SECUREBOX

SecureBox
Anhang:
Technische Beschreibung der Produkte und Dienstleistungen

Inhalt

SECUREBOX

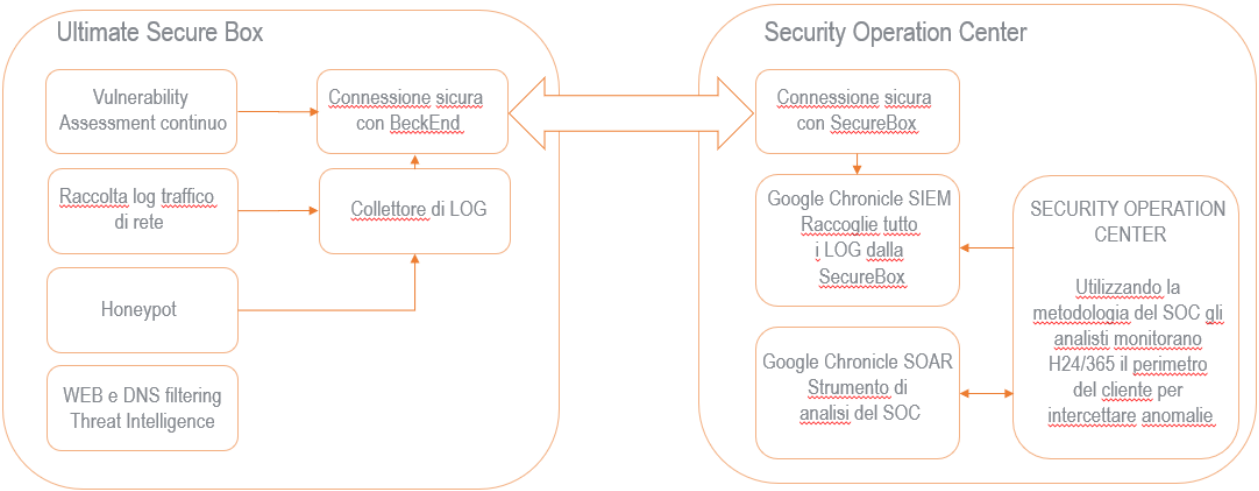
Was ist dieSecureBox

Die SecureBox-Lösung von INFOSECBOX besteht aus einem Gerät, das – im Gegensatz zu bisher auf dem Markt verfügbaren – nicht nur eine Vielzahl von Cyber-Sicherheitsfunktionen erfüllt, sondern auch als Enabler für einen Managed Detection and Response (MDR)-Dienst dient, der von einem Security Operation Center (SOC) rund um die Uhr betrieben wird. Dieses überwacht die Infrastruktur des Kunden kontinuierlich, kann jederzeit Anomalien erkennen und prompt reagieren, indem es diese meldet oder, wo möglich, Sicherheitsvorfälle aktiv bearbeitet.

Die Lösung bietet umfassenden Schutz gegen Ransomware und fortschrittliche Angriffe, die künstliche Intelligenz nutzen, sowie Datenschutz und Kontrolle der Nutzergeräte. Zudem schützt sie Schwachstellen, prüft die Reputation von URLs (Webadressen) und filtert riskante Webkategorien.

Wie funktioniert die SecureBox

Die Architektur, auf der der durch die SecureBox ermöglichte Dienst basiert, ist eine Eigenentwicklung von INFOSECBOX und umfasst die folgenden logischen Komponenten:



Die SecureBox arbeitet direkt in der Infrastruktur des Kunden: Sie führt die aktivierten Cyber-Sicherheitsfunktionen aus, erstellt eine sichere VPN-Verbindung zwischen der Infrastruktur des Kunden und dem Backend des SOC und überträgt die gesammelten Daten sowie die vor Ort durchgeführten Analyseergebnisse.

Im SOC werden die Daten aggregiert, normalisiert und mit Back-End-Technologien verarbeitet, während die Mitarbeiter die eingehenden Signale rund um die Uhr überwachen und festgestellte Anomalien bearbeiten.

Wie wird die SecureBox installiert?

Die SecureBox wurde so konzipiert, dass sie äußerst einfach zu installieren ist. Sie kann in verschiedenen Netzwerkkonfigurationen des Kunden integriert werden. Im Folgenden sind die Hauptanwendungsfälle dargestellt. Bei komplexeren Netzwerken oder besonderen Konfigurationen muss gemeinsam mit dem Kunden analysiert werden, wo die SecureBox integriert und welche Diensttypen aktiviert werden können.

