Komm ins #TeamBSI

Wir sind die Cybersicherheitsbehörde des Bundes. Gemeinsam gestalten wir mit derzeit rund 1.800 Beschäftigten eine sichere digitale Zukunft für Deutschland. Durch die rasante Entwicklung der Digitalisierung wächst – neben unseren Aufgaben – auch unser Team stetig weiter. Hierfür suchen wir engagierte Fachkräfte, die mit uns eine sichere digitale Welt gestalten.

IT-Security Analystin/Analyst (w/m/d) im Bereich „Erstellung und Anpassung von Signaturen“

(Entgeltgruppe E 13 TVöD bzw. die vergleichbare Besoldungsgruppe gemäß BBesO)

unbefristet am Dienstort Bonn

Das Referat I 33 ist Teil des Bundes Security Operations Center (BSOC). Dies umfasst unter anderem Dienstleistungen zur Erfassung und Auswertung von Protokollierungs- und Sensordaten sowie zur Erkennung und Abwehr von Schadsoftware in E-Mails und Webverkehr. Hierfür hat das BSI verschiedene Systeme entwickelt, die kontinuierlich an die Bedrohungslage angepasst werden. Insbesondere die Erstellung und Fortschreibung der hierfür erforderlichen Muster und Signaturen liegt in der Verantwortung von Referat I 33. Ziel hierbei ist es, durch eine größtmögliche Automatisierung unter Nutzung aktueller Produkte und KI-unterstützter Verfahren ausreichend Freiräume für die notwendigen manuellen Analysen zu schaffen, die unter Einhaltung enger rechtlicher Vorgaben erfolgen.

1. PLATZ
Attraktivste Arbeitgeber 2026
Für Akademiker_innen
Öffentlicher Sektor / NGO's
trendence

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Aufgabenschwerpunkte des Referats:

- die Analyse von Cyber-Angriffen zur Erstellung von Signaturen für die eingesetzten zentralen und dezentralen Detektionssysteme,
- die Bereitstellung und Auswertung von Operativer Threat Intelligence zur Verbesserung von Signaturen,
- die Konfiguration der Anomalie- bzw. Mustererkennung in den Detektionssystemen auf der Basis von Verfahren zum maschinellen Lernen oder KI,
- den Aufbau von Simulationsumgebungen zur Ermittlung der Wirksamkeit der genutzten Erkennungsmethoden und
- die Durchführung von Umgehungstests.

Was dieses Referat prägt, ist ein starker Teamgeist, ein hohes Maß an technischer Expertise und der Anspruch die Detektion von Cyber-Angriffen zu gestalten und kreative Lösungen mit innovativen Ansätzen zu entwickeln.

Ihre Tätigkeiten sind:

- Analyse und Auswertung aktueller "Trends" im Bereich Detektion zur Erstellung von Signaturen.
- Identifikation und Auswertung von OSINT-Informationen, Produktentwicklungen und Publikationen zu neuen Detektionsansätzen hinsichtlich der Verwendbarkeit im BSOC und prototypische Entwicklung neuer Analysemechanismen zur Detektion.
- Identifikation von fachlich technischen Voraussetzungen und Lösungen für eine automatisierte Analyse von Schadsoftware und Konzeption und Entwicklung von Container basierten Softwaremodulen und Schnittstellen, sowie modul- und produktübergreifenden Datenaustauschformaten.
- Konzeption für eine automatisierte Erstellung von Detektionsmustern bzw. Signaturen anhand von Protokoll- und Protokollierungsdaten im Kontext §§ 8 und 9 BSIG.
- Entwicklung und Implementierung von Diensten zur Erhebung und Verwaltung von Kennzahlen für §§ 8 und 9 Bericht BSIG.
- Beschaffung und Auswahl geeigneter TI-Quellen. Ableitung geeigneter Einflussgrößen und Bildung geeigneter Kennzahlen zur Beschreibung.
- Zusammenarbeit mit weiteren operativen Bereichen des BSI z.B. CERT Bund (Computer Emergency Response Team), Mobile Incident Response Teams (MIRT), Technische Analyse / Forensik, Threat Intelligence, Cyber-Abwehrzentrum etc.

Ihr Profil:

- Ein abgeschlossenes bzw. kurz vor dem Abschluss stehendes Studium (Diplom Univ./Master) der Fachrichtungen Informatik, technische Informatik, IT-Sicherheit, Physik, Mathematik, Nachrichten-, Kommunikations-, Elektrotechnik oder Wirtschaftsinformatik.
- Gute Kenntnisse und idealerweise bereits praktische Erfahrungen in einem oder mehreren der folgenden Bereiche:
    - TCP/IP, aktuelle Netzwerk-, Server- und Softwaretechnologien (Layer 1-7)
    - Gängige Dateitypen (PDF, PE32, DOCX etc.)
    - Betriebssysteme und Standardanwendungen
    - Auswertung von Logdaten zum Betriebs- oder Sicherheitsmonitoring
    - Erfahrung im Umgang mit LLMs und agentischen Workflows.
- Die wesentlichen Cyberangriffsformen sind Ihnen bekannt, u.a. haben Sie sich mit dem Thema Advanced-Persistant-Threat (APT) auseinandergesetzt.
- Von Vorteil sind Detailkenntnisse in folgenden Bereichen:
    - Signaturformate wie Yara, ClamAV oder Snort
    - Analyse von Programmen (vor allem PE32), Skripten (Powershell, JS, VBS, VBA etc.) und Dokumenten (MS-Office, PDF, RTF etc.)
    - Programmierung (z.B. Python, C/C++, Rust, Bash)
    - Installation, Konstellation und Nutzung des Elastic Stack

