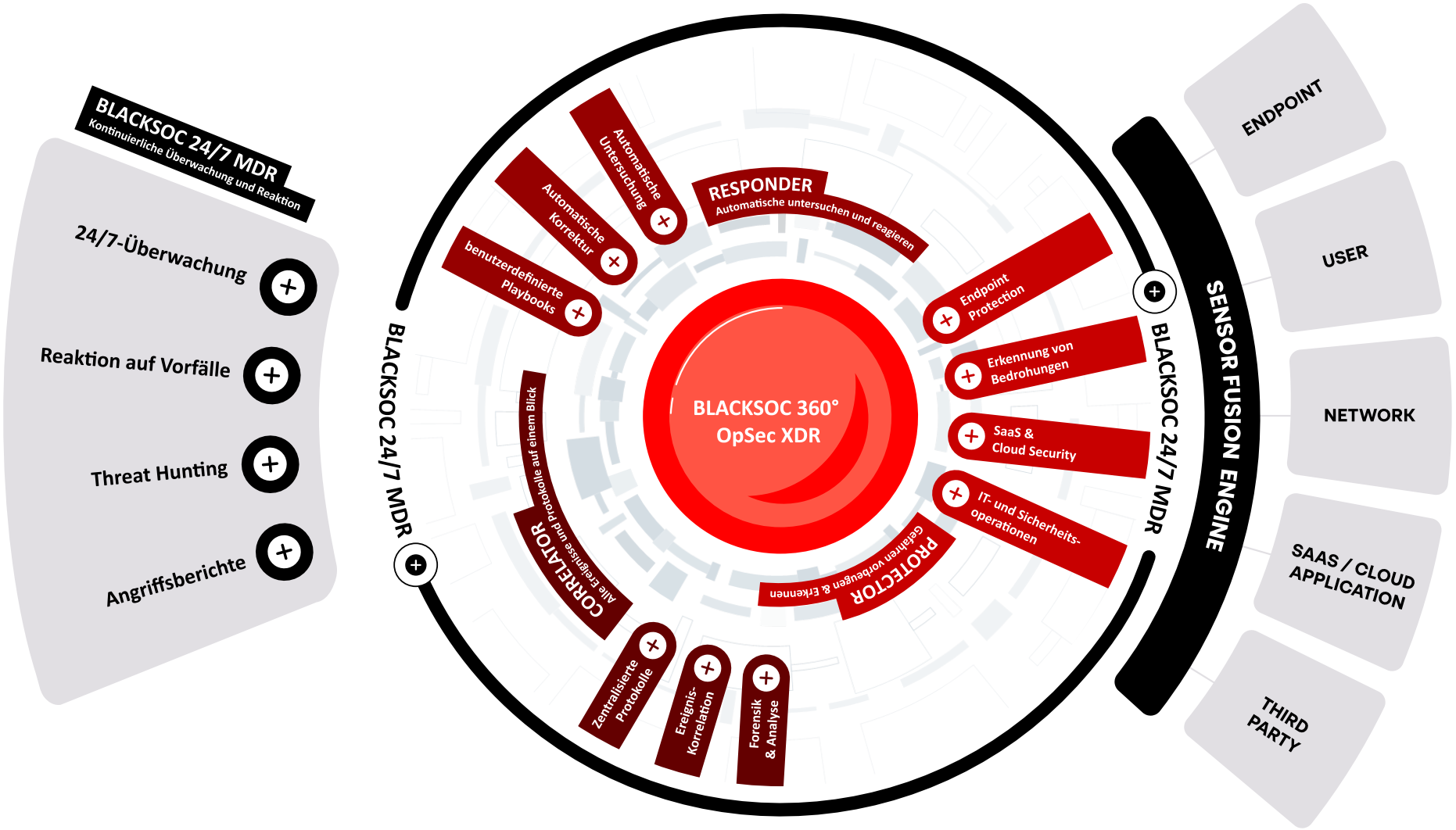