Damit die SecureBox korrekt funktioniert, sind folgende technische Anforderungen zu beachteni:

- Die maximale empfohlene Benutzerzahl beträgt 50. Höhere Werte erfordern eine technische Überprüfung.
- Das Netzwerk, in dem die SecureBox untergebracht ist, muss Zugang zum Internet haben.
- Die SecureBox sollte in der Regel zwischen der Firewall und dem Switch positioniert sein, um den gesamten Netzwerkverkehr sehen zu können.
- Die SecureBox muss an einem geeigneten Ort mit ausreichender Belüftung aufgestellt werden.
- Die Verkabelung sollte mit geeigneten Kabeln (mindestens Netzwerkkabel Cat.5E) erfolgen.

Fall 1 – Kundenrouter/Firewall des Telekommunikationsanbieters

Dies ist der einfachste Fall. Der Kunde verwendet den vom Anbieter bereitgestellten Router, der sowohl als Router als auch als Firewall dient. Derselbe Router fungiert als DNS- und DHCP-Server sowie als WLAN-Zugangspunkt. Innerhalb des Kundennetzwerks sollte mindestens ein Switch vorhanden sein. Falls keiner vorhanden ist, wird ein solcher zusammen mit der SecureBox bereitgestellt.

In diesem Fall bietet die SecureBox zusätzlich Funktionen als Zugangspunkt und wird mit zwei WLAN-Netzwerken geliefert: einem „Gast“-Netzwerk und einem „Kunden“-Netzwerk.

Abbildung 1: Schema der Installation eines Kunden mit Router/Firewall eines Telekommunikationsanbieters

Fall 2 – Kunde mit separatem Router und Firewall in einem nicht segmentierten Netzwerk

In diesem Szenario trennt der Kunde den Router von der Firewall, wobei die Firewall als DNS- und DHCP-Server fungiert. Es gibt außerdem einen zentralen Switch (Core Switch) und Zugangspunkte (Access Points).

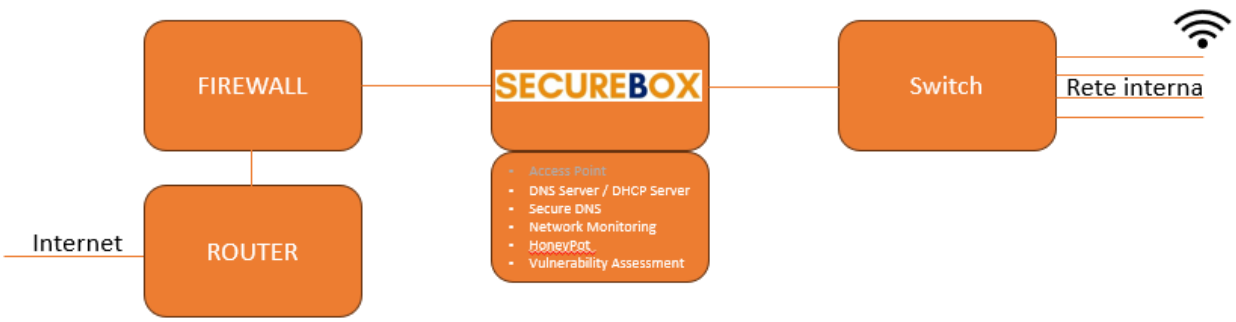


Abbildung 2: Schema der Installation eines Kunden mit separatem Router, Firewall und Access Points

Fall 3 – Kunde mit separatem Router und Firewall in einem nicht segmentierten Netzwerk und einem Windows-DNS-/DHCP-Server

