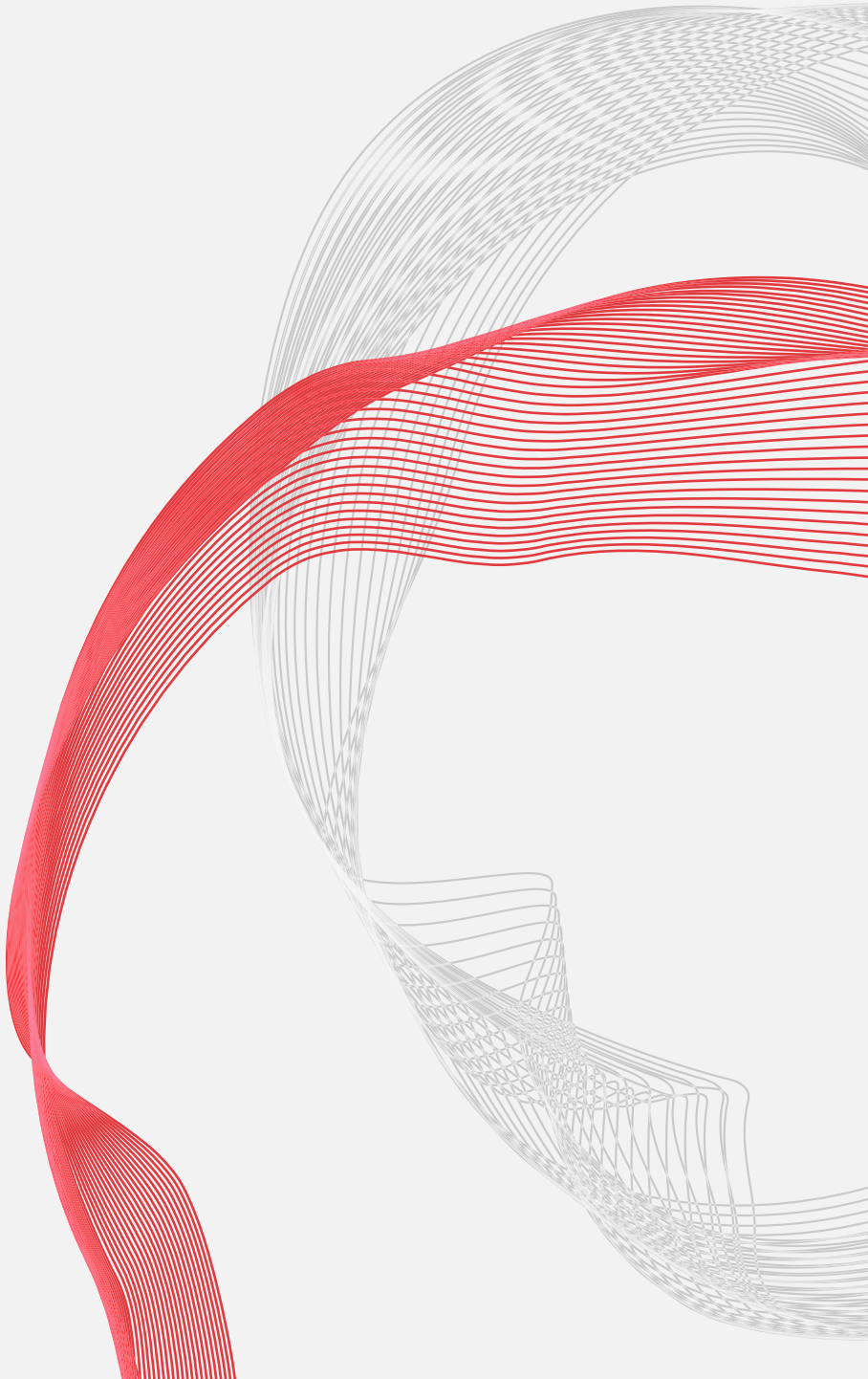
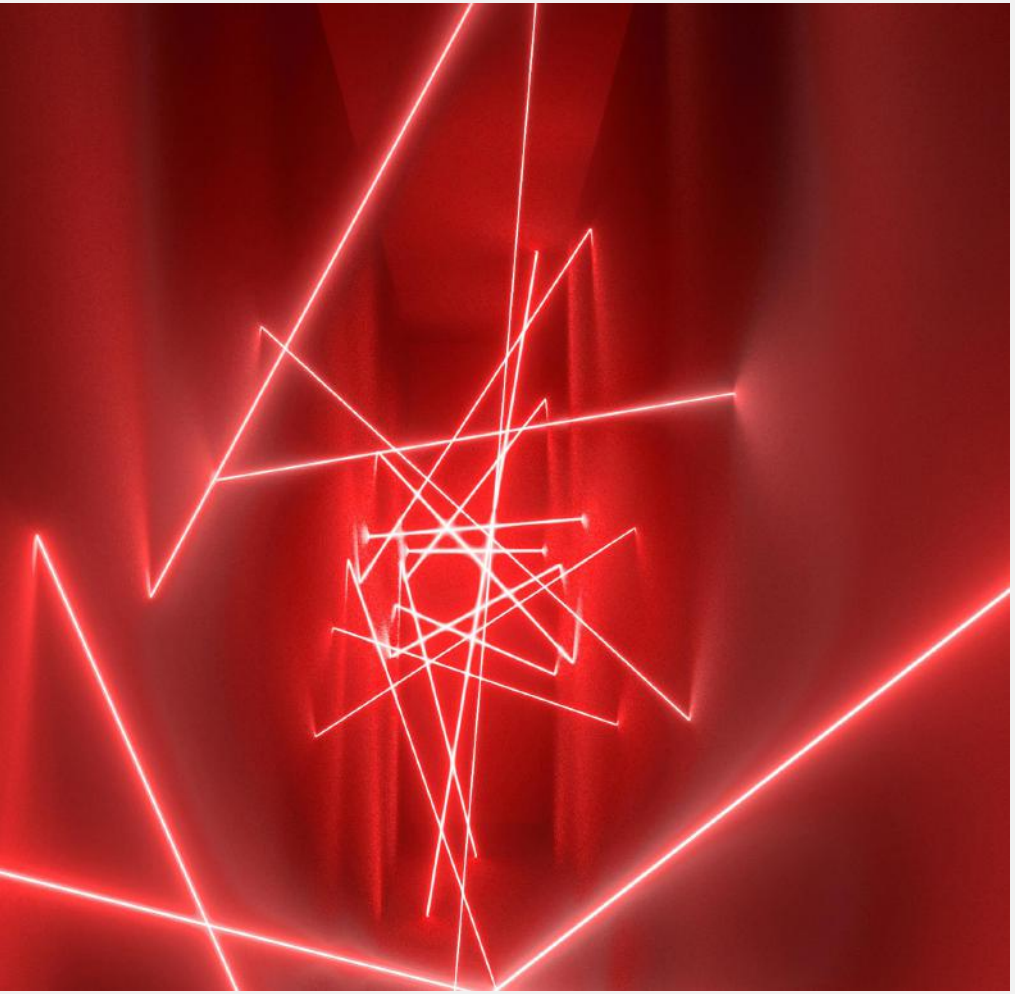
Höhere Leistung im SOC

