KI-ABWEHRZENTRUM

Das Security Operations Center der Zukunft. Ihre Lösung gegen die Cyberangriffe von morgen.

Ihr Kontakt zum KI-ABWEHRZENTRUM

ASOFTNET GmbH & Co. KG
Haarbergstr. 63, 99097 Erfurt

Telefon: +49 361 775195-00
Telefax: +49 361 775195-09
E-Mail: info@asoftnet.de

www.ki-abwehrzentrum.de

VORWORT

Die Welt befindet sich inmitten einer digitalen Revolution, die von Künstlicher Intelligenz (KI) angetrieben wird. Diese Technologie verändert die Art und Weise, wie wir arbeiten, kommunizieren und leben. KI kann Daten schneller analysieren, Muster erkennen, die dem menschlichen Auge entgehen, und Aufgaben autonom ausführen, die früher nur von Menschen erledigt werden konnten.

Doch mit diesen Fortschritten gehen auch erhebliche Risiken einher. KI kann manipuliert werden, um Cyberangriffe zu verstärken, Desinformationskampagnen zu automatisieren oder sogar autonome Waffensysteme zu steuern. Diese Bedrohungen betreffen nicht nur einzelne Individuen, sondern können ganze Nationen destabilisieren und globale Krisen auslösen.

Das KI-ABWEHRZENTRUM wurde ins Leben gerufen, um diesen Herausforderungen zu begegnen und eine sichere Nutzung von KI zu gewährleisten. Es ist das Security Operations Center der Zukunft: Ein SOC, das mittels KI Angriffe erkennt und abwehrt – schneller und effizienter als ein Mensch es je könnte. Unser Ziel ist es, die positiven Seiten von KI zu nutzen, um die negativen zu bekämpfen. Wir glauben daran: Die Zukunft der IT-Sicherheit heißt KI-ABWEHRZENTRUM.

Alexander Sowinski
Gründer des KI-ABWEHRZENTRUMS
CEO, ASOFTNET GmbH & Co. KG

INHALT

UNSERE MISSION:
SCHUTZ DURCH INNOVATION

Da die Bedrohungen durch KI täglich wachsen, ist es unsere oberste Priorität, Sicherheit durch ständige Innovation zu gewährleisten. Das KI-ABWEHRZENTRUM sieht seine Mission darin, die Gesellschaft vor den potenziellen Gefahren von KI zu schützen, während es gleichzeitig die Möglichkeiten dieser Technologie für intelligente Schutzmaßnahmen fördert.

Dies bedeutet: Wir reagieren nicht nur reaktiv auf Bedrohungen, sondern suchen proaktiv nach neuen Wegen, um Sicherheitslücken aufzudecken und zu schließen sowie geplante Angriffe zu erkennen, bevor sie ausgenutzt werden können.

So erreichen wir sie

Durch die Entwicklung fortschrittlicher Technologien, die den neuesten Bedrohungen gewachsen sind, wollen wir sicherstellen, dass die KI zum Wohl der Gesellschaft eingesetzt wird und ihre Risiken minimiert werden.

Unsere Arbeit vereint Expertise aus den Bereichen Cybersicherheit, Maschinelles Lernen, Ethik und Krisenmanagement, um ganzheitliche Lösungen zu entwickeln, die dem rasanten Fortschritt von KI-Technologien gewachsen sind.

KI ZWISCHEN NUTZEN & GEFAHR

Die Möglichkeiten von KI sind schier unbegrenzt: Vom autonomen Fahren über medizinische Diagnosen bis hin zur Effizienzsteigerung in der Industrie – die Potenziale dieser Technologie sind enorm.

DOCH WO LICHT IST, IST AUCH SCHATTEN

KI kann genauso gut für destruktive Zwecke eingesetzt werden, etwa zur Durchführung von Cyberangriffen, zur Automatisierung von Desinformationskampagnen oder zur Steuerung autonomer Waffensysteme. Darüber hinaus stellt die rasante Entwicklung der KI auch ethische Herausforderungen dar: Wer trägt die Verantwortung, wenn ein KI-System eine fatale Entscheidung trifft? Wie verhindern wir, dass KI-Systeme ungewollt Vorurteile verstärken oder diskriminierende Entscheidungen treffen? Diese Fragen zeigen, dass die Einführung und der Einsatz von KI-Technologien sorgfältig geplant und überwacht werden müssen.