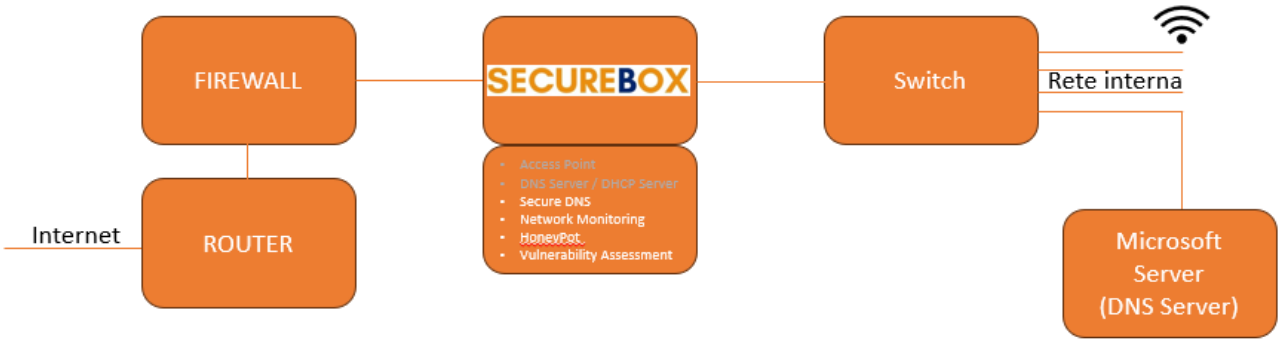


Abbildung 3: Für dieses Szenario wird der Netzwerkaufbau um einen internen Microsoft-Server ergänzt, der die DNS- und DHCP-Funktionen übernimmt.

Alle anderen Szenarien erfordern eine vorherige Analyse der Infrastruktur sowie eine gemeinsame Zusammenarbeit zwischen den Technikern von INFOSECBOX und dem Kunden, um die richtigen Konfigurationen vorzunehmen und die Funktionen zu aktivieren, die mit der Kundeninfrastruktur kompatibel sind.

Die technischen Funktionen der SecureBox

Web- und DNS-Filterung, aktualisiert durch Cyber Threat Intelligence (Anwendbar für die Fälle 1 und 2)

Die Web- und DNS-Filterung ist ein wesentlicher Bestandteil der Cybersicherheit. Diese Dienste nutzen Informationen aus Bedrohungsquellen, um Netzwerke und Systeme vor Angriffen zu schützen.

Web-Filterung: Kontrolliert und beschränkt den Zugriff auf bestimmte Websites, indem schädliche oder potenziell gefährliche Seiten blockiert werden. Mithilfe von Threat Intelligence kann der Filter Seiten erkennen und blockieren, die Malware, Phishing oder andere Bedrohungen verbreiten.

DNS-Filterung: Überwacht den DNS-Verkehr und blockiert den Zugriff auf bösartige oder verdächtige Domains. Dieser Filter identifiziert über Threat Intelligence Domänen, die mit schädlichen Aktivitäten in Verbindung stehen, und verhindert die Interaktion mit diesen.

Durch die Integration von Threat Intelligence werden diese Dienste ständig aktualisiert, sodass sie schnell auf neue Bedrohungen reagieren können.

Deep Packet Inspection - Analyse des Netzwerkverkehrs

Die SecureBox enthält ein Modul zur Netzwerkverkehrsanalyse, das in der Lage ist, Cyberangriffe auf Netzwerkebene zu erkennen und zu verhindern. Es bietet eine Reihe fortschrittlicher Funktionen

- **Erkennung von Eindringlingen:**
  Überwacht kontinuierlich den Netzwerkverkehr, um verdächtige Aktivitäten oder bekannte Angriffssignaturen zu identifizieren.
  Nutzt digitale Signaturen, heuristische Methoden und Verhaltensanalysen zur Erkennung von Bedrohungen.
- **Angriffsprävention:**
  Erkennt verdächtige Aktivitäten und ermöglicht es dem SOC, sofortige Maßnahmen zu ergreifen. Maßnahmen umfassen das Blockieren oder Neutralisieren der Bedrohung, z. B. durch temporäre Änderungen an Firewall-Regeln oder Benachrichtigung der Systemadministratoren.
- **Verkehrsfilterung**:
  Analysiert den Netzwerkverkehr in Echtzeit und filtert potenziell gefährliche Datenpakete.
  Überprüft Netzwerkprotokolle, verwaltet Verbindungen und blockiert bösartige Pakete.
- **Prävention bekannter und unbekannter Angriffe:**
  Neben der Erkennung von Signaturen bekannter Angriffe verwendet das Modul fortschrittliche Techniken wie Verhaltensanalysen und maschinelles Lernen, um unbekannte Bedrohungen oder Malware-Varianten zu identifizieren.
- **Schutz vor Zero-Day-Angriffen:**
  Das Modul erkennt und mildert Schwachstellen, die noch nicht bekannt oder gepatcht sind (sogenannte Zero-Day-Angriffe).
- Dies geschieht durch die Identifikation anomaler Verhaltensmuster, die auf Versuche hindeuten, eine Schwachstelle auszunutzen.

