AIRLOCK®
SECURE ACCESS HUB

WEBROOT
Smarter Cybersecurity™

Airlock® Threat Intelligence

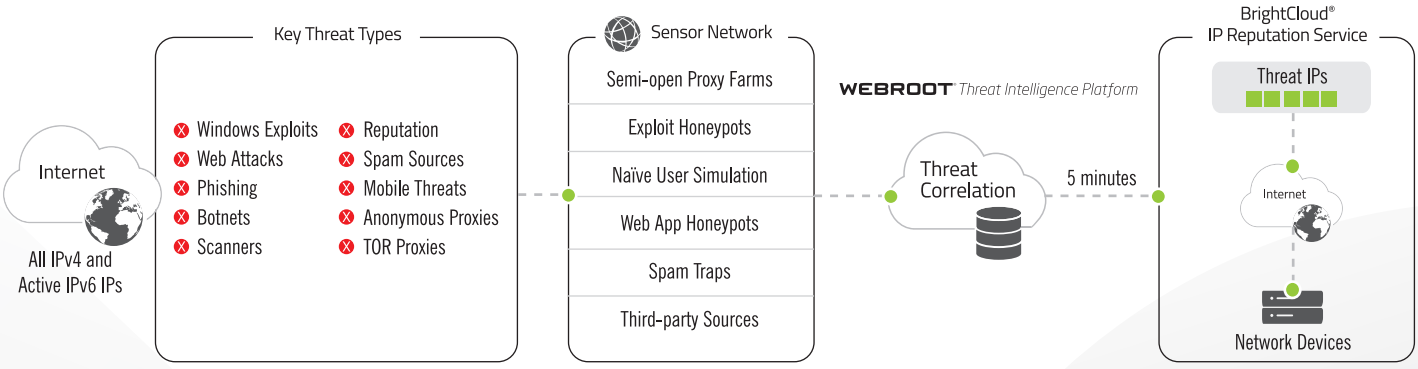
Gezielte Angriffe gegen IT Services erfolgen oft global und koordiniert. Viele der dafür verwendeten Computer, wie beispielsweise Botnet Zombies, sind kein unbeschriebenes Blatt und die Wahrscheinlichkeit ist hoch, dass sie andernorts bereits auffällig wurden. Airlock® integriert deshalb den BrightCloud® Threat Intelligence Service von Webroot® und kann damit in Echtzeit bösartige Clients identifizieren und diese blockieren, bevor sie Schaden anrichten. Die neue Verwaltung von IP-Adresslisten ergänzt die Threat Intelligence Feeds optimal und ermöglicht damit die Umsetzung von umfangreichen IP-basierten Zugriffsregeln.

Threat Intelligence powered by Webroot®

Der BrightCloud® Threat Intelligence Service von Webroot® liefert hochqualitative und globale Bedrohungsdaten in Echtzeit. IP Adressen, welche Angriffe durchführen, zu Botnets gehören, mit Malware infiziert sind, Spam verschicken, Phishing Angriffe ausführen oder via TOR und andere Proxies zugreifen, landen sofort auf einer entsprechenden Blacklist. In Airlock® ist der Threat Intelligence Service von Webroot® als Modul integriert und die IP Reputation Daten werden laufend aktualisiert. Auf Knopfdruck lassen sich bösartige IP Adressen blockieren, noch bevor sie überhaupt auf geschützte Services zugreifen können.

Effektive Sicherheit

Airlock® integriert nahtlos den Threat Intelligence Service von Webroot®. Damit werden basierend auf bereitgestellten Kategorien und Vertrauensstufen automatisch gefährliche Clients blockiert und der Schutz der Applikationen vor Missbrauch zusätzlich erhöht. Der Webroot® BrightCloud® Threat Intelligence Service ist eine proaktive, automatisierte Sicherheitslösung, die eine effektive Richtliniendurchsetzung gegen die aktuellsten Bedrohungen in Echtzeit bietet. Der Service ist technisch vollständig integriert inklusive automatischen Datenupdates. Eine aufwändige Integration der Services in die eigene Applikationslandschaft entfällt.



