sure[secure]
your security operations center

secure mag

Cyber Resilience strategisch gedacht

Die Kombination aus SOC + Cyberversicherung im Unternehmenskontext

Intro

Cyberangriffe lassen sich nicht verhindern, aber ihre Auswirkungen lassen sich kontrollieren.

Digitale Angriffe gehören längst zum Alltag von Unternehmen, Behörden und Organisationen jeder Größe. Die Frage ist heute nicht mehr, ob ein Angriff stattfindet, sondern wann. Und wie schnell und wirksam darauf reagiert werden kann.

Viele Unternehmen investieren in technische Schutzmaßnahmen und organisatorische Vorgaben, um ihre Risiken zu reduzieren. Aber auch die beste Verteidigung bietet keinen absoluten Schutz. Systeme können kompromittiert werden, Schwachstellen bleiben unentdeckt, und menschliches Fehlverhalten lässt sich nie vollständig ausschließen.

Im entscheidenden Moment kommt es darauf an, Angriffe so früh wie möglich zu erkennen, präzise zu analysieren und sofort Gegenmaßnahmen einzuleiten. Denn je schneller eine Bedrohung eingedämmt wird, desto geringer sind die Auswirkungen auf den Betrieb, die Reputation und die Finanzen eines Unternehmens.

Ein wesentliches Risiko bleibt jedoch trotz schneller Reaktion bestehen: die finanziellen Schäden.

Kosten für Betriebsunterbrechungen, externe Experten, Wiederherstellungsmaßnahmen oder Rechtsberatung summieren sich schnell und können existenzbedrohende Ausmaße annehmen. Vor allem kleine und mittlere Unternehmen stehen hier oft vor enormen Herausforderungen, da Rücklagen oder Ressourcen fehlen, um kurzfristig große Schäden aufzufangen.

Deshalb reicht es nicht aus, nur auf operative Reaktionsfähigkeit zu setzen. Unternehmen benötigen eine umfassende Absicherung, die technische, organisatorische und finanzielle Risiken gleichermaßen berücksichtigt.

Unser Ansatz verbindet genau diese beiden Welten:

Mit unserem Security Operations Center (SOC) erkennen und analysieren wir Angriffe in Echtzeit, steuern Gegenmaßnahmen und verschaffen Unternehmen wertvolle Zeit im Ernstfall. Parallel dazu ergänzt eine Cyberversicherung die technische Abwehr um einen finanziellen Schutz, der die wirtschaftlichen Folgen eines Angriffs abfedert und es Unternehmen ermöglicht, nach einem Vorfall schnell wieder handlungsfähig zu sein.

Business Resilience als Führungsaufgabe. Ein integrierter Ansatz wird zum Muss.

In einer zunehmend unsicheren digitalen Welt wird Business Resilience zu einem strategischen Muss: die Fähigkeit eines Unternehmens, digitale Schocks nicht nur zu überstehen, sondern ihnen aktiv zu begegnen und gestärkt daraus hervorzugehen. Dabei geht es nicht nur um Technologie oder Notfallpläne. Resilienz ist eine Führungsaufgabe, die tief in die Verantwortung des Managements hineinreicht.

Es geht um die Sicherung von Arbeitsplätzen und Geschäftskontinuität, um die Vermeidung von Reputations- und Vertrauensverlust, um die Sicherung der wirtschaftlichen Handlungsfähigkeit und um die Verantwortung gegenüber Kunden, Partnern und der Gesellschaft. Nicht zuletzt leistet Business Resilience einen entscheidenden Beitrag zur digitalen Souveränität - gerade in Europa ein zentrales Thema.

Wer Resilienz aufbaut, schützt nicht nur das eigene Unternehmen, sondern trägt auch zur Widerstandsfähigkeit und Verlässlichkeit der gesamten Wirtschaft bei. Doch der Aufbau von Resilienz ist kein einmaliges Projekt. Es erfordert Strategien, Strukturen und Lösungen, die technisch, organisatorisch und finanziell ineinandergreifen.

