Senior Cyber-Security Consultant

M. Sc. IT-Security Maksim Melnik

A professional certified cyber-security consultant with expertise in penetration testing, incident response and python programming.

Residence	Frankfurt, Germany
Born	02. February 1993
Languages	German, English, Russian
Email	maksim@mmelnik.de
Website	mmelnik.de
GitHub	github.com/KeksTheAllmighty
StackOverflow	stackoverflow.com/users/5173658/maksim-melnik
LinkedIn	linkedin.com/in/maksim-melnik

Areas of Expertise and Skills

IT-Security: Penetration Testing (Web, Network, Mobile, OT), Phishing Campaigns, Vulnerability Scanning, Red Teaming, Blue Teaming, SOC, Threat Hunting, Security Monitoring, Log Analysis, Incident Response, Use Case and Playbook Development, SIEM, EDR, NDR, XDR, SOAR, MDR, IDS, IPS, Firewall Configuration

Technologies and Frameworks: Burpsuite, Metasploit, Cobalt Strike, Nessus, Bloodhound, GoPhish, Active Directory, Microsoft Sentinel, Microsoft Defender, ArcSight, Palo Alto, Splunk, ELK, Elasticsearch, Opensearch, Hive, Thor, Asgard, Azure, AWS, Google Cloud, Docker, Ansible, Packer, Terraform, Git, Jenkins

Programming Languages: Python, Java, Powershell, Bash, C, C#, C++, HTML, PHP, CSS, Javascript, Dart, Solidity, Gradle, Assembler

Education

B. Sc. Computer Science @ TU-Darmstadt

2012-2016

Thesis: Private Set Intersection based on Elliptic Curve Cryptography

M. Sc. IT-Security @ TU-Darmstadt

2016-2020

Information Security
Network Security
Embedded System Security
Public Key Infrastructures
Cryptography
Cryptocurrencies
Post-Quantum Cryptography
Security of Critical Infrastructures
Data Mining and Machine Learning
Thesis: Social-media based detection of crisis events

Certifications

Google Cybersecurity
Splunk Fundamentals
LPIC-1
CompTIA Security+
CompTIA PenTest+
CompTIA CySA+
eJPT
eCPPTv2
OSCP
OSDA

Experience

Senior Cybersecurity Analyst @ ACG - KFW

November 2020 - Present

- **Cyber Defense & Incident Response Expertise**
  - Cyber Defense Strategy: Expertise in developing and implementing Cyber Defense strategies, including the application of advanced frameworks and integration of security solutions for early detection and prevention of threats
  - Incident Response: Extensive experience in Incident Response and conducting forensic investigations, including identification, analysis, and mitigation of security incidents across complex IT infrastructures
- **Frameworks and Technologies**
  - MITRE ATT&CK Framework: Professional application of the MITRE ATT&CK Framework for analyzing and identifying attack methods, building targeted defense strategies, and optimizing threat detection along the Cyber Kill Chain
  - SIEM (Security Information and Event Management): Long-standing experience in implementing and managing SIEM solutions (e.g., Elastic, Splunk, ArcSight) to monitor IT systems and identify security-relevant events
  - EDR (Endpoint Detection and Response): Expertise in utilizing and managing EDR systems (e.g., Elastic, Splunk, ArcSight) for analysis and defense against threats on endpoints, with continuous security monitoring
  - XDR (Extended Detection and Response): Proficient in the use and integration of XDR technologies (e.g., Microsoft, Palo Alto) for holistic threat detection and analysis across endpoints, networks, and cloud platforms
  - MDR (Managed Detection and Response): Experience in providing and implementing MDR services (e.g., Microsoft MDR) for proactive threat monitoring and response
  - SOAR (Security Orchestration, Automation, and Response): Expertise in utilizing SOAR technologies to automate security operations, reduce response times, and increase operational efficiency when handling security incidents
- **Vulnerability and Threat Analysis**
  - Advanced Persistent Threat Detection: Experience in deploying specialized tools for detecting Advanced Persistent Threats (APT), including the use of Thor (APT scanner) for identifying and analyzing targeted attacks
  - Compromise Assessment: Conducting Compromise Assessments using tools like Asgard and Thor (Nextron Systems) for in-depth security incident analysis and identifying compromised systems
- **Use Case Development and Integration**
  - Use Case Design & Optimization: Expertise in designing, implementing, and optimizing Use Cases to improve the detection capabilities and efficiency of security solutions (SIEM, EDR, XDR)
  - Event Source Integration: Experience in integrating event and log sources into SIEM, EDR, and XDR systems, including the development of connectors for sourcing and analyzing security-relevant events from various platforms
- **Proactive Threat Detection and Analysis**
  - Cyber Attack Detection & Analysis: Expertise in monitoring, detecting, and analyzing cyber-attacks and compliance violations to minimize risks and ensure conformity with security standards
  - Anomaly and Attack Pattern Detection: Proficient in detecting anomalies and attack patterns along the Cyber Kill Chain, identifying early indicators of attacks and enabling fast response
  - Phishing Email Analysis: In-depth experience in analyzing phishing emails, identifying malicious software and social engineering techniques used in attacks

