
BrightFlare
Security
that
enables
business.
Digitale Geschäftsmodelle, vernetzte Produktionsumgebungen und softwaregetriebene Produkte verändern die Sicherheitsanforderungen von Unternehmen grundlegend. BrightFlare schützt dort, wo IT, OT und Software zusammenkommen – strukturiert, technisch fundiert und unternehmerisch gedacht.
All for One
BLUEZONE
© 2026
brightflare.io

Übersicht I

EINFÜHRUNG:
Sicherheit ist heute ein Management-Thema 04

Fünf Kompetenzfelder. Ein integrierter Sicherheitsansatz. 06

Unser Portfolio 07

01 **OT-SECURITY** 08

- Compliance & regulatorische Anforderungen 09
- Network Security & (Micro-)Segmentation 10
- Asset- & Vulnerability Management 10
- Secure Remote Access für OT-Umgebungen 11

02 **IT-SECURITY** 13

- Network & Perimeter Security 15
- Endpoint & Mobile Security 15
- Identity & Data Exposure Protection 16
- AI-Security 17
- Cloud & M365 Security 18

03 **SAP SECURITY** 19

- Proaktive SAP Security 20
- Echtzeit-SAP-Security-Monitoring 20
- Business Continuity & Datensicherheit für SAP 21
- Integration in die Security Operations 21

Übersicht II

04 SECURE SOFTWARE DEVELOPMENT 22

- Code Reviews 24
- Security Trainings für Softwareentwicklung 25
- Security in CI und CD Pipelines 25
- Cyber Resilience Act 27

05 SECURITY OPERATIONS 29

- Penetration Testing 30
- Red Teaming & Adversary Simulation 30
- Awareness Trainings & Phishing Campaigns 31
- Physical Access & Social Engineering 31
- Managed SOC Service 33
- Continuous Threat Exposure Mangement (CTEM) & External Risk Management (ERM) 34

BrightFlare x All for One x BlueZone
Gebündelte Expertise. 36

Warum BrightFlare:
Technologie. Erfahrung. Handschlagqualität. 38



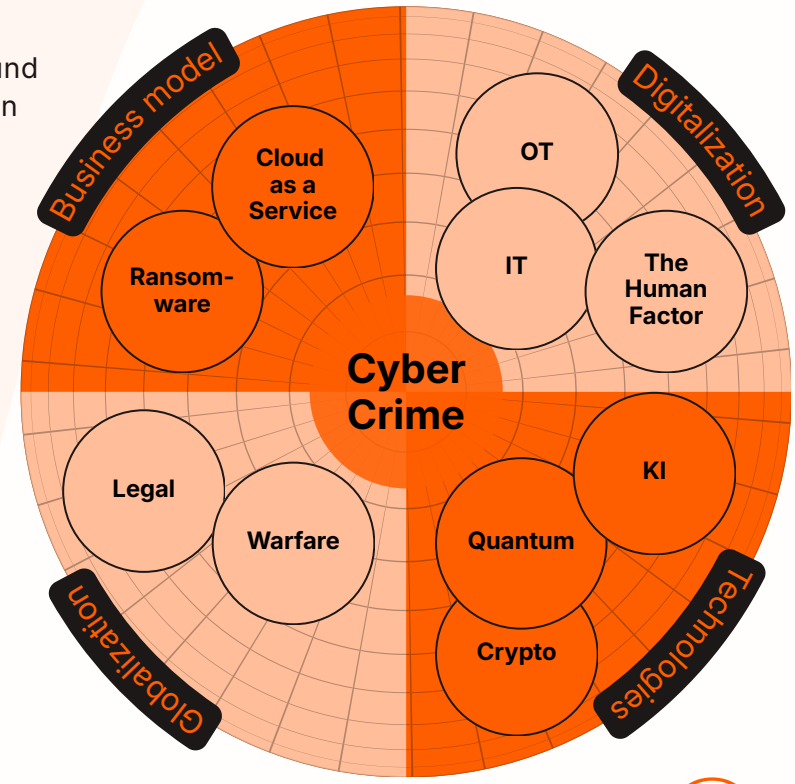
Sicherheit ist heute ein Management-Thema

Digitale Geschäftsmodelle, vernetzte Produktion und regulatorischer Druck verändern die Risikolandschaft grundlegend.

Digitale Transformation ist für technologiegestützte Unternehmen Realität. Produktionsanlagen sind vernetzt, Produkte enthalten immer mehr Software, Entwicklungsprozesse laufen cloudbasiert und Partner und Lieferketten sind oftmals hochgradig digital integriert. Was früher physisch getrennt war, ist heute zumindest logisch verbunden. Was früher lokal begrenzt war, ist heute meist global erreichbar. Diese Vernetzung schafft Effizienz, neue Geschäftsmodelle und Innovationsgeschwindigkeit. Gleichzeitig entstehen damit aber auch systemische Abhängigkeiten.

Je stärker Prozesse, Produkte und Produktionsumgebungen digitalisiert und automatisiert sind, desto unmittelbarer wirken sich Sicherheitsvorfälle auf die operative Stabilität, die Lieferfähigkeit, und das geistige Eigentum und die Reputation eines Unternehmens aus.

In industriellen Umgebungen geht es dabei nicht nur um Datenverlust, sondern um Produktionsstillstände, physische Sicherheitsrisiken („Safety“) und wirtschaftliche Folgeschäden.
Diese Entwicklung wird zusätzlich durch globale technologische und geopolitische Dynamiken verstärkt, die die wirtschaftlichen und gesamtgesellschaftlichen Auswirkungen von Cyberangriffen kontinuierlich erhöhen. Eine strukturelle Trendwende ist dabei nicht erkennbar.



„Ganzheitliche Cybersecurity heißt, Unternehmen nicht nur in einzelnen Bereichen zu begleiten, sondern Sicherheitsrisiken umfassend zu identifizieren, Bedrohungen frühzeitig zu erkennen, effektiv darauf zu reagieren und langfristig belastbare Sicherheitslösungen zu schaffen.
Ob Microsoft, SAP, individuelle Software oder andere Systemlandschaften – BrightFlare denkt Sicherheit ganzheitlich. Und zwar nicht nur für IT-, sondern ebenso für OT-Umgebungen. Das ist der Anspruch von BrightFlare.“

Markus Seme
CEO bei BrightFlare



Der technologische Fortschritt – insbesondere die rasante Entwicklung Künstlicher Intelligenz – automatisiert und skaliert sowohl Angriff als auch Verteidigung. Zukünftige agentische Systeme werden diese Dynamik weiter verstärken. Technologie potenziert die Fähigkeiten beider Seiten gleichermaßen.

Für Unternehmen bedeutet das: **Sicherheit ist kein statischer Zustand.** Schutzmechanismen, Architekturen und Prozesse müssen kontinuierlich weiterentwickelt werden. Eine einmalige Implementierung genügt nicht. Cyber Security erfordert laufende Anpassung an neue Technologien, neue Angriffsmuster und neue regulatorische Rahmenbedingungen.

Cybercrime kennt keine geografischen Grenzen. Angreifer operieren global, oft geschützt durch politische Grauzonen oder strategische Interessen einzelner Staaten. Hybride Konflikte verlagern sich zunehmend in den digitalen Raum, und die Trennlinien zwischen staatlichen, wirtschaftlichen und kriminellen Akteuren verschwimmen.

Parallel dazu hat sich Cybercrime zu einer professionellen, arbeitsteiligen Ökonomie entwickelt. Ransomware-as-a-Service, spezialisierte Initial-Access-Broker, Malware-Entwickler und Geldwäsche-Netzwerke bilden eine globale Wertschöpfungskette. **Angriffe werden modularisiert, skaliert und industriell organisiert.**

Unternehmen stehen damit keinen isolierten Hacker-Gruppen gegenüber, sondern einem hochprofessionellen, wirtschaftlich strukturierten Angreifer-Ökosystem. Cybercrime agiert effizient, spezialisiert und international vernetzt – mit klarer Rollenverteilung und unternehmerischer Logik.

Hinzu kommt ein **wachsender regulatorischer Rahmen.** Mit Vorgaben wie NIS2, dem Cyber Resilience Act oder der EU-Maschinenverordnung wird Cyber Security zunehmend zur formalen Unternehmenspflicht.

Sicherheit betrifft damit nicht nur technische Abteilungen, sondern Geschäftsleitung und Produktverantwortung gleichermaßen. Cyber Security ist damit kein isoliertes IT-Thema mehr, sondern ein **zentraler Bestandteil strategischer Unternehmensführung.**

Sie beeinflusst Stabilität, Wettbewerbsfähigkeit und regulatorische Sicherheit gleichermaßen. Der verantwortungsvolle Umgang mit digitalen Risiken ist deshalb heute eine Führungsaufgabe.

Fünf Kompetenzfelder. Ein integrierter Sicherheitsansatz.

Sicherheit entsteht nicht in Silos – sondern im Zusammenspiel von IT, OT, Software/SAP und kontinuierlicher Überprüfung.

Unternehmen arbeiten heute gleichzeitig in mehreren technischen Bereichen, die sich im täglichen Betrieb deutlich unterscheiden. IT bildet dabei häufig die digitale Grundlage dafür: Netzwerke, Identitäten, Endgeräte, Cloud-Umgebungen und Datenflüsse sichern Kommunikation und Geschäftsprozesse.