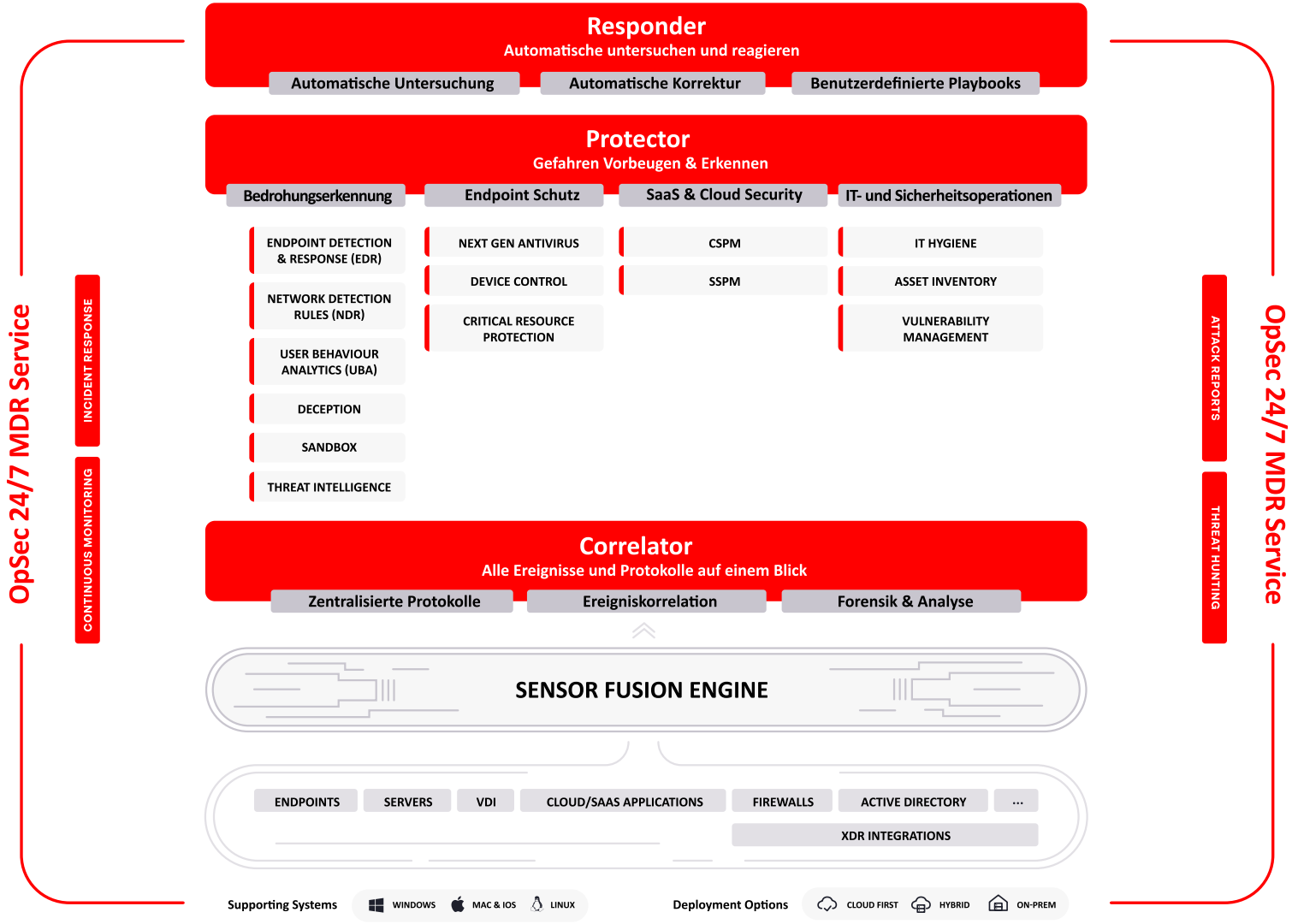

