QNTROL

CYBERSECURITY FULL-SERVICE

für Unternehmen und Einrichtungen zum Monatspreis

- Security Software & Hardware
- Vor-Ort-Team-Service & Notfallequipment
- 24/7 Lagezentrum & Reaktion
- Backup-Systeme & Stand-by-Strukturen
- Anwaltliche Vollbetreuung
- Mitarbeiterschulung & Pentesting

Cybersecurity Full-Service

Cyber.Qntrol ist eine extrem leistungsstarke und anbieterübergreifende Cybersecurity-Servicelösung.

Cyber.Qntrol vereint marktführende Produkte und Kompetenzen zu einer intelligenten und schlagkräftigen jedoch unkomplizierten Cybersecurity-Gesamtlösung. Diese kann wahlweise On-Premise oder Cloud-basiert genutzt werden. Dabei dient Qntrol als Single Point of Contact und zentraler Dienstleister, mit eigenem 24/7-Lagezentrum im Leistungsverbund mit weiteren Spezialkompetenzen, wie der Qntrol.Legal Anwaltskanzlei.

Cyber.Qntrol Komponenten auf einen Blick

P-Level	**Protection & Performance**	Durch professionelle Sicherheit werden Bedrohungen erst gar nicht zu Gefahren. Dies geschieht durch Härtung der Syste-me, aber auch durch Sensibilisierung und Schulung der Mitarbeiter.	✓ Beratung ✓ Planung ✓ Realisierung
D-Level	**Defense & Detection**	Mittels hybrider Detektion werden Bedro-hungen erkannt und eliminiert. Insbeson-dere für die Erkennung gezielter Angriffe ist heutzutage eine effektive Zusammen-arbeit von Mensch und KI sowie die Verwendung mehrerer Systeme der Schlüssel.	✓ Firewall ✓ Viren- und Malware-Scanner ✓ Authentifizierung & Beschränkungen
C-Level	**Command & Control**	Alle Levels und Ereignislevel müssen zentral koordiniert und orchestriert werden. Dies geschieht im Qntrol.Center, das als Lagezentrum die Drehscheibe für alle Alerts und Notrufe ist und zur zentralen Verwaltung dient.	✓ 24/7 Verfügbarkeit ✓ Koordinierung und Orchestrierung aller Levels ✓ Alarmierung von Entscheidungsträgern und Force ✓ Dokumentation aller Vorgängen
R-Level	**Redundancy & Recovery**	Incident Response bedeutet angemessene und umgehende Reaktion auf Vorfälle. Wo Software und eigene Möglichkeiten nicht mehr weiterhelfen, kommen Qntrol Vor-Ort-Teams zum Einsatz und bringen Leihgeräte und Spezialequipment mit. Cybersecurity bedeutet auch Vorsorge zu treffen.	✓ Krisenkommunikationssupport ✓ Qntrol Vor-Ort-Teams (Rapid Response) ✓ Notfalltechnik (Notfallinternet, Notfalltelefonsystem, Notstrom) ✓ Incident-Leih-Equipment (Notebooks, Drucker, Funkgeräte, Media-Ausrüstung, etc.)
I-Level	**Intelligence & Investigation**	Das 24/7-Lagezentrum von Qntrol sucht aktiv nach Gefahren und Bedrohungen, um Anzeichen auf Cyber-Angriffe oder beispielsweise geleakte Dateien im Darkweb frühzeitig zu erkennen und abzuwehren.	✓ 24/7 Threat-Monitoring ✓ 24/7 Threat-Hunting ✓ 24/7 Media- & Brand-Monitoring ✓ 24/7 Desinformation-Monitoring ✓ 24/7 Fake-Monitoring ✓ 24/7 Darkweb-Monitoring
L-Level	**Legal & Law**	Jeder Cybervorfall bedarf einer rechtlichen Einschätzung und Beratung, vor allem, um sich konform zu verhalten. Qntrol.Legal bietet als Anwaltskanzlei umfassende juristische Unterstützung aus einer Hand.	✓ 24/7 Cyber-Rechtsberatung ✓ Rechtsbetreuung bei Cyberlagen (Datendiebstahl, Datenschutzverstöße, digitaler Erpressung, etc.) ✓ Forensik und Ermittlungen ✓ Behördenbetreuung

Umfassender Schutz aller Systemkomponenten

Endpunkte-Schutz
Cyber.Qntrol schützt sämtliche physischen Endpunkte im eigenen Netzwerk. Von stationären PCs über Notebooks bis hin zu Mobilgeräten.

Cloud-Schutz
Cyber.Qntrol schützt Cloud-Computer, Cloudspeicher und Cloud-Systeme sowie virtuelle Computer (VM's).

Netzwerk-Schutz
Cyber.Qntrol schützt Netzwerkgeräte wie Server und Netzwerkfestplatten (NAS) sowie virtuelle Instanzen.