In Produktions- und Industrieumgebungen gelten jedoch andere Rahmenbedingungen. Anlagen laufen im Dauerbetrieb, Ausfälle verursachen unmittelbare wirtschaftliche Schäden, Wartungsfenster sind begrenzt. Sicherheitsmaßnahmen müssen hier Schutz bieten, ohne Verfügbarkeit und Performance zu beeinträchtigen. In der Softwareentwicklung wiederum stehen Architekturentscheidungen, Codequalität, Release-Zyklen und regulatorische Anforderungen im Mittelpunkt. Sicherheit entsteht hier im Entwicklungsprozess – nicht erst im laufenden Betrieb. Diese Bereiche unterscheiden sich technisch und organisatorisch deutlich. Gleichzeitig sind sie im Unternehmen eng miteinander verbunden. Ein Produktionsunternehmen benötigt IT-Sicherheit, muss aber zusätzlich industrielle Netze und Anlagen absichern.

Ein Softwareunternehmen braucht eine stabile IT-Basis, muss jedoch vor allem sichere Entwicklungsprozesse gewährleisten. Ein Maschinen- und Anlagenbauer vereint Produktion und eigene Softwareentwicklung – und trägt Verantwortung in beiden Bereichen. Ein wirksamer Schutzansatz muss all diese Unterschiede berücksichtigen und dennoch integrieren.

Unser Portfolio

Fünf Kompetenzfelder.

Der Aufbau unseres Portfolios ist daher entlang dieser operativen Bereiche strukturiert: IT-Security als Fundament, OT-Security für industrielle Umgebungen, Secure Software Development für sichere Produkte und Anwendungen, sowie SAP-Security, um ganzheitliche Sicherheitskonzepte entlang der gesamten Wertschöpfungskette zu gewährleisten.

Security Operations steht als verbindendes Element über alle Bereiche hinweg. Dadurch können wir sehr unterschiedliche Szenarien ganzheitlich abdecken – vom klassischen IT-Betrieb über industrielle Produktionsnetze bis hin zu Unternehmen, die eigene Software entwickeln, betreiben und als Produkt verantworten.

SW

Secure Software

- Code Reviews
- Security Trainings for Developers
- CI/CD Pipeline Security
- Cyber Resilience Act (CRA)

OT

OT-Security

- Compliance & Regulatories
- Network Security & (Micro-) Segmentation
- Asset- & Vulnerability Management
- Secure Remote Access (rPAM)



IT

IT-Security

- Network & Perimeter Security
- Endpoint & Mobile Security
- Identity & Data Exposure Protection
- Cloud & M365 Security

SecOps

Security Operations

- Penetration Testing
- Red Teaming & Adversary Simulation
- Awareness Trainings & Phishing Campaigns
- Physical Access & Social Engineering
- Continuous Threat Exposure Protection (CTEM)
- Managed SOC Service

BrightFlare

01

OT-Security

Zum Schutz Ihrer produktiven Wertschöpfung.

© 2026

OT-Security. Schutz Ihrer produktiven Wertschöpfung.

Industrieunternehmen sind heute digitale Unternehmen. Produktionsanlagen erzeugen Daten, Maschinen kommunizieren über Plattformen, Steuerungssysteme sind mit IT und Cloud-Diensten verbunden.

Die Verbindung von realer und digitaler Welt schafft Effizienz, Transparenz und neue Geschäftsmodelle. Doch mit jedem weiteren Schritt in Richtung Digitalisierung und Automatisierung, entstehen neue Herausforderungen und verschiebt sich auch die Verantwortung.

Daten fließen über Unternehmensgrenzen hinweg. Servicepartner greifen remote auf interne Anlagen zu. Lieferketten und Produktionsumgebungen sind immer stärker vernetzt. Die industrielle Wertschöpfung ist damit nicht nur physisch, sondern auch digital exponiert.

In diesem Umfeld entscheidet Cyber Security nicht nur über den Schutz Ihrer Daten und Ihres „Intellectual Property" – sie entscheidet über Produktionsfähigkeit, Wettbewerbsfähigkeit und manchmal auch über die Zukunft des Unternehmens.

Genau hier beginnt OT-Security.

Wir arbeiten seit vielen Jahren mit Industrie-, Produktions- und Maschinen- und Anlagenbauunternehmen zusammen. Wir kennen die Anforderungen an Verfügbarkeit, Wartungszyklen und betriebliche Stabilität ebenso wie die technischen Besonderheiten industrieller Netze und Steuerungssysteme. OT-Security ist für uns kein Zusatz zur IT-Security, sondern ein eigenständiges Spezialisierungsfeld.

Sie erfordert methodisches Vorgehen, technisches Detailverständnis und ein tiefes Verständnis für industrielle Abläufe.

Compliance & regulatorische Anforderungen

Mit NIS2, dem Cyber Resilience Act (siehe Kapitel 4) und Normen wie IEC 62443 steigen die Anforderungen an industrielle Sicherheit deutlich.

Unternehmen müssen Risiken systematisch bewerten, Maßnahmen dokumentieren und ihre Schutzkonzepte nachvollziehbar strukturieren.

Wir unterstützen bei der **Analyse bestehender Konzepte** und Architekturen, bei **Gap-Analysen gegenüber regulatorischen Vorgaben** und bei der **schrittweisen Umsetzung von Verbesserungsmaßnahmen** oder Implementierungen – praxisnah und umsetzungsorientiert.

Weiterführende Informationen zu Regulatorik & Compliance finden Sie unter www.brightflare.io

Network Security & (Micro-)Segmentation

Historisch gewachsene und nicht segmentierte Netze zählen zu den häufigsten strukturellen Schwachstellen in OT-Umgebungen. Fehlende Zonenbildung und unkontrollierte Kommunikationsbeziehungen ermöglichen im Ernstfall eine unkontrollierte, interne Ausbreitung eines Angriffes. Eine klare Segmentierung nach Zonen und Funktionen reduziert die Angriffsfläche erheblich und begrenzt potenzielle Auswirkungen auf definierte Bereiche.

Wir entwickeln **belastbare Zonen- und Segmentierungskonzepte** und setzen technische Maßnahmen um, die Sicherheitsanforderungen und betriebliche Verfügbarkeit gleichermaßen berücksichtigen. Moderne Technologien ermöglichen dabei auch in OT-Umgebungen die Umsetzung fein granularer Kontrollmechanismen – bis hin zur Mikrosegmentierung einzelner Systeme oder Kommunikationspfade.

Asset- & Vulnerability Management

Transparenz über eingesetzte Systeme ist die Grundlage jeder wirksamen OT-Sicherheitsstrategie. In vielen industriellen Umgebungen fehlt jedoch eine vollständige, **aktuelle Übersicht** über Assets, Software-Stände, Kommunikationsbeziehungen und bekannte Schwachstellen.

Mit **regulatorischen Anforderungen wie NIS2 und dem Cyber Resilience Act** wird ein strukturiertes Asset- und Vulnerability-Management zunehmend zur Pflicht.

Unternehmen müssen nachvollziehbar darlegen können, welche Systeme im Einsatz sind, welche Risiken bestehen und wie diese priorisiert adressiert werden.

Wir unterstützen bei der systematischen **Erfassung industrieller Assets**, der kontinuierlichen **Schwachstellenbewertung** und der risikobasierten **Maßnahmenplanung.**



„Was ich an den handelnden Personen hinter BrightFlare besonders schätze, sind Integrität, Teamgeist und ein ausgeprägtes Verantwortungsbewusstsein. Diese Werte prägen die Zusammenarbeit – und sind gerade im sensiblen Bereich der IT- und OT-Sicherheit von zentraler Bedeutung.“

Dr. Andreas Opelt,
CEO bei der Saubermacher AG

Dabei setzen wir auf OT-spezialisierte Lösungen – beispielsweise Plattformen wie **Claroty** – die industrielle Protokolle, Geräteklassen und Kommunikationsmuster verstehen und eine fundierte Bewertung ohne Beeinträchtigung des Betriebs ermöglichen.

So entsteht Transparenz, die nicht nur Compliance-Anforderungen erfüllt, sondern konkrete Entscheidungsgrundlagen für Priorisierung und Investitionen liefert.

Secure Remote Access für OT-Umgebungen

Der Fernzugriff auf Produktionsanlagen ist heute betrieblicher Standard – und zugleich einer der kritischsten Angriffspunkte.

Klassische VPN-Lösungen gewähren häufig weitreichende Netzwerkzugriffe. Wird ein Zugang kompromittiert, kann sich ein Angreifer lateral im Netz bewegen und sensible Systeme erreichen. Unser Ansatz für Secure Remote Access basiert auf dem Zero-Trust-Prinzip: Zugriffe werden identitätsbasiert, kontextabhängig und granular auf einzelne Systeme oder Funktionen beschränkt. Netzwerkweite Freigaben werden vermieden.

Für diese Anforderungen setzen wir unter anderem auf **Cyolo PRO** – aus unserer Sicht eine der derzeit führenden Lösungen für sicheren Fernzugriff in OT-Umgebungen.

Secure Remote Access mit Cyolo PRO

Cyolo PRO (Privileged Remote Operations) ist eine herausragende und von Gartner ausgezeichnete Secure Remote Access-Lösung, die speziell auf die Anforderungen von OT- und kritischen Infrastrukturen ausgelegt ist.

Entwickelt für hybride, cloud-integrierte, cloud-averse oder vollständig offline arbeitende Umgebungen, ermöglicht Cyolo PRO sicheren, zuverlässigen Zugriff auf OT-Systeme – auch für privilegierte interne Nutzer und externe Servicepartner.

Eine Partnerschaft mit Mehrwert

BrightFlare ist **Cyolo Elite Partner!** Durch die langjährige erfolgreiche Zusammenarbeit sowie zahlreiche erfolgreiche Use Cases und implementierte Fernzugriffslösungen bei unseren Kund:innen wurde BrightFlare 2026 als Cyolo Elite Partner ausgezeichnet.

Cyolo

Cyolo Pro - sicherer Fernzugriff leicht gemacht.