Das KI-ABWEHRZENTRUM sieht sich in der Verantwortung, nicht nur technologische, sondern auch gesellschaftliche und ethische Aspekte zu berücksichtigen.

206 Milliarden Euro
Schaden pro Jahr
durch Datendiebstahl,
Spionage und Sabotage*

Zeitraum bis zur
Angriffserkennung:
ohne SOC: 165 Tage,
mit SOC: 1 Tag

*Quelle: Bitkom 2023

DARUM EIN KI-ABWEHRZENTRUM

Die Möglichkeiten und Einsatzbereiche von KI entwickeln sich unaufhaltsam weiter. Mit ihnen steigt auch die Abhängigkeit von KI-Systemen. Noch dazu sind diese Systeme anfällig für Angriffe und Missbrauch. Die Folgen können weitreichend sein.

Ein gezielter Angriff auf kritische Infrastrukturen, wie das Stromnetz, die Wasserversorgung oder Finanzsysteme, könnte das gesellschaftliche Leben zum Stillstand bringen und enorme Schäden verursachen.

Das KI-ABWEHRZENTRUM soll solche Szenarien verhindern und die Sicherheit von Unternehmen und Organisationen, der Bevölkerung sowie der wirtschaftlichen Systeme gewährleisten. Durch die enge Zusammenarbeit mit internationalen Partnern, Forschungseinrichtungen und der Industrie setzen wir globale Standards und schaffen eine sichere Basis für die wirksame Abwehr von Cyberangriffen und den Fortschritt bei deren Vorhersage.

IHR SICHERHEITSPLUS

+ 360° Securitybetrachtung
+ Proaktive Abwehr gegen KI-basierte Angriffe
+ Deutlich schnellere Analyse durch KI und Vorhersage des nächsten Ziels
+ Aufklärung im Darknet, bevor ein Angriff stattgefunden hat
+ Konzentration auf die wesentlichen Angriffsvektoren
+ Stetiges Training und Lernen der KI im KI-ABWEHRZENTRUM

KI-Abwehr verwendet modernste Technologien für umfassenden Schutz Ihrer IT-Infrastruktur und Daten.

WIE FUNKTIONIERT EIN KI-ABWEHRZENTRUM? AUFGABEN & FUNKTIONEN

1 ÜBERWACHUNG & FRÜHERKENNUNG

Unsere hochqualifizierten Teams nutzen modernste Technologien, um potenzielle Bedrohungen in Echtzeit zu identifizieren. Dazu gehört die Analyse von Datenströmen aus verschiedenen Quellen, einschließlich Darknet-Foren, sozialen Medien und spezifischen Kommunikationskanälen von Cyberkriminellen. Durch den Einsatz fortschrittlicher Algorithmen und Überwachungssysteme können wir aufkommende Gefahren schnell erkennen und Gegenmaßnahmen einleiten. Ihre Systeme werden rund um die Uhr von Experten überwacht, die mithilfe modernster Technologien Bedrohungen in Echtzeit identifizieren und abwehren. Dies gewährleistet einen kontinuierlichen Schutz Ihrer digitalen Assets.

2 ENTWICKLUNG VON SCHUTZMECHANISMEN

Im KI-ABWEHRZENTRUM entwickeln wir fortschrittliche Abwehrmechanismen, um Angriffe, die durch KI verstärkt oder initiiert werden, effektiv abzuwehren. Dies umfasst sowohl softwarebasierte Lösungen und KI-basierte Anomalie-Erkennungssysteme als auch physische Sicherheitsmaßnahmen.

3 KRISENMANAGEMENT & KOORDINATION

Im Falle eines KI-basierten Angriffs oder einer Anomalie stehen wir bereit, um schnell und koordiniert zu handeln. Unser Zentrum fungiert als zentrale Anlaufstelle für alle relevanten Akteure, um die Reaktion auf Krisenfälle zu steuern und Schäden zu minimieren.

4 FORSCHUNG & ETHIK

Neben der Abwehr von Bedrohungen engagieren wir uns für die Erforschung von ethischen Standards im Umgang mit KI. Wir setzen uns dafür ein, dass die Entwicklung und der Einsatz von KI-Technologien verantwortungsvoll und zum Wohle der Gesellschaft erfolgen.

Die dynamische Bedrohungslage macht es unerlässlich, auf Angriffe nicht nur zu reagieren, sondern diese proaktiv zu verhindern.