Genau hier setzt unsere Kombination aus Security Operations Center und Cyberversicherung an: als pragmatischer Hebel für schnelle Reaktion, finanzielle Absicherung und nachhaltige Stabilität. Im nächsten Abschnitt zeigen wir, wie Resilienz anhand des international etablierten Fünf-Säulen-Modells systematisch gedacht und aufgebaut werden kann.

Foto: Philipp Skucha (CEO securance, CIO suresecure)

Die fünf Säulen der Resilienz und die Rolle der Cybersecurity als Teil davon

Risk Proof: A Framework for Building Organizational Resilience in an Unvertain Future

The five pillars of resilience

Quelle: World Economic Forum

- **Operationale Resilienz**

  Die Fähigkeit zur Aufrechterhaltung oder raschen Wiederherstellung des Betriebs im Falle von Störungen wie IT-Ausfällen, Datenverlusten oder Produktionsausfällen. Im Cyberkontext geht es vor allem um Reaktionsgeschwindigkeit: Wie schnell lassen sich Systeme isolieren, wiederherstellen oder alternativ betreiben? Ohne robuste Detektions- und Interventionsmechanismen drohen lange Ausfälle und Dominoeffekte.

- **Soziale Resilienz**

  Die Fähigkeit, Mitarbeitende, Partner und die Öffentlichkeit in der Krise mitzunehmen - durch transparente Kommunikation, Vertrauen und Führung. Cyberangriffe sind oft auch interne Schocks: Verunsicherung, Schuldzuweisungen und Kontrollverlust können Teams lähmen. Krisenkommunikation, Awareness und Unterstützung durch externe Experten helfen, das soziale Gefüge im Unternehmen zu stabilisieren.

- **Strategische Resilienz**

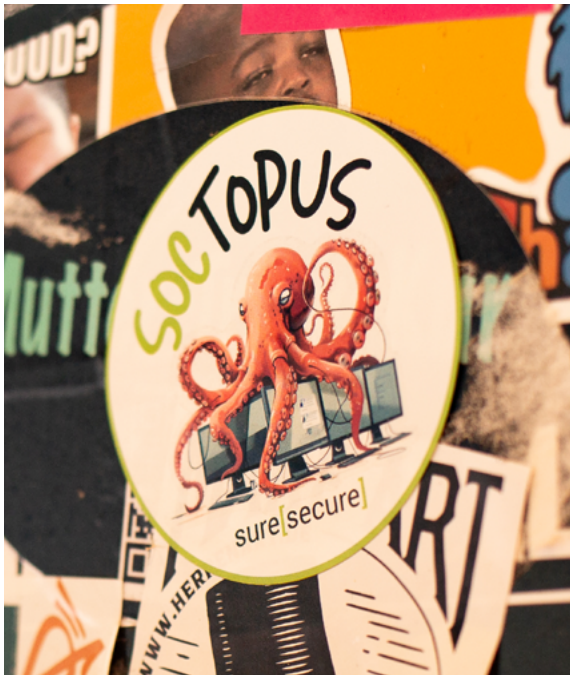
  Die Fähigkeit, auch unter Druck strategische Ziele weiterzuverfolgen und sich flexibel an veränderte Bedingungen anzupassen. Resiliente Unternehmen investieren antizipativ in Sicherheitsstrukturen, Prozesse und Partnerschaften und nicht erst reaktiv nach einem Vorfall. SOC + Cyberversicherung sind Ausdruck einer solchen strategischen Vorausschau: Sie sichern langfristige Handlungsfähigkeit in einem unsicheren Umfeld.

- **Finanzielle Resilienz**

  Die wirtschaftliche Fähigkeit, Krisen zu überstehen, ohne zentrale Geschäftsbereiche zu gefährden. Im Falle eines Cyberangriffs können immense Kosten entstehen: Betriebsunterbrechung, Wiederherstellung von Daten, Zahlungen an IT-Dienstleister, Erpressungsgelder, PR- und Rechtskosten oder gar Reputationsverlust mit Umsatzeinbußen. Eine Cyberversicherung federt genau diese Belastungen ab. So werden Bilanz und Liquidität geschützt.