„VPN frei" und Zero Trust basiert

Cyolo PRO verbindet Benutzer nicht auf Netzwerkebene, sondern authentifiziert auf Identitäts- und Applikationsebene – nach dem Zero-Trust-Prinzip.



„Identity First" Authentifizierung auch für Legacy Systeme

Moderne Identitätskontrollen, Multi-Factor-Authentication (MFA) und privilegierte Zugriffskontrollen lassen sich ohne Änderungen an bestehender OT-Infrastruktur nutzen.



Granulare Zugriffskontrolle und Überwachung

Cyolo PRO erlaubt präzise Richtlinien für Benutzer, Anwendungen, Zeit, Ort und weitere Kontextparameter.



Agentenfrei und intuitiv benutzbar

Externe Dienstleister, OEM-Techniker oder interne Teams können ohne zusätzliche „Software Agents" über Browser oder native Protokolle (z. B. RDP, SSH) sicher zugreifen.



Infrastruktur-unabhängige und hybride Bereitstellung

Die Lösung passt sich bestehenden Netzwerken an, ob on-prem, cloudbasiert oder völlig isoliert.



Dezentrale Architektur mit zentraler Governance

Cyolo PRO kombiniert zentralisierte Richtlinienverwaltung mit dezentraler Kontrolle vor Ort.

BrightFlare

02

IT-Security

Vom Produktportfolio zum echtzeitfähigen Betriebsmodell.

© 2026

IT-Security. Vom Produktportfolio zum echtzeitfähigen Betriebsmodell.

Über viele Jahre hinweg lag der Schwerpunkt von klassischer IT-Security auf Schutzmaßnahmen: Firewalls, Endpoint-Security, Patch-Programme, Netzwerksegmentierung. Diese Kontrollen sind auch weiterhin noch notwendig, aber sie reichen heute nicht mehr aus, um die reale Angriffsfläche moderner Organisationen abzubilden.

Gartner prognostiziert, dass bereits in den kommenden Jahren mehr als die Hälfte der Angriffsfläche großer Unternehmen, aus nicht patchbaren Angriffsflächen („Exposures“) bestehen wird. Fehlkonfigurationen, Identitäten, API-Tokens, SaaS-Abhängigkeiten, externe Assets oder Supply-Chain-Risiken entziehen sich dann klassischen „Patch-the-CVE“-Programmen. Sicherheit kann bereits heute nicht mehr allein über Schwachstellenlisten gesteuert werden.

Gleichzeitig entstehen viele **Angriffe außerhalb der eigenen Perimeter.** Offene Subdomains, geleakte Zugangsdaten, Lookalike-Domains oder Fehlkonfigurationen in Cloud-Umgebungen werden häufig genutzt, bevor das Monitoring interner, sicherheitsrelevanter Betriebsdaten („Telemetrie“) Alarm schlägt.

Parallel dazu beschleunigt **künstliche Intelligenz** sowohl Angriff als auch Verteidigung. GenAI gestützte Angriffe, automatisierte Phishing Kampagnen und die zunehmende Nutzung maschineller Identitäten erweitern die Angriffsfläche nochmals deutlich.

Zusätzlich steigt der **Druck auf Security Operations Teams,** Ereignisse schneller zu erkennen und automatisiert darauf zu reagieren. Vor diesem Hintergrund verschiebt sich der Fokus von passivem Monitoring hin zu aktiven, automatisierten Interventionen in Echtzeit.
Konzepte wie Continuous Threat Exposure Management (CTEM) beschreiben einen kontinuierlichen Zyklus aus Transparenz, Priorisierung, Validierung und Umsetzung – verständlich für das Business und operativ umsetzbar für Technikteams.

Um diese Dynamiken strukturiert zu steuern, ist ein ganzheitliches und integriertes Betriebsmodell erforderlich. Angelehnt an das NIST Cybersecurity Framework 2.0 lassen sich Cyber-Sicherheitsfähigkeiten entlang eines klaren Risiko-Lebenszyklus organisieren: **Identify, Protect, Detect, Respond, Recover und Govern.**

Dieses Modell ersetzt die Tool-Landkarte durch eine Outcome-Landkarte. Es verbindet Transparenz, Schutzmechanismen, Echtzeit-Erkennung, strukturierte Reaktion und organisatorische Steuerung zu einem integrierten Sicherheitsbetrieb.

Für größere Organisationen ist vollumfänglicher Cyberschutz damit weniger eine Frage einzelner Produkte als eine Frage der Integration dieser Funktionen in ein belastbares, kontinuierlich steuerbares Betriebsmodell.

Network & Perimeter Security

Auch wenn sich der klassische Perimeter immer mehr verschiebt, bleibt die kontrollierte Steuerung von Datenverkehr eine zentrale Sicherheitsfunktion.

Netzwerk- und Perimeter-Sicherheit stellt sicher, dass Kommunikationsbeziehungen nachvollziehbar, regelbasiert und risikoorientiert gesteuert werden – zwischen Standorten, Rechenzentren, Cloud-Umgebungen und externen Partnern. Wir übernehmen **Planung, Architektur, Integration sowie Betrieb moderner Firewall- und Netzwerk-Sicherheitslösungen.**

Dabei setzen wir unter anderem auf Produkte von **Check Point**, einer der führenden Anbieter von Cyber Security Technologien.

Neben der Implementierung verantworten wir die laufende Optimierung von Regelwerken, die Anpassung an neue Anforderungen und die kontinuierliche Weiterentwicklung der Sicherheitsarchitektur.

Network & Perimeter Security ist damit kein einmaliges Projekt, sondern ein dauerhaft betreuter Bestandteil des IT-Sicherheitsbetriebs.

Endpoint & Mobile Security

Endgeräte sind heute einer der dynamischsten Bestandteile der Angriffsfläche.

Laptops, mobile Geräte und Homeoffice-Arbeitsplätze greifen auf zentrale Systeme, Cloud-Dienste und sensible Daten zu. Und das immer öfters außerhalb klassischer Netzwerkschutzmechanismen.

Endpoint- und Mobile Security stellt sicher, dass diese Geräte selbst zur kontrollierten Sicherheitszone werden. Ziel ist es, Bedrohungen frühzeitig zu erkennen, Schadsoftware zu blockieren und kompromittierte Systeme isolieren zu können, ohne die Arbeitsfähigkeit der Organisation zu beeinträchtigen.

Wir **planen, implementieren und betreiben** moderne Endpoint und Mobile Security Lösungen auf Basis von **Check Point „Harmony“.**

Die Plattform kombiniert Threat Prevention, Anti-Ransomware-Mechanismen, Phishing-Schutz und gerätebasierte Zugriffskontrollen in einer integrierten Architektur.

Eine starke Partnerschaft

BrightFlare ist **Check Point Partner!** Durch die langjährige erfolgreiche Zusammenarbeit und die Umsetzung zahlreicher Security-Projekte unterstützen wir unsere Kund:innen dabei, ihre IT-Infrastruktur mit führenden Lösungen nachhaltig zu schützen.

CHECK POINT

Identity & Data Exposure Protection

Identitäten sind heute das primäre Angriffsziel moderner Cyberangriffe. **Phishing, Account Takeover, kompromittierte Zugangsdaten** und **unkontrollierte Nutzung von GenAI-Tools** zählen zu den häufigsten Eintrittspunkten erfolgreicher Sicherheitsvorfälle.

Die meisten Risiken entstehen dabei im Arbeitsalltag, beim Emailen, Browser Zugriffen auf nicht vertrauenswürdige Websites, Collaboration-Plattformen und KI-Anwendungen.

Unseren Lösungen rund um „Identity & Data Exposure Protection“ adressieren genau diese Ebene und sind noch dazu einfach, kostengünstig und skalierbar nutzbar.

Der Leistungsbereich umfasst unter anderem:

- **Schutz von Email- und Collaboration** Plattformen vor Phishing, Malware und Account Takeover
- **Browser-basierte Sicherheitsmechanismen** gegen Zero-Day-Phishing und Datenabfluss
- **Absicherung der Nutzung von GenAI und LLM Plattformen** um zu Verhindern, dass sensible Daten das eigene Unternehmen verlassen
- **Schutz vor nicht vertrauenswürdigen Domains und externer Phishing-Infrastruktur**, über hochintelligente DNS Filersysteme

Identity & Data Protection bildet damit die Schutzschicht für den heute am stärksten exponierten Bereich moderner IT: **Benutzeridentitäten und Datenflüsse.**

Verschiedene Pakete, die sich an Ihre Anforderungen anpassen.

Basic

Zwei Bausteine kombiniert – für einen soliden Grundschutz.

Was ist inkludiert?

- Email- & Collaboration
- Deception & Fraud

Advanced

Best Seller

Sicherheit direkt dort, wo Phishing und moderne Web-Angriffe heute stattfinden.

Was ist inkludiert?

- Email- & Collaboration
- Deception & Fraud
- Browser & Phishing

AI

Sichere Nutzung von ChatGPT & LLM's im eigenen Unternehmen.

Was ist inkludiert?

- Browser & Phishing
- GenAI & LLM

Weiterführende Informationen zu Identity & Data Exposure Protection finden Sie unter brightflare.io/pakete/identity-and-data-exposure-protection

Sicherheit für den Einsatz und die Entwicklung von Künstlicher Intelligenz.

Künstliche Intelligenz wird zunehmend integraler Bestandteil moderner Geschäftsprozesse. Ob durch die Nutzung externer AI-Services oder die Entwicklung eigener Modelle – Unternehmen profitieren von Effizienzgewinnen und neuen Möglichkeiten der Automatisierung. Gleichzeitig entstehen neue Risiken. Sensible Daten werden in AI-Systeme eingebracht, Entscheidungen werden automatisiert getroffen und AI-Anwendungen häufig dezentral genutzt. Unkontrollierte Nutzung („Shadow AI"), Datenabfluss oder gezielte Angriffe auf Modelle sind dabei reale Szenarien.

