ALTERSOLUTIONS DEUTSCHLAND

KOMPETENZPROFIL

5342

Kontaktieren Sie uns

IT Security Engineer

Management Summary

- Mehr als Sieben Jahre privat und beruflich im Penetration Testing und der IT / IT-Sicherheit (WLAN Auditing, Datenbank Penetration, mobile Penetration Test Systeme, Anti-Spam & Malware Protection)
- Stark ausgeprägte Neugier gegenüber physischen und digitalen Schwachstellen, dessen Identifikation und Auflösung und hohe Disziplin im Sicherheitsgedanken für den Kunden lösungsorientiert zu denken und zu handeln, hohe Kundenservicementalität und Kommunikationsfähigkeit sowie internationale Berufserfahrung bei einem führenden deutschen Anti-Spam Cloud Software Hersteller (Service & Kommunikation, Monitoring, Backend Analysen mit Linux)
- Hervorzuhebende Projekte und Referenzen:
  - Berufsausbildungsabschlussprojekt Diakovere Berufsbildungswerk Annastift gGmbH – Penetration Teststation zur zeitgesteuerten Analyse von Schwachstellen im Produktivfirmennetzwerk
  - Berufsausbildung Englisch - Kurs C1 – Kursprojekt: Erstellen eines interaktiven Workshops zum Exploit „Eternal Blue“ und Durchführung mit Kursteilnehmern (Capture the Flag)
  - Hornetsecurity GmbH: Telefonleitfaden – Projekt: Erstellung eines Kommunikationsleitfadens zur telefonischen Kundenkommunikation
  - Hornetsecurity GmbH: Permanente Servicetätigkeiten in Fragen von 1st und 2nd Level Support unterschiedlichster internationaler Branchenkunden (z. B. CLAAS, HDI, Swisscom, Miele, Dekra oder Otto) und Beratung bei allen Kundenanfragen zu den gängigsten Sicherheitsprodukten der Unternehmung und Unterstützung im Bedarf bei Projekten zur Kunden Awareness und Anti-Phishing Kampagnen sowie bei Cybersecurity Incidents

- Deka Bank Projekt mit tagesgeschäftlicher Beratung in der Abteilung IT-Sicherheit mit Schwerpunkt auf das Anti Spam & Phishing Geschäft sowie Security Incident Bearbeitung, SIEM, Threat Hunting, Threat Intelligence, Dispatching, Mitarbeitereinarbeitung, Use Case Anpassungen und Erstellung
- Security Engineer & SOC 1/2nd Level Analyst Liebherr Projekt: Erstellung und Beratung bezüglich Erkennungsregelwerken in Elastic via SIEM, Mitarbeitereinarbeitung, Anti-Spam / Phishing und Umgang in Bearbeitung von ProofPoint Alarmen sowie Alarmen aus dem Monitoring des MDE (Microsoft Defender for Endpoints) für Tiefenanalysen, Templateerstellung und Prozessmitaufbau eines angehenden SOC wurden mitunterstützt.

ALTER SOLUTIONS DEUTSCHLAND

KOMPETENZPROFIL

Persönliche Daten

Berufserfahrung	**8,5 Jahre**
Branchenkenntnisse	Bank, Bildung, Softwarehersteller – Cloud SaaS – Antispam & Malware Protection Services, Baumaschinen / Industrial
Verfügbarkeit	Nach Absprache

Ausbildung

09/2016 – 07/2019	Fachinformatiker*in – Systemintegration

Weiterbildungen

02 / 2024	OSDA (OffSec Defense Analyst)
2021	Altaro VM Backup & Certified Professional [Level 100 – 300]
2021	Pentesting Kurs (Udemy)
2021	26 PenTests Training (auf Maschinen bei Hack the Box)
2019	Ethical Hacking Kurs & Abschlussprojektarbeit

Sprachkenntnisse

Deutsch	Sehr gute Kenntnisse
Englisch	Sehr gute Kenntnisse

Methoden-, Technologie- und Tool-Kenntnisse

Methoden	ITIL, Wasserfallmodell, Ethical Hacking, Penetration Testing, Offensive Security Defender Analyst (OSDA zertifiziert)

