Lena Hartmann | Senior IT-Sicherheitsingenieurin

Friedrichstraße 123, Berlin, Berlin, Deutschland, 10117
+49 30 12345678 • lena.hartmann@security-mail.de • https://www.lhartmann.dev
@lhartmann • @lhartmann

Basisinformationen

- Mehr als 7 Jahre Erfahrung in der IT-Sicherheit mit Fokus auf Angriffserkennung, Incident Response und Sicherheitsarchitekturen
- Fundierte Kenntnisse in Penetrationstests, Schwachstellenmanagement und der Absicherung von Cloud-Infrastrukturen
- Erfahrung mit SIEM-Systemen (Splunk, Wazuh), Firewalls und IDS/IPS sowie der Automatisierung von Sicherheitsprozessen
- Teamorientiert, analytisch und kommunikationsstark; gewohnt, komplexe Sicherheitsrisiken verständlich zu erklären

Ausbildung

Technische Universität Berlin **https://www.tu.berlin**
Master, IT-Sicherheit, Punkte: 1.3 *Okt. 2016–Sept. 2018*

- Schwerpunkt auf angewandter Kryptographie und der Absicherung verteilter Systeme
- Masterarbeit zum Thema Ërkennung von Advanced Persistent Threats mittels Machine Learning"
- Praktische Erfahrung durch Laborprojekte zu Penetrationstests und Sicherheitsarchitekturen

Kurse: Kryptographie und Sicherheitsprotokolle, Netzwerksicherheit und Firewalls, Secure Software Engineering, Incident Response und Forensik, Datenschutz und Compliance, Cloud Security und Virtualisierung

Hochschule für Technik und Wirtschaft Berlin **https://www.htw-berlin.de**
Bachelor, Informatik, Punkte: 1.7 *Okt. 2012–Sept. 2016*

- Grundlagen in Programmierung, Datenbanken und Netzwerktechnik
- Wahlpflichtmodule zu IT-Sicherheit und Systemadministration

Berufserfahrung

SAP SE **https://www.sap.com**
Senior IT-Sicherheitsingenieurin *Apr. 2020–Heute*

- Leitung von Penetrationstests und Sicherheitsaudits für cloudbasierte Unternehmensanwendungen
- Entwicklung und Betrieb von SIEM-Regeln zur Erkennung von Angriffsmustern und Anomalien
- Durchführung von Incident-Response-Maßnahmen und forensischen Analysen bei Sicherheitsvorfällen
- Mitwirkung bei der Implementierung und Zertifizierung nach ISO 27001 und BSI-Grundschutz
- Automatisierung von Sicherheitsprüfungen mit Python und Terraform

Schlüsselwörter: Penetration Testing, SIEM, Incident Response, ISO 27001, Cloud Security

Deutsche Telekom AG **https://www.telekom.com**
IT-Sicherheitsanalystin *Okt. 2018–März 2020*

- Überwachung und Analyse von Sicherheitsereignissen im 24/7-Security-Operations-Center
- Bearbeitung von Sicherheitsvorfällen nach definierten Playbooks und Eskalationsprozessen
- Durchführung von Schwachstellenanalysen und Bewertung von Risiken in Netzwerk- und Systemumgebungen
- Erstellung von Sicherheitsreports und Präsentationen für technische und nicht-technische Stakeholder

Schlüsselwörter: SOC, SIEM, Schwachstellenanalyse, Netzwerksicherheit, Incident Response

Sprachen

Deutsch: Muttersprache oder zweisprachig — **Schlüsselwörter**: Muttersprache

Englisch: Verhandlungssichere Kenntnisse — **Schlüsselwörter**: Verhandlungssicher, TOEFL 110

Französisch: Gute Kenntnisse — **Schlüsselwörter**: Grundkenntnisse

Fähigkeiten

Netzwerksicherheit: Experte — **Schlüsselwörter**: Firewalls, VPN, IDS/IPS, Wireshark, Netzwerksegmentierung

