based on users and processes

I have developed dynamic playbooks and custom integrations to accelerate security operations and reduce manual workload. Additionally, I have designed automation strategies to enhance SOC processes and improve overall efficiency.

SIEM:

I have 3 years of experience in SIEM, during which I have worked on log management, event correlation, threat hunting, and security event analysis. I have effectively utilized SIEM platforms to participate in log collection, indexing, correlation rule creation, and custom dashboard development processes.

Skills:

SIEM management and event correlation rule creation

- Log analysis and data normalization
- Development of custom alert mechanisms and automation processes
- SIEM platform integration and customized report generation
- Dashboard creation and advanced query development

Throughout my career, I have worked with various SIEM solutions to optimize log management and event monitoring for enterprise systems. I have developed custom rules and dashboards to accelerate incident management processes, reduce false positives, and improve system performance.

Database Activity Monitoring (DAM):

I have worked with Database Activity Monitoring (DAM) platforms to track and analyze database activities, ensuring real-time detection of suspicious behavior and policy violations. By integrating DAM solutions with SIEM platforms, I developed custom correlation rules to enhance security monitoring and improve incident response.

Skills:

- Monitoring and analyzing database activities in DAM platforms
- Writing SIEM correlation rules for database security events
- Detecting unauthorized access, privilege abuse, and anomaly behaviors
- Integrating DAM logs with SIEM for enhanced security visibility
- Developing custom alerts and dashboards for database security incidents

By leveraging Database Activity Monitoring (DAM) solutions, I improved database security posture by identifying potential threats and optimizing SIEM rules to detect suspicious database activity proactively.

Malware Analysis:

I have gained experience in identifying suspicious files, URLs, and malware infection vectors through malware analysis processes. By utilizing static and dynamic analysis techniques, I examined the functionality of malicious software and classified threats to develop effective defense strategies.

Skills:

- Analyzing malware infection vectors and propagation methods
- Conducting dynamic analysis in sandbox environments
- Examining malware structure and functionality through static analysis
- Investigating suspicious files and URLs to generate threat intelligence
- Reverse engineering techniques for malware analysis

Through my analyses, I identified malware infection methods and their impact, developing effective mitigation strategies. I also contributed to updating security policies by classifying different threat groups.

Picus:

I have utilized Picus Security to conduct attack simulations and developed custom correlation rules on the SIEM to detect security gaps. By analyzing simulation results, I created alert mechanisms to identify threats and optimized incident management processes.

Skills:

- Conducting attack simulations with Picus Security
- Writing SIEM correlation rules based on simulation results
- Enhancing log analysis and attack detection processes
- Creating custom alert mechanisms to reduce false positives
- Integrating SIEM for faster security event detection

By leveraging Picus attack simulations, I identified security weaknesses in SIEM and developed proactive solutions to detect threats in advance.

ACADEMIC HISTORY

Gebze Technical University (2016-2021)

Computer Engineering

During my education at Gebze Technical University, Computer Engineering Department, I focused on algorithms, software development, databases, network security, and artificial intelligence. I applied theoretical knowledge to practical projects and gained expertise in network security, cybersecurity, and system programming.

Key Courses & Skills:

- Programming Languages: C, C++, Python, Java
- System Programming and Operating Systems
- Network Security and Cryptography
- Database Management and Big Data
- Machine Learning and Artificial Intelligence Applications
- Embedded Systems and Hardware Programming

Sakarya University (2021-2022)

Computer Engineering

During my studies in the Computer Engineering program at Sakarya University, I focused on cybersecurity, network security, cryptography techniques, and security management. Throughout my education, I gained in-depth knowledge in areas such as system security, attack detection, secure software development, and cyber threat analysis, and participated in various projects in these fields.

Key Courses & Skills:

- Network Security and Cryptography
- Cybersecurity and Threat Analysis
- System Security and Penetration Testing
- Encryption Methods and Secure Communication
- Attack Detection and Incident Response
- Secure Software Development and Security Testing
- Software Engineering and Secure Coding

Throughout my education, I gained valuable experience in developing defense strategies against cyberattacks and identifying security vulnerabilities.

CERTIFICATION

Cortex XSOAR Administrator:DeploymentCortex XSOARAdministrator:Deployment-->Palo Alto Networks

Python İle Devops TemelleriPython İle Devops Temelleri-->Türkiye Bankalar Birliği

Foundations of Threat HuntingFoundations of Threat Hunting-->Picus Security

Fundamentals of Modern Log Management Practices-->Picus Security

CyberOps AssociateCyberOps Associate-->Cisco

CCNA: Introduction to NetworksCCNA: Introduction to Networks-->Cisco

Splunk 7.x Fundamentals Part 1Splunk 7.x Fundamentals Part 1-->Splunk

Splunk Infrastructure OverviewSplunk Infrastructure Overview-->Splunk

REFERENCES

Akif Mert Avcı
Head Of Secure Banking, VakıfBank

- Phone: 0216 666 80 10
- Email: AkifMert.AVCI@vakifbank.com.tr

Erdem Yolaş

Technical Manager, VakıfBank

- Phone: 0216 666 85 62
- Email: Erdem.YOLAS@vakifbank.com.tr