Technologien	WLAN / LAN / WAN, Backup & Storage, SaaS, IoT (Blockchain, Zahlungsverkehr, Netzwerke, dezentrales Hosting IPFS) elektrotechnische Grundlagen, Elektronische Systeme mit Raspberry Pi, Virtualisierung unter VirtualBox, VMWare, ProxMox, OSInt
Tools	Windows, Linux – Kali Linux, Debian, Ubuntu, MS Office, Libre Office, MS Visual Studio, allen gängigen Tools aus Backtrack & Kali Linux, insbesondere: Metasploit, Faraday, OpenVAS, Nessus, Cobalt Strike (Armitage), nmap, wireshark sqlmap, jSQL, shodan, hashcat, crunch, cut, hydra, Burp Suite, Nikto, v3n0m Dork Scanner, fluxion evil twin, mdk3, sslStrip, GhostPhisher, SET, macchanger, proxychains, OWASP-ZAP, Vega, wpscan, aircrack-ng Suite, Wifite, reaver, Maltego,
Sonstiges	Programmierung mit Bash, VBA, VB Classic, VB.Net und Visual C++, Elastic Stack, Splunk / SIEM / Use Cases

ALTER SOLUTIONS DEUTSCHLAND

KOMPETENZPROFIL

Projekterfahrung

Security Engineer – SOC

Zeitraum	11/2024 – 06/2024
Branche	Baumaschinen / Diverse
Kunde	Liebherr
Projektumfeld	Cyber Security / SOC
Tätigkeiten	Tagesgeschäftliche Mitarbeit und Beratung: - Erstellung von Detection Rules zur Erkennung von Bedrohungen nach MITRE - Security und Support Engineering bezüglich JIRA Ticket System / Confluence / Elastic Stack - Palo Alto und ZScaler Proxy Auswertungen in SIEM (ELK Stack) - Anti-Spam und Phishing mit Proofpoint - Microsoft Defender for Endpoint Tiefenanalysen bezüglich des Alert Monitorings und Ticketbearbeitung - Mitarbeitereinarbeitung SOC Tier 1 / 2 Analyst - Prozessmitgestaltung / SOP Erstellung / Templateerstellung im Ticket Processing für MDE & ProofPoint - Ticketreview- und Improvement im Daily Business - Windows und Linux Endpunkt Analyse bei aktuellen Alarmen der MDE
Methoden	Security Analysis, Security Engineering – SIEM, OSDA (SOC-200)

Technologien/ Tools	**Anwendungssoftware**: Google Chrome, Microsoft Edge, MS Office Paket (darunter MS Word, MS Excel, MS Skype, MS Teams, MS Project, MS Outlook), Jira, KeePass **Individualsoftware**: Jira, Confluence **Systemsoftware**: MS Windows, Unix basierende Systeme **Technologien**: Microsoft Defender for Endpoint, ProofPoint

ALTERSOLUTIONS DEUTSCHLAND

KOMPETENZPROFIL

SoC Analyst – IT Security Management

Zeitraum	06/2021 – 09/2023
Branche	Banken, Finanzen
Kunde	Deka Bank Frankfurt am Main
Projektumfeld	Cyber Security / Malware
Tätigkeiten	➢ Einarbeitung neuer Mitarbeiter ➢ Mitarbeiter- und Kundenkommunikation ➢ Security Incident Analyse & Lösungen ➢ Beauftragung externer Dienstleister zur Auftragserfüllung ➢ Beratung zu Spam & Phishing ➢ Tiefenanalyse bei Spam & Phishing inkl. Headeranalyse und Beratung ➢ Monitoring aller Systeme bzgl. Richtlinienverletzungen und Netzwerkanomalien ➢ Threat Hunting ➢ Reporting / Dokumentation an Gruppenleitung / Vorstand ➢ Erweiterung des internen Wikis ➢ Korrespondenz und Organisation zwischen Fachabteilungen intern ➢ Priorisierung und Eskalation ➢ Dispatching von Cases (ITIL) ➢ Use Case Anpassungen, Logikerarbeitung und Erstellung ➢ Skripting und Templateerstellung
Methoden	IT Betrieb nach ITIL, Incident Management, Incident Response, Monitoring, 2nd & 3rd Level Support, MITRE, OWASP 10

Technologien/ Tools	**Anwendungssoftware**: Google Chrome, Microsoft Edge, MS Office Paket (darunter MS Word, MS Excel, MS Skype, MS Teams, MS Project, MS Outlook), ITSM Remedy, KeePass **Individualsoftware**: Gitlab, Ironport, Splunk, Radar Services, Kibana, FireEye AX, HX, NX, FireEye ETP Email Security Solution **Systemsoftware**: MS Windows, Unix basierende Systeme **Technologien**: Advanced Threat Protection, Targeted Forensics Fraud Filter, URL Rewriting, Spam und Malware Protection und Filteranpassungen, Tiefenanalyse des Mailheaders, Content Filter, Reporting, Auditing, E-Mail Log-Analyse, Webfilter, SPF, DKIM, DMARC, ITSM BNC Remedy, Kibana, Radar Services, Splunk, Ironport, FireEye Produkte, SIEM, Reverse Engineering

