



# Cyber Defense Service

**ISPIN AG ZURICH**  
swiss made security.

Moderne Cyber-Angriffe sind lautlos, komplex und oft massgeschneidert. Die wachsende Bedrohungslage, der Mangel an qualifiziertem Fachpersonal und die steigende Komplexität erschwert es Unternehmen, sich erfolgreich gegen Cyber-Angriffe zu schützen.

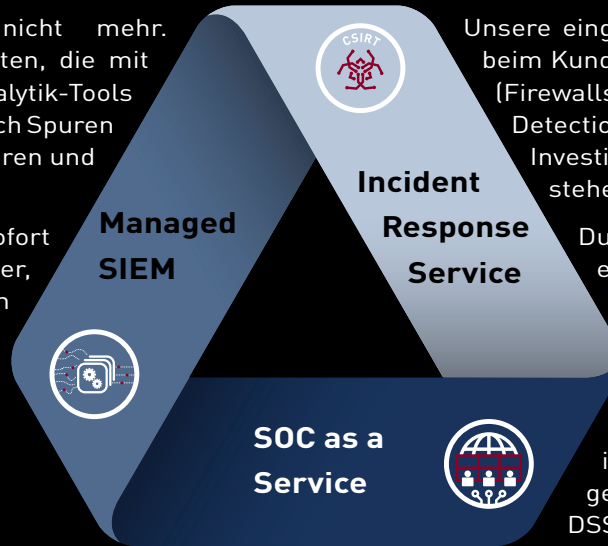
Prävention alleine reicht nicht mehr. Unternehmen brauchen Experten, die mit Einsatz von modernsten Analytik-Tools methodisch und strukturiert nach Spuren suchen, Verdachtsmomente klären und bei Gefahren aktiv handeln.

Unseren Kunden steht ab sofort ein in der Schweiz ansässiger, erstklassiger Next Generation Managed Cyber Defense

Service zur Verfügung. Es werden alle Qualitäten vereint, um Ihnen eine umfassende Erkennung, Analyse und Response zu Cyberangriffen anzubieten. Die Lösung ist für gezielte und moderne Angriffsszenarien konzipiert.

Unsere eingesetzte Fabric integriert bereits beim Kunden eingesetzte Securitylösungen (Firewalls, IDS/IPS, SIEM, Threat Detection uvm.). Dadurch wird der Investitionsschutz der bereits im Einsatz stehenden Technologien garantiert.

Durch eine konsequent entwickelte Architektur wird sichergestellt, dass Ihre sensiblen Daten niemals Ihr Unternehmen verlassen. Somit wird die Konformität zu vielen schweizerischen und internationalen Regulationen gewährleistet (z.B. FINMA, PCI-DSS, GDPR).



## Threats. Mastered.



### SOC as a Service

- Operativer Betrieb des SOC am Standort Bassersdorf
- Modernste, in Europa entwickelte Technologie
- Internationales Expertenteam
- Klare Service Level Agreements und dokumentierte Prozesse
- Festgelegte Servicezeiten
- Incident Response und Echtzeit-Alarmierung



Managed Incident Response



IT Risk Detection



### Managed SIEM

- Herstellerunabhängige Sammlung, Analyse, Aggregation und Korrelation
- Kontinuierlich weiterentwickelte und massgeschneiderte Regelsätze
- Playbooks mit etablierten Prozessen und branchenspezifischen Use Cases
- Risikobasiertes Alarmierung



Advanced Cyber Threat Detection



Vulnerability Management



Intrusion Detection



Managed Detection



### Incident Response Service

- Unkomplizierte Notfallunterstützung durch ausgewiesene Securityexperten
- Vor-Ort Koordination bei Security Incidents
- Durchführung von forensischen Untersuchungen
- Technische Beratung zu Securityfragen
- Proaktives Threat Hunting und Research
- Kontinuierlicher Wissenstransfer