- **Organisationale Resilienz**

  Die Fähigkeit der Organisation als Ganzes, anpassungs- und entscheidungsfähig zu bleiben. Dazu gehören klare Prozesse, verlässliche Entscheidungswege, robuste Partnerschaften und ein Mindset, das Veränderung als Normalzustand begreift. SOC + Cyberversicherung bieten hier strukturierte Handlungssicherheit: Wer weiß, was im Ernstfall zu tun ist und wer helfen kann, bleibt steuerungsfähig.



SOC + Cyberversicherung als Hebel für drei dieser Säulen

Die Kombination SOC + Cyberversicherung adressiert gezielt die drei Säulen der Resilienz, die im Kontext von Cyberangriffen am stärksten unter Druck stehen:

1. Operationale Resilienz: Durch schnelle Erkennung und Reaktion via SOC
2. Finanzielle Resilienz: Durch die Absicherung aller relevanten Schadensarten
3. Organisationale Resilienz: Durch klare Prozesse, externe Expertise und reduzierte Komplexität im Ernstfall

So ergibt sich eine handfeste Argumentation, warum Unternehmen ihr Schutzkonzept ganzheitlich aufstellen sollten und warum ein einfaches, integriertes Bundle aus Sicht der Unternehmensführung besonders attraktiv ist.

Die zwei Seiten der Resilienz: Erkennen und Abfedern

Resilienz in der Cybersicherheit hat zwei Dimensionen:

Schnelles Erkennen, Reagieren und Begrenzen von Angriffen: das ist die Aufgabe eines Security Operations Centers.

Abfedern finanzieller Folgen, um die Handlungsfähigkeit zu sichern: dafür sorgt eine Cyberversicherung.

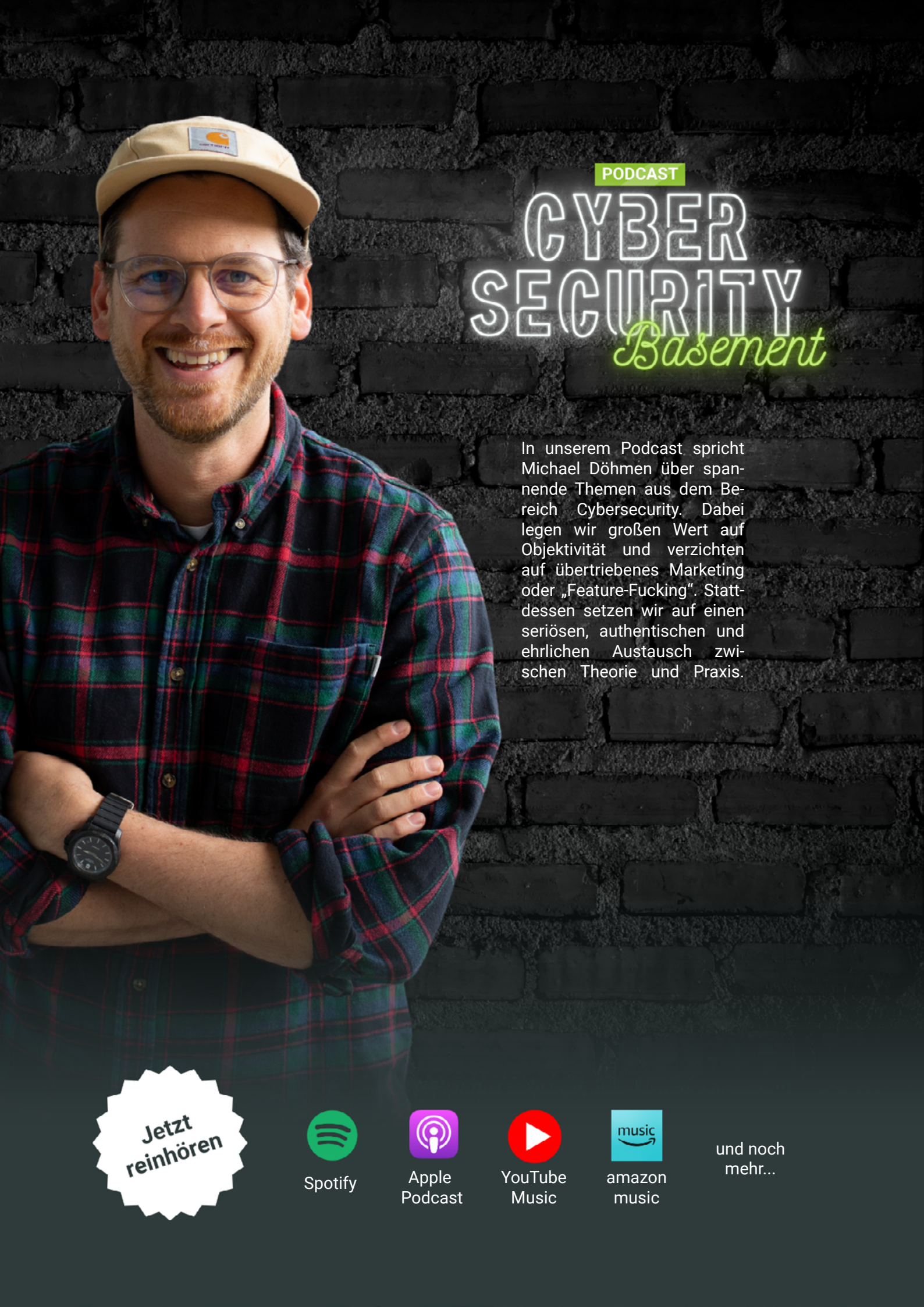
Foto: Georg Lauenstein (Senior Detection Engineer, suresecure)