Web- & E-Mail-Schutz
Cyber.Qntrol schützt sowohl E-Mails am Endpunkt, als auch Browser- und Webaktivitäten.

Remote-Schutz
Cyber.Qntrol sichert Remote-Arbeitsplätze ab - egal wo sich diese befinden.

IoT- & BYOD-Schutz
Cyber.Qntrol schützt IoT-Geräte wie IP-Kameras, Drucker sowie Senso-ren etc. und ermöglicht BYOD-Sicherheit durch Richtlinien.

Weitreichender Schutz vor Cyber-Bedrohungen


Ransomware


DDoS-Angriffe


E-Mailangriffe


Schädliche Websites


Malware


Phishing


Trojaner


Social-Engineering


Exploits


Dateilose Angriffe


Spyware


Viren

Cryptojacking


Systemausfälle


Sabotage

Cyberlagen erkennen, abwehren und bewältigen

⚠ Ransomware-Attacken
Bei Ransomware-Angriffen werden Daten gezielt kriminell verschlüsselt, um den Datenzugriff für die Opfer des Angriffs erst nach Zahlung eines Lösegeldes (engl. Ransom) wieder in Aussicht zu stellen.

⚠ DDoS-Attacken
Mit DDoS-Angriffen werden Systeme (Bsp. Webseiten) mit einer systematischen Überflutung von Anfragen (bspw. Seitenaufrufen) gezielt überlastet und dadurch stark bis vollständig funktionsbeeinträchtigt, so dass diese den eigentlichen Dienst nicht mehr erbringen können (engl. DDoS – Distributed-Denial-of-Service).

⚠ E-Mail-Attacken
Durch gezielte E-Mail-Angriffe oder als zufälliger Teil von Massen-E-Mail-Angriffen versuchen Angreifer über E-Mails die E-Mail-Empfänger dazu zu bringen, Passwörter, Informationen sowie weitere Daten preiszugeben (Phishing) oder Schadensoftware auszuführen.

⚠ Social-Engineering-Attacken
Social-Engineering-Angriffe variieren von sehr echt wirkenden Phishing-E-Mails, gehen über gekonnte Betrugsanrufe bis hin zu persönlichen Besuchen von Personen mit falschem Erscheinen vom Paketboten bis zu Polizei und Co. Bei noch massiveren Formen von Angriffen werden die Zielpersonen vorher systematisch ausgekundschaftet und teilweise auch elektronisch ausgespäht. Ziel sind Informationsdiebstahl, Trickbetrügereien oder auch Industriespionage.

⚠ Desinformations-Attacken
Eine Desinformationskampagne ist eine Form von Beeinflussungs- oder Sabotageangriffen und zielt darauf ab, falsche, irreführende oder provozierende Informationen zu verbreiten. Häufig entfaltet sich eine Desinformationskampagne am wirkungsvollsten über kompromittierte Cyberstrukturen des Opfers selber. Eine effektive Aufklärung und Bekämpfung ist heutzutage auch immer mehr eine technische Angelegenheit.

⚠ Lieferketten-Attacken
Bei Angriffen auf die Lieferkette kann es entweder darum gehen, die Lieferkette selber zu stören (Sabotage) oder einen anderen Cyberangriff (Ransomware-Attacke, Phishing-Attacke, Social-Engineering-Attacke etc.) durchzuführen, indem über einen vermeintlich vertrauenswürdigen Partner in der Lieferkette in das Ziel-System eingedrungen werden kann.

⚠ Cryptojacking-Attacken
Beim Cryptojacking geht es darum fremde Rechner für Cryptomining zu nutzen. Dabei entstehen teilweise Störungen durch gekaperte Rechenleistungen und der Stromverbrauch steigt immens. Als Nebenfolge werden häufig auch während der Einrichtungs- und Nutzungsphase Daten aus den betroffenen Systemen gestohlen, um diese, wenn das illegale Cryptomining entdeckt und beseitigt wurde, im Darknet zu kapitali-sieren.

⚠ Sabotage & Malware
Malware ist Software, die Angreifer nutzen, um die IT-Struktur zu beschädigen, zu zerstören oder sich unautorisierten Zugang zu verschaffen.

Qntrol.Center

Rund um die Uhr Erkennung, Abwehr sowie Bewältigung von Gefahren und Lagen

Orchestrierung

Über das Qntrol.Center werden alle Cybersecurity-Komponenten miteinander verbunden und orchestriert. Dabei integrieren wir nahtlos mit bereits bestehenden Produkten und Strukturen.