REIFEGRADMODELL FÜR SICHERHEITSPROZESSE

Inhaltsverzeichnis





01 Warum Sicherheitsprozesse so wichtig sind

Cybersicherheit wird zu einem ernstzunehmenden Problem für kleine und mittelständische Unternehmen (KMU) genauso wie für Großunternehmen, die sich alle den neuen Sicherheits- und Geschäftsrisiken stellen müssen. Die schwerwiegendsten Risiken sind dabei wie folgt:

1. **Kein Unternehmen ist gegen Sicherheitsverletzungen gefeit.** Unternehmen jeder Größe und in jeder Branche müssen ihren Sicherheitsstatus stärken, um es mit den komplexen Bedrohungen unserer Zeit aufzunehmen.

2. **Organisationen können nicht mit der steigenden Zahl und Raffinesse der Bedrohungen mithalten.** Die Bedrohungslandschaft hat sich sehr stark weiterentwickelt, was Anzahl sowie Raffinesse der Angriffe anbelangt. Es gibt mittlerweile so viele verschiedene und komplexe Bedrohungen, dass Unternehmen diese nicht mehr bewältigen können.

3. **Eine erfolgreiche Datensicherheitsverletzung kostet ein Unternehmen** nicht nur Zeit, Ressourcen und den guten Ruf, sondern auch Geld. Zusätzlich zu den Ausgaben für die Erkennung, die Schadensminderung und die Wiederherstellung nach einem Sicherheitsverstoß entstehen auch langfristige Kosten.

4. **Vergrößerung der Angriffsfläche.** Die steigende Zahl der von zuhause aus arbeitenden Mitarbeiter und die häufigere Nutzung der Cloud haben nicht nur die Vernetzung von Unternehmen beschleunigt, sondern auch das Potenzial für Gefährdungen erhöht.

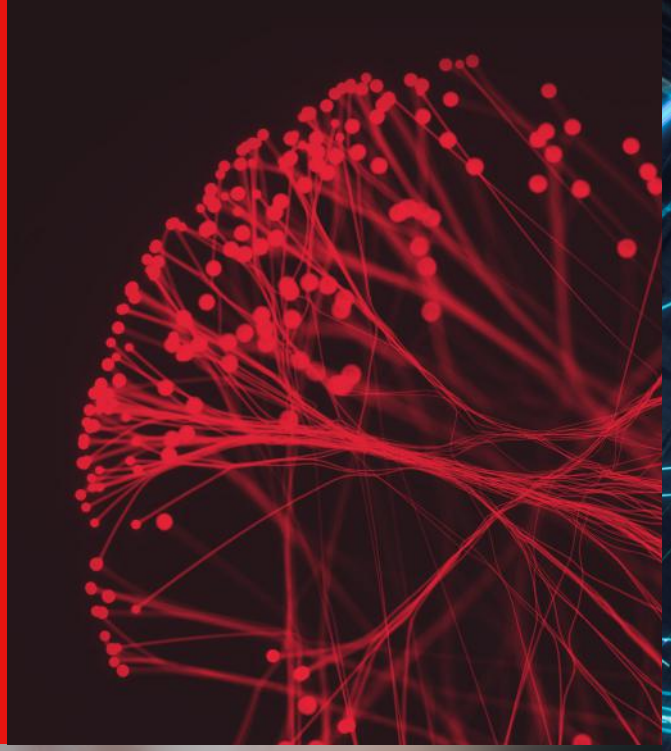
5. **Unzureichende Erkennungs- und Reaktionszeit:** Hacker haben genug Zeit, sich in den Systemen frei zu bewegen und ihre Ziele zu erreichen, wie das Herausfiltern von Daten oder das Ausführen von Malware, ohne von einer Sicherheitslösung bemerkt zu werden.

6. **Unternehmen haben zudem mit Compliance-Verpflichtungen zu kämpfen,** die eine Erfüllung bestimmter Cybersicherheitsanforderungen erfordern.

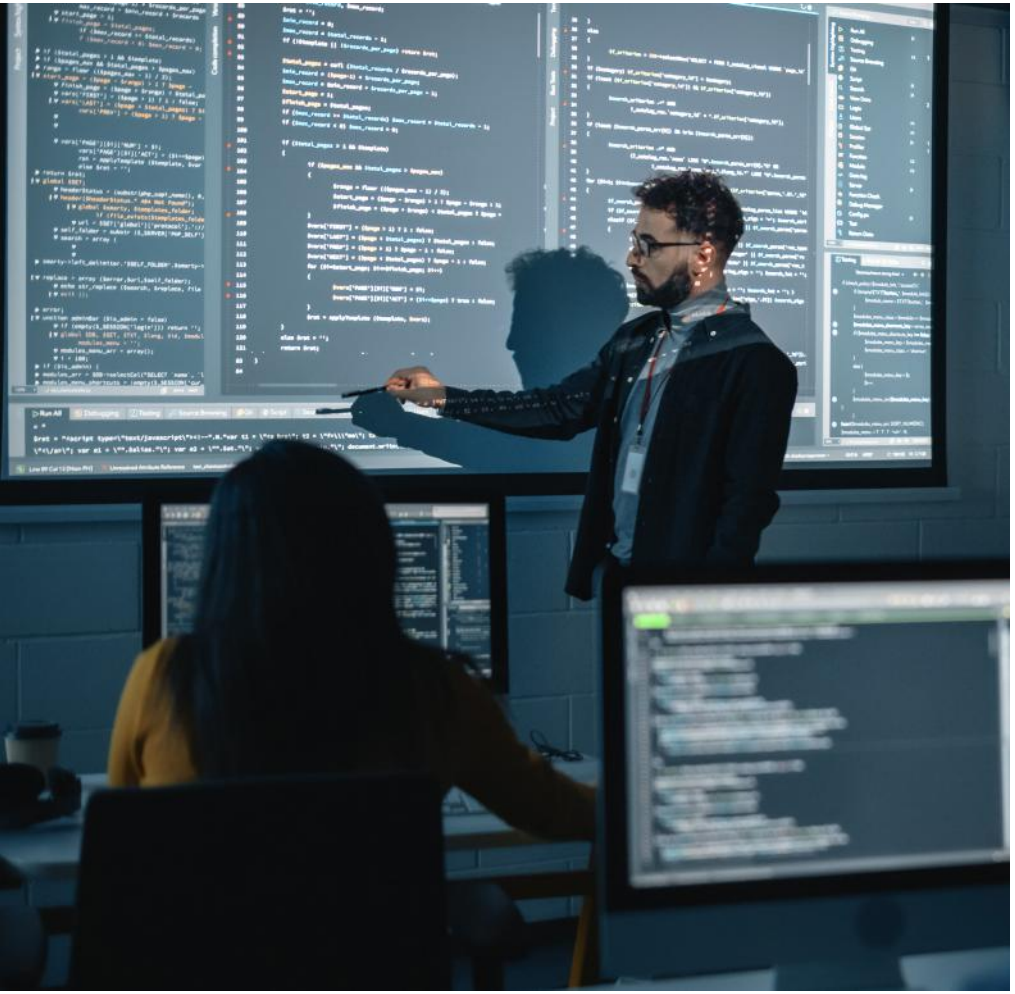
Gleichzeitig müssen Unternehmen zahlreiche Herausforderungen bezüglich der Verstärkung ihrer Widerstandsfähigkeit gegenüber Cyberangriffen bewältigen.

