UMB Security Intelligence – Detection & Response

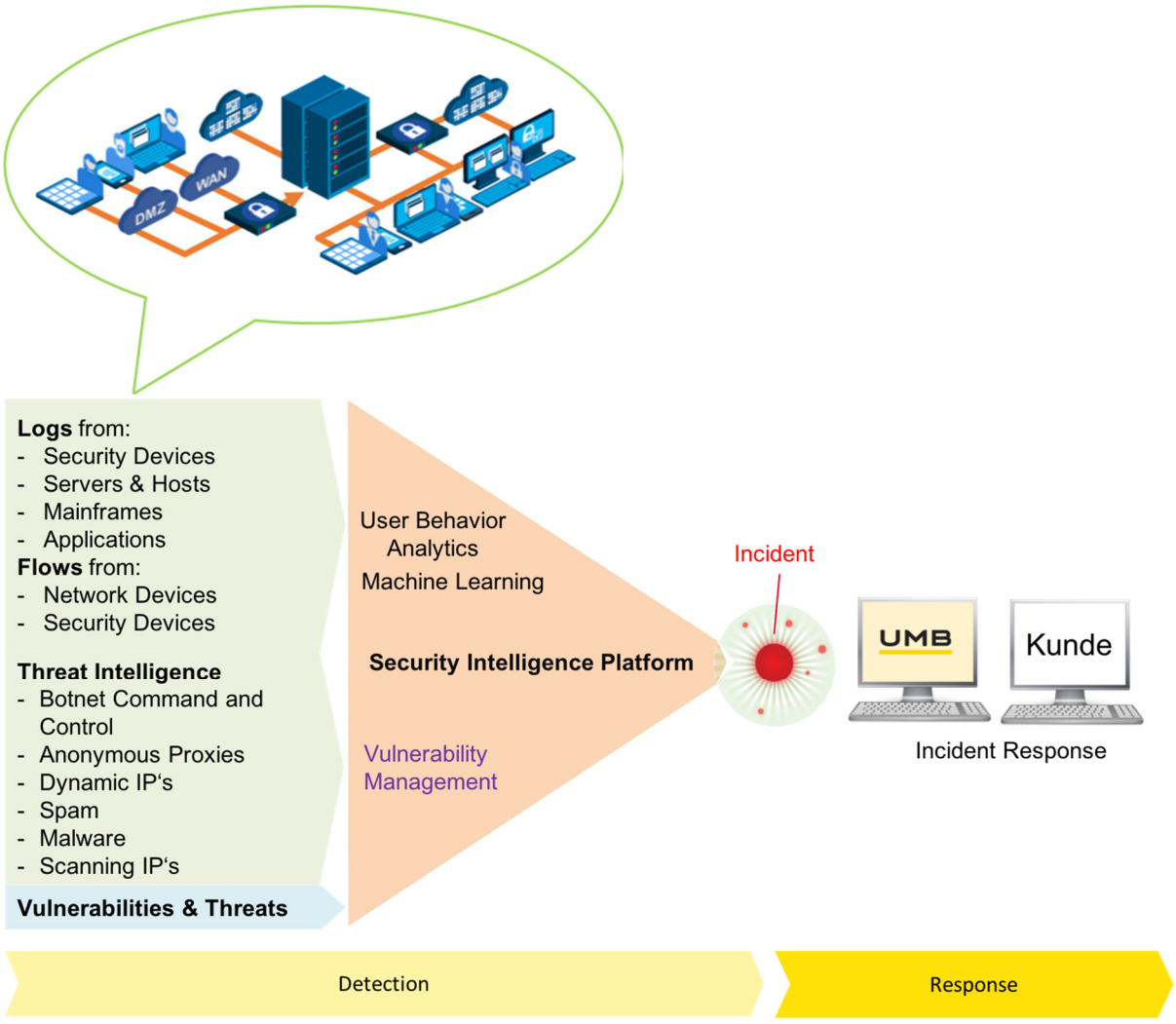
Erkennung und Abwehr von Bedrohungen.