BLACKSOC
HUNT + DESTROY | FULLY MANAGED
Cyber-Bedrohungen gezielt zerstören
Das einfache Hunt & Destroy Komplettpaket für Ihre Sicherheit.
Alles zum SOC as a Service von
protectONE™
....protect your Business

BlackSOC Security Plattform



BLACKSOC HUNT + DESTROY | FULLY MANAGED by protectONE™ ....protect your Business

BlackSOC Security Plattform



BLACKSOC
HUNT + DESTROY | FULLY MANAGED

by

protectONE™
....protect your Business

Keine Verstöße mehr. Keine Überstunden mehr.

Protector™

Vorbeugen & Erkennen

Verhinderung und Erkennung von Bedrohungen durch die kombinierten Fähigkeiten von NGAV, EDR, NDR, UBA, Deception und mehr.

ENDPUNKTSCHUTZ: Endpunkt-Bedrohungen, einschließlich NGAV, Gerätekontrolle, Schutz kritischer Ressourcen und mehr.

ERWEITERTE ERKENNUNG VON BEDROHUNGEN: Die erweiterte Transparenz über Endgeräte, Netzwerke und Benutzer bietet mehrschichtige Schutzfunktionen wie EDR, Deception, Regeln zur Analyse des Benutzerverhaltens, Netzwerkerkennungsregeln, Sandboxing und Bedrohungsdaten.

CSPM & SSPM: Überwachen und korrigieren Sie Konfigurationsfehler bei SaaS- und Cloud-Anwendungen, um Sicherheitsrisiken zu vermeiden.

IT- UND SICHERHEITSOPERATIONEN: Umfangreiche betriebliche Funktionen wie IT-Hygiene, Schwachstellenmanagement und Asset Inventory Fähigkeiten sind von Haus aus enthalten.

Responder™

Automatische untersuchen und reagieren

Automatisiert alle erforderlichen Untersuchungs- und Reaktionsmaßnahmen in der gesamten Umgebung.

AUTOMATISIERTE UNTERSUCHUNG: BLACKSOC leitet automatisch eine Untersuchung ein, sobald eine hochriskante Bedrohung erkannt wird, um sofort die Ursache und das gesamte Ausmaß des Angriffs aufzudecken.

AUTOMATISCHE KORREKTUR: BLACKSOC bietet die größte Auswahl an automatisierten Abhilfemaßnahmen, um erkannte Bedrohungen an Endpunkten, in Netzwerken, bei Anwendern und SaaS Anwendungen sofort einzudämmen und zu beseitigen.

SANIERUNGSHANDBÜCHER: Nutzen Sie vorgefertigte oder benutzerdefinierte Playbooks, die mehrere Abhilfemaßnahmen kombinieren, um alle Spuren der identifizierten Bedrohungen zu beseitigen.

Correlator™

Alle Ereignisse und Protokolle auf einem Blick

Sammelt und korreliert Alarm- und Aktivitätsdaten zu verwertbaren Vorfällen und bietet so wesentliche SIEM-Funktionen.

ZENTRALISIERTE PROTOKOLLVERWALTUNG: Sammelt und integriert wichtige Protokolldaten, die für die Bedrohungsanalyse benötigt werden, und verwendet dazu eine leistungsstarke Abfragesprache sowie intuitive Grafiken und Dashboards.

EREIGNIS-KORRELATION: Analysiert Signale von nativen BLACKSOC-Kontrollen, Systemprotokollen und anderen Quellen, um Daten zu verwertbaren Vorfällen zu korrelieren.

FORENSICS: Untersuchen Sie Bedrohungen und führen Sie eine Bedrohungsjagd durch mit sofortigem Zugriff auf forensische Artefakte, die von BLACKSOC-Agenten, Protokollen und anderen Systemressourcen gesammelt wurden, unter Verwendung leistungsstarker Such- und Visualisierungstools.