1. **Unternehmen leiden darunter, dass sie keine oder nur wenig interne Fachkompetenz vorweisen können.**
2. **Die Anzahl und Komplexität der unverbundenen Sicherheitstools und -kontrollen nimmt zu, weshalb Mitarbeiter oft Warnmeldungen gegenüber desensibilisiert werden (Alarmmüdigkeit) und ihnen zu viel Zeit widmen, die für strategische Geschäftsinitiativen genutzt werden sollte.**
3. **Mangel an Automatisierung und Prozessen für die Optimierung von Bedrohungserkennung, Untersuchungen und Reaktionen auf Sicherheitsvorfälle.**
4. **Cyberversicherungen haben ihre Vertragsbedingungen verschärft und stellen nun weitaus mehr Fragen über die Cyberbetriebsumgebung und Risikosteuerung der Antragsteller.**

In diesem E-Book erläutern wir genau, wie Sie Ihr SOC (Security Operations Center) aufbauen sollten und welche wesentlichen Fähigkeiten zur Bewältigung der Herausforderungen von heute Sie benötigen.



WatchGuard



02 10 wichtige Aufgaben eines modernen Security Operations Center

1 **Vorbeugende Sicherheit.** Dieser Schritt beinhaltet sämtliche Maßnahmen, die den Erfolg von Angriffen verhindern sollen, z. B. die regelmäßige Wartung und Aktualisierung bestehender Systeme, die Aktualisierung von Firewall-Richtlinien, die Behebung von Schwachstellen mit Patches und das Whitelisting, Blacklisting und Sichern von Anwendungen.

2 **Normalisierung und Management des Datenspeichers.** Das moderne SOC ist dafür verantwortlich, die Ereignisse und Protokolle des Netzwerks, die Anwender, die Endpoint-Aktivität und die Datenübertragung im gesamten Unternehmen zu erfassen, zu pflegen und regelmäßig zu überprüfen. Diese Daten helfen den Bedrohungsjägern, unerkannte Bedrohungen aufzudecken, und können für die Schadensminderung und Forensik verwendet werden.

3 **Kontinuierliche proaktive Überwachung und Erkennung verdächtiger Aktivitäten.** Die vom modernen SOC verwendeten Tools bieten ununterbrochene Aktivitätsüberwachung und informieren Sie über jegliche verdächtige Handlungen. Die kontinuierliche Überwachung ermöglicht dem SOC die umgehende Identifizierung aufkommender Bedrohungen, sodass schnell vorbeugende oder schadensmindernde Maßnahmen ergriffen werden können. Durch das Automatisieren der Verhaltensanalyse minimieren die Monitoring-Tools die Menge der von Menschen durchzuführenden Bewertungen und Analysen.

4 **Indikatoren für Kompromittierung und Bedrohungsbewertung, -priorisierung und -korrelation.** SOC-Analysten prüfen unter Zuhilfenahme automatisierter Sicherheitsanalysen (ML/KI) jede Warnmeldung und jeden Indikator für einen Angriff, ignorieren Falschmeldungen und bestimmen den Schweregrad der Bedrohungen. Auf diese Weise werden aufkommende Bedrohungen angemessen bewertet und die dringendsten Probleme werden zuerst behandelt.

5 **Die Jagd nach Bedrohungen ist ein Analysten-zentrierter Prozess,** mit dem Unternehmen verborgene, komplexe Bedrohungen, die von automatisierten Kontrollmechanismen für die Prävention und Erkennung übersehen werden, proaktiv ans Licht bringen und aufhalten können, bevor es zu Schäden kommt. Dabei lösen Mechanismen automatisch Indikatoren für einen Angriff aus, um zu gewährleisten, dass die Bedrohung schneller erkannt wird.

6 **Untersuchung von Grundursachen.** Nach einem Sicherheitsvorfall und während eines Angriffs ist das moderne SOC dafür verantwortlich, herauszufinden, was genau passiert ist, einschließlich dem Wann, Wie und Warum. Während der Untersuchung nutzen moderne SOC-Analysten Protokolle, Ereignisse, Threat Intelligence, Sicherheitsanalysen und weitere Informationen, um das Problem und dessen Quelle aufzuspüren. Diese Daten unterstützen sie dabei, in Zukunft auf ähnliche Probleme effektiv zu reagieren oder sie ganz zu vermeiden.

