**Nicht für Endkunden**

# Security-Lösungen von plusserver


## 1. Endpoint Detection & Response (EDR)

| | |
|---|---|
| Was | Erkennung von Anomalien & Abwehr von Angriffen auf den durch den EDR-Agenten geschützten Systemen |
| Wo | MacOS Linux, Windows, Server & Clients, alle Cloud-Provider & on premises |
| Wofür | • Kernfunktionen: Schutz vor Viren, Malware, Ransomware, Exploits<br>• Ergänzende Funktionen: Phishing, Web-Schutz, Mail-Client-Schutz, Bruteforce-Absicherung, Network Intrusion Detection |
| Wie | • EDR-Agent (= Software) wird auf den zu schützenden Systemen installiert<br>• Anbindung der EDR-Lösung an das plusserver Security Operations Center zur 24x7 Überwachung und Bewertung der durch die EDR-Lösung erkannten Anomalien |
| Warum ps | • EDR + SOC als günstiger Einstieg in 24/7-SOC-Überwachung für optimale Detektion und Reaktion<br>• Verarbeitung der Daten im plusserver-Rechenzentrum (DSGVO-Konformität und Datensouveränität)<br>• Betrieb und Wartung durch plusserver im Full Managed Service<br>• Unkomplizierte Erweiterung der Überwachung bis hin zu einem Full-SOC-Betrieb jederzeit möglich<br>• 24x7 Support und Service in deutscher Sprache |

**Nicht für Endkunden**

## 2. Security Scanner

| | |
|---|---|
| Was | Prüfung der über das Netzwerk erreichbaren Systeme und Dienste auf Schwachstellen (Beispiele: Betriebssysteme, Applikationen, Netzwerkgeräte, Peripherie) |
| Wo | Alle extern und intern erreichbaren IP-Adressen in der plusserver-Infrastruktur, bei Drittanbietern (auch Hyperscaler) sowie on premises und mobile Endgeräte |
| Wofür | • Aufdecken von Schwachstellen in Software und Fehlkonfigurationen<br>• Identifizieren von Schatten-IT |
| Wie | • Provisionierung des Accounts<br>• Angabe der IP-Adressen im Webinterface<br>• Start des Scans<br>• Ausgabe der Ergebnisse und Reports |
| Warum ps | • Bereitstellung des Accounts durch plusserver für den Kunden<br>• 24x7 Support durch plusserver<br>• Plattform aus Deutschland<br>• Optional: Full Managed Service durch den Partner oder plusserver |

**Nicht für Endkunden**

## 3. Security Operations Center

| | |
|---|---|
| Was | • Überwachung aller sicherheitsrelevanten Ereignisse aus der gesamten IT-Infrastruktur<br>• 24x7 Bewertung und Analyse von Sicherheitsvorfällen<br>• Begleitung des Incident- und Schwachstellenprozesses des Kunden |
| Wo | Komplette Infrastruktur des Kunden |
| Wofür | • Zusammenführung von sicherheitsrelevanten Informationen<br>• Rückschlüsse auf mögliche Angriffe auf die IT-Infrastruktur<br>• Bewertung der Angriffe und Ableitung von Handlungsempfehlungen durch SOC-Analysten<br>• Alarmierung und Begleitung bei etwaigen Notfallmaßnahmen |
| Wie | • Kickoff zur Definition des Scopes (Sizing und ggfls. Vorprojekt)<br>• Anbindung der Kundeninfrastruktur<br>• Regelwerksdesign und organisatorische Abstimmungen<br>• Tuningphase und Überführung in den Livebetrieb<br>• Regelmäßiger Jour fixe mit dem plusserver SOC-Team |
| Warum ps | • Datenschutz: Betrieb der SIEM-Plattform und Datenhaltung ausschließlich in den deutschen plusserver-Rechenzentren (ISO 27001, BSI C5)<br>• Datensouveränität: Analyse und Speicherung der Protokolle und Netzwerk-Metadaten im eigenen Unternehmen möglich<br>• Reibungslose Kommunikation: Sitz der SOC-Analysten ausnahmslos in Deutschland; 24/7 Support in deutscher und englischer Sprache<br>• Kein Vendor Lock-in: Vollständige Herausgabe der Daten nach Beendigung des Services<br>• Technologieoffenheit: Einbindung Ihrer vorhandenen Infrastruktur<br>• Flexibilität: Hochgradige Individualisierung möglich bis hin zur Integration kundeneigener Produkte oder Entwicklungen<br>• Rundum-Service: Unser Partner-Ökosystem kann Sie in allen Bereichen unterstützen (einschließlich der von Ihnen verwendeten Lösungen & Produkte) |