BLACKSOC
HUNT + DESTROY | FULLY MANAGED

by

protectONE™
....protect your Business

360° OpSec XDR: Umfassende Cybersicherheit war noch nie so einfach

CyOps™ 24/7 MDR

Kontinuierliche Überwachung und Reaktion

Ein erstklassiges, verwaltetes Erkennungs- und Reaktions-Teams sorgt dafür, dass Sie sicher und geschützt sind.

24/7-ÜBERWACHUNG: Stellt sicher, dass gefährliche Bedrohungen rund um die Uhr erkannt und angemessen behandelt werden - ideal für Teams mit begrenzten Ressourcen.

REAKTION AUF VORFÄLLE: Unterstützung bei Remote Incident Response mit Untersuchung, umfassendem Abhilfeplan und Anleitung.

THREAT HUNTING: Jagen Sie proaktiv nach versteckten Bedrohungen in der gesamten Umgebung.

ANGRIFFSBERICHTE: Schriftlicher Überblick und detaillierte technische Einblicke in Angriffstechniken.

Das derzeitige Sicherheitskonzept ist fehlerhaft.

Unternehmen sind derzeit gezwungen, ein teures, komplexes, aus mehreren Produkten bestehendes Sicherheitspaket mit mühsamen manuellen Prozessen zu verwenden, was dazu führt, dass die IT-Sicherheitsteams überfordert und erschöpft sind. Schlimmer noch: Dieser unzusammenhängende, ressourcenintensive Ansatz lässt sie immer noch blind und anfällig für heimliche Angriffe werden.

Bringen Sie wieder Vernunft in die Cybersicherheit mit einem neuen Ansatz, der den Schutz Ihres Unternehmens einfach und stressfrei macht.

Cybersecurity leicht gemacht.

Die durchgängige, nativ automatisierte XDR-Plattform von BLACKSOC wurde wurde speziell für schlanke IT-Sicherheitsteams entwickelt. BLACKSOC ist sofort einsatzbereit, radikal einfach zu bedienen, wird durch einen kostenlosen 24/7-MDR-Service unterstützt und zu den effektivsten Gesamtbetriebskosten angeboten und ermöglicht jedem Unternehmen einen umfassenden und effizienten Schutz, unabhängig von seinen Ressourcen, der Größe seines Teams oder seinen Fähigkeiten.

Mit vollständiger Transparenz von Endpunkten, Benutzern, Netzwerken, SaaS- und Cloud-Anwendungen sowie umfangreichen automatisierten Reaktionsmöglichkeiten ist es die Vision von BLACKSOC, Sicherheitsteams in die Lage zu versetzen, ihre Cybersicherheit auf Autopilot zu stellen und ihre begrenzten Ressourcen auf die Verwaltung der Sicherheit zu konzentrieren, anstatt sie zu betreiben.

Wichtigste Vorteile

End-to-End-Schutz erhalten
mit einer nativen, einheitlichen Plattform für Erkennung, Prävention, Korrelation, Untersuchung und Reaktion über Endgeräte, Benutzer, Netzwerke, SaaS- und Cloud-Anwendungen hinweg.

Nutzen Sie native Reaktionsautomatisierung
die die manuelle Arbeit auf ein Minimum reduziert, so dass Sie mehr Zeit für das Sicherheitsmanagement, als für die Bedienung der Systeme haben.

Erzielen Sie vollständige Transparenz
für tiefen und akkuraten Schutz vor Bedrohungen, über Ihre gesamte Umgebung hinweg.

Maximieren Sie Ihren ROI
mit den effektivsten TCO und durch die Reduzierung des Ressourcenbedarfs.

Erhalten Sie inneren Frieden durch 24/7 Schutz
während das proaktive MDR-Team von Cynet Ihre Umgebung kontinuierlich überwacht und fachkundige Unterstützung und Anleitung bietet.