SOC: Schnelligkeit entscheidet

Ein Security Operations Center erkennt Angriffe in Echtzeit, analysiert sie und koordiniert sofortige Gegenmaßnahmen. Es verhindert den Angriff nicht, aber es sorgt dafür, dass aus Minuten keine Stunden und aus Tagen keine Wochen werden. So werden Folgeschäden drastisch reduziert.

Cyberversicherung: Sicherheit für die Bilanz

Auch mit der besten Technik lassen sich Schäden nicht immer vermeiden. Datenverluste, Betriebsunterbrechungen, PR-Krisen oder Lösegeldforderungen können schnell existenzbedrohende Ausmaße annehmen. Hier greift die Cyberversicherung: Sie trägt die finanziellen Folgen und stellt Expertenteams für Forensik, Krisenkommunikation und Rechtsberatung bereit.

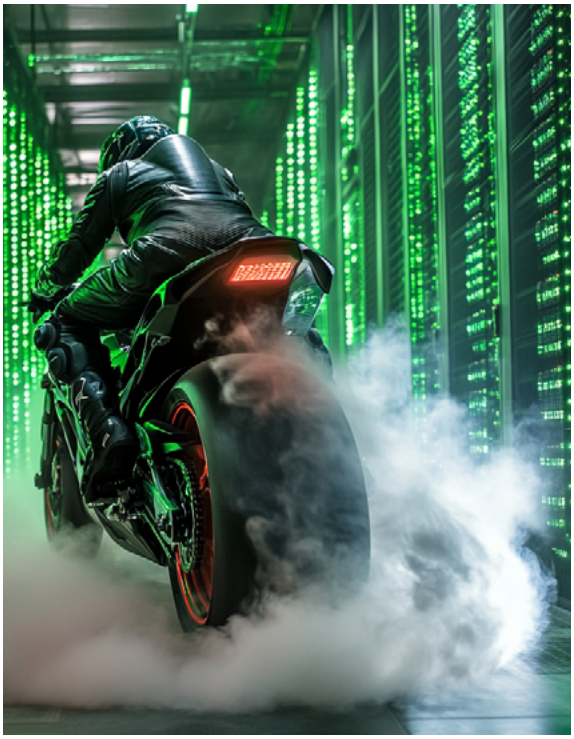

PODCAST
CYBER SECURITY
Basement
In unserem Podcast spricht Michael Döhmen über spannende Themen aus dem Bereich Cybersecurity. Dabei legen wir großen Wert auf Objektivität und verzichten auf übertriebenes Marketing oder „Feature-Fucking“. Stattdessen setzen wir auf einen seriösen, authentischen und ehrlichen Austausch zwischen Theorie und Praxis.
Jetzt reinhören
Spotify
Apple Podcast
YouTube Music
amazon music
und noch mehr...