Das 24/7 Lage- und Koordinationszentrum von Qntrol ist das Sicherheits-Nervenzentrum der Full-Service Cybersecurity-Komplettlösung Cyber.Qntrol. Hier werden Tag und Nacht Warnmeldungen bearbeitet, Alerts bewertet, Systeme und ihre Komponenten sowie Märkte, Medien, das Darknet und andere Quellenorte nach Gefahrentrends und aktiven Bedrohungen analysiert. Vom Qntrol.Center aus werden potenzielle Bedrohungen oder eingetretene Lagen erkannt und abgewehrt sowie notwendige Bewältigungen koordiniert.

Qntrol.Center- Lagebeobachtung

Detection
- Alerts von der Cybersecurity-Suite
- Alerts von Sicherheitssoftware
- Alerts von Gefahrenmeldeanlagen wie BMA, EMA, etc.
- Alerts von Sensoren, Kameras etc.

Monitoring
- KI Threat-Monitoring
- Lieferketten-Monitoring
- Medien- & Reputations-Monitoring
- Desinformations- & Fake-Monitoring
- Darkweb-Monitoring

Intelligence
- Active-Threat-Hunting
- Suspicious-Behavior-Hunting
- Connection-Hunting
- Background-Screening
- OSINT-Informationsgewinnung

Qntrol.Center- Lagemanagement

Lageblätter
Für unterschiedliche Lagen, vom Stromausfall über Cyberangriffe bis hin zu Brandsituationen oder Reputationsangriffe usw. sind im Qntrol.Center pro Kunde eigene Lageblätter hinterlegt. Auf Basis dieser Checklisten und Handbücher werden die jeweiligen Lagen professionell und oft eigenständig bearbeitet.

Alarmierung
Das Qntrol.Center erbringt umfassende Alarmierungsleistungen und integriert dabei bestehende Kommunikationsmittel und auf Wunsch auch private Telefon-nummern der Kunden. Darüber hinaus betreibt Qntrol eigene Alarmierungsstrukturen. Die Alarmierung umfasst auch immer ein Fachbriefing der Entscheidungsträger beim Kunden.

Koordination
Bei unterschiedlichen Lagen, bis hin zu größeren oder länger andauernden Lagen, übernimmt das Qntrol.Center Informationsaustausch-, Dokumentierungs- und Koordinationsaufgaben. Das Qntrol.Center entsendet Qntrol Rapid-Response-Teams mit wenn nötig Notfallequipment und Leih-Ersatzgeräten.

Redundanz & Ausfallsicherheit

Das Qntrol.Center ist mehrfach redundant abgesichert und so in hohem Maße ausfallsicher. Dazu werden Software-, Hardware- sowie Provider-Redundanzen und Notfalltechnik genutzt.

Mehrfache Internetanbindung
Glasfaser, DSL, Kabel, 4G/5G, Satellit

Multi-Telefon-System
Hardware Hot-Standby, Cloud-Standby, Provider-Standby

Notstrom
USV, Generator, Solar

Mehrere Standorte
Backupstandorte stationär und mobil

Ersatzstrukturen
Schlüsseltechnik mehrfach vorhanden

Cybersecurity Software und bestehende Systeme

Cyber.Qntrol und die dafür verwendeten Komponenten integrieren nahtlos in bereits vorhandene Systeme. Auch bestehende Sicherheitskomponenten, wie Firewalls oder Antiviren-Software können weiter genutzt und müssen nicht ausgetauscht werden.

Provider & Partner

Qntrol ist von verschiedenen Software- und Hardwarelösungen direkt Partner. Dadurch ist Qntrol in der Lage, etwa von Bitdefender, jedes Modul der Sicherheitssoftware individuell zusammenzustellen, was eine Maßanpassung an die Kundenbedürfnisse ermöglicht und eine hohe Kostensteuerbarkeit für Cyber.Qntrol Kunden bedeutet. Qntrol ist selber Provider und kann so beispielsweise eigene Telefonanschlüsse und andere Anbindungskomponenten direkt schalten und überblicken, wodurch andere Sicherheits-layers eingebracht werden und weitreichende Redundanzen in der Sicherheitsarchitektur möglich sind.

Bitdefender Managed Service Provider | FORTINET Partner | ZOHO Certified Partner

Qntrol (HQ Berlin) - Ein Unternehmen der GP George GmbH | Savignyplatz 9-10, 10623 Berlin | T: +49 (0)30 23 595 0 | E: contact@qntrol.eu
Kontakt Key Account Management: Lennart Kirstein, T: +49 (0)30 23 595 0891, E: kirstein@qntrol.eu | Kontakt Qntrol.Center: Louis Acksel, T: +49 (0)30 23 595 0151, E: acksel@qntrol.eu
Kontakt Operations Management: Yuri Smith T: +49 (0)30 23 595 0898, E: smith@qntrol.eu | Kontakt Legal & Compliance: Rechtsanwalt Jakob Seifert, T: +49 (0)30 23 595 0691, E: seifert@qntrol.eu