BLACKSOC
HUNT + DESTROY | FULLY MANAGED

by

protectONE™
....protect your Business

All in ONE-Pakete flexibel zum Buchen

Essential

- ✓ 5/9 Threat Hunting
- ✓ 5/9 MDR Support
- ✓ Produktübergreifende Datenquellen (z. B. Firewall, E-Mail)
- ✓ Beseitigen von Bedrohungen und ihren Folgen

Complete

- ✓ **7/9 Threat Hunting**
- ✓ **7/9 MDR Support**
- ✓ Produktübergreifende
- ✓ Datenquellen (z. B. Firewall, E-Mail)
- ✓ Beseitigen von Bedrohungen und ihren Folgen
- ✓ **Deep learning malware analysis**

Elite

- ✓ **7/24 Threat Hunting**
- ✓ **7/24 MDR Support**
- ✓ Produktübergreifende
- ✓ Datenquellen (z. B. Firewall, E-Mail)
- ✓ Beseitigen von Bedrohungen und ihren Folgen
- ✓ Deep learning malware analysis
- ✓ **Bedrohungsfälle (Ursachenanalyse)**
- ✓ **Live-Fernreaktion auf Vorfälle**
- ✓ **Angriffsberichte & Forensik**
- ✓ **Honeypots<**

Alle Funktionen und Leistungen

BLACKSOC HUNT + DESTROY | FULLY MANAGED by protectONE™ ....protect your Business

Überblick über das Angebot

protectONE Managed Endpoint Detection and Response (EDR) wurde entwickelt, um die Endpunkte der Kunden zu schützen. Sie kombiniert die Leistung der besten EDR-Lösungen mit einem 24x7- oder 8x5-Eliteteam von Sicherheitsexperten. Sie sind bereit die raffiniertesten und fortschrittlichsten Cyberangriffe zu identifizieren, zu untersuchen und darauf zu reagieren.

Die Managed EDR-Services schützen die Endpunkte des Kunden durch die Erkennung von Malware, einschließlich Ransomware-Varianten, Zero-Days, Nicht-Malware und dateilosen Angriffen. Sie nutzen die neueste Sicherheitstechnologie in Übereinstimmung mit den Best Practices der Branche und den Geschäftsanforderungen des Kunden.

Fähigkeiten

- Entwurf von Richtlinien, kontinuierliche Überprüfung und Anpassung an bewährte Verfahren und Kundenanforderungen
- Standard-Framework für das Onboarding und die Verwaltung von Endpunkt-Agenten und der EDR-Konsole
- Verwaltung des Zustands und Status von Konsole und Agenten
- 24x7 oder 8x5 Vorfall-, Warn-, Untersuchungs- und Reaktionsdienste
- Bereitstellung von Technologiemanagement und administrativem Support

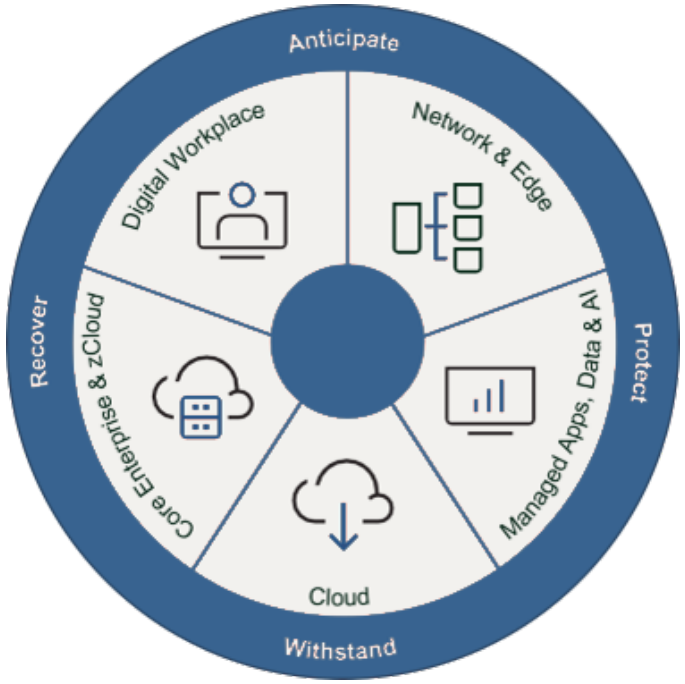
Solution Elements

- Deployment Services werden vom spezialisierten Expertenteam von protectONE erbracht
- Der Dauerbetrieb wird vom protectONE in Deutschland durchgeführt
- Die Implementierung wird von einem deutschen Projektmanager vor Ort koordiniert