- **Integration mit Threat Intelligence:**
  Das IPS-Tool wird mit den Threat-Intelligence-Diensten von INFOSECBOX integriert, um in Echtzeit Informationen über neue Bedrohungen zu erhalten.
  Sicherheitsrichtlinien werden entsprechend angepasst.
- **Regelmäßige Updates der Signaturen und Regeln:**
  Um die Effektivität zu gewährleisten, wird das Modul regelmäßig mit den neuesten Signaturen und Regeln aktualisiert, um Schutz vor den neuesten Bedrohungen zu bieten.

Honeypot

Ein Honeypot ist ein Element der IT-Infrastruktur, das speziell dafür konzipiert ist, Cyberangriffe anzuziehen und abzufangen:

- Attraktivität: Ein Honeypot ist so konzipiert, dass er für Angreifer wie ein interessantes Ziel erscheint. Er kann ein authentisches System oder eine Ressource simulieren, um Aufmerksamkeit zu erregen und schädliche Interaktionen anzuziehen.
- Isolierung: Der Honeypot wird in einer logisch isolierten Umgebung implementiert, um zu verhindern, dass ein Angriff von ihm auf den Rest der Infrastruktur übergreift.
- Überwachung: Er zeichnet sorgfältig alle Aktivitäten auf, die in seinem Inneren stattfinden. Dazu gehören Zugriffsversuche, Interaktionen mit dem System und anomales Verhalten, das auf einen Angriff hindeuten könnte.
- Flexibilität: Honeypots können so konfiguriert werden, dass sie unterschiedliche Arten von Systemen und Diensten emulieren. Dadurch können Administratoren den gewünschten Grad an Komplexität und Spezifität wählen.

Vorteile eines Honeypots können sein:

- Frühzeitige Erkennung: Da ein Honeypot darauf ausgelegt ist, Aufmerksamkeit zu erregen, kann er Angriffe in einer sehr frühen Phase erkennen. Dies ermöglicht es den Systemadministratoren, einzugreifen, bevor der Angriff die Hauptnetzwerkstruktur erreicht.
- Sammlung von Informationen: Honeypots liefern wertvolle Informationen über die Taktiken, Techniken und Verfahren (TTP) der Angreifer. Diese Daten können verwendet werden, um die Verteidigungsmaßnahmen zu verbessern und die allgemeine Sicherheit zu stärken.
- Studium des Angreiferverhaltens: Durch die Analyse der Interaktionen mit dem Honeypot gewinnen SOC-Analysten ein tieferes Verständnis für das Verhalten der Angreifer. Dies erleichtert die Vorbereitung auf ähnliche Bedrohungen in der Zukunft und erweitert das Wissen für alle Kunden von INFOSECBOX.
- Funktion als Falle: Honeypots können als eine Art "Falle" für Angreifer dienen. Das Angreifen eines Honeypots kann die Angreifer von kritischeren Zielen in der Infrastruktur ablenken.
- Entwicklung und Test neuer Abwehrmaßnahmen: Honeypots bieten eine kontrollierte Umgebung, in der neue Verteidigungstechniken und Sicherheitsmaßnahmen getestet werden können, ohne dass Risiken für das Hauptnetzwerk entstehen.
- Prävention bekannter Bedrohungen: Honeypots können so konfiguriert werden, dass sie gezielt bestimmte Arten bekannter Angriffe anziehen. Dies hilft, bereits identifizierte Bedrohungen zu verhindern und bekannte Risiken zu minimieren.

Der Honeypot ist ein wertvolles und laut INFOSECBOX fundamentales Werkzeug für die Cybersicherheit. Er bietet eine strategische Möglichkeit, Bedrohungen zu untersuchen, zu erkennen und zu mindern, indem Cyberangriffe aktiv analysiert und abgefangen werden.