Penetration Testing: Erfahren — **Schlüsselwörter**: Metasploit, Burp Suite, Nmap, OpenVAS, Nessus

Incident Response: Erfahren — **Schlüsselwörter**: SIEM (Splunk, Wazuh), Forensik, Threat Hunting, Playbook-Entwicklung

Cloud Security: Fortgeschritten — **Schlüsselwörter**: AWS, Azure, IAM, Kubernetes, Terraform

Compliance und Datenschutz: Erfahren — **Schlüsselwörter**: ISO 27001, BSI-Grundschutz, DSGVO, Risikomanagement

Programmierung und Automatisierung: Erfahren — **Schlüsselwörter**: Python, Bash, PowerShell, Git, CI/CD

Auszeichnungen

Cybersecurity Excellence Award

Bundesverband IT-Sicherheit e.V. *Nov. 2022*

- Auszeichnung für die erfolgreiche Einführung eines unternehmensweiten Threat-Intelligence-Programms
- Anerkennung für besonderes Engagement in der Nachwuchsförderung im Bereich IT-Sicherheit

Zertifikate

Certified Information Systems Security Professional (CISSP) **https://www.isc2.org**

ISC2 *Juni 2021*

Offensive Security Certified Professional (OSCP) **https://www.offsec.com**

Offensive Security *Nov. 2019*

ISO/IEC 27001 Lead Auditor **https://www.tuv.com**

TÜV Rheinland *März 2020*

Veröffentlichungen

Zeitschrift für IT-Sicherheit **https://www.zeitschrift-it-sicherheit.de/artikel/apt-ml**

Erkennung von Advanced Persistent Threats mittels Machine Learning *Dez. 2019*

- Analyse von Netzwerk- und Hostdaten zur frühzeitigen Erkennung komplexer Angriffsmuster
- Vergleich verschiedener Machine-Learning-Verfahren hinsichtlich Genauigkeit und False-Positive-Rate
- Praxisnahe Evaluation in einer virtualisierten Unternehmensumgebung

Projekte

Aufbau eines Security Operations Center (SOC)

Zentraler Aufbau eines SOC zur Erkennung und Reaktion auf Sicherheitsvorfälle in einer hybriden Cloud-Umgebung.Jan. 2021–Dez. 2021

- Konzeption und Implementierung eines SOC für die zentrale Überwachung von Sicherheitsereignissen
- Integration von SIEM-, Ticketing- und Threat-Intelligence-Systemen
- Definition von Alarmierungs- und Eskalationsprozessen

Schlüsselwörter: SOC, SIEM, Threat Intelligence, Incident Response

Threat-Intelligence-Plattform

Eine Plattform zur Sammlung, Normalisierung und Priorisierung von Threat-Intelligence-Daten aus verschiedenen Quellen.März 2019–Feb. 2

- Entwicklung einer Plattform zur Aggregation und Auswertung von Threat-Intelligence-Feeds
- Automatisierte Anreicherung von Sicherheitsereignissen mit Kontextdaten
- Bereitstellung von Dashboards für das Sicherheitsteam

Schlüsselwörter: Threat Intelligence, Python, APIs, Elasticsearch

Interessen

Capture the Flag (CTF): HackTheBox, TryHackMe, CTF-Wettbewerbe

Open Source: Security-Tools, GitHub, Community

Sport: Laufen, Klettern, Radfahren

Ehrenamtliche Tätigkeiten

Bundesverband IT-Sicherheit e.V. **https://www.bv-it-sicherheit.de**

Mentorin für Nachwuchskräfte *Jan. 2021–Heute*

- Betreuung von Studierenden und Berufseinsteigern bei CTF-Wettbewerben und Sicherheitsprojekten
- Durchführung von Workshops zu Themen wie Penetration Testing und Incident Response
- Förderung des Austauschs zwischen Hochschulen und Industrie