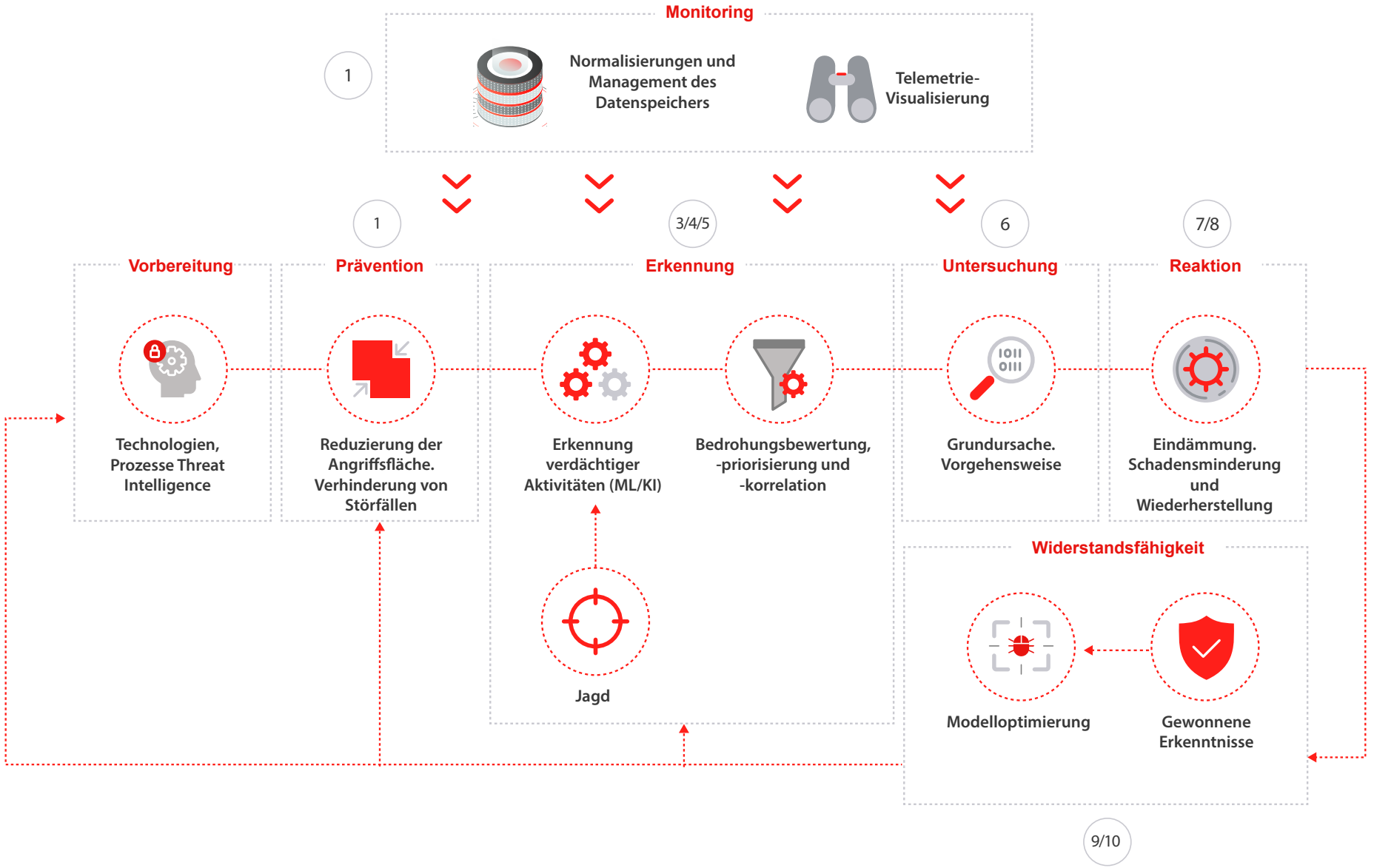
7 **Reaktion auf Gefahren.** Sobald ein Sicherheitsvorfall bestätigt wurde, kann das moderne SOC als „Ersthelfer" reagieren und Maßnahmen zur Eindämmung ergreifen, z. B. die Isolierung von Endpoints, das Beenden schädlicher Prozesse (oder das Verhindern von deren Ausführung), das Löschen von Dateien und mehr. Ziel ist es, im erforderlichen Umfang zu reagieren und dabei die Geschäftskontinuität so wenig wie möglich zu beeinflussen.

8 **Schadensminderung und Wiederherstellung.** Nach einem Sicherheitsvorfall bemüht sich das moderne SOC, Systeme und verlorengegangene oder kompromittierte Daten wiederherzustellen. Dazu kann es nötig sein, Endpoints zu löschen und neu zu starten, Systeme neu zu konfigurieren oder – im Falle von Ransomware-Angriffen – praktikable Backups bereitzustellen, um das Schadprogramm zu umgehen. Wenn dieser Schritt erfolgreich durchgeführt wird, werden das Netzwerk und die Endpoints wieder in den Zustand versetzt, den sie vor dem Vorfall aufwiesen.

9 **Gewonnene Erkenntnisse.** Leider wird oft übersehen, wie wichtig das Besprechen gewonnener Erkenntnisse ist, wenn es darum geht, den Sicherheitszustand eines Unternehmens und dessen Bereitschaft, sich zukünftigen Sicherheitsvorfällen zu stellen, zu verbessern. Dies unterstützt die Beurteilung der Sicherheitsrisiken für das Unternehmen und dessen Leistung bei der Reaktion auf einen Sicherheitsvorfall, die Identifizierung von Herausforderungen und die Verbesserung von möglichen Reaktionen auf einen zukünftigen Vorfall.

10 **Optimierung des Modells für Sicherheitsprozesse.** Eine effektive Verteidigung erfordert eine anpassbare Sicherheitsarchitektur, die dem Unternehmen die Ausführung optimierter Sicherheitsprozesse ermöglicht. Dieser Ansatz verbessert die Wirksamkeit durch Integration, Automatisierung und Orchestrierung und reduziert die Anzahl der Arbeitsstunden bei gleichzeitiger Verbesserung des Sicherheitsmanagements im Unternehmen.

- Konsolidierung der Sicherheit
- Automatisierung der Sicherheit
- Verstärkung der Sicherheitsprozesse
- Optimierung der Widerstandsfähigkeit gegen Cyberangriffe



nº 10 wichtige Aufgaben eines modernen Security Operations Center (Seiten 5 und 6)

03 Technologieeinsatz im SOC

Jede einzelne Aufgabe des SOC hängt in hohem Maße von Technologie ab. Der richtige Technologieansatz und die passende Strategie wirken sich bei der angestrebten Minimierung der MTTD/MTTR wesentlich auf die organisatorischen Fähigkeiten und Kosten aus. Es gibt verschiedene Strategien und Ansätze für die Realisierung von technologisch ausgereiften SOC-Funktionen. Dabei empfiehlt sich für Teams im Bereich Sicherheitsprozesse auf jeden Fall eine moderne und in hohem Maße integrierte, technologische, Cloud-basierte Plattform, die folgende Anforderungen erfüllt:

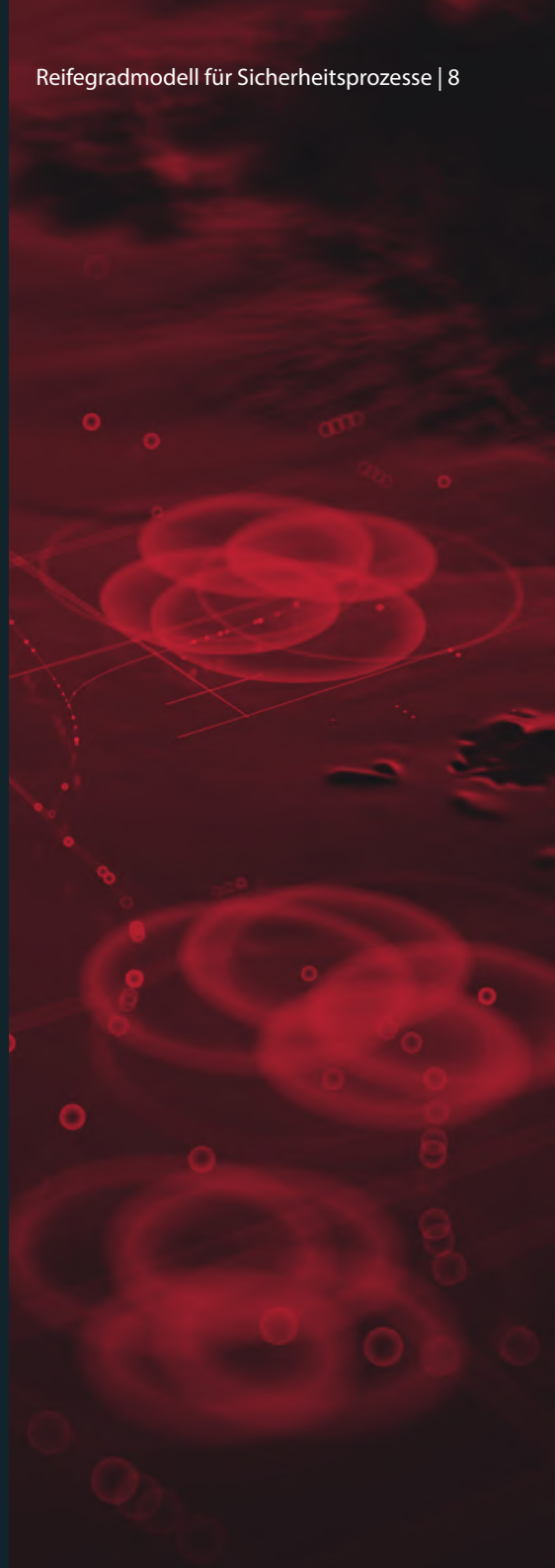
1. **Zentrale Visualisierung und Suchfunktionen:** Zentrale Suchfunktionen für alle Daten aus der verteilten IT-Infrastruktur, einschließlich umgehendem Zugriff auf Sicherheitswarnungen und komplette Telemetrie zur Beschleunigung von Bedrohungsuntersuchungen und Reaktionen auf Sicherheitsvorfälle durch sofortige Visualisierung.

2. **Ganzheitliche Bedrohungsanalysen:** Der Einsatz von künstlicher Intelligenz, TTP-basierten Szenario-Analysen und tiefgreifenden Kontextanalysen sämtlicher forensischer Daten zur Erkennung von komplexen Bedrohungen und zur akkuraten Priorisierung von Bedrohungen über die gesamte Angriffsfläche hinweg.

3. **Störfallmanagement:** Funktionen, die Sicherheitsteams dazu befähigen, in kollaborativen und effizienten Arbeitsabläufen mit einer zentralen und sicheren Fallmanagement-Plattform zu interagieren und die Bemühungen zur Untersuchung von Bedrohungen und zur Reaktion auf Sicherheitsvorfälle zu verwalten und zu beschleunigen.

4. **Aufgabenautomatisierung:** Die Automatisierung von routinemäßigen und zeitaufwendigen Aufgaben zur Unterstützung der Untersuchung von Bedrohungen und der Reaktion auf Sicherheitsvorfälle, z. B. die automatische Ausführung von Schadensminderungen und Gegenmaßnahmen zur Eindämmung und Neutralisierung von Bedrohungen.

5. **Operative Kennzahlen:** Die Fähigkeit, Messgrößen zu den wichtigsten Leistungskennzahlen (Key Performance Indicators, KPI) und Service-Level-Vereinbarungen (Service Level Agreements, SLA) einfach zu erfassen und effektiv zu melden.



WatchGuard®

04 Messen der SOC-Ergebnisse

Wie bei anderen wesentlichen Betriebsvorgängen auch, möchten Unternehmen die Wirksamkeit ihrer Sicherheitsprozesse messen können, um zu ermitteln, ob KPI und SLA erfüllt werden. Im Folgenden werden die minimalen und wesentlichen operativen Kennzahlen beschrieben, mit denen Unternehmen die aktuelle Betriebsleistung bezüglich der Ermittlung von Cyberbedrohungen und der Reaktion darauf messen und kommunizieren können.

1. **Durchschnittliche Zeit bis zur Erkennung (Mean Time to Detect, MTTD)** Gibt an, wie lange es dauert, bis ins Netzwerk eingedrungene Bedrohungen erkannt werden. Dies ist eine wesentliche Kennzahl für die Bestimmung der Effektivität von Sicherheitsprozessen und der Fähigkeit der Bedrohungsjäger und Tier-1-SOC-Analysten.