Rahmen für Cyber-Resilienz

cyber resilience

Die Fähigkeit, ungünstige Bedingungen, Belastungen, Angriffe und Kompromittierungen im Zusammenhang mit cybergestützten Geschäftsabläufen zu antizipieren, sich dagegen zu schützen, ihnen standzuhalten und sich davon zu erholen.



Security Assurance Services

Bewerten und Benchmarken des Reifegrads der Ausfallsicherheit. Einblick in wichtige Bedrohungen und Schwachstellen, Verwaltung der Compliance

- Sicherheit, Strategie und Risiko-management
- Offensive Sicherheitstests
- Verwaltung der Einhaltung von Vorschriften

Zero Trust Services

Schützen Sie wichtige Geschäftsdaten und Anwendungen in einer sicheren Infrastruktur

- Identitäts- und Zugriffsmanagement
- Endpunktsicherheit
- Netzwerksicherheit
- Anwendungs- und Workload-Sicherheit
- Datenschutz und Privatsphäre
- Analyse, Automatisierung und Orchestrierung

Security Operations & Response Services

Erkennen und Reagieren auf einen erkannten Sicherheitsvorfall

- Erweiterte Erkennung von Bedrohungen
- Reaktion auf Vorfälle und Forensik

Incident Recovery Services

Mildern Sie die Auswirkungen von Unterbrechungen mit Funktionen zur automatischen Wieder-herstellung kritischer Geschäftsprozesse und Daten

- Cyber Incident Recovery
- Managed Backup Services
- Hybrid Platform Recovery
- Data Center Design & Facilities

Antizipieren → Schützen → Widerstehen → Erholen

Cybersecurity + Erholen

Fundiertes Fachwissen | Bewährte Prozesse | Intelligente Automatisierung

BLACKSOC HUNT + DESTROY | FULLY MANAGED by protectONE™ ....protect your Business

Umsetzung und Lieferkonzept

Phase	Planen	Implementieren	Übergang	Endzustand
Hochrangige Aktivitäten	• Kick-off-Meeting durchführen • Validierung des Umfangs • Projektzeitplan und Kommunikationsplan • Einigung über die Projektleitungn	• Ermitteln der aktuellen Sicherheitstopologie für die Endgeräteerkennung • Verstehen der in Frage kommenden Systeme • Überprüfung des Designs und der Architektur der vorgeschlagenen Lösung • Beginn der Einführung von Agenten / Bereitstellung von EDR auf den betroffenen Servern • Durchführung der Due Diligence nach dem Rollout	• Übergang zum SOC-Team von protectONE • Übergabe der operativen Verantwortung • Folge-/Zusatzdienste & Sanierung • Kunden-/ protectONE-Akzeptanz	• Durchführen von stationärem Betrieb • Bereitstellung, Überwachung, Alarmierung und Berichterstattung • Überwachung von Konsole und Systemzustand
Erreichbare Ergebnisse oder Meilensteine	– Detaillierter Projekt- und Durchführungsplan	– EDR-Tool auf allen Servern installieren	– Übergang zum BAU-Team abgeschlossen	– Endzustand SOC Operations

BLACKSOC HUNT + DESTROY | FULLY MANAGED by protectONE™ ....protect your Business

Funktionsmodell Endzustand

Sie als Kunde

- Änderungswünsche senden
- Hinweis auf zusätzliche Geräte, die geschützt werden müssen
- Validieren der monatlichen Berichte