Unsere Vision ist eine Welt, in der KI sicher, verantwortungsbewusst und zum Wohl der gesamten Menschheit eingesetzt wird.

Das KI-ABWEHRZENTRUM wird auch in Zukunft eine zentrale Rolle dabei spielen, diese Vision Wirklichkeit werden zu lassen.

DIE ZUKUNFT DER CYBERSECURITY? KI IST GEKOMMEN, UM ZU BLEIBEN!

Die Entwicklung von KI-Technologien schreitet in einem atemberaubenden Tempo voran, und mit ihr auch die Komplexität der Bedrohungen, denen wir uns stellen müssen. In den kommenden Jahren werden wir wahrscheinlich MIT VÖLLIG NEUEN FORMEN VON ANGRIFFEN UND HERAUSFORDERUNGEN KONFRONTIERT sein, die wir uns heute noch nicht vorstellen können.

MIT DEM KI-ABWEHRZENTRUM BLEIBEN WIR DESHALB STÄNDIG AM PULS DER ZEIT

- Dafür beobachten wir alle Entwicklungen in der Cybersecurity genauestens.
- Wir investieren in die Aus- und Weiterbildung unserer Experten, um sicherzustellen, dass sie die neuesten Entwicklungen verstehen und darauf reagieren können.
- Darüber hinaus werden wir unsere Forschungskapazitäten weiter ausbauen und neue Technogogie-Partnerschaften eingehen, um stets weiterzuentwickeln und einen Schritt voraus zu sein.

SOC AS A SERVICE
DIE ENTWICKLUNG GEHT WEITER

Die Cybersicherheitslandschaft entwickelt sich rasant weiter. SOC as a Service ist darauf ausgelegt, mit diesen Entwicklungen Schritt zu halten. Zu den wichtigsten zukünftigen Trends gehören:

ERWEITERTE AUTOMATISIERUNG

Der Trend geht hin zu noch umfassenderer Automatisierung in der Bedrohungserkennung und -abwehr. Dies umfasst die Entwicklung selbstlernender Systeme, die in der Lage sind, Bedrohungen autonom zu identifizieren und darauf zu reagieren.

ZERO TRUST-ARCHITEKTUREN

Zero Trust-Sicherheitsmodelle werden integriert, bei denen kein Nutzer oder Gerät automatisch als vertrauens-würdig angesehen wird. Dies erfordert eine ständige Überprüfung und Authentifizierung aller Zugriffe auf das Netzwerk

INTEGRATION VON SOAR

SOAR kombiniert verschiedene Sicherheitsdisziplinen – von Netzwerksicherheit über Endpunktschutz bis hin zur Bedrohungserkennung – in einer einheitlichen Plattform. SOC as a Service wird zunehmend auf SOAR-Lösungen basieren, um eine noch umfassendere Sicherheitsabdeckung zu bieten.

SOC as a Service ist eine hochmoderne Lösung, die auf den neuesten technologischen Entwicklungen basiert.

SOC AS A SERVICE ZAHLT SICH AUS FÜR SIE
FACTS & FIGURES

SCHNELLE ERKENNUNG UND ABWEHR VON CYBERANGRIFFEN

Fallstudien zeigen, wie SOC as a Service Unternehmen dabei geholfen hat, schwerwiegende Cyberangriffe in Echtzeit zu erkennen und abzuwehren, bevor erheblicher Schaden entstehen konnte.

VERBESSERUNG DER COMPLIANCE

Unternehmen, die SOC as a Service implementiert haben, konnten ihre Compliance-Anforderungen besser erfüllen und gleichzeitig das Risiko von Datenschutzverletzungen minimieren.

SKALIERBARKEIT UND FLEXIBILITÄT

SOC as a Service hat sich als flexible Lösung erwiesen, die sich an die wachsenden Anforderungen von Unternehmen anpassen lässt. Egal, ob es sich um ein schnell wachsendes Start-up oder einen etablierten Großkonzern handelt, die Lösung kann skaliert werden, um den Schutzbedarf zu decken.

SECURITY-STEP-UP:
MEHR SERVICE, MEHR SICHERHEIT

Im Zeitalter der Digitalisierung sehen Sie und Ihr Unternehmen sich ständig neuen und immer raffinierteren Cyberbedrohungen ausgesetzt.

Angesichts der steigenden Bedrohungslage, der zunehmenden Komplexität von IT-Infrastrukturen und der Verbreitung von Cloud-Technologien müssen Sie Ihre Cybersicherheitsstrategie proaktiv gestalten.