Ergon Informatik AG | Merkurstrasse 43 | CH-8032 Zürich | Telefon: +41 44 268 89 00 | E-Mail: info@airlock.com

Die Vorteile der Kombination

Durch die enge Integration in Airlock® entstehen viele Vorteile für Sie: Die Threat Informationen können in Airlock® vielseitig genutzt werden, um maximale Sicherheit zu gewährleisten. Einerseits werden sie auf der Web Application Firewall für das Blocking und Labelling genutzt. Zusätzlich können die Informationen auch an Back-ends weitergleitet werden, welche selbst Logik darauf aufbauen können, wie z.B. eine selektive Transaktionssignierung oder auch Betrugserkennung. Auch im Bereich der risikobasierten Authentifizierung werden die Daten von Airlock nahtlos genutzt. Zudem sind die Threat Kategorien auch im Airlock® Reporting integriert und erlauben übersichtliche Dashboards zu den Angriffsversuchen.

Die Webroot® Plattform

Die Webroot®-Plattform nutzt Machine Learning, um täglich 500 Milliarden Datenobjekte zu erkennen, zu analysieren und zu klassifizieren, darunter 37 000 bösartige URLs, 15 000 Phishing-Sites und 100 000 bösartige IP-Adressen.

Brightcloud® IP Reputation

Der BrightCloud® IP Reputation Service veröffentlicht dynamische Informationen über risikoreiche IP-Adressen und gibt Einblicke in die eingehende Kommunikation mit einer dynamische Blacklist mit ~ 6 Millionen bösartigen IP-Adressen und Updates alle 5 Minuten. Die IPs werden in 10 Kategorien unterteilt, darunter Windows Exploits, Phishing, Botnets und Spamquellen.

Webroot® Threat Intelligence Funktionen:

- Prediktive Intelligenz, realisiert durch eine kontextbezogene Datenbank und kombiniert mit einer historischen Datenbank für zusätzliche Erkenntnisse über Bedrohungen.
- Intelligenz auf der Grundlage einer umfassenden globalen Abdeckung und umfangreichen, realen Daten.
- Laufend aktualisierte Daten in Echtzeit mit Reputationsbewertung und aktivem Bedrohungsstatus
- Fortschrittliches Cloud-basiertes, maschinelles Lernen mit enormer Rechenleistung und patentierten mathematischen Modellen in Verbindung mit menschlichem Feedback, Bedrohungsforschung und Threat Reverse Engineering.

Webroot® Threat Kategorien:

Spam Quellen: IP-Adressen, die Spam-Nachrichten durch einen Proxy tunneln, abnormale SMTP Aktivitäten und Spam Aktivitäten über Foren erzeugen.

Windows Exploits: IP-Adressen, die an der Verteilung von Malware, Shell Code, Rootkits, Würmern oder Viren für Windows beteiligt sind.

Web Angriffe: IP-Adressen, die mit Cross-Site Scripting, iFrame Injection, SQL Injection, Cross Domain Injection oder Domain Passwort Brute Force Angriffe auf Verwundbarkeiten in Webservern abzielen.

Botnets: IP-Adressen, die als Botnet Command und Control (C&C) Center agieren und infizierte Zombie Maschinen kontrollieren.

Denial of Service: Die Denial of Service Kategorie umfasst DoS, DDoS, anomale Sync Floods und Erkennung von anomalem Traffic.

Scanners: IP-Adressen, die unauthorisierte Wiedererkennungsaktivitäten durchführen wie Probing, Host Scanning, Port Scanning oder Brute Force Login Versuche.

Phishing: IP-Adressen, die Phishing Sites hosten und Sites die auf andere betrügerischen Aktivitäten bezogen sind.

TOR Proxy: IP-Adressen, die als Ausgangsknoten für das TOR Netzwerk agieren. Exit nodes sind der letzte Punkt entlang der Proxy Kette und machen eine direkte Verbindung zum beabsichtigten Ziel.

Proxy: IP-Adressen, die Proxy Dienste anbieten inklusive sowohl VPN als auch Open Web Proxy Dienste.

Mobile Threats: Denial of Service, Packet Sniffing, Address Impersonation und Session Hijacking