Kontinuierliche Schwachstellenbewertung

Der von den Analysten von INFOSECBOX bereitgestellte Dienst zur kontinuierlichen Schwachstellenbewertung, der durch das Modul der SecureBox ermöglicht wird, ist ein fortlaufender Prozess zur Identifikation, Bewertung und Behebung von Schwachstellen in einem IT-System.
Merkmale eines kontinuierlichen Schwachstellenbewertungsdienstes:

- Regelmäßige Scans: Führt periodische (monatliche) Scans des Systems durch, um mögliche Schwachstellen und Sicherheitslücken zu identifizieren.
- Tiefgehende Analyse: Neben automatisierten Scans werden auch detaillierte Analysen durch Experten durchgeführt, um den Kontext der erkannten Schwachstellen zu bewerten und deren Einfluss auf die Gesamtsicherheit zu bestimmen.
- Priorisierung von Schwachstellen: Kategorisiert die Schwachstellen nach ihrem Risikoniveau und der Dringlichkeit der Behebung, sodass sich Sicherheitsexperten auf die kritischsten Bedrohungen konzentrieren können.
- Kontinuierliches Monitoring: Es handelt sich nicht um eine einmalige Aktivität, sondern um einen kontinuierlichen Prozess, der neue Schwachstellen im Laufe der Zeit aufgrund neuer Bedrohungen oder Systemaktualisierungen überwacht.
- Detaillierte Berichte: Liefert Berichte über die Ergebnisse der Scans, einschließlich spezifischer Empfehlungen zur Behebung der gefundenen Schwachstellen.

Wichtigkeit eines kontinuierlichen Schwachstellenbewertungsdienstes:

- Vorbeugende Identifikation von Schwachstellen: Er ermöglicht es, Schwachstellen zu erkennen und zu beheben, bevor sie von böswilligen Angreifern ausgenutzt werden können, wodurch das Risiko einer Kompromittierung verringert wird.
- Aufrechterhaltung der Systemsicherheit: Unterstützt die kontinuierliche Sicherheit der IT-Infrastruktur, da sich Bedrohungen im Laufe der Zeit weiterentwickeln und neue Schwachstellen durch Software- oder Systemaktualisierungen entstehen können.
- Einhaltung gesetzlicher Vorschriften: Viele Sicherheitsstandards und Vorschriften verlangen eine kontinuierliche Bewertung von Schwachstellen. Beispielsweise können Unternehmen im Finanz- oder Gesundheitssektor verpflichtet sein, solche Bewertungen durchzuführen, um spezifische regulatorische Anforderungen zu erfüllen.
- Reduzierung finanzieller Risiken: Die rechtzeitige Behebung von Schwachstellen kann helfen, erhebliche Kosten zu vermeiden, die durch Sicherheitsverletzungen, den Verlust sensibler Daten oder Reputationsschäden entstehen könnten.
- Sicherheitsbewusstsein: Bietet einen klaren Überblick über den Sicherheitsstatus der IT-Umgebung, sodass Systemadministratoren und Sicherheitsverantwortliche fundierte Entscheidungen zum Schutz des Systems treffen können..

- Anpassung an neue Bedrohungen: Eine kontinuierliche Bewertung ermöglicht es, mit aufkommenden Bedrohungen Schritt zu halten und die Abwehrmaßnahmen kontinuierlich an neue Schwachstellen und Angriffe anzupassen.

Der Dienst zur kontinuierlichen Schwachstellenbewertung ist entscheidend, um die Sicherheit der IT-Infrastruktur aufrechtzuerhalten, Schwachstellen rechtzeitig zu identifizieren und zu beheben sowie sich effektiv an die sich ständig weiterentwickelnden Bedrohungen im Bereich der Cybersicherheit anzupassen.

Cyber Security Awareness

"Cyber Security Awareness" contenuto nella soluzione SecureBox è una piattaforma online Der Dienst "Cyber Security Awareness", der in der SecureBox-Lösung enthalten ist, stellt eine Online-Plattform zur Verfügung, die sich der kontinuierlichen Schulung und Sensibilisierung der Mitarbeiter im Bereich Cybersicherheit widmet.

Über diesen Service können Kunden ihre Mitarbeiter selbstständig anmelden. Diese erhalten Zugriff auf kurze monatliche Schulungen mit wenigen abschließenden Verständnisfragen. Jede Lektion, die nur wenige Minuten dauert, behandelt wichtige Themen wie Phishing, Social Engineering, sichere Passwortverwaltung und andere relevante Aspekte der Informationssicherheit.

Die Bedeutung dieser Schulungsmaßnahmen ist vielfältig:

- Sie steigern das Bewusstsein und die Vorbereitung der Mitarbeiter, um alltägliche Cyber-Bedrohungen zu erkennen und zu bewältigen. Dies reduziert das Risiko von Sicherheitsvorfällen, die zu finanziellen Verlusten und Reputationsschäden führen können, erheblich.
- Viele Datenschutzvorschriften, wie die DSGVO, verlangen von Unternehmen, angemessene Maßnahmen zu ergreifen, um die Informationssicherheit zu gewährleisten. Dies schließt die Schulung des Personals über die Bedeutung von Datensicherheit und die entsprechenden Schutzmaßnahmen ein.

