Threats. Mastered. – Neues hochmodernes Cyber Defense Center

Alle Unternehmen sehen sich komplexen Herausforderungen im Bereich Cyber Security gegenüber:

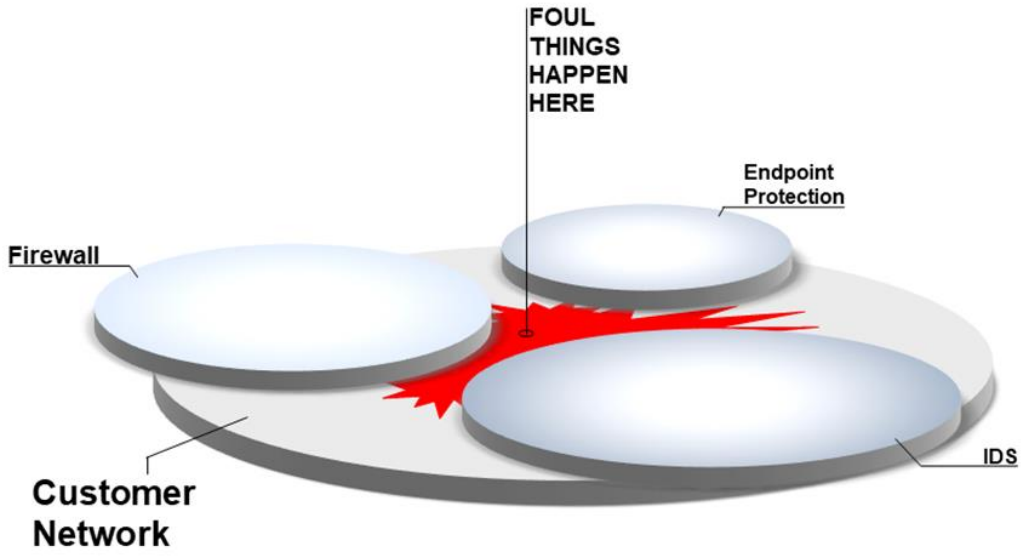
- **Wie können moderne, gezielte Angriffsszenarien erkannt werden?**
- **Wie wird eine Korrelation über Ereignisse oder Ereignisketten hergestellt?**
- **Wie kann das Risikopotential bewertet werden?**
- **Wie erhält man anwendbare Anleitungen für die Behandlung von Risiken?**
- **Wie kann überprüft werden, ob Verbesserungen erfolgreich waren?**
- **Wie wird ein effizienter Informationsfluss zu allen Beteiligten gestaltet?**
- **Wie wird Risikotransparenz, von IT- zu Geschäftsrisiko, gewährleistet?**
- **Wie können Kosten in der IT-Sicherheit gespart werden?**

Der digitale Wandel und Progress sorgt als treibende Kraft dafür, dass immer mehr und immer kritischere Vorgänge elektronisch und über das Internet bereitgestellt werden. Die Ziele für die Cyber-Angreifer werden täglich lukrativer und die Möglichkeiten vielfältiger und ausgeklügelter.

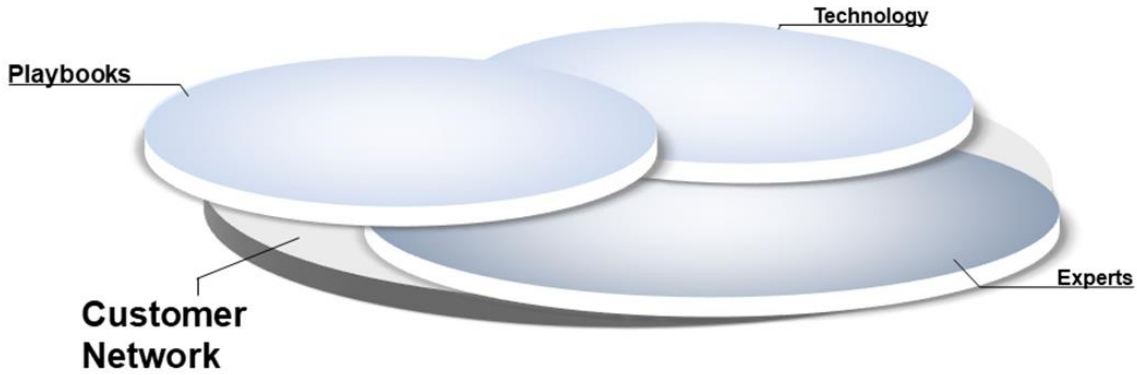
Aufgrund der steigenden Komplexität der IT, der wachsenden Bedrohungen und des Mangels an Fachpersonal ist es heute kaum mehr möglich, sich gegen alle Attacken zu schützen. Cyber-Angriffe sind still, komplex und immer öfter massgeschneidert. Prävention alleine hilft nicht mehr. In der unsicheren digitalen Welt zu bestehen erfordert permanentes Suchen und Eruieren von Gefahren sowie aktives Handeln.