Managed Security Services wie MDR, SOC as a Service und KI-ABWEHRZENTRUM bieten genau die Lösung, die Sie benötigen, um Ihr Unternehmen effektiv zu schützen und gleichzeitig flexibel und skalierbar zu bleiben.

Security-Audit	MDR	SOC as a Service	KI-ABWEHRZENTRUM
Regelmäßiger Security-Statusreport	24/7/365 Managed Security		
	Überwachung der IT-Systeme	Proaktive Threat-Analyse	
	Auswertung der Alarme	Auswertung mit mehreren Tools	
	Erste Gegenmaßnahmen	Playbooks & erste Gegenmaßnahmen	
		30 Minuten Reaktionszeit	
		Forensische Analyse	
		Incident Response	
		Threat-Hunting	
		Darknet-Analyse	
		Aufklärung im Internet + Darknet	
			Automatisierte Erkennung KI-basierter Angriffe
			KI-basierte Gegenmaßnahmen + Angriffsabwehr
			Vorhersage der nächsten Angriffe

ALEXANDER SOWINSKI
AUS ERFURT AUF SECURITY-MISSION FÜR DEUTSCHLAND

Sicherheit bestimmt schon mein gesamtes berufliches Leben. Als ehemaliger Soldat mit langjähriger Erfahrung in NATO-Einsätzen war es mir ein persönliches Anliegen, das Thema Sicherheit auf den IT-Bereich zu übertragen. So entstand im Jahr 2014 in die ASOFTNET GmbH mit Fokus auf IT-Sicherheitsberatung und Managed Security Services.

2018 folgte eine strategische Partnerschaft mit dem Jenaer Softwarehersteller Enginsight. Sie hatte maßgeblichen Einfluss auf die Gründung unseres eigenen Security Operations Centers (SOC) in 2020. Anfangs skeptisch betrachtet, entwickelte sich das Erfurter SOC schnell zu einem gefragten und unverzichtbaren Bestandteil unseres Portfolios. Heute ist es ein hochmodernes Zentrum, das proaktiv Bedrohungen erkennt und abwehrt. Und es soll nicht das Einzige bleiben: Anfang 2025 werden wir ein weiteres SOC in Wismar eröffnen. In Nordrhein-Westfalen wird es in 2026 einen dritten Standort geben. Dafür baue ich mein Team aus hochqualifizierten Experten sukzessive weiter aus. Wir sorgen dafür, dass die IT-Sicherheit unserer Kund:innen – Banken, Industrieunternehmen, Energieversorger und soziale Einrichtungen – auf höchstem Niveau gewährleistet ist.

Besonders stolz bin ich auf unser KI-ABWEHRZENTRUM, das Ende 2023 in Betrieb ging. Auch dessen kontinuierliche Weiterentwicklung liegt mir sehr am Herzen. Ich bin überzeugt davon, dass darin die Zukunft der Cyberabwehr liegt und hoffe, die Technologie wird künftig noch vielen mehr zugutekommen.

Ihr Alexander Sowinski

GEMEINSAM FÜR EINE SICHERERE IT-WELT
KOOPERATIONEN UND NETZWERKE

Um unsere Ziele zu erreichen, arbeiten wir im KI-ABWEHRZENTRUM eng mit einer Vielzahl von nationalen und internationalen Partnern zusammen. Diese Kooperationen umfassen Regierungsbehörden, private Unternehmen, Forschungseinrichtungen und Nichtregierungsorganisationen.

Durch den Austausch von Wissen und Ressourcen können wir Bedrohungen schneller erkennen und effektiver darauf reagieren. Unsere internationalen Netzwerke ermöglichen es uns, globale Bedrohungstrends zu überwachen und länderübergreifende Abwehrstrategien zu entwickeln.

Zudem engagieren wir uns in der Standardisierung und Harmonisierung von Sicherheitsprotokollen auf internationaler Ebene, um sicherzustellen, dass der Schutz vor KI-basierten Bedrohungen weltweit gewährleistet ist. Diese Zusammenarbeit ist entscheidend, um ein globales Sicherheitsnetz zu schaffen, das die Gesellschaft vor den wachsenden Gefahren der KI schützt.

ENGINSIGHT IBM Silver Partner consistec DriveLock Mitigant KELA

www.ki-abwehrzentrum.de

qSOFTNET
IT-Security | Security Operation Center | IT-Forensik