CSIRT



Forensik

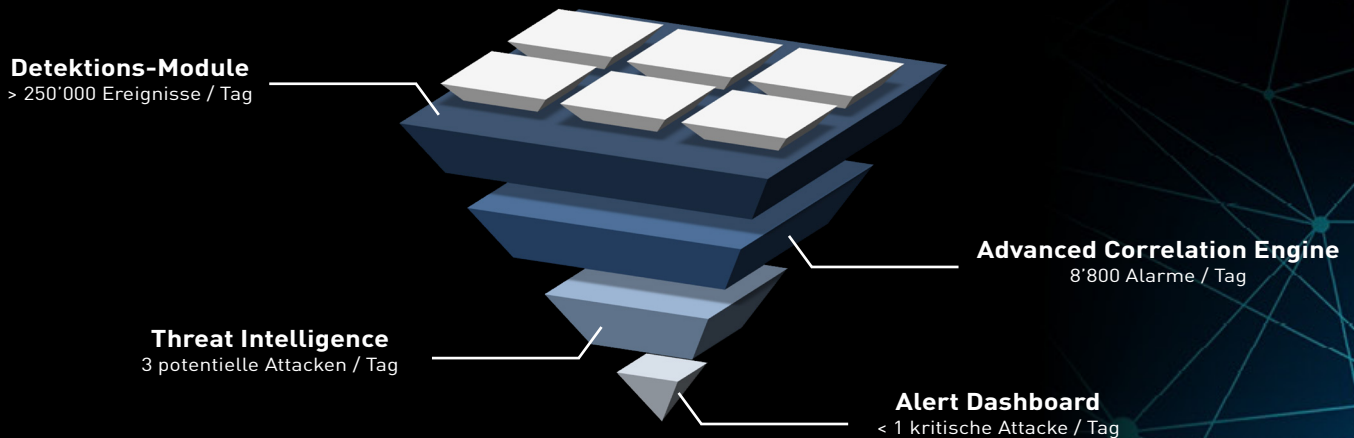


**Ihre Daten verlassen  
niemals Ihr Unternehmen.**

**Aus der Schweiz.**



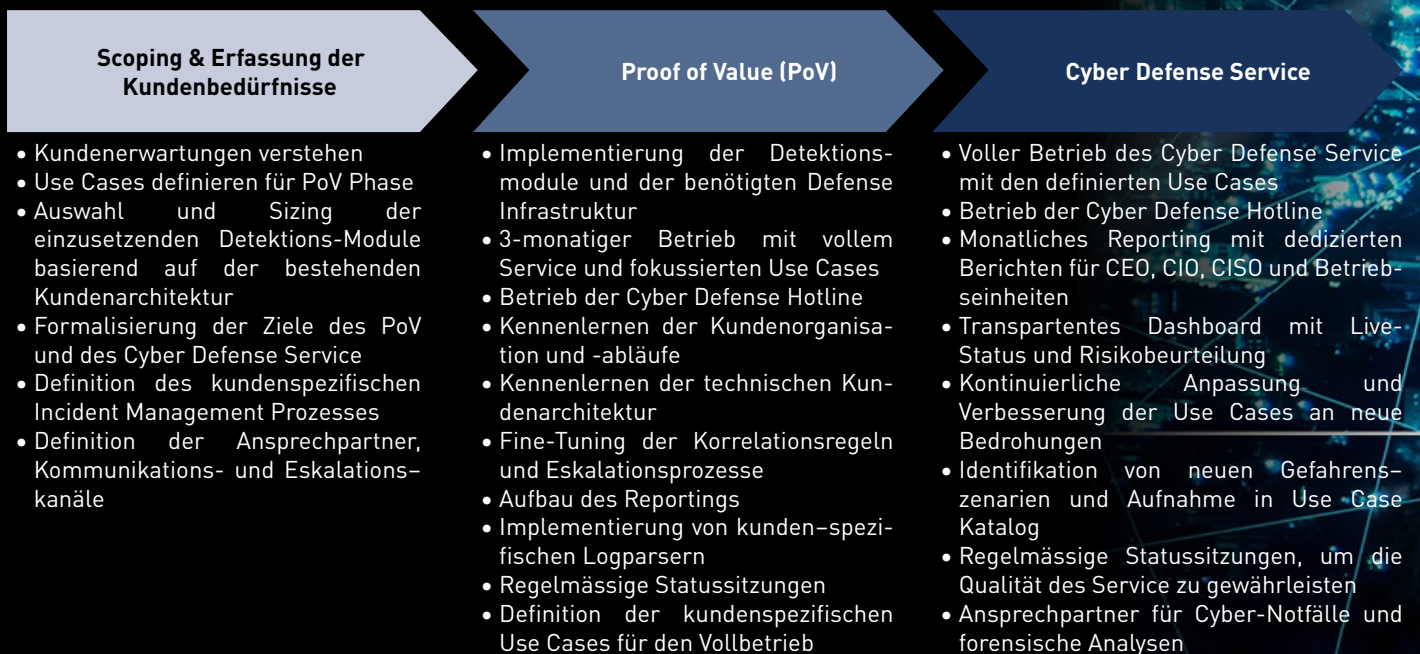
## Die Arbeit eines Cyber Defense Centers



Der Einsatz von hochentwickelter Analysetechnologie ermöglicht eine umfassende Überwachung Ihrer digitalen Infrastruktur. Die daraus gewonnene Einsicht maximiert die Korrelierbarkeit der gesammelten Daten, und unser Team kann daraus weiterführende Ereignisketten erstellen. Durch Automation stellen wir sicher, dass nur dann ein Mensch intervenieren muss, wenn eine kritische bzw. massgebliche Entscheidung getroffen werden muss. Unsere eingesetzte Fabric integriert bereits im Einsatz stehende Securitylösungen. Dadurch können Sie die Cyber Defense Services der ISPIN AG sofort nutzen, ohne Ihre bestehende Infrastruktur umzubauen. Wenn eine Bedrohung erkannt wird, erfolgt eine sofortige Alarmierung an Ihrer Fachleute. Unsere Cyber Threat-Experten unterstützen Sie dann im Bedarfsfall mit Knowhow und Prozeduren zur Beseitigung der Bedrohung.

Der Cyber Defense Service kann entweder als selbständiger Service in Ihre bestehende ITIL-Organisation integriert oder als komplette Lösung, zusammen mit ISPIN Cyber Care und ISPIN Cyber Guard, bezogen werden. Wir nennen dieses Konzept «Fusion».

## Der Weg zum Cyber Defense Service



### Kontaktieren Sie uns.

Gerne stellen wir unseren Cyber Defense Service näher vor. Kontaktieren Sie uns für mehr Informationen.



Pascal Imthurn, Head Cyber Defense Center  
+41 44 838 31 11  
pascal.imthurn@ispin.ch oder cyberdefense@ispin.ch

**Threats.  
Mastered.**