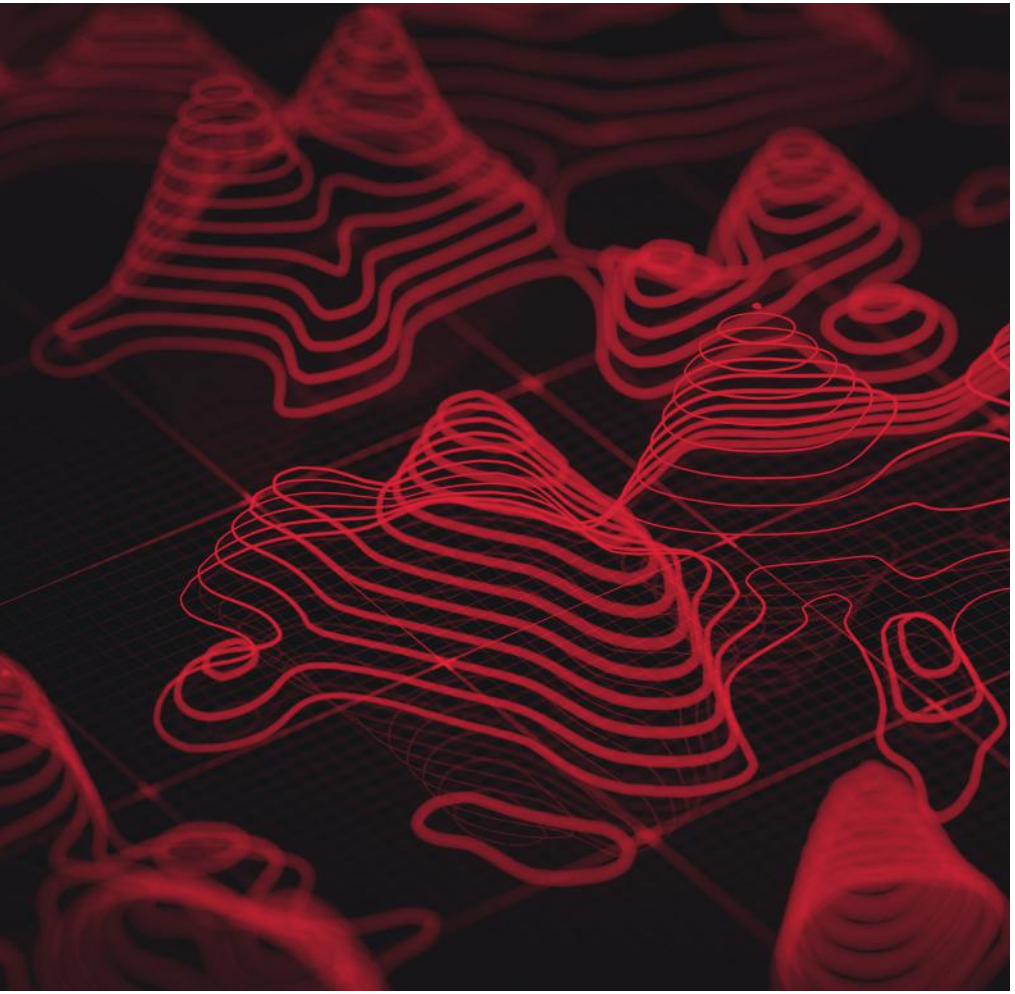
   MTTD-Berechnung: Die durchschnittliche Zeit, die es dauert, einzelne Sicherheitsvorfälle innerhalb eines bestimmten Zeitraums (Monat, Quartal, Jahr) zu erkennen. Die jeweilige Zeit bis zur Erkennung ist die Zeitdifferenz zwischen dem ersten Indikator für den Angriff (erster Nachweis) und der Qualifizierung der Bedrohung für eine vollständige Untersuchung (Zeitpunkt der Erstellung eines Störfalls).

2. **Durchschnittliche Zeit bis zur Reaktion (Mean Time to Response, MTTR)** Dies ist die Zeit, die für die Untersuchung und Schadensminderung der erkannten Bedrohungen erforderlich war. Dies ist eine wesentliche Kennzahl für die Bestimmung der Effektivität von Sicherheitsprozessen und der Fähigkeit der Tier-2- und Tier-3-Analysten und Hilfeleistenden des SOC. Eine hohe MTTR kann auf langsame und schwache SOC-Technologie in den für die Bedrohungsuntersuchung und Schadensminderung zuständigen Bereichen sowie auf mangelnde Automatisierung hinweisen.

   MTTR-Berechnung: Die durchschnittliche Zeit, die es dauert, einzelne Sicherheitsvorfälle innerhalb eines bestimmten Zeitraums (Monat, Quartal, Jahr) zu untersuchen und auf sie zu reagieren. Die jeweilige Zeit bis zur Reaktion ist die Zeitdifferenz zwischen dem Start der Untersuchung (Zeitpunkt der Erstellung eines Falls) und dem Zeitpunkt, an dem der Sicherheitsvorfall als entschärft eingestuft wird.

Wenn der Reifegrad der Sicherheitsprozesse eines Unternehmens verbessert wird, steigt die Effizienz der Erkennungs- und Reaktionsabläufe, was die MTTD sowie die MTTR beschleunigt. Eine reduzierte MTTD/MTTR senkt das Risiko von Cybersicherheitsvorfällen mit schweren Auswirkungen.

WatchGuard®



05 Reifegradmodell für Sicherheitsprozesse

Das Reifegradmodell für Sicherheitsprozesse beurteilt die aktuellen Fähigkeiten eines Unternehmens, die für Cyberrisiken und -vorfälle anfallenden Kosten durch Verringerung der für die Erkennung von und Reaktion auf Bedrohungen erforderlichen Zeit zu senken, die Widerstandsfähigkeit gegen Cyberbedrohungen zu stärken und einen Plan für den Ausbau dieser Fähigkeiten im Laufe der Zeit zu erstellen.

Unternehmen ohne Sicherheitsfachkräfte sollten mit einem Managed Security Services Provider (MSSP) oder einem modernen SOC zusammenarbeiten. Dabei müssen diese Dienstleister die nötigen Investitionen getätigt haben, um das Unternehmen beim Erreichen eines höheren Sicherheitsniveaus unterstützen zu können, und sie müssen über qualifizierte Mitarbeiter verfügen, die jederzeit mit dem Sicherheitsteam zusammenarbeiten können. Natürlich können Unternehmen auch ihr eigenes Team aufbauen, wenn ihnen die entsprechenden Ressourcen und angemessen erfahrene Mitarbeiter zur Verfügung stehen.

> Das Reifegradmodell für Sicherheitsprozesse beschreibt fünf Stufen auf dem Weg zum optimalen Reifegrad der Sicherheitsprozesse. Jede Stufe baut auf der vorherigen auf und beinhaltet zusätzliche Technologie und Verfahrensverbesserungen, mit denen die Fähigkeiten der Sicherheitsprozesse eines Unternehmens gestärkt und die MTTD/MTTR reduziert werden.

In der nachfolgenden Tabelle werden die einzelnen Stufen auf Endpoint-Ebene detailliert beschrieben. Dabei werden die wesentlichen technologischen und auf Arbeitsabläufe/Verfahren bezogenen Funktionen genannt, die auf jeder Stufe implementiert werden sollten. Die Fähigkeiten der oberen Stufen entsprechen einem sehr hohen Niveau und können daher als Leitlinien für Unternehmen gelten. Die Art und Weise, in der die einzelnen Fähigkeiten bereitgestellt werden, unterscheidet sich je nach Unternehmen.

