QUIRSO.
Cyber Security for Germany

Managed Deception & Response

Weniger Lärm. Mehr Sicherheit.

QUIRSO Managed Deception and Response

Managed Detection & Response von QUIRSO schützt Ihre IT rund um die Uhr. Wir erkennen Angriffe früh, reagieren schnell und reduzieren Schäden effektiv – für maximale Sicherheit, Transparenz und echte Handlungsfähigkeit im Ernstfall.

Grenzen von herkömmlichen Managed Detection and Response Lösungen

Managed Detection and Response (MDR) ist ein etablierter Ansatz zur Erkennung von Cyberbedrohungen, bringt jedoch in der Praxis einige Herausforderungen mit sich.

False Positives sind ein Problem

Viele MDR-Lösungen basieren auf der Auswertung großer Mengen an Logs und Telemetriedaten. Das führt häufig zu einer hohen Anzahl an Alarmen, von denen ein erheblicher Teil False Positives sind. Security-Teams verbringen dadurch viel Zeit mit der Analyse und Priorisierung, anstatt sich auf echte Bedrohungen zu konzentrieren.

Hohe Kosten durch Komplexität

Zudem entsteht durch die Abhängigkeit von umfangreichen Datenquellen ein hoher Infrastruktur- und Integrationsaufwand. Logdaten müssen gesammelt, gespeichert und verarbeitet werden, was sowohl die Komplexität als auch die Kosten erhöht. Gerade für kleine und mittelständische Unternehmen kann dies schnell zur großen Belastung werden.

Angriffe werden zu spät erkannt

Ein weiteres Problem ist die zeitverzögerte Erkennung von Angriffen. Da viele MDR-Systeme auf Verhaltensanalysen und Korrelationen angewiesen sind, werden Angriffe oft erst erkannt, wenn bereits auffällige Aktivitäten oder Schäden entstanden sind. Dadurch kann sich die sogenannte Dwell Time verlängern, in der sich Angreifer unbemerkt im Netzwerk bewegen.

Insgesamt stoßen klassische MDR-Ansätze daher oft an ihre Grenzen, wenn es um präzise, schnelle und ressourcenschonende Bedrohungserkennung geht.

Genau hier setzt unser Managed Deception & Response Ansatz an.

Warum QUIRSO Managed Deception and Response?

Viele klassische Sicherheitslösungen erzeugen eine große Menge an Logdaten und Alarmen, die aufwendig analysiert werden müssen.

Der andere Ansatz mit QMDR

QUIRSO Managed Deception and Response (QMDR) verfolgt einen anderen Ansatz: Angreifer werden gezielt durch attraktive digitale Köder angelockt.

Diese sogenannten Deception-Assets, etwa Decoy-Systeme, gefälschte Zugangsdaten oder scheinbar wertvolle Dateien, sind für normale Benutzer irrelevant. Interagiert jemand damit, ist das ein klarer Hinweis auf eine kompromittierte Umgebung.

Das Ergebnis: hochpräzise Detektionen mit minimalen Fehlalarmen.

Fordern Sie ihre Demo an:

mdr@quirso.de

Was ist QUIRSO Managed Deception and Response?

QMDR vereint Cyberabwehrtechnologie mit direkter, professioneller Reaktion auf Cyberangriffe. Die Lösung kombiniert eine 24/7 Managed Deception-Plattform mit dem QUIRSO Rapid Incident Response Service. Hinter diesem Service steht ein hoch spezialisiertes Team, das rund um die Uhr auf Vorfälle reagiert.

Angreifer werden sehr früh erkannt

Durch diese Kombination werden Angreifer bereits in frühen Phasen sichtbar, bevor sie Schaden anrichten können. Hochpräzise Alarme sorgen dafür, dass Security-Teams nur auf echte Bedrohungen reagieren müssen, während False Positives auf ein Minimum reduziert werden.

Angriffe stoppen - Schaden vermeiden

Im Ernstfall greift das Incident-Response-Team sofort ein, analysiert die Angriffe mithilfe von Live-Forensik und stoppt Bedrohungen schnell und effektiv.
QUIRSO Managed Deception and Response bietet präzise, schnelle und kosteneffiziente Cyberabwehr – ideal für Unternehmen, die sich gegen moderne Angriffe wappnen möchten, ohne zusätzliche Komplexität, großen Infrastrukturaufwand und hohe Kosten.

Vorteile von QMDR

Frühe Angriffserkennung

Angreifer werden bereits während der Aufklärungsphase oder bei lateralen Bewegungen im Netzwerk entdeckt – lange bevor Schaden entsteht.