Ihr protectONE Account Team

Benjamin Valentini (pONE)

- Beziehung zu Eskalationsstelle für das Account-Team
- Teilnahme an Kontrollen
- Verwaltung von Vertragsänderungen

Endpoint Detection and Response Team

Analyst Level 1 (Triage)

- Überwachenvon Endpunkten Ereignisse und -warnungen.
- Ermittlung von Vorfällen auf der ersten Ebene und Erstellung von Tickets.
- Bearbeiten von Konfigurationsänderungen am EDR-Tool.
- Verwalten des EDR-Tools und Installieren von Agenten.

Analyst Level 2 (Incident Responder)

- Endpunkt-Reaktion
- Erstellung von Berichten zur Ursachenanalyse (RCA).
- Durchführung von Richtlinienüberprüfungen und ordnungsgemäße Abstimmung des EDR-Tools.
- Bereitstellung von monatlichen EDR-Berichten.

Analyst Level 3

- Proaktives Durchsuchen von Sicherheitsdaten, um Bedrohungen zu erkennen und darauf zu reagieren.
- Bereitstellung von EDR-Support der dritten Ebene.

Umfang der Infrastruktur

- AIX
- Appliance
- HMC
- Linux on SO Boxes
- ONTAP on NetApp File Server / Appliance
- PhotoOS on a vCenter Server
- RED Hat Enterprise /AS
- VioServer
- VMWare ESXi
- Windows Svr 2008
- Windows Svr 2012
- Windows Svr 2016
- Windows Svr 2019
- Windows Clients