Ein **wirksamer Sicherheitsansatz** umfasst daher:

- Transparenz über eingesetzte AI-Services und deren Nutzung
- Schutz sensibler Daten bei der Verwendung von AI-Anwendungen
- Absicherung eigener AI- und LLM-Systeme gegen Manipulation und Missbrauch
- Integration in bestehende Security- und Compliance-Strukturen

Wir unterstützen Unternehmen dabei, AI sicher und kontrolliert einzusetzen – von der **Definition klarer Governance-Strukturen** bis hin zur **technischen Umsetzung.**

Ziel ist es, Künstliche Intelligenz als Innovationstreiber zu nutzen, ohne dabei Sicherheit und Compliance zu gefährden.

„AI entfaltet ihren Wert erst dann nachhaltig, wenn sie sicher, kontrolliert und verantwortungsvoll eingesetzt wird. Unternehmen müssen heute nicht nur ihre Daten beim Einsatz externer AI-Services schützen, sondern auch eigene Modelle und LLM-Systeme gegen Manipulation, Missbrauch und unkontrollierte Nutzung absichern. Für uns bedeutet AI Security deshalb, Governance, Compliance und technische Schutzmaßnahmen so zu verbinden, dass Innovation möglich bleibt – ohne die Sicherheit des Unternehmens zu gefährden."

Andreas Joham
Chief Technology Officer



Cloud & M365 Security

Sicherheit für moderne Cloud-Arbeitsplätze und digitale Kollaboration.

Cloud-Plattformen wie Microsoft 365 sind heute zentraler Bestandteil moderner IT-Landschaften. Identitäten, Daten, Kommunikationswege und Geschäftsprozesse sind eng miteinander verknüpft und häufig direkt über das Internet erreichbar.

Damit entsteht eine der dynamischsten und zugleich kritischsten Angriffsflächen im Unternehmen. Fehlkonfigurationen, unzureichend genutzte Sicherheitsfunktionen oder kompromittierte Identitäten können unmittelbare Auswirkungen auf die gesamte Organisation haben.

Wir betrachten Cloud- und M365-Sicherheit daher nicht als Einzelmaßnahme, sondern als Bestandteil eines integrierten Sicherheitsbetriebs.

Wir unterstützen Unternehmen dabei:

- bestehende Cloud- und M365-Umgebungen strukturiert zu analysieren und aus Angreiferperspektive zu bewerten
- Schwachstellen, Fehlkonfigurationen und ungenutzte Sicherheitsfunktionen systematisch zu identifizieren
- moderne Sicherheitsarchitekturen umzusetzen – insbesondere im Bereich Identity, Zugriffskontrolle und Datenprotektion
- Detection- und Monitoring-Funktionen zu integrieren und in bestehende Security Operations einzubinden
- regulatorische Anforderungen und Best Practices nachhaltig zu verankern

Die Ergebnisse werden **risikobasiert priorisiert und in konkrete Maßnahmen überführt** – von der gezielten Optimierung bis hin zur technischen Implementierung.

So entsteht keine punktuelle Verbesserung, sondern eine Cloud-Sicherheitsarchitektur, die langfristig betreibbar ist, sich an neue Anforderungen anpasst und den sicheren Einsatz moderner Arbeitsweisen ermöglicht.

Microsoft aws

BrightFlare

03

SAP Security Services

Wir sorgen für die Sicherheit Ihrer SAP-Systeme.

© 2026

SAP-Security. Wenn Sicherheit über die Geschäftsfähigkeit entscheidet.

SAP-Applikationen sind geschäftskritische Anwendungen, die zentrale Prozesse in den Bereichen Finanzen, Logistik, Produktion und Personalwesen integrieren. Gleichzeitig sind sie ein zunehmend attraktives Ziel für Cyberangriffe.

Hohe Systemkomplexität, lange Patch-Zyklen und die tiefe Einbindung in Geschäftsprozesse erfordern einen spezialisierten Sicherheitsansatz, der weit über klassische IT-Sicherheitsmaßnahmen hinausgeht. SAP-Security ist für uns daher kein “Add-On”, sondern ein integraler Bestandteil einer IT-Security Strategie & Betrieb.

Unsere SAP-Security-Services verbinden tiefgehende SAP-Technologie-Expertise mit moderner Cybersecurity und etablierten Security-Operations-Modellen. Ziel ist es, SAP-Landschaften (on-prem, Cloud) ganzheitlich abzusichern – von Identitäts- und Berechtigungskonzepten über proaktives Vulnerability Management bis hin zu Echtzeit-Bedrohungserkennung und strukturierter Incident Response.

Proaktive SAP-Security

Viele erfolgreiche Angriffe nutzen bekannte, jedoch nicht geschlossene Schwachstellen oder unsichere Konfigurationen in SAP-Systemen aus. Unsere proaktiven Services setzen genau hier an:

Wir schließen Sicherheitslücken, bevor sie ausgenutzt werden können.

Mithilfe spezialisierter SAP-Security-Scanner und fundierter Expertenanalysen bewerten wir kontinuierlich Systemkonfigurationen, Berechtigungen und bekannte Schwachstellen. Die Ergebnisse werden risikobasiert priorisiert, im geschäftlichen Kontext eingeordnet und in konkrete, umsetzbare Handlungsempfehlungen für produktive SAP-Umgebungen übersetzt.

Darüber hinaus unterstützen wir unsere Kunden beim Aufbau nachhaltiger SAP-Security-Baselines, Hardening-Standards und Security-Roadmaps – ausgerichtet an regulatorischen Anforderungen wie NIS2, DORA sowie internen Governance-Vorgaben.

Echtzeit-SAP-Security-Monitoring

Präventive Maßnahmen allein reichen heute nicht mehr aus. Moderne Angriffe bleiben häufig über Wochen oder Monate unentdeckt. Unser Echtzeit-SAP-Security-Monitoring kombiniert SAP-native Audit-Daten mit einer cloud-nativen SIEM/SOAR-Plattform auf Basis Microsoft Sentinel und einem globalen 24/7 Security Operations Center.

Sicherheitsrelevante Ereignisse aus SAP-Systemen (on-prem, SAP Private Cloud, RISE, SAP on Azure sowie SAP BTP) werden agentenlos erfasst und mit IT- und Cloud-Telemetriedaten korreliert. Fortgeschrittene Detection-Use-Cases identifizieren verdächtige Aktivitäten wie Missbrauch privilegierter Berechtigungen, unautorisierte Konfigurationsänderungen, auffällige Transporte oder ungewöhnliche Zugriffsverhalten.

Erkannte Incidents werden von erfahrenen Security-Analyst:innen analysiert und gemäß definierter Playbooks behandelt – von Alarmierung und Eindämmung bis zur koordinierten Incident Response.

Business Continuity & Datensicherheit für SAP

Cyberangriffe zielen häufig nicht nur auf den Diebstahl von Daten ab, sondern darauf, Geschäftsprozesse durch Verschlüsselung oder Manipulation von SAP-Systemen lahmzulegen.

Unsere Services für Business Continuity und Datensicherheit stärken die Widerstandsfähigkeit Ihrer SAP-Landschaft.

Dazu gehören sichere, unveränderliche Backup-Konzepte, strukturierte Wiederherstellungsstrategien sowie regelmäßige Überprüfungen der Restore-Fähigkeit. So stellen wir sicher, dass der SAP-Betrieb auch im Fall von Ransomware oder destruktiven Angriffen schnell und verlässlich wiederhergestellt werden können.

Integration in die Security Operations

SAP-Security wird nicht isoliert betrachtet. Wir integrieren SAP-spezifisches Monitoring und Sicherheitskontrollen in ein ganzheitliches Security-Operations-Modell. SAP-Ereignisse, Identitäten und Systemrisiken fließen in das übergreifende Lagebild ein und ermöglichen eine einheitliche Sicht über IT-, Cloud- und SAP-Umgebungen hinweg.
Sicherheitsverantwortliche und Management erhalten dadurch eine fundierte Entscheidungsgrundlage, können Maßnahmen risikoorientiert priorisieren und Compliance-Anforderungen gegenüber Auditoren und Regulatoren nachvollziehbar belegen.
Mit unseren SAP-Security-Services und Lösungspartnern unterstützen wir Unternehmen dabei, sich von reaktiver Schadensbegrenzung hin zu proaktivem Schutz und resilientem Betrieb zu entwickeln – und damit den digitalen Kern des Unternehmens nachhaltig abzusichern.



„SAP-Systeme bilden in vielen Unternehmen das digitale Rückgrat zentraler Geschäftsprozesse. Ihre Bedeutung wird oft erst dann sichtbar, wenn sie beeinträchtigt sind. Entsprechend hoch sind die Anforderungen an Sicherheit, Stabilität und Betrieb. Gerade in komplexen SAP-Landschaften zeigt sich, dass klassische IT-Sicherheitsansätze allein nicht ausreichen. Entscheidend ist ein tiefes Verständnis der Systeme, ihrer Prozesse und Abhängigkeiten – und die Fähigkeit, Security konsequent in den laufenden Betrieb zu integrieren."

Dr. Ulrich Faisst
CTO All for One Group SE

BrightFlare

04

Secure Software Development

Security by Design.

© 2026

Sichere Softwareentwicklung.
Security by Design.