ALTERSOLUTIONS DEUTSCHLAND

KOMPETENZPROFIL

IT-Service Operator

Zeitraum	08/2019 – 05/2021
Branche	Softwarehersteller d. kritischen Infrastruktur – Cloud SaaS – Anti Spam & Malware Protection Services
Kunde	Hornetsecurity GmbH
Projektumfeld	Anti-Spam & Service
Tätigkeiten	➢ Internationaler First & Second Level Support im 24/7 Schichtbetrieb - Ticketbearbeitung & Telefon nach ITIL in OTRS und Zendesk ➢ Kundendeeskalation und Kundenzufriedenheit ➢ Monitoring der Infrastruktur (Spamversand Prävention, Interne sowie Kundeninfrastrukturfehlerbehebung und Eskalation) ➢ Bearbeitung von Service Incidents intern, sowie Cyber Security Incidents mit Kunden ➢ Unterstützen von Awareness Kampagnen und Anti-Phishing Kampagnen bei Kundenprojekten
Tätigkeiten	➢ Backendanalysen unter Linux zur Ermittlung von individuellen Kundensachverhalten technischer Natur zu allen Produkten des Unternehmens
Methoden	IT Betrieb nach ITIL, Incident Management, Incident Response, LPIC01

Technologien/ Tools	**Anwendungssoftware**: Google Chrome, Mozilla Firefox, Opera, Microsoft Edge, MS Office Paket (darunter MS Word, MS Excel, MS Skype, MS Teams, MS Project, MS Outlook), OTRS, Zendesk, Thunderbird, KeePass, PWgen, EMLConverter **Individualsoftware**: Gitlab, YouTrack, Dokumentation mit Wiki, On-Premises Exchange, Office365 Mail Cloud, Virtualisierung & Backup mit Altaro VM Backup, Icinga Monitoring mit Nagstamon, eigenentworfene E-Mail-Headeranalyse Tools und Loganalysetools unter Bash **Systemsoftware**: MS Windows, Debian, Ubuntu, Kali Linux, Backend on Windows 10 (Ubuntu WSL) **Technologien**: Advanced Threat Protection, Targeted Forensics Fraud Filter, URL Rewriting, E-Mail Encryption durch S/MIME, PGP, TLS, EMIG, Websafe, Spam und Malware Protection und Filteranpassungen mit Regular Expressions , O365 Total Protection & Encryption, rechtssichere Archivierung, E-Mail Continuity, erweitertes E-Mail-Routing, E-Mail Compliance, Content Filter, Quarantäne Reporting, Auditing, Control Panel Services (E-Mail Live Tracking), Whitelabeling, Webmailer, encrypted Cloud Storage, Signatur- und Disclaimer, Webfilter, SPF, DKIM, DMARC, DNS, telnet, LDAP & Active Directory, bash, OTRS, Zendesk, SMTP, POP3, IMAP, postfix, dovecot

ALTER SOLUTIONS DEUTSCHLAND

KOMPETENZPROFIL

Projektmitwirkende*r

Zeitraum	01/2020 - 03/2020
Branche	Softwarehersteller d- kritischen Infrastruktur – Cloud SaaS – Anti Spam & Malware Protection Services
Kunde	Hornetsecurity GmbH
Projektumfeld	Erstellen eines Leitfadens für Telefontrainings zur internen Mitarbeiterschulung gegenüber Kunden
Tätigkeiten	➢ Informationsbedarfsanalyse ➢ Konzeptionierung und Struktur des Projektumfangs ➢ Umsetzung der Inhalte im Team ➢ Kontrolle auf Ausrollbarkeit ➢ Projektabschluss und Aussichten sowie Dokumentation
Technologien/Tools	Wasserfallmodell, Partiell ITIL, MS Word, MS Skype, MS Teams, MS Outlook, GANTT

ALTERSOLUTIONS DEUTSCHLAND

KOMPETENZPROFIL

Projektleiter*in und Projektausführende*r

Zeitraum	03/2019
Branche	Bildung
Kunde	DIAKOVERE Annastift Leben und Lernen gGmbh
Projektumfeld	Erstellen einer Penetration Teststation zur zeitgesteuerten Netzwerksicherheitsanalyse
Tätigkeiten	➢ Konzeptionieren des Projektrahmens & Kundengespräch ➢ Konzeption der benötigten ganzheitlichen Ressourcen zur Projekterfüllung
Tätigkeiten	➢ Analyse unter Berücksichtigung der Kundenspezifikationen ➢ System Realisierung ➢ Kontrolle nach Umsetzung auf Funktionalität, Sicherheit und Komfort ➢ Projektabschluss & Dokumentation ➢ Kurzschulung & Projektübergabe
Technologien/Tools	Wasserfallmodell, MS Office, Sophos Firewall Interface, Kali Linux & Toolset, OpenVAS, ProxMox Hypervisor, GANTT