**Nicht für Endkunden**

## 4. Security Operations Center – Third-Party EDR-Modul

| | |
|---|---|
| Was | • Überwachung aller sicherheitsrelevanten Ereignisse der durch die EDR-Lösung des Kunden abgesicherten Clients & Server (= Endpoints)<br>• 24x7 Bewertung und Analyse von Sicherheitsvorfällen<br>• Begleitung des Incident- und Schwachstellenprozesses des Kunden |
| Wo | Anbindung der durch den Kunden bereitgestellten und gemanagten EDR-Lösung |
| Wofür | • Zusammenführung von sicherheitsrelevanten Informationen<br>• Rückschlüsse auf mögliche Angriffe auf die IT-Infrastruktur<br>• Bewertung der Angriffe und Ableitung von Handlungsempfehlungen durch SOC-Analysten<br>• Alarmierung und Begleitung bei etwaigen Notfallmaßnahmen |
| Wie | • Kickoff zur Definition des Scopes (Sizing und ggfls. Vorprojekt)<br>• Anbindung der EDR-Lösung des Kunden<br>• Regelwerksdesign und organisatorische Abstimmungen<br>• Tuningphase und Überführung in den Livebetrieb<br>• Regelmäßiger Jour fixe mit dem plusserver SOC-Team |
| Warum ps | • Datenschutz: Betrieb der SIEM-Plattform und Datenhaltung ausschließlich in den deutschen plusserver-Rechenzentren (ISO 27001, BSI C5)<br>• Datensouveränität: Analyse und Speicherung der Protokolle und Netzwerk-Metadaten im eigenen Unternehmen möglich<br>• Reibungslose Kommunikation: Sitz der SOC-Analysten ausnahmslos in Deutschland; 24/7 Support in deutscher und englischer Sprache<br>• Kein Vendor Lock-in: Vollständige Herausgabe der Daten nach Beendigung des Services<br>• Modularer Ansatz: Einfacher und niederschwelliger Einstieg durch einzelne Third-Party-SOC-Module (EDR/Network)<br>• Technologieoffenheit: Einbindung Ihrer vorhandenen Infrastruktur<br>• Flexibilität: Hochgradige Individualisierung möglich bis hin zur Integration kundeneigener Produkte oder Entwicklungen<br>• Rundum-Service: Unser Partner-Ökosystem kann Sie in allen Bereichen unterstützen (einschließlich der von Ihnen verwendeten Lösungen & Produkte) |

**Nicht für Endkunden**

## 5. Security Operations Center – Third-Party Network-Modul

| | |
|---|---|
| Was | • Überwachung aller sicherheitsrelevanten Ereignisse aus der Firewall-Infrastruktur des Kunden<br>• 24x7 Bewertung und Analyse von Sicherheitsvorfällen<br>• Begleitung des Incident- und Schwachstellenprozesses des Kunden |
| Wo | Anbindung der durch den Kunden bereitgestellten und gemanagten Firewall-Infrastruktur |
| Wofür | • Zusammenführung von sicherheitsrelevanten Informationen<br>• Rückschlüsse auf mögliche Angriffe auf die IT-Infrastruktur<br>• Bewertung der Angriffe und Ableitung von Handlungsempfehlungen durch SOC-Analysten<br>• Alarmierung und Begleitung bei etwaigen Notfallmaßnahmen |
| Wie | • Kickoff zur Definition des Scopes (Sizing und ggfls. Vorprojekt)<br>• Anbindung der Firewall-Infrastruktur des Kunden<br>• Regelwerksdesign und organisatorische Abstimmungen<br>• Tuningphase und Überführung in den Livebetrieb<br>• Regelmäßiger Jour fixe mit dem plusserver SOC-Team |
| Warum ps | • Datenschutz: Betrieb der SIEM-Plattform und Datenhaltung ausschließlich in den deutschen plusserver-Rechenzentren (ISO 27001, BSI C5)<br>• Datensouveränität: Analyse und Speicherung der Protokolle und Netzwerk-Metadaten im eigenen Unternehmen möglich<br>• Reibungslose Kommunikation: Sitz der SOC-Analysten ausnahmslos in Deutschland; 24/7 Support in deutscher und englischer Sprache<br>• Kein Vendor Lock-in: Vollständige Herausgabe der Daten nach Beendigung des Services<br>• Modularer Ansatz: Einfacher und niederschwelliger Einstieg durch einzelne Third-Party-SOC-Module (EDR/Network)<br>• Technologieoffenheit: Einbindung Ihrer vorhandenen Infrastruktur<br>• Flexibilität: Hochgradige Individualisierung möglich bis hin zur Integration kundeneigener Produkte oder Entwicklungen<br>• Rundum-Service: Unser Partner-Ökosystem kann Sie in allen Bereichen unterstützen (einschließlich der von Ihnen verwendeten Lösungen & Produkte) |

**Nicht für Endkunden**

## 6. Workload Protection

| | |
|---|---|
| Was | • Multi-Cloud-fähige und Cloud-native Lösung zur ganzheitlichen Absicherung von Kundenumgebungen<br>• Laufzeitschutz für Prozesse und Anwendungen in Containern<br>• Web-Application- und API-Firewall zur Verhinderung von Angriffen<br>• Schwachstellenprüfung von Containern und Images<br>• Werkzeuge zur Implementierung von IT-Sicherheit in die Software-Entwicklung |
| Wo | • Hyperscaler (z. B. AWS, Google Cloud, Azure, Alibaba und Oracle)<br>• Kubernetes (z. B. plusserver Kubernetes Engine) |
| Wofür | • Ganzheitliche Sicht auf Multi-Cloud-Infrastrukturen inkl. automatisierter Inventarisierung<br>• Erkennen und Blockieren von Angriffen auf Container, Web-Applikationen und Cloud-Umgebungen<br>• Risikomanagement zur Priorisierung von Bedrohungen und vorgefertigte Benchmarks nach Industrie-Standards (CIS, NIST, PCI-DSS etc.) |
| Wie | • Bereitstellung des Zugangs für den Kunden<br>• Eintägige Einweisung und Schulung des Kunden |
| Warum ps | Alles aus einer Hand:<br>• Ergänzung zur Managed-Kubernetes-Plattform von plusserver<br>• Optionale Integration in das plusserver Security Operations Center<br>• Unterstützung bei der Cloud-Transformation durch Consulting |