Konventionelle Sicherheitseinrichtungen wie Firewalls, IDS/IPS Systeme, Endpoint Security- und Antivirenlösungen etc. schützen ein Unternehmen am Perimeter.

Um festzustellen, ob die Perimeter Sicherheitseinrichtungen durch eine Attacke kompromittiert wurden und sich ein Angreifer Zugang zu internen Systemen verschafft hat und sich eventuell lateral über das Netzwerk auf weitere Systeme ausbreitet, benötigt es eine Detection (Monitoring) Lösung.

Die UMB **Detection & Response** Lösung (siehe Bild unten) besteht aus technischen Komponenten, Personen und Prozessen:

- Alle Informationen, welche relevant sind, ein Unternehmen vor externen und internen Bedrohungen zu schützen, werden in der Phase **Detection** in Security Intelligence Lösung gesammelt und ausgewertet.
- Mögliche Bedrohungen (Incidents) werden in der Phase **Response** analysiert und die notwendigen Schritte zur Behebung eingeleitet (Remediation).



UMB Detection & Response Lösung

Security Intelligence – On-Premise oder aus den UMB Datacenters.

UMB bietet Security Intelligence Lösungen sowohl als On-Premise Lösung beim Kunden oder als Security Intelligence Service aus den Datacenters der UMB an.

Für On-Premise Security Intelligence Lösungen beim Kunden bietet UMB folgende Dienstleistungen an:

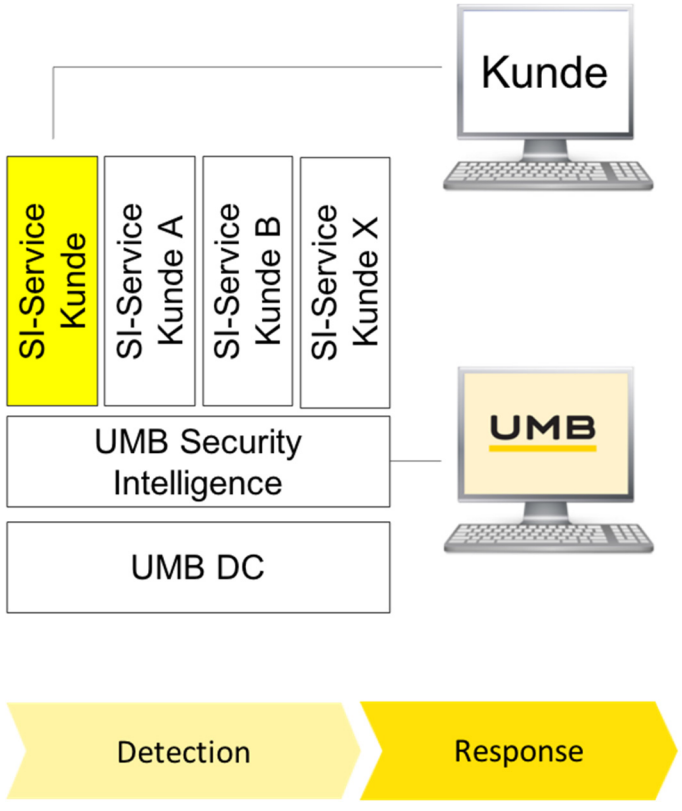
Implementation Services

- Pre-Sales Beratung
- PoC-Planung & Durchführung
- Planung der Implementierung
- Installation & Konfiguration
- On-Boarding der Log-Sourcen & Flows
- Use Cases entwickeln/umsetzen
- Custom Development (wenn erforderlich)
- Unterstützen bei der Integration mit vorhandenen Umsystemen (z.B. Ticketing, Incident Management)
- Unterstützung bei der Anpassung der internen Abläufe

Operational Services

Betriebsunterstützung oder Betrieb der QRadar-Platform des Kunden (remote/on-premise)

Security-Intelligence-as-a-Service aus den Datacenters der UMB bezieht der Kunde mit einem zu definierenden Engagement des Kunden.



Kontakt:
Gion-Clau Camenisch
Teamleader Enterprise
Security Intelligence
+41 44 805 29 13
gion.camenisch@umb.ch