	Reifephasen der Sicherheitsprozesse (Endpoint-Sicherheit)				
Fähigkeiten	**1**	**2**	**3**	**4**	**5**
	MINIMAL **Stufe 0**	REAKTIV **Stufe 1**	PROAKTIV **Stufe 2**	VERWALTET **Stufe 3**	OPTIMIERT Reduzierte MTTD/MTTR **Stufe 4**
		Stufe 0+	**Stufe 1+**	**Stufe 2+**	**Stufe 3+**
Verbesserter Sicherheitsstatus				Gewonnene Erkenntnisse Fortlaufende Verbesserungen des Sicherheitsstatus	
Jagd auf Bedrohungen (Threat Hunting)				Auf Analysen und intelligente Technologie (IOCS/YARA-Regeln) gestützte Jagd auf Bedrohungen	Proaktive, auf Erkenntnisse und Hypothesen gestützte Jagd auf Bedrohungen
Untersuchung				Sicherheitskontrollen haben die Untersuchung von erkannten Bedrohungen automatisiert	SOC-Analysten untersuchen mithilfe von Technologie Sicherheitsvorfälle (Analyse von Vorgehensweise und Grundursache)
Reaktion			Reaktionen werden durch aufdeckende Sicherheitskontrollen (Security Detective Controls, EDR) automatisiert	Manuelle Eindämmung und Reaktion	Automatisierte Reaktion über Sicherheitskontrollen hinweg
Erkennung			Erkennungen werden über EDR gemeldet	Ungewöhnliches Verhalten wird mittels Sicherheitskontrollen erkannt und gemeldet (Indikatoren für Angriff). Validierung durch SecOps-Team	Von SOC erstellte Verhaltenserkennung Störfallmanagement Korrelation der Indikatoren für niedriges Vertrauen, die auf Angriffe hinweisen
Monitoring		Zustandsüberwachung durch Sicherheitskontrollen Identifizierung ungeschützter Geräte	Das Sicherheitsteam überwacht die von den Sicherheitskontrollen gemeldeten Erkennungen	Das für Sicherheitsprozesse zuständige Team (SecOps) überwacht ungewöhnliches Verhalten, das mittels Sicherheitskontrollen erkannt wurde	24/7-SOC: kontinuierliche Aktivitätsüberwachung (Kombination aus Automatisierung und der Arbeit der Analysten)
Vorbeugung Sicherheitshygiene und ASR	Sicherheitskontrollen gegen bekannte Bedrohungen	Schwachstellenmanagement	Anpassung der Sicherheitsrichtlinien gemäß Prioritäten Absicherung von Anwendungen	Schatten-IT und Erkennung von Fehlkonfigurationen Absicherung fortgeschrittener Richtlinien	

Abbildung 1. Die schnellere Erkennung von und Reaktion auf Cyberbedrohungen hängt direkt vom Reifegrad Ihrer Sicherheitsprozesse ab.

Während die für Sicherheitsprozesse zuständigen Teams ihre Fähigkeiten zur Durchführung dieser Operationen ausbauen, nehmen auch die Komplexität und die erforderlichen Investitionen zu. Es wird jedoch leichter, solche Bedrohungen, die bestehende Sicherheitskontrollen umgehen könnten, früher zu erkennen.

Vertikal gibt es verschiedene Stufen, die das komplette Lebenszyklusmanagement einer Bedrohung definieren – solide Cybersicherheitsprogramme sollten diese sämtlich abdecken. Sicherheitsprozesse, die diese Programme steuern, beginnen bei vorbeugenden Maßnahmen, Hygiene und Richtlinien zur Reduzierung von Angriffsflächen, gefolgt von der Zustandsüberwachung von Sicherheitskontrollen und automatisierten Sicherheitsmaßnahmen zur Erkennung und Reaktion. Ausgereifte Cybersicherheitsprogramme beinhalten unter anderem folgende Prozesse:

1. **Jagd auf Bedrohungen** zur Verbesserung der Erkennung von und der vorbeugenden Maßnahmen gegen zuvor unbekannte TTP (Taktiken, Techniken und Prozesse), die von Angreifern genutzt werden.
2. **Tiefgreifende Untersuchung von Sicherheitsvorfällen** zur Bestimmung der Vorgehensweisen und der Grundursache, die dazu führen, dass Bedrohungen in die Umgebung eindringen.
3. **Analyse der gewonnenen Erkenntnisse** zur Reduzierung der Angriffsoberfläche und zur Verhinderung von Angriffen durch dieselben Angreifer und Methoden.

> Sämtliche Stufen umfassen Maßnahmen und Praktiken, die das Lebenszyklusmanagement verbessern, Risiken reduzieren und die Zeit bis zur Erkennung von und Reaktion auf Vorfälle verringern.

Das Ergebnis ist ein stärkerer Sicherheitsstatus und ein Unternehmen, das Bedrohungen gegenüber resistenter wird, während es die verschiedenen Reifephasen durchläuft. Die Durchführung dieser Tätigkeiten kann höchst komplex sein, insbesondere auf den höchsten Stufen, was qualifiziertes Personal und klar definierte Prozesse erfordert.

Moderne SOC benötigen Transparenz und Sicherheitspraktiken, die weit über den traditionellen Umfang und die herkömmlichen Endpoint-Sicherheitswarnungen hinausgehen.