BLACKSOC HUNT + DESTROY | FULLY MANAGED by protectONE™ ....protect your Business

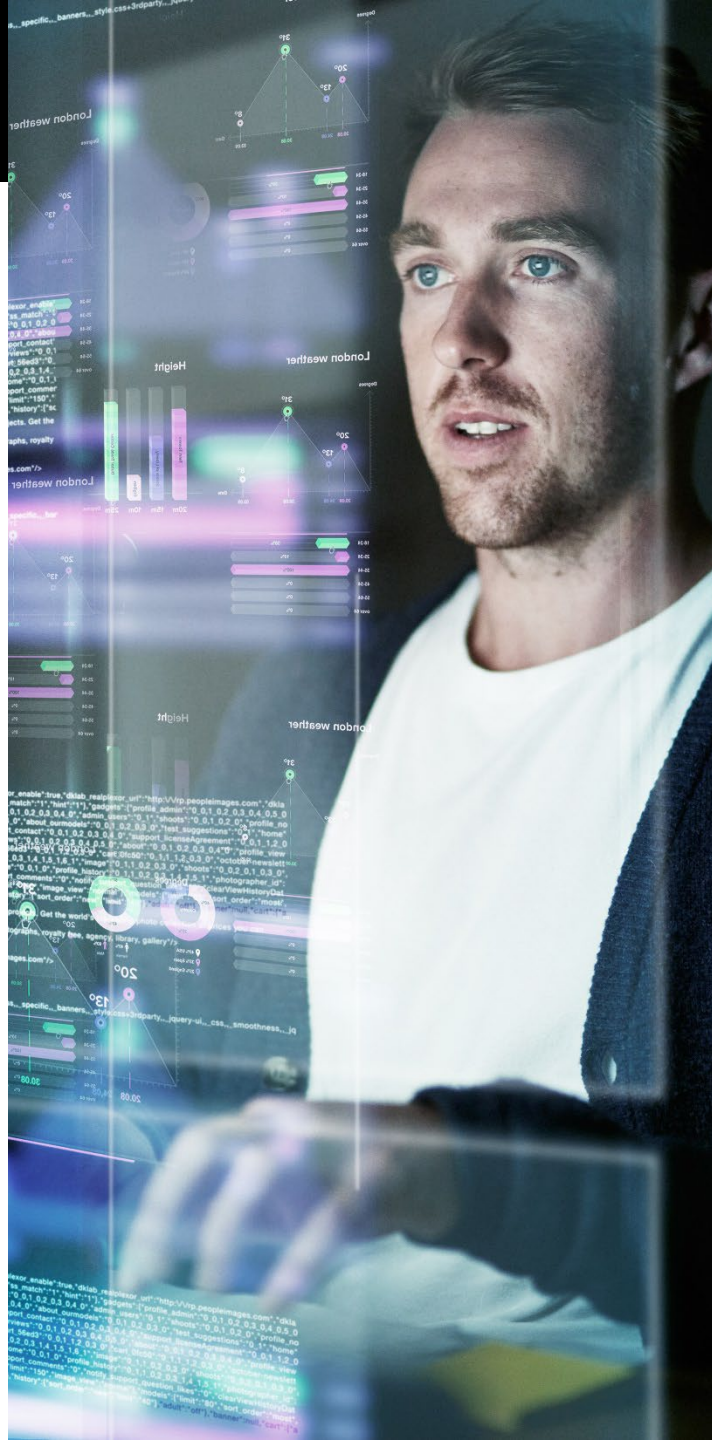
Servicezeiten und SLAs

Servicezeiten

Managed Service	Servicezeiten
Endpoint Detection & Response (EDR)	24/7

SLAs für die Reaktion auf Vorfälle und deren Lösung :

Managed Service	Priorität	Definition	MITRE ATT&CK Tactics	Reaction Time Target to Respond
Endpoint Detection & Response (EDR)	1 (Krtisch)	Vorfälle, die für den Kunden eine erhebliche Störung verursachen und die Sicherheit des gesamten Unternehmens beeinträchtigen.	Erstzugriff, Ausführung, Persistenz, Eskalation von Privilegien, Umgehung von Verteidigungsmaßnahmen, Zugriff auf Zugangsdaten, Entdeckung, seitliche Bewegung, Sammlung, Befehl und Kontrolle, Exfiltration, Auswirkungen	30 Minuten
	2 (Hoch)	Vorfälle mit erheblichen Auswirkungen für den Kunden, die mehrere Systeme oder kritische Infrastrukturen betreffen.	Erstzugriff, Ausführung, Persistenz, Eskalation von Privilegien, Umgehung von Verteidigungsmaßnahmen, Zugriff auf Zugangsdaten, Entdeckung, seitliche Bewegung, Sammlung, Befehl und Kontrolle	1 Stunde
	3 (Mittel)	Vorfälle mit mäßigem Schaden für den Kunden, die eine begrenzte Anzahl von Systemen oder Diensten betreffen.	Erstzugang, Ausführung, Persistenz, Umgehung der Verteidigung, Entdeckung, Befehl und Kontrolle	4 Stunden
	4 (Niedrig)	Vorfälle mit minimalen Auswirkungen für den Kunden, die Umgehungs-möglichkeiten bieten oder nur eine begrenzte Störung verursachen.	Erstzugang, Erkennung, Befehl und Kontrolle	1 Geschäftstag



BLACKSOC HUNT + DESTROY | FULLY MANAGED by protectONE™ ....protect your Business

Nächste Schritte

Benjamin Valentini:
bv@protectone.net

Website:
www.protectone.net

Telefon:
+49 1716 92 75 65

ProtectONE:
info@protectone.net
+49 2902 6530 856

Sie möchten jetzt die Sicherheit Ihres Unternehmens auf die nächste Stufe heben? Nehmen Sie einfach Kontakt auf und wir kümmern uns um alles.

Oder haben Sie noch Fragen?

Wenn Sie nach Fragen haben, können wir diese schnell und unkompliziert klären. Nehmen Sie einfach per Mail oder Telefon Kontakt auf und wir stehen Ihnen Rede und Antwort.

KONTAKTIEREN SIE UNS

BLACKSOC
HUNT + DESTROY | FULLY MANAGED

by

protectONE™
....protect your Business