Für Unternehmen, die eigene Software entwickeln – ob als eigenständiges Produkt, als Bestandteil einer Maschine oder als digitale Serviceplattform – ist Sicherheit längst nicht mehr nur ein Thema der internen IT. Sie ist Teil der Produktverantwortung. Software wird verkauft, integriert und vernetzt.

Software läuft bei Kundinnen und Kunden, in kritischen Produktionsumgebungen oder in sensiblen Infrastrukturen. Und sie bleibt dort oft viele Jahre im Einsatz.

Mit dem **Cyber Resilience Act** verändert sich der Maßstab grundlegend. Hersteller digitaler Produkte müssen nachweisbar sichere Entwicklungsprozesse etablieren, Schwachstellen über den gesamten Lebenszyklus steuern und Sicherheitsvorfälle transparent behandeln. Sicherheit wird damit nicht nur technisch erwartet, sondern regulatorisch eingefordert.

Gleichzeitig steigt die **technische Komplexität.** Moderne Software besteht aus Open Source Komponenten, APIs, Cloud Services, Containern und automatisierten Build Prozessen. Continuous Integration und Continuous Deployment erhöhen die Entwicklungsgeschwindigkeit und damit auch die Geschwindigkeit, mit der Fehler oder Schwachstellen ausgeliefert werden können. Risiken in der Software Lieferkette sind heute ein reales Szenario.

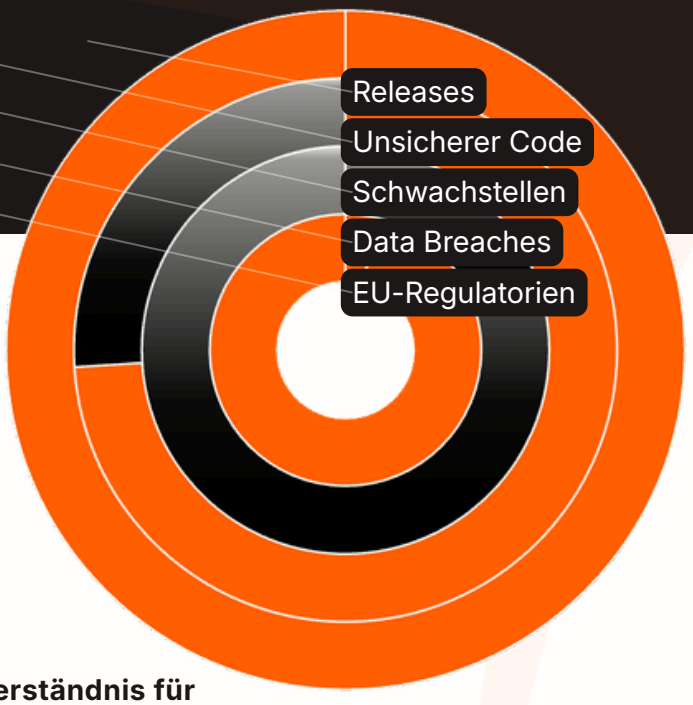
Für Unternehmen bedeutet das: **Sicherheit muss dort verankert sein, wo Architekturentscheidungen getroffen werden, wo Code entsteht und wo Releases freigegeben werden.** Nicht erst im laufenden Betrieb.

Wir bringen langjährige Erfahrung aus der Software- und Produktentwicklung mit. Aus Projekten, in denen Plattformen aufgebaut, DevOps Umgebungen betrieben und marktfähige Produkte verantwortet wurden. Wir kennen die Dynamik von Release-Zyklen, die Spannungsfelder zwischen Geschwindigkeit und Qualität sowie die realen Herausforderungen moderner Entwicklungsorganisationen.

Security in der Softwareentwicklung bedeutet für uns daher nicht zusätzliche Kontrolle von außen, sondern gezielte Unterstützung im Entwicklungsprozess selbst. Dazu gehören praxisnahe Trainings für Entwickler:innen, strukturierte Code Reviews durch Security Expert:innen, sowie die Integration automatisierter Sicherheitsprüfungen direkt in CI und CD Pipelines.

Deshalb ist sichere Software heute wichtiger denn je:

100x	Eine Schwachstelle kostet **bis zu 100× mehr**, wenn sie erst nach dem Release entdeckt wird.
74%	aller Sicherheitsvorfälle entstehen durch fehlerhaften oder unsicheren Code.
20%	weniger neue Schwachstellen im ersten Jahr, bei Unternehmen, die Entwickler:innen richtig schulen.
4 Mio	EUR beträgt der durchschnittliche Schaden eines Software-basierten Data Breach.
X Line	EU-Regularien wie NIS2, DORA oder der CRA verlangen „Security by Design“ – also Sicherheit von der ersten bis zur letzten Codezeile.



Code Reviews

Unsere Security Code Reviews werden von erfahrenen Security Expert:innen und Pentestern gemeinsam mit den Entwicklerteams unserer Kund:innen durchgeführt.

Ziel ist nicht nur das **Identifizieren einzelner Schwachstellen**, sondern das **gemeinsame Verständnis für sicherheitsrelevante Muster, Architekturentscheidungen und potenzielle Risikofaktoren.**

Im Rahmen der Analyse betrachten wir unter anderem Authentifizierungs- und Autorisierungslogiken, Eingabevalidierung und Datenverarbeitung, den Einsatz kryptographischer Funktionen, API- und Schnittstellenimplementierungen, sowie sicherheitsrelevante Aspekte von Open Source Abhängigkeiten.

Findings werden **strukturiert priorisiert, nachvollziehbar dokumentiert** und im **direkten Austausch diskutiert.**

Der Fokus liegt dabei auf praktischer Umsetzbarkeit. Reviews sollen nicht bremsen, sondern die Codequalität erhöhen und Entwickler:innen befähigen, Sicherheitsanforderungen künftig selbstständig und frühzeitig zu berücksichtigen.

Security Trainings für Softwareentwicklung

Sichere Software entsteht nicht durch Richtlinien allein, sondern durch das **Verständnis realer Angriffe.**

Unsere Trainings zeigen Entwickler:innen wie Schwachstellen tatsächlich ausgenutzt werden und wie sie sich im Code wirksam verhindern lassen.

Die Workshops werden von **erfahrenen Pentestern und Softwareexperten** durchgeführt, die aktuelle Angriffstechniken aus der Praxis kennen und diese direkt in nachvollziehbare Entwicklungsprinzipien übersetzen.

Statt abstrakter Theorie arbeiten die Teilnehmenden mit realistischen Szenarien, analysieren Exploits in geschützten Übungsumgebungen und entwickeln sichere Lösungsansätze für ihre eigenen Projekte.

Die **Trainingsinhalte sind modular aufgebaut** und lassen sich zu **unternehmensspezifischen Lernpfaden** kombinieren.

Ein besonderer Fokus liegt auf nachhaltiger Verankerung: Wir unterstützen beim Aufbau interner Security Champions, stellen praxisnahe Checklisten und Integrationsbeispiele bereit.

Security in CI und CD Pipelines

Moderne Software entsteht in **hochautomatisierten DevOps Umgebungen.**

Continuous Integration und Continuous Deployment beschleunigen Entwicklung und Auslieferung, können jedoch auch Schwachstellen in hoher Geschwindigkeit verbreiten, wenn Sicherheitsprüfungen nicht systematisch integriert sind.

Wir unterstützen Unternehmen dabei, Sicherheitsmechanismen **direkt in ihre bestehenden CI und CD Pipelines zu integrieren.**

Dazu gehören automatisierte Code-Analysen, Dependency-Scans, Container- und Image-Prüfungen, sowie strukturierte Qualitäts-Gates vor Releases.

Ein besonderer Fokus liegt auf der Absicherung der Software-Lieferkette. Themen wie SBOM-Generierung, Integritätsprüfungen von Abhängigkeiten, Schutz von Secrets sowie sichere Konfiguration von Build-Umgebungen werden strukturiert berücksichtigt.

Ziel ist eine Pipeline, die Geschwindigkeit und Sicherheit miteinander verbindet. Transparent, nachvollziehbar und anschlussfähig an bestehende Entwicklungsprozesse.

Ethical Hacking
- echte Einblicke von einem Pentester!

Jetzt Blogartikel unter
brightflare.io/knowhow nachlesen!

Security Trainings aus Sicht eines Angreifers.

Unsere Secure Software Development Trainings vermitteln Sicherheit dort, wo sie entsteht, im Code und in der Architektur. Entwickler:innen lernen nicht nur Sicherheitsprinzipien, sondern erleben reale Angriffsszenarien aus der Perspektive erfahrener Pentester.

So entsteht ein tiefes Verständnis für Schwachstellen, Exploit-Techniken und wirksame Gegenmaßnahmen, abgestimmt auf reale Entwicklungsprozesse und regulatorische Anforderungen wie den Cyber Resilience Act.

Was unsere Trainings abdecken:

- **OWASP Top 10 & Web Security Fundamentals** - Aktuelle Angriffsvektoren, typische Schwachstellen und praxisnahe Labs mit Exploit und Fix in sicheren Übungsumgebungen.
- **API Security & moderne Authentifizierung** – Security bei REST und GraphQL, sicheres Handling von Token, OAuth2, Sicherheit von Sessions und Schutz vor typischen API-Angriffsmustern.
- **Secure Coding Practices** - Sichere Eingaben, Autorisierungskonzepte, Management von Secrets, kryptographische Grundlagen und robuste Fehlerbehandlung.
- **Threat Modeling & Security by Design** - Strukturierte Analyse von Angriffsflächen bereits in der Architekturphase, noch vor der ersten produktiven Codezeile.
- **Security in CI und CD Pipelines** - Integration von automatisierten Code-Scans, Checks von Dependencies, SBOM Generierung und Gates für Releases direkt in bestehende Build-Prozessen.
- **Dependency & Supply Chain Security** - Absicherung externer Komponenten, Schutz vor Dependency Confusion und strukturierter Umgang mit Open Source Risiken.
- **Container & Cloud Security** - Absicherung von Images, Kubernetes Grundlagen, Sicheres Management von Rechten und Secrets, sowie sichere Betriebsmodelle.