Durch diese Schulungen verbessern Unternehmen nicht nur ihre Einhaltung der gesetzlichen Vorschriften, sondern fördern auch eine robustere Sicherheitskultur innerhalb ihrer Organisation.

Dark Web Visibility

Der Dienst "Dark Web Visibility" wurde entwickelt, um Unternehmen dabei zu helfen, kompromittierte oder gestohlene Informationen (z. B. persönliche Daten, Zugangsdaten, Finanzdaten) zu identifizieren und darauf zu reagieren, wenn diese im Dark Web veröffentlicht oder verkauft werden.

Erkennung basierend auf der Domain:
Das Monitoring beginnt mit der Identifizierung der Unternehmensdomain des Kunden als Schlüssel zur Nachverfolgung von Datenlecks. Jegliche Referenzen auf die Unternehmensdomain, deren Subdomains oder zugehörige E-Mail-Adressen werden erfasst und zur weiteren Untersuchung gemeldet.

Techniken des Monitorings:

- *Regelmäßige Scans: Der Dienst nutzt fortschrittliche Software, um das Dark Web zu durchsuchen. Dies umfasst versteckte Foren, illegale Marktplätze, Chatrooms und andere digitale Untergrundplattformen.*
- *Künstliche Intelligenz und maschinelles Lernen: Algorithmen werden verwendet, um Muster gestohlener Daten zu erkennen und mit dem Kunden in Verbindung zu bringen. Dazu gehört die Identifikation von Strukturen in den entwendeten Daten sowie deren wahrscheinlicher Ursprung.*
- *Benachrichtigungssysteme: Sofortige Benachrichtigungen erfolgen, wenn Informationen identifiziert werden, die die Domain des Kunden betreffen. Dies ermöglicht eine schnelle Reaktion*.

Reporting:
Kunden erhalten eine Übersicht der gesammelten Informationen über ein Webportal, das Zugriff auf alle Dienste der SecureBox-Lösung bietet. Dieses Portal zeigt die Art der gefundenen Informationen, deren Standort im Dark Web und Empfehlungen zur Schadensbegrenzung in verständlicher Weise an.

Vorteile:

- Schadensprävention: Reduziert das Risiko finanzieller Verluste und Reputationsschäden, indem die Exposition sensibler Daten minimiert wird.
- Einhaltung gesetzlicher Vorschriften: Unterstützt die Einhaltung geltender Datenschutzbestimmungen, indem Verstöße rechtzeitig gemeldet werden.

Durch die Nutzung des Dark-Web-Visibility-Dienstes können Unternehmen einen proaktiven Ansatz zum Schutz ihrer sensiblen Informationen verfolgen und mögliche Bedrohungen antizipieren, bevor sie sich negativ auf die Organisation auswirken.

Dieser Service ist unerlässlich für Unternehmen, die ein hohes Maß an Cybersicherheit aufrechterhalten und die Risiken im Zusammenhang mit der Präsenz von Unternehmensdaten im Dark Web effektiv verwalten möchten.

Beschreibung der SOC-Dienste rund um die Uhr

Der vom SOC bereitgestellte MDR-Dienst, der rund um die Uhr und 365 Tage im Jahr aktiv ist, bildet das Herzstück des Angebots und den besonderen Mehrwert der SecureBox. Der Dienst umfasst die Überwachung, Benachrichtigung und, wenn möglich, die aktive Reaktion auf Sicherheitsvorfälle. Dieser Service wird durch eine speziell entwickelte Plattform ermöglicht, die auf einem innovativen Technologie-Stack basiert:

- Proprietäres Framework (Autonomic Incident Response):
- Abdeckung der Bedrohungserkennung durch Mapping der Techniken des MITRE ATT&CK-Frameworks und Anwendung des Autonomic Incident Response (AIR)-Frameworks von INFOSECBOX. Dieses Framework kann Alarme aus den Telemetriedaten der Systeme/Technologien des Kunden im definierten Perimeter identifizieren und qualifizieren.
- SOAR / Incident Response: Google Chronicle SOAR (Owner-Tenant MSSP).
- Security Data Lake / SIEM: Google Chronicle (dedizierter Tenant für den Kunden).
- Nutzung der SecureBox-Module: Verwendung der integrierten SecureBox-Module zur detaillierten Analyse und Datensammlung.