Es ist von zunehmender Wichtigkeit, zu erkennen, wann ein Angriff auf die Unternehmung erfolgreich ist. Dazu sind Experten nötig, welche basierend auf modernen Analytik-Tools methodisch und strukturiert nach Spuren suchen, Verdachtsmomente klären und bei Gefahren aktiv Handeln.

Was die Vergangenheit zeigt, ist, dass Technologie alleine nicht ausreicht. Denn die Angreifer adaptieren ihre Attacken und bewegen sich zwischen den Technologien unerkannt.



Nebst dem Einsatz von Spitzentechnologie braucht es eine perfekt abgestimmte Maschinerie von Technologien, Sicherheitsexperten und effizienten Prozessen, um diese Blindspots abzusichern. Die Nachhaltigkeit bestehender Technologien wird dabei gewahrt und unterstützt.



Die ISPIN AG hat mit ihrem Cyber Defense Service ein Komplettpaket zusammengestellt, welches sich diesen Herausforderungen annimmt.

- **Technologien:** Zu den state-of-the-art mehrstufigen Erkennungsmodulen kommt eine Advanced Correlation und Risikoerkennung dazu.
- **Experten:** Unseren Kunden steht ein eingespieltes internationales Expertenteam zur Verfügung.
- **Playbooks:** Geübte und gelebte Prozeduren, mit Knowhow-Feedback-Loop zurück in den Service.

Unseren Kunden steht ab sofort einen in der Schweiz ansässigen, erstklassigen **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 konzipiert für gezielte und modernste Angriffsszenarien**.

Der Einsatz von **Spitzentechnologie** ermöglicht eine vollständige **Rundumsicht** Ihrer digitalen Infrastruktur. Die daraus gewonnene Einsicht maximiert die Korrelierbarkeit der vorhandenen Daten, und unser Team kann daraus weitführende **Ereignisketten** erstellen. Durch **Automation** stellen wir sicher, dass nur dann ein Mensch intervenieren muss, wenn eine kritische bzw. massgebliche Entscheidung getroffen werden muss. Unser eingesetztes **Fabric** integriert bereits bestehende Plattformen. Dadurch wird die Nachhaltigkeit bereits bestehender Technologie unterstützt und gewährt.

Wenn eine Bedrohung erkannt wurde, erfolgt eine Alarmierung **an Ihre Profis**. Unsere Cyber Threat-Experten unterstützen Sie dann im Bedarfsfall mit Knowhow und Prozeduren zur Bereinigung der Bedrohung.

Längst ist klar, dass es nur noch darum geht, wann und wie heftig eine Cyber-Attacke erfolgen wird. Um jederzeit auf alle Eventualitäten vorbereitet zu sein, muss fortwährend sichergestellt sein, dass alle Daten konsequent abgespeichert werden. Daraus erreichen wir zusätzlich eine **Perfektion in der Analysentiefe** und eine **Komplettabdeckung in der Ereignisbreite**.

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

Ihr Unternehmen profitiert von dieser **Synergie** und kann diesen Service zu einem Preis und in einer Qualität beziehen, welcher seinesgleichen auf dem Markt sucht.

Alle Use Cases können Ihrem Geschäftsrisiko zugeordnet werden, wodurch Sie eine **messbare Risikotransparenz** erhalten.

Swiss Class und die sensiblen Daten bleiben beim Kunden

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