Cyber Resilience Act

CRA Executive Briefing & Gap-Analyse

Wir ordnen den Cyber Resilience Act (CRA) strategisch und operativ ein: Geltungsbereich, Rollen und Pflichten sowie die Verankerung der Compliance in Produkt und Prozessen. Dabei erfassen wir den Ist-Stand Ihrer Prozesse und Produkte objektiv und unabhängig und zeigen, wo Abläufe bereits den Vorgaben entsprechen und wo noch gezielte Anpassungen nötig sind. Aus prozessualer und technischer Sicht bewerten wir, wie z.B. Threat Modeling, Secure Coding und Testing verankert sind, wie Schwachstellen kontinuierlich und systematisch identifiziert, gemeldet und gehoben werden und wie die erforderliche Dokumentation erstellt wird.

Das Briefing fokussiert auf Governance, Verantwortlichkeiten und konkrete Handlungsfelder und richtet sich vor **allem an Entscheider:innen für Technologie, Produkt, R&D sowie Compliance, Security und Service.**

Als Ergebnis erhalten Sie ein gemeinsames Verständnis der Auswirkungen auf Ihr Portfolio und Ihre Prozesse sowie eine **klare, priorisierte Übersicht über abgedeckte Themen und offene Punkte** – als fundierte Basis für Ihre Maßnahmenplanung: strukturiert, nachvollziehbar und umsetzbar.

Software-Refactoring & Modernisierung

Wenn Pentests, Code- und Architektur-Reviews oder Regularien wie der CRA Handlungsbedarf in Ihrer Software aufzeigen, greifen wir ein.

Wir bewerten wirtschaftlich, ob **gezieltes Refactoring oder ein Neuaufbau** sinnvoller ist, schließen Sicherheitslücken und reduzieren technische Schulden. Auf Basis der Findings und eines kompakten Requirement Engineerings modernisieren wir z.B. Architektur, Module und Build-Umgebung, **verbessern Sicherheit, Performance, Stabilität und Wartbarkeit.** Das Ergebnis ist eine modernisierte, anforderungsgerechte und sichere Lösung: Gehärteter Code, aktualisierte Abhängigkeiten, automatisierte Tests und dokumentierte Schnittstellen.

Sie profitieren von höherer Sicherheit und Qualität sowie niedrigerer Total Cost of Ownership (TCO).

CRA-Checkliste:

01 Betroffenheit prüfen & Produktportfolio analysieren

02 Sichere Entwicklung verbindlich verankern

03 Prozesse, Rollen und Dokumentation definieren

04 Umsetzung schrittweise vorbereiten

05

Security Operations

Security unter Realbedingungen prüfen.

© 2026

Security Operations. Security unter Realbedingungen prüfen.

Sicherheitskonzepte wirken auf dem Papier oft schlüssig. Entscheidend ist jedoch, ob sie einem realen Angriff standhalten.

Technische Schutzmaßnahmen, Prozesse und Richtlinien entfalten ihre Wirkung erst dann vollständig, wenn sie unter realistischen Bedingungen überprüft und danach nochmals optimiert werden. Gleichzeitig bleibt der Mensch einer der zentralen Faktoren in jeder Sicherheitsarchitektur. Und das als Schutzmechanismus ebenso wie als potenzieller Angriffsvektor.

Mit strukturierten Penetration Tests und Red Teaming Campaigns prüfen wir die Widerstandsfähigkeit technischer Systeme, Netzwerke und Anwendungen. Awareness Trainings, Phishing Kampagnen und Social Engineering Tests analysieren und stärken das Sicherheitsverhalten Ihrer Mitarbeiter:innen im Arbeitsalltag.

Gemeinsam verbindet das technische Angriffssimulation mit menschlicher Realität. Ziel ist nicht das Aufzeigen einzelner Schwachstellen, sondern die objektive Bewertung der tatsächlichen Sicherheitswirksamkeit und möglicher Angriffsflächen über Systeme, Prozesse und Personen hinweg.

Sicherheit wird damit überprüfbar, messbar und lässt sich dadurch auch gezielt verbessern.

Mit Continuous Threat Exposure Management (CTEM) und unserem Managed SOC ergänzen wir unseren Kompetenzbereich gezielt.



„Unser Job ist es nicht nur für eine Überprüfung in Systeme zu hacken – unser Job ist es auch zu verhindern, dass andere es erfolgreich tun. Wir denken wie Angreifer, analysieren Schwachstellen und zeigen Organisationen, wo ihre Sicherheitsannahmen nicht der Realität standhalten."

Erlend Depine
Head of Security Testing
bei BrightFlare

Penetration Testing

Penetration Tests dienen der strukturierten und kontrollierten Überprüfung technischer Systeme auf reale Angreifbarkeit.

Dabei simulieren wir **unter definierten Rahmenbedingungen** und vorheriger Absprache mit den jeweiligen Verantwortlichen, die Vorgehensweise potenzieller Angreifer und analysieren, ob und wie Schutzmaßnahmen überwunden werden können.

Im Unterschied zu rein automatisierten Schwachstellenscans **kombinieren wir methodisches Vorgehen mit manueller Analyse** durch erfahrene Security Expert:innen bzw. Pentester:innen (sog. „Ethical Hacker“).

Die Ergebnisse werden **nachvollziehbar dokumentiert, risikobasiert priorisiert** und gemeinsam mit den verantwortlichen Teams besprochen oder dem Management präsentiert. Dadurch erhalten Sie nicht nur nur Transparenz über bestehende Risiken und Gewissheit über die Effektivität Ihrer Cyber Sicherheit, sondern auch eine konkrete Entscheidungsgrundlage für wirksame Verbesserungsmaßnahmen.

Red Teaming & Adversary Simulation

Mit unserem „Red Teaming & Adversary Simulation“ Service prüfen die Widerstandsfähigkeit Ihres Unternehmens unter realitätsnahen Angriffsbedingungen. Anders als bei klassischen Penetration Tests stehen nicht isolierte Systeme oder Schwachstellen im Fokus, sondern die **ganzheitliche Betrachtung** technischer, organisatorischer und menschlicher Verteidigungsmechanismen.

Im Rahmen eines “Red Teamings“ simulieren wir gezielte Angriffsszenarien, die sich an realen Bedrohungsakteuren orientieren. Bei Adversary Simulationen wird zusätzlich das Vorgehen konkreter Angreiferprofile nachgebildet. Das beinhaltet Themen wie typische Taktiken, Techniken und Angriffsketten.

Dabei wird überprüft, wie effektiv bestehende Schutzmaßnahmen greifen, wie schnell Angriffe erkannt werden und wie koordiniert die Reaktion erfolgt. Ziel ist eine belastbare Einschätzung der operativen Resilienz und wie gut Ihre Sicherheitsarchitektur, Monitoring, Prozesse und Teams unter realem Druck zusammenspielen. Und natürlich auch, wo strategische Verbesserungen notwendig sind.



„Ich kenne mehrere Mitglieder des Teams von BrightFlare seit vielen Jahren aus dem Umfeld der Austrian Cyber Security Challenge. Wer dort regelmäßig überzeugt, bringt nicht nur technisches Können mit, sondern echtes Verständnis für komplexe Sicherheits-Herausforderungen und die Fähigkeit, auch unter anspruchsvollen Bedingungen fokussiert zu bleiben. Diese fachliche Substanz, gepaart mit der Handschlagqualität des Führungsteams, zeichnet BrightFlare aus.“

Joe Pichlmayr
CEO bei Ikarus Security Software und Vorstand bei CSA

Awareness Trainings & Phishing Campaigns

Technische Schutzmaßnahmen können nur wirksam sein, wenn Mitarbeitende Risiken erkennen und angemessen reagieren.

Angreifer nutzen gezielt menschliche Verhaltensmuster, Zeitdruck und Gewohnheiten aus, um in Organisationen einzudringen.

Unsere Awareness Trainings vermitteln **praxisnahes Verständnis für aktuelle Angriffsmethoden**, insbesondere im Bereich **Phishing, Social Engineering** und **digitale Manipulation.**

Ziel ist nicht die reine Wissensvermittlung, sondern die Stärkung eines reflektierten Sicherheitsverhaltens im Arbeitsalltag, durch nachhaltig einprägsame interaktive Szenarien und Simulationen.

Ergänzend führen wir strukturierte Phishing Kampagnen durch, um das tatsächliche Reaktionsverhalten im Unternehmen zu analysieren.

Die Ergebnisse werden anonymisiert ausgewertet und dienen als Grundlage für gezielte Verbesserungsmaßnahmen und nachhaltige Sensibilisierung.

Damit entwickelt sich Awareness von einer einmaligen Schulung zu einem kontinuierlichen Bestandteil Ihrer Sicherheitskultur weiter.

Physical Access & Social Engineering

Social Engineering Tests gehen über klassische Awareness Trainings oder Phishing Kampagnen hinaus.

Während digitale Kampagnen primär das Verhalten im virtuellen Kontext (Emails, etc.) prüfen, analysiert Social Engineering gezielt, **wie Angreifer organisatorische und physische Schwachstellen** ausnutzen könnten.

Dabei simulieren wir realitätsnahe Szenarien wie telefonische Täuschungsversuche, gezielte Informationsbeschaffung oder den Versuch, physischen Zutritt zu Gebäuden, Produktionsbereichen oder sensiblen Infrastrukturen zu erlangen.