Zusätzliche Dienste des SOC in Verbindung mit der SecureBox:

- **Threat Intelligence**:
  Der Dienst umfasst die interne Nutzung durch das Analystenteam und die Automatisierung auf der SOAR-Plattform. Dies beinhaltet verschiedene Tools für Cyber Threat Intelligence und Intelligence-Feeds, die die Erkennung verbessern und die Reaktionsphase bei bekannten Angriffsmethoden effektiver gestalten.
- **Threat Hunting**:
  Proaktive Bedrohungssuche, sowohl für bekannte als auch unbekannte Bedrohungen, durchgeführt von spezialisierten Analysten.
- Innerhalb des Kundenperimeters erfolgt dies mithilfe des Technologie-Stacks und der kontinuierlichen Identifikation von Angriffsmustern. Diese können anschließend durch SIEM-Regeln und SOAR-Playbooks automatisiert erkannt werden.

Alle vom SOC bereitgestellten Dienste werden vollständig remote erbracht.

Servicelevel des SOC

Der Service wird rund um die Uhr (H24) an 365 Tagen im Jahr angeboten.

Die Service Level Agreements (SLAs) gelten für Vorfälle, die von der SecureBox gemeldet werden, beispielsweise bei der Erkennung eines Datendiebstahls zu einer als bösartig eingestuften IP-Adresse.):

Priorität	Bearbeitungszeit	Mögliche Maßnahmen	Beispiele
Kritisch	1 Stunde	Benachrichtigung / Reaktion	Kompromittierung kritischer Systeme mit möglicher Datenexfiltration. Ein Mission-Critical-System wird angegriffen.
Hoch	4 Stunden	Benachrichtigung / Reaktion	Systeme oder Assets wurden bestätigt oder wahrscheinlich kompromittiert. Keine Mission-Critical-Systeme betroffen. Sensible Daten befinden sich in den betroffenen Systemen.
Mittel	8 Stunden	Benachrichtigung / Reaktion	Keine kritischen Systeme betroffen. Wenige oder keine sensiblen Daten betroffen (möglicherweise ein Kundenendpunkt wie ein Desktop oder Laptop).

Allgemeine Annahmen und Ausschlüsse

Dieser Abschnitt listet allgemeine Annahmen und Ausschlüsse auf, die ausdrücklich erwähnt werden müssen.

- **Bereitstellung und Installation:**
  Das in der SecureBox-Lösung enthaltene Produkt wird an den angegebenen Standort geliefert und in die Infrastruktur des Kunden von einem internen technischen Ansprechpartner des Kunden mit Remote-Unterstützung durch die Techniker von INFOSECBOX installiert.
- **Unterstützung bei der Installation:**
  Der Service umfasst die Unterstützung bei der Installation eines oder mehrerer SecureBox-Produkte in der Kundeninfrastruktur.
- **Vertragsabschluss und notwendige Unterlagen:**
  Zum Zeitpunkt des Vertragsabschlusses müssen alle Formulare ausgefüllt werden, die für die ordnungsgemäße Erbringung der vorgesehenen Dienstleistungen erforderlich sind. Diese sind im Anhang „SECUREBOX - TECHNISCHER VORABFRAGEBOGEN KUNDE (jjjjmmtt)“ enthalten und umfassen Informationen zur Komplexität der IT-Infrastruktur des Kunden, die zu benachrichtigenden Ansprechpartner im Falle eines Vorfalls oder einer Meldung sowie die Angabe des Installationsstandorts der SecureBox.
- **Lizenzen:**
  Alle Lizenzen für die in der SecureBox-Lösung verwendeten Produkte sowie für die Servicebereitstellung sind in den Kauf- und/oder monatlichen Abonnementkosten enthalten.
- **Notfallverfahren:**
  Bei schwerwiegenden Fehlfunktionen des SecureBox-Produkts muss sofort das Notfallverfahren (Isolierung der SecureBox) eingeleitet werden, bis die Ersatz-SecureBox eintrifft.
- **Remote-Aktivierung:**
  Sofern keine besonderen Anforderungen zusätzlich zum Service bewertet werden müssen, werden alle Aktivierungsphasen remote durchgeführt.
- **Remote-Dienstleistung:**
  Der SOC-MDR-Dienst wird immer remote erbracht.