Maßnahmen und Risiken von Sicherheitsprogrammen

Stufe 0 MINIMAL	• Auf Vorbeugung ausgerichtet (Firewalls, Antivirus-Programme usw. vorhanden). Ansatz der reaktiven Verteidigung • Technologie und Funktionssilos • Kein zentraler Überblick über Ereignisse • Keine formellen Verfahren zur Erkennung von und Reaktion auf Sicherheitsvorfälle • Jagd auf Bedrohungen findet nicht bei oberflächlichen Angriffen statt • Blind, was unbekannte und ausgefeilte Bedrohungen angeht • Eingeschränkte Praktiken für Sicherheitsprozesse • Nicht definierte oder nur grundlegende Sicherheitsrichtlinien	**Stufe 3** VERWALTET	• Mehr als nur die Erfüllung unbedingt erforderlicher Compliance-Anforderungen mit dem Ziel, die Sicherheitseffizienz und -effektivität zu maximieren • Es wurde erkannt, dass das Unternehmen die meisten Bedrohungen nicht erkennen kann; Streben nach Verbesserungen, die sowohl die Erkennung von als auch die Reaktion auf Bedrohungen mit schweren Auswirkungen optimieren, wobei der Schwerpunkt auf die am meisten gefährdeten Bereiche gelegt wird • Es wurden formelle Verfahren etabliert und Verantwortungen zugewiesen, welche die Überwachung der Sicherheitsumgebung und Warnmeldungen zu hohen Risiken regeln • Es wurde ein grundlegendes formelles Verfahren für die kontinuierliche Überwachung, Verhaltensanalysen für die Erkennung von ungewöhnlichen Vorkommnissen und die Eindämmung von Bedrohungen in der Umgebung mithilfe von EDR/NDR-Sicherheitslösungen etabliert • Ganzheitliche Zentralisierung von Protokolldaten und Sicherheitsvorfällen • IOC-basierte Threat Intelligence, die in Analysen und Workflows integriert wurde • Sicherheitsanalysen zur Erkennung der TTP (Taktik, Technik und Prozess) bekannter Bedrohungen • Grundlegende operative Kennzahlen zu MTTD/MTTR
Stufe 1 REAKTIV	• Minimale Zustandsüberwachung von Sicherheitskontrollen und Gefahrenabwehr • Praktiken zur Reduzierung von Angriffsflächen, z. B. Analyse bekannter Schwachstellen, Patch-Management und Erkennung von ungeschützten Ressourcen • Protokoll- oder Vorfallerfassung und -speicherung stützen sich hauptsächlich auf Compliance- und Revisionsanforderungen • Keine formellen Verfahren zur Erkennung von und Reaktion auf Sicherheitsvorfälle • Mangelnde Technologien für die konsistente und periodische Identifizierung von verdächtigen Aktivitäten • Blind, was unbekannte und ausgefeilte Bedrohungen sowie ATP mit Living-Off-The-Land-Angriffsmethoden angeht	**Stufe 5** OPTIMIERT	• Ganzheitliche Zentralisierung von Protokolldaten und Sicherheitsvorfällen mit ausreichend Aufbewahrungszeit, um hochentwickelte dauerhafte Bedrohungen (Advanced Persistent Threats, ATP) untersuchen zu können • Formelle und ausgereifte Aktivitätsüberwachung • Unternehmensübergreifendes Fallmanagement, Zusammenarbeit und Automatisierung • Holistische Forensik für Netzwerk, Server und Endpoint • Branchenspezifische IOC- und TTP-gestützte Threat Intelligence, die in Sicherheitsanalysen und -arbeitsabläufe integriert wurde • Erweiterte Sicherheitsanalysen für holistische Anomalie-Erkennung (via KI/ML-basierter Multi-Vektor-Verhaltensanalyse, die von SOC-Analysten angeleitet wird) • Etablierte, dokumentierte und ausgereifte Untersuchungs- und Reaktionsprozesse mit Standard-Playbooks • Etabliertes, funktionelles, durchgehend agierendes internes oder virtuelles SOC mit Analysten, Hilfeleistenden und Bedrohungsjägern • Einsatz automatisierter Verfahren zur Bedrohungsqualifizierung, -untersuchung und -reaktion, wo immer möglich • Architektur, Bedrohungsjäger und SOC-Techniker befassen sich mit neuen Gefahren • Erweiterte operative Kennzahlen zu MTTD/MTTR und historische Trendanalyse • Tiefgreifende Untersuchung von Grundursache und Vorgehensweise des Angriffs. Aus der Untersuchung gewonnene Erkenntnisse. Fortlaufende Verbesserung der SOC-Verfahren und -Tools
Stufe 2 PROAKTIV	• Lösungen für die Erkennung von und Reaktion auf Bedrohungen für Endpoints (EDR) und Netzwerke (NDR) vorhanden, mit minimaler Integration, werden in Silos ausgeführt • Starke und ausgereifte Sicherheitsrichtlinien bereitgestellt, mit vordefinierten Konfigurationsvorlagen zur Vermeidung von menschlichem Irrtum • Kontinuierliche Überwachung von Aktivitäten durch erweiterte Sicherheitskontrollen • Minimale Zentralisierung von Protokolldaten und Sicherheitsereignissen für den Fall einer Datensicherheitsverletzung, mit Schwerpunkt auf Servern und kritischen Ressourcen • Grundlegende Analyse-, Überwachungs-, Erkennungs- und Reaktionsverfahren etabliert, basierend auf Fähigkeiten zur Sicherheitskontrolle während der Geschäftszeiten • Mangelnde Mitarbeiter und Verfahren für die effektive Beurteilung und Priorisierung von Warnmeldungen • Widerstandsfähiger gegen Cyberkriminelle, es sei denn, es erfolgen unbekannte, ausgefeilte Angriffe auf blinde Flecken, wie ungeschützte Endpoints		

06 Mit solidem Reifegradmodell für Sicherheitsprozesse ein höheres Niveau erreichen

Bevor Sie Ihre Sicherheitsprozesse auf ein höheres Niveau anheben können, müssen Sie Ihre aktuellen Fähigkeiten beurteilen und anschließend einen Strategieplan für die Erweiterung Ihrer Fähigkeiten entwerfen.

> Das Quiz zum Reifegrad Ihrer Sicherheitsprozesse lässt Sie wissen, wie Ihr Unternehmen aufgestellt ist.

Sobald Sie die Grundlagen beherrschen, können Sie fortschrittliche Technologien, wie Automatisierung, maschinelles Lernen und künstliche Intelligenz, bestmöglich nutzen. Außerdem können Sie einen maßgeschneiderten Plan entwerfen, um den Reifegrad Ihrer Sicherheitsprozesse gemäß der Tabelle zu erhöhen.

Wenn die MTTD/MTTR sinkt, wird auch das Risiko von Cybersicherheitsvorfällen mit schweren Auswirkungen verringert.

WatchGuard®

WATCHGUARD FÜR SOC
STÄRKEN SIE IHRE SICHERHEITSPROZESSE

Arbeiten Sie intelligenter, statt härter. Ihr Team für Sicherheitsprozesse kann die Initiative ergreifen und Bedrohungen stets einen Schritt voraus bleiben.

Auf unserer Website erfahren Sie, wie:

www.watchguard.com/wgrd-products/security-operations-center-soc

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cybersicherheit. Unser Unified Security Platform®-Ansatz ist speziell auf Managed Service Providers ausgelegt, damit sie erstklassige Sicherheit bieten können, mit der ihre Unternehmen an Größe und Geschwindigkeit gewinnen und gleichzeitig die betriebliche Effizienz verbessern können. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, welche die fünf wichtigen Elemente einer Sicherheitsplattform umfassen – umfassende Sicherheit, kollektive Intelligenz, betriebliche Ausrichtung und Automatisierung – und sorgen somit für den Schutz von mehr als 250.000 Kunden. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.com.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 **INTERNATIONALER VERTRIEB:** +1 206 613 0895 **WEB** www.watchguard.com