Gerade der physische Zugang eröffnet Angreifern zusätzliche Möglichkeiten, vom Anschluss manipulierter Geräte bis hin zum direkten Zugriff auf interne Systeme, die rein virtuelle Angriffe nicht bieten.

Die Tests erfolgen unter klar definierten Rahmenbedingungen und mit abgestimmten Verantwortlichkeiten.

Ziel ist dabei, die Bewertung organisatorischer Abläufe, Zutrittskontrollen, Eskalationswege und Sicherheitskultur.

Geprüfte Kompetenz und jahrelange Erfahrung.

Unsere Security Engineers besitzen international anerkannte Offensive-Security-Zertifizierungen wie **OSCP** (Offensive Security Certified Professional), OSWP (Offensive Security Wireless Professional), **GWAPT** (GIAC Web Application Penetration Tester), **CRTL** (Certified Red Team Lead) und **CRTO** (Certified Red Team Operator). Darüber hinaus engagiert sich BrightFlare aktiv in der österreichischen Cybersecurity-Community. Außerdem fördern wir die Initiativen zur Stärkung der Cybersecurity-Kompetenz in Österreich.



Penetration Testing – Tested by ethical hackers

Unser Penetration Testing Service bietet Ihnen eine strukturierte und unabhängige Überprüfung Ihrer Systeme auf reale Angreifbarkeit.

Wir analysieren Ihre Infrastruktur aus der Perspektive eines Angreifers, bewerten konkrete Risiken und liefern priorisierte Handlungsempfehlungen zur nachhaltigen Erhöhung Ihrer Resilienz.

Unser Ansatz geht über automatisierte Schwachstellenscans hinaus. Ziel ist nicht das bloße Identifizieren technischer Lücken, sondern die realitätsnahe Bewertung tatsächlicher Ausnutzbarkeit und geschäftlicher Auswirkungen.

Was unser Penetration Testing besonders macht:

- **Strukturiertes Vorgehensmodell** – Jedes Engagement beginnt mit einem klar definierten Scoping und Zielsetzung. Auf Basis von „Intelligence Gathering“ und „Threat Modeling“ werden realistische Angriffsszenarien entwickelt und kontrolliert durchgeführt. Alle Aktivitäten erfolgen nachvollziehbar dokumentiert und mit anschließender Systembereinigung.
- **Manuelle Analyse und individuelle Exploits** – Neben automatisierten Verfahren setzen wir gezielte manuelle Prüfmethoden ein. Wo es sinnvoll ist, demonstrieren wir reale Angriffspfade oder entwickeln spezifische Exploits, um Auswirkungen transparent zu machen.
- **Technische Tiefe und klare Priorisierung** – Die Ergebnisse werden in einem umfangreichen technischen Bericht dokumentiert. Ergänzend erhalten Sie eine managementtaugliche Übersicht mit klar priorisierten Maßnahmen zur Risikoreduktion.
- **Persönliches Debriefing mit Ihrem Entwicklungsteam** – Findings werden nicht nur übergeben, sondern im direkten Austausch besprochen. Ziel ist eine umsetzbare Verbesserung Ihrer Sicherheitsarchitektur und der praktischen Widerstandsfähigkeit.

Managed SOC Service

Eine kontinuierliche, professionelle Sicherheitsüberwachung ist schlichtweg unverzichtbar. Mit unserem Managed SOC Ansatz unterstützen wir Unternehmen dabei, sicherheitsrelevante Ereignisse frühzeitig zu erkennen, wirksam zu bewerten und strukturiert darauf zu reagieren. Je nach Anforderungen bieten wir dafür passende Modelle – von bewährten Standardservices bis hin zu individuell entwickelten Lösungen.

Managed SOC mit Arctic Wolf
Gemeinsam mit Arctic Wolf bieten wir ein Managed SOC mit bewährtem, skalierbarem Service-Modell. Unternehmen profitieren von kontinuierlicher Überwachung, priorisierter Analyse sicherheitsrelevanter Ereignisse und klaren Eskalationswegen. So entsteht eine leistungsfähige Security-Operations-Basis, die interne Teams entlastet und die Reaktionsfähigkeit im Ernstfall verbessert.

Was Kund:innen an Arctic Wolf Managed SOC besonders schätzen:

- **Schneller Einstieg**
  Ein bewährtes Managed-SOC-Modell ermöglicht eine schnelle und strukturierte Umsetzung professioneller Security Operations.
- **24/7 Überwachung**
  Sicherheitsrelevante Ereignisse werden kontinuierlich beobachtet, analysiert und priorisiert – auch außerhalb klassischer Geschäftszeiten.
- **Entlastung interner Teams**
  Ihr internes Security- oder IT-Team wird im Tagesgeschäft spürbar entlastet und kann sich stärker auf strategische Aufgaben konzentrieren.
- **Skalierbares Betriebsmodell**
  Die Lösung eignet sich besonders für Unternehmen, die auf ein standardisiertes, erprobtes und effizient betriebenes SOC-Modell setzen möchten.
- **Mehr Transparenz**
  Sicherheitsrelevante Aktivitäten werden strukturiert sichtbar gemacht, damit Risiken schneller erkannt und bewertet werden können.

Eine bewährte Partnerschaft

BrightFlare ist **Arctic Wolf Partner!** Durch die langjährige erfolgreiche Zusammenarbeit und die Umsetzung zahlreicher Security-Projekte unterstützen wir unsere Kund:innen dabei, ihre IT-Sicherheitsstrategie mit einer leistungsstarken Managed-SOC-Lösung nachhaltig zu stärken.

ARCTIC WOLF

Individuelle SOC-Lösung mit All for One

Gemeinsam mit der All for One Group realisieren wir individuelle Managed-SOC-Lösungen für spezialisierte Anforderungen. Dieser Ansatz richtet sich an Unternehmen, die über Standardmodelle hinausdenken und eine Lösung benötigen, die sich präzise an Infrastruktur, Prozesse, Compliance-Vorgaben und branchenspezifische Anforderungen anpasst. So schaffen wir Security Operations, die nicht nur leistungsfähig, sondern auch passgenau integriert sind.

Ergänzend dazu steht ein partnerschaftlicher und beratungsnaher Ansatz im Mittelpunkt: Gemeinsam mit der All for One Group analysieren wir bestehende Sicherheitsstrukturen, identifizieren relevante Handlungsfelder und entwickeln darauf aufbauend ein Betriebsmodell, das sowohl strategische als auch operative Anforderungen berücksichtigt. Dadurch entstehen Managed-SOC-Lösungen, die sich flexibel in bestehende IT- und Security-Architekturen einfügen, vorhandene Systeme gezielt einbinden und zugleich die Grundlage für eine langfristig belastbare Sicherheitsorganisation schaffen.

- **Individuelle Möglichkeiten**
  Flexible Managed-SOC-Modelle, die sich gezielt an Ihre Umgebung und Anforderungen anpassen.
- **24/7 Überwachung**
  Kontinuierliche Überwachung sicherheitsrelevanter Ereignisse – rund um die Uhr.
- **Spezielle Anforderungen**
  Passgenaue Lösungen für komplexe Infrastrukturen, Compliance-Vorgaben und Bedarfe.

Continuous Threat Exposure Mangement (CTEM) & External Risk Management (ERM)

Moderne IT-Security erfordert mehr als das Abarbeiten einzelner Schwachstellen. Entscheidend ist die kontinuierliche Steuerung der tatsächlichen Angriffsfläche. Und das Intern, als auch Extern.

Continuous Threat Exposure Management (CTEM) organisiert genau diesen Prozess: Transparenz schaffen, Risiken priorisieren, reale Ausnutzbarkeit bewerten und Maßnahmen gezielt umsetzen.

Ziel ist nicht die Maximierung von Findings, sondern die messbare Reduktion relevanter Schwachstellen in der eigenen Landschaft.