Was uns noch wichtig ist:

- Sie arbeiten gerne strategisch und können Prozesse strukturiert voranbringen.
- Sie haben ein verbindliches und freundliches Auftreten sowie eine überzeugende mündliche und schriftliche Ausdrucksfähigkeit.
- Im Team arbeiten Sie aufgeschlossen, sind kritikfähig und bringen sich kooperativ sowie eigeninitiativ in Ihre Arbeit ein.
- Das #TeamBSI profitiert von Ihrer entscheidungsfreudigen und zielgerichteten Arbeitsweise.
- Ihre Motivation lebenslang zu lernen und sich dadurch in Ihren Fähigkeiten, Fertigkeiten und Ihrem Wissen kontinuierlich weiterzuentwickeln.
- Sie verfügen über sehr gute deutsche und gute/sehr gute englische Sprachkenntnisse in Wort und Schrift (Deutsch mind. C 1).
- Sie bringen die Bereitschaft zur Teilnahme an Fortbildungen sowie zur Übernahme gelegentlicher Dienstreisen - unter Berücksichtigung der Vereinbarkeit von Familie und Beruf - mit.

Was wir bieten:

- Eine anspruchsvolle und abwechslungsreiche Aufgabe mit gesellschaftlichem Mehrwert bei der Gestaltung einer sicheren digitalen Zukunft Deutschlands.
- Vereinbarkeit von Privat- und Berufsleben durch flexible Arbeitsgestaltung, die Möglichkeit zum mobilen Arbeiten in Deutschland sowie Teilzeitarbeit- weitere Infos als FAQ.
- Eine gezielte Einarbeitung und gute Entwicklungsmöglichkeiten durch Fort- und Weiterbildungsangebote zur persönlichen und fachlichen Qualifikation.
- Einen sicheren und krisenfesten Arbeitsplatz, die Perspektive einer Verbeamtung sowie ein vielseitiges Gesundheitsangebot.
- Eine monatliche BSI-Zulage in Höhe von 200 €.
- Unterstützung bei den Umzugskosten oder Zahlung von Trennungsgeld unter bestimmten Voraussetzungen.
- Ein vergünstigtes Monatsticket für den Personennahverkehr (Job-Ticket) oder alternativ ein vergünstigtes Deutschlandticket.

Mehr über uns gibt es auf #TeamBSI und auf unseren sozialen Netzwerken

Sie haben Interesse? Dann bewerben Sie sich jetzt im Team BSI bis zum 22.07.2026

Ihr Kontakt zu uns:

- Fragen zur Personalgewinnung: Vera Hanses (Personalgewinnung des BSI) unter 0228 99 9582 6719
- Fachliche Fragen: Dr. Marcel Langenberg (Referatsleitung I 33) unter 0228 99 9582 6763
- Fragen zum Bewerbungsmanagementsystem: Servicezentrum Personalgewinnung des Bundesverwaltungsamtes unter 0228 99 358 87500

1. PLATZ
Attraktivste Arbeitgeber 2026
Für Akademiker_innen
Öffentlicher Sektor / NGO's
trendence

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Wissenswertes:

- Wir als BSI möchten Frauen ausdrücklich ermutigen, sich zu bewerben. Bei gleicher Qualifikation werden Frauen nach Bundesgleichstellungsgesetz bevorzugt berücksichtigt. Diversität und geschlechterunabhängige berufliche Gleichstellung sind für uns wichtige Bestandteile der Personalpolitik. Über Bewerbungen von Menschen jeder Herkunft sowie aller geschlechtlichen Identitäten und sexueller Orientierungen, Altersgruppen, Religionen und Weltanschauungen freuen wir uns.
- Das BSI sieht sich in besonderer Weise der gleichberechtigten Teilhabe von Menschen mit Behinderungen am gesellschaftlichen Leben verpflichtet. Daher sehen wir nicht nur den Bewerbungen von schwerbehinderten und ihnen gleichgestellten Menschen sehr gerne entgegen, sondern wir werden sie bei gleicher Eignung und vorbehaltlich gesetzlicher Regelungen bevorzugt berücksichtigen. Es wird lediglich ein Mindestmaß an körperlicher Eignung verlangt.
- Mit der Unterzeichnung der Charta der Vielfalt und unserer Mitgliedschaft bei Employers for Equality stehen wir für ein wertschätzendes und vorurteilsfreies Arbeitsumfeld.
- Ihr Einverständnis zur Durchführung einer erweiterten Sicherheitsüberprüfung nach § 9 SÜG (Sicherheitsüberprüfungsgesetz) ist Voraussetzung für eine Bewerbung. Diese Sicherheitsüberprüfung darf nicht zum Ergebnis haben, dass ein Sicherheitsrisiko vorliegt, das der sicherheitsempfindlichen Tätigkeit entgegensteht (§ 14 SÜG).
- Bei ausländischen Bildungsabschlüssen ist ein entsprechender Nachweis über die Gleichwertigkeit mit einem deutschen Abschluss erforderlich (Übersetzungen sind nicht ausreichend). Wir bitten um Vorlage der Feststellung der Vergleichbarkeit durch die Zentralstelle für ausländisches Bildungswesen (ZAB). Weitere Informationen dazu finden Sie hier.
- Für uns hat ein verantwortungsbewusster Umgang mit personenbezogenen Daten hohe Priorität. Wir möchten, dass Sie wissen, wann welche Daten erhoben und wie sie verwendet werden. Das BSI hat technische und organisatorische Maßnahmen getroffen, die sicherstellen, dass die Vorschriften über den Datenschutz beachtet werden. Unsere detaillierten Datenschutzbedingungen finden Sie hier.