Hochpräzise Alarme

Da legitime Nutzer nicht mit Deception Assets interagieren, entstehen sehr wenige Fehlalarme. Ihr Security-Team kann sich auf echte Bedrohungen konzentrieren.

Schnelle Incident Response

Sobald ein Deception-Alert ausgelöst wird, reagiert unser Security- und Incident-Response-Team sofort. Mithilfe von Live-Forensik analysieren wir den Angriff und leiten Maßnahmen zur Eindämmung ein.

Kürzere Dwell Time

Angreifer werden schneller erkannt und gestoppt, wodurch sich die Zeit reduziert, in der sie sich unentdeckt im Netzwerk bewegen können.

Kosteneffiziente Security

Im Vergleich zu klassischen Monitoring-Lösungen benötigt Deception deutlich weniger Log-Daten und Infrastruktur, wodurch Kosten und Komplexität erheblich reduziert werden.

Erleben Sie es live. Jetzt Demo anfragen oder individuelles Angebot erhalten.

Wir beantworten Ihre Fragen:

Stefan Zimmermann

Denis Szadkowski

QUIRSO.
Cyber Security for Germany

August-Bebel-Str. 26-53
14482 Potsdam
sales@quirso.de

Der Unterschied, der Angreifer sichtbar macht

Kriterium	Klassische MDR	QUIRSO MDR
Erkennungsansatz	⚠ Signaturen & Verhalten	✅ Täuschung & Interaktion
Detektionsqualität	⚠ viele False Positives	✅ nahezu keine Fehlalarme
Reaktionsgeschwindigkeit	⚠ oft verzögert	✅ sofort
Sichtbarkeit	⚠ indirekt	✅ direkt & eindeutig
Ressourcenaufwand	⚠ hoch	✅ gering
Angriffsphase	⚠ spät erkannt	✅ Früherkennung
Komplexität	⚠ hoch	✅ schlank
Mehrwert	⚠ Monitoring	✅ aktive Verteidigung

Mehr als Deception: Ein vollständiger Response-Ansatz

Bei QMDR handelt es sich nicht nur um eine Deception-Lösung, sondern um einen vollumfänglichen Managed Service, der aus Deception-Technologie, Deception Engineering and Rapid Incident Response besteht.

Unsere Expertise für Ihren Schutz

Unsere hochqualifizierten Experten entwickeln gemeinsam mit unseren Managed Deception and Response-Kunden eine Deception-Strategie, die sich nahtlos in die bestehende IT-Umgebung integriert und Angreifer gezielt in die Irre führt. Sobald ein Alarm der Deception-Lösung ausgelöst wird, reagiert unser Incident-Response-Team sofort, analysiert den Vorfall in Echtzeit und leitet gezielte Gegenmaßnahmen ein. So kombiniert QUIRSO präzise Täuschung, Expertenwissen und schnelle Reaktion, um Angreifer frühzeitig zu stoppen und Schäden zuverlässig zu verhindern.

Maximale Wirkung in Ihrer bestehenden Sicherheitslandschaft

QUIRSO Managed Deception & Response lässt sich problemlos in bestehende Security-Monitoring-Umgebungen integrieren. Ob SIEM-Systeme, Endpoint Detection & Response oder andere Monitoring-Tools – unsere Lösung liefert hochpräzise Alerts, die sich direkt in Ihre bestehenden Workflows einfügen.

So profitieren Unternehmen von früherer Angriffserkennung, minimalen Fehlalarmen und schneller Incident Response, ohne bestehende Security-Investitionen ersetzen oder komplexe Schnittstellen aufbauen zu müssen.

Flexibel einsetzbar – in jeder Umgebung

QUIRSO Managed Deception & Response lässt sich nahtlos in Cloud-, On-Premise- sowie hybride Infrastrukturen integrieren – sowohl in klassischen IT- als auch in sensiblen OT-Umgebungen. Durch gezielt platzierte Deception-Assets werden Angreifer unabhängig von der Architektur frühzeitig erkannt, ohne den laufenden Betrieb zu beeinträchtigen. Die Lösung ist skalierbar, unauffällig und passt sich Ihrer bestehenden Sicherheitslandschaft flexibel an.

Einsatzbereich	unterstützt
Cloud	✅
On-Premise	✅
Hybrid	✅
IT	✅
OT	✅

QUIRSO.
Cyber Security for Germany

August-Bebel-Str. 26-53
14482 Potsdam
sales@quirso.de