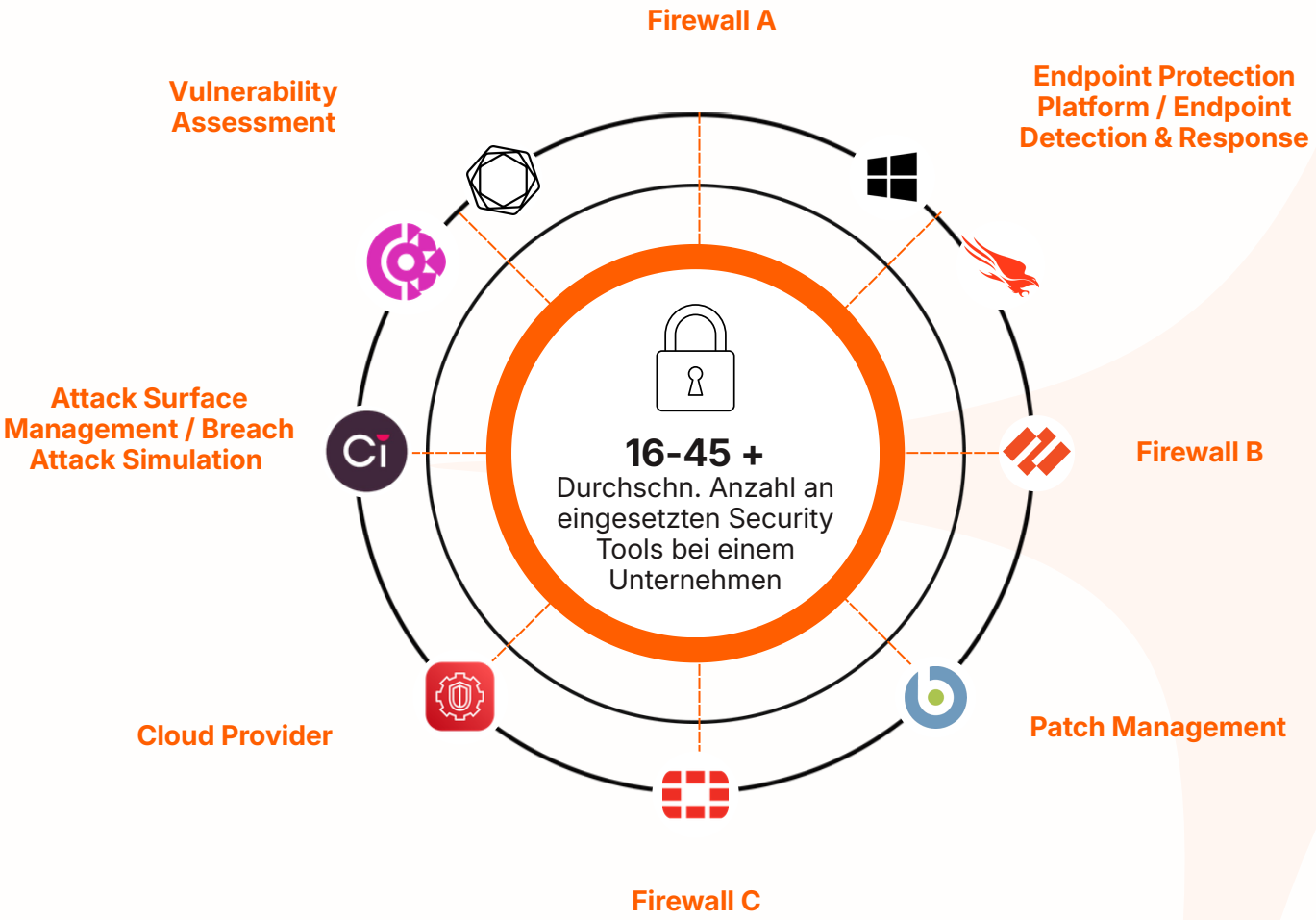
Was Infinity CTEM besonders macht:

- Risikobasierte Priorisierung statt Alert Flut
- Remediation ohne Betriebsunterbrechung
- Integriert in bestehende Sicherheitsarchitekturen
- Kontinuierliche Reduktion der Angriffsfläche

External Risk Management (ERM) ergänzt diese Sicht um die externe Perspektive. Es analysiert, welche Systeme, Domains, Zugangsdaten oder Cloud-Ressourcen von außen sichtbar und potenziell ausnutzbar sind. Jene Informationen, die Angreifer vor einem Angriff nutzen.

Wir unterstützen Sie bei der **Einführung und Umsetzung von CTEM oder ERM Lösungen.**

Dabei setzen wir unter anderem auf führende Technologien von Check Point.



Continuous Threat Exposure Management (CTEM)

Das Check Point Infinity TEM verbindet Transparenz, Priorisierung und Maßnahmenumsetzung in einem kontinuierlichen Prozess und orientiert sich dabei am tatsächlichen Risiko, nicht an isolierten CVSS-Werten.

Damit ermöglicht es Ihrem Unternehmen, Schwachstellen, Fehlkonfigurationen, Identitätsrisiken und externe Angriffsflächen ganzheitlich zu bewerten und strukturiert zu reduzieren.

BrightFlare x All for One x BlueZone
Gebündelte Expertise.

BrightFlare, die All for One Group und Blue Zone bündeln ihre Kompetenzen, um Unternehmen im DACH-Raum ganzheitlich bei Cybersecurity, Software-Modernisierung und der Entwicklung intelligenter digitaler Lösungen zu unterstützen.

Die Zusammenarbeit verbindet spezialisierte Sicherheitskompetenz mit umfassender IT- und Transformationsberatung sowie tiefem Know-How in individueller Software- und IoT-Entwicklung. So entsteht ein leistungsstarkes Angebot für Unternehmen, die ihre IT-, Produkt- und Produktionsumgebungen wirksam schützen, modernisieren und weiterentwickeln wollen.

Der Mehrwert für Ihr Unternehmen

Durch die Zusammenarbeit entsteht ein integriertes Angebot aus IT-Transformation, Cybersecurity und individueller Software-/IoT-Entwicklung. Unternehmen profitieren von:

- ganzheitlichem Schutz für IT-, OT- und produktnahe Software-Landschaften
- kombinierter Expertise aus Security-Spezialisten, Software- & IoT-Experten
- skalierbaren Leistungen von der Strategie bis zur technischen Umsetzung
- moderner Entwicklungskompetenz für komplexe, kundenspezifische Anforderungen
- frühzeitiger Integration von Security, Qualität und Compliance in Digitalisierungs- und Modernisierungsvorhaben

So können Sicherheitsanforderungen frühzeitig in Digitalisierungs-, Entwicklungs- und Transformationsprojekte integriert werden, statt erst im Nachhinein adressiert zu werden.

BrightFlare x All for One x BlueZone
Gebündelte Expertise.

BrightFlare bringt tiefgehende Expertise im Bereich Cybersecurity ein, insbesondere beim Schutz industrieller Anlagen und kritischer Infrastrukturen. Das Leistungsportfolio umfasst IT-Security, OT-Security, und Secure Software Development, ergänzt durch Security Operations als verbindendes Element über alle Bereiche hinweg. Ziel ist es, Bedrohungen frühzeitig zu erkennen, Angriffe wirksam abzuwehren und resiliente Sicherheitsstrukturen über die gesamte Systemlandschaft hinweg zu schaffen.

www.brightflare.io

BrightFlare

Die **All for One Group** ist ein internationaler IT-, Consulting- und Service-Provider mit starkem SAP-Fokus. Mit dem klaren Anspruch Technologie in konkreten Business Nutzen zu wandeln, begleitet und unterstützt das branchenspezialisierte Unternehmen seine mehr als 4.500 mittelständisch geprägten Kunden – darunter viele Familienunternehmen – aus Deutschland, Österreich, Polen und der Schweiz bei der nachhaltigen Unternehmenstransformation und auf ihrem Weg in die Cloud.

www.all-for-one.com

All for One

Blue Zone entwickelt individuelle Software- und IoT-Lösungen von der Idee bis zum fertigen Produkt. Das Unternehmen verfügt über mehr als 20 Jahre Erfahrung in Embedded Systems, PC-Software sowie Web-/Cloud-Anwendungen und begleitet Kunden bei der Weiterentwicklung und Modernisierung intelligenter Produkte. Ergänzt wird das Angebot durch Beratung und Workshops. Der Fokus liegt auf kundenspezifischen Lösungen auch für komplexe Anforderungen – von der Geräte- und Maschinenanbindung bis zu Edge-to-Cloud-Architekturen.

www.blue-zone.at

BLUEZONE

Warum BrightFlare?
Technologie. Erfahrung. Handschlagqualität.

Cyber Security ist Vertrauenssache.
Vertrauen entsteht dann, wenn Zertifikate und Hochglanzfolien bereits in Vergessenheit geraten sind, wenn die Realität des Alltags einkehrt und mal nicht alles nach Plan läuft. Und Vertrauen wächst, durch Haltung, Kompetenz, Verlässlichkeit und durch ehrliche und beständige Zusammenarbeit.

BrightFlare ist kein Beratungsunternehmen und kein anonymer Konzern. Wir sind ein eingespieltes Team aus Ingenieur:innen, Security-Expert:innen und Technologieverantwortlichen, das seit vielen Jahren zusammenarbeitet und jahrzehntelange Erfahrung in unterschiedlichsten Technologiebereichen vereint.
Unsere Wurzeln liegen in Industrie, Produktion und internationalen Softwareprojekten. In führenden Rollen eines großen internationalen Technologieberaters haben wir Cybersecurity Lösungen aufgebaut, kritische Infrastrukturen abgesichert und komplexe Transformationsprogramme verantwortet. BrightFlare ist die konsequente Weiterentwicklung dieser Erfahrung – unternehmerisch unabhängig, technologisch fokussiert und operativ exzellent ausgerichtet.

Technologie

Wir setzen auf praxiserprobte, führende Technologien und integrieren sie mit architektonischem Verständnis. Dabei denken wir nicht in Produktkategorien, sondern in funktionierenden Sicherheitsarchitekturen. IT, OT und Softwareentwicklung verbinden wir zu integrierten Sicherheitskonzepten, die Risiken priorisieren und nachhaltig wirksam sind.

Erfahrung

Erfahrung bedeutet für uns mehr als Projektlaufzeit. Sie bedeutet, operative Verantwortung getragen zu haben. Entscheidungen unter Druck zu treffen. Sicherheitsarchitekturen nicht nur zu planen, sondern im laufenden Betrieb zu verantworten. Wir kennen die Realität von Produktionsunternehmen, von Softwareherstellern und von komplexen IT-Organisationen. Dieses Verständnis prägt unsere Lösungen ebenso wie unsere Arbeitsweise – pragmatisch, strukturiert und wirksam.

Handschlagqualität

Wir verstehen uns nicht als Lieferant, sondern als Partner auf Augenhöhe. Wir übernehmen Verantwortung, kommunizieren offen und stehen auch dann an Ihrer Seite, wenn Situationen kritisch werden. Unsere Zusammenarbeit beginnt mit einem klaren Verständnis Ihrer Ziele. Wir arbeiten strukturiert, ohne unnötige Bürokratie, und liefern Ergebnisse, die nachvollziehbar und belastbar sind. Auf unsere Zusagen können Sie sich verlassen – dafür stehen wir mit unserem Namen.



Sprechen Sie mit uns.

Kontakt

contact@brightflare.io
+43 316 438000

www.brightflare.io

Adresse

BrightFlare FlexCo
Lastenstraße 11-15
8020 Graz