Gemeinsam stärker: Warum die Kombination entscheidend ist

Ein Securtiy Operations Center ohne Versicherungsschutz lässt Unternehmen im Ernstfall finanziell allein. Eine Versicherung ohne aktives Monitoring riskiert verzögerte Reaktionen und hohe Schadenssummen. Erst die Kombination beider Bausteine bietet Sicherheit:

1. Technische Resilienz durch schnelle Erkennung und Reaktion
2. Finanzielle Resilienz durch Absicherung aller relevanten Schadensarten

Business Resilience entsteht also nicht durch Entweder-Oder - sondern durch Sowohl-als-auch.



Das Beste aus beiden Welten - ohne Kompromisse

Unser Bundle aus SOC + Cyberversicherung adressiert genau diese beiden Bedürfnisse und geht sogar noch einen Schritt weiter:

- Keine Risikoprüfung nötig: unabhängig von Branche, Vorschäden oder Vorerkrankungen der IT
- Sofortige Einsatzbereitschaft: Schutz ohne langwierige Antragsprozesse
- Kombinierbar mit bestehenden Versicherungen: als Erweiterung oder Zusatzmodul
- Flexible Upgrades: für wachsende Anforderungen
- Umfassende Leistungen: inkl. Eigenschäden, PR-Kosten, Dienstleisterausfall, Erpressung und Forensik

Für wen ist das sinnvoll?

Das kombinierte Schutzpaket aus SOC + Cyberversicherung richtet sich insbesondere an mittelständische und große Unternehmen, die ihre Widerstandsfähigkeit gegen digitale Risiken gezielt stärken wollen. Es eignet sich sowohl für Organisationen mit bereits etablierten Sicherheitsmaßnahmen als auch für Unternehmen, die bislang noch keine umfassende Cyberstrategie verfolgen.

Besonders attraktiv ist die Lösung auch für Firmen, die bereits über eine Cyberversicherung verfügen und diese um einen aktiven, technischen Schutz ergänzen möchten - ohne dabei komplizierte Risikoprüfungen oder langwierige Vertragsprozesse in Kauf nehmen zu müssen.

Unser Managed SOC - ohne Kompromisse:

- Automated Response (SOAR)
- Standard Sources
- Cyberaudit
- Incident Response
- suresecure Detection Rules
- Incident Drill
- Customer Success Manager
- Attack Surface Monitoring
- SIEM
- Vulnerability Management
- Security Advisory
- Cyberinsurance

Google Security Operations

Google Threat Intelligence

securance

DUAL

Business gut, alles gut.

Cyber Resilience darf kein Flickenteppich sein. Unternehmen brauchen ein integriertes Schutzkonzept, das Technik und Absicherung wirksam verbindet. Mit unserem CyberBundle aus SOC + Cyberversicherung schaffen wir genau diese Verbindung. Ohne Risikodialog, ohne Umwege.

Einfach. Effektiv. Sicher.

Security up. Risk down. Denn echte Resilienz hört nicht bei Technik auf - sie beginnt mit dem richtigen Zusammenspiel.

Weitere Informationen zum Thema:

Podcast-Folge:

Der heilige Gral
SOC + Cyberversiche-rung ohne Risikodialog

Podcast-Folge:

Mit Cyberaudit und IT-Si-cherheit auf der sicheren Seite

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.de

securance GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 211 88 23 02 84

E-Mail: kontakt@securance.de
www.securance.de