- **Threat Hunting & Technical Consultation**
  - Proactive Threat Hunting: Extensive experience in threat hunting to proactively identify hidden threats and close security gaps
  - Technical Consulting: Providing technical consulting services to clients on deploying protective measures against known and unknown attack methods, as well as strategically improving their security architecture
  - SOC Process Development: Assisting clients in setting up and optimizing SOC processes, including defining security policies and implementing efficient security operations
- **Penetration Testing & Security Assessment**
  - Conducted penetration tests on internal web applications and external-facing services, identifying security vulnerabilities and providing mitigation strategies
  - Performed manual and automated security testing, utilizing tools such as Burp Suite, Metasploit, Nmap and Nessus
  - Documented findings in comprehensive security reports with risk assessments and remediation steps
- **Capture The Flag (CTF) Challenge Development**
  - Designed and set up multiple CTF challenges for internal training and cybersecurity competitions
  - Created real-world attack scenarios to enhance employees' practical security skills
  - Developed challenges covering web security, reverse engineering, cryptography, and forensics
- **Cybersecurity Awareness Training**
  - Led internal cybersecurity awareness training to educate employees on best security practices
  - Covered topics such as phishing attacks, password hygiene, social engineering, and incident response
  - Designed interactive training sessions, including simulated phishing campaigns and hands-on workshops

Financial Markets Data Science & DevOps @ xploras

November 2021 - February 2023

- Configured trading bots using python Freqtrade library
- Implemented trading strategies and backtest process using python TA-Lib, backtrader libraries
- Analyzed performance of trading strategies
- Created a Python Flask website to showcase machine learning approach for stock price forecasting
- Configured GitHub Workflows to build and deploy Google Cloud instances with Ansible and Packer and Terraform

Student Developer @ Ericsson

May 2016 - November 2020

- Developed Gradle scripts for test and deployment of Ericsson BSCS product
- Configured Jenkins jobs for deployment and test of the Ericsson BSCS product
- Developed internal PHP web-applications
- Integrated SSO using Java Keycloak IDM into the internal Spring product
- Implemented high performance messaging system using Java Apache Kafka
- Performed Java resource consumption analysis of the internal Java application using JNI/JVMTI
- Developed Python Robot Tests using Selenium for the internal web application
- Developed a Flutter-application for finding general goods in supermarkets

Student Research Assistant @ TU Darmstadt

November 2017 - June 2018
January 2019 - July 2019

- Developed Wordpress PHP plugin for submission of cyber crime reports
- Designed a PoC of a Hyperledger Smart-Contract
- Implemented a Python LSTM model to forecast Linux machine's vulnerability
- Django backend was implemented to interact with the application

Other

- Participated in Computer Chaos Group meetups @ Darmstadt.
- Participated in numerous CTF events
- Achieved 1st Place @ Merck Hackathon where a Speech-to-Text and Text-to-Speech chat-bot was deployed in Azure infrastructure
- Discovered and reported kernel vulnerability @ TU-Darmstadt.
- Co-Authored a paper