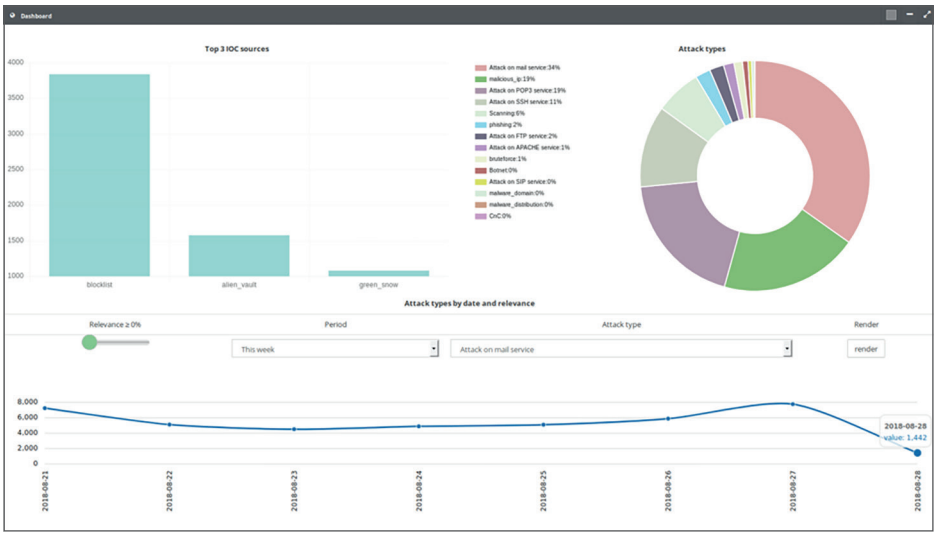
ALLIACERT

Ihr Notfall-Einsatzteam

Wie kann AlliaCERT Ihr Unternehmen unterstützen?

Während das SOC kontinuierlich Ihre Sicherheit überwacht, bei einem Vorfall alarmiert, erste Analysen vornimmt und sofort Maßnahmen ergreift, kümmert sich das CERT um die tiefergehende Analyse, Behebung des Vorfalles, Planungen und Verwundbarkeitsmanagement. So ist es vom Vorteil die CERT-Analysen und -Meldungen in das SOC Monitoring einfließen zu lassen. Zusammen bilden beide ein starkes Team gegen die Angriffe auf die Cybersicherheit.

Mit unserer Lösung AlliaCERT (CERT = Computer Emergency Response Team) bieten wir Ihnen eine Abwehrzentrale mit Rundumschutz, welche Ihr Unternehmen mit Informations- und Warndiensten, sowie bei der Bewältigung von Sicherheitsvorfällen unterstützt. Mit rund 15 Experten bietet AlliaCERT Ihnen Alarmierungs-, Informations-, Überwachungs-, sowie Analysedienste.



WARUM IST ALLIACERT DAS RICHTIGE FÜR MEIN UNTERNEHMEN?

- Axians bietet Ihnen ein wettbewerbsfähiges, wirtschaftlich vorteilhaftes Angebot
- Sie bekommen ein erfahrenes Team von Experten für die Implementierung und das Management von AlliaCERT zur Seite gestellt
- Langjährige Partnerschaften mit ähnlichen Organisationen weltweit, die Sie gegen Angriffe verteidigt, unabhängig vom Herkunftsland des Angreifers
- Partnerschaften mit mehreren Herausgebern und Marktvertretern, die uns einen schnellen Zugang zu Sicherheitsinformationen ermöglicht
- Ein beauftragter Überwachungsdienst (im Managed Service Modus), der für die Einhaltung internationaler Standards unerlässlich ist
- Verschiedene leistungsstarke Professional Services, welche auf Ihre Bedürfnisse angepasst sind
- Angemessene und maßgeschneiderte Überwachung Ihrer IP-Domains und IS-Software
- Sie haben einen direkten Ansprechpartner und eine Telefon-Hotline, für alle Fragen zum Thema Cybersicherheit und Schwachstellenmanagement

Kernthemen von AlliaCERT im Detail

Überwachung

- Veröffentlichung von Sicherheitshinweisen und -warnungen
- Schwachstellen und Zero-day-Analyse
- Malware Analyse
- Umfangreiche Meldungen zu Bedrohungen
- Nachrichten und Neuigkeiten im Newsletter
- Konforme Sicherheitshinweise: CVE, CVSS v3, CWE, CPE, Bugtrack
- Schwachstellen-Datenbank-Indizierung von bis zu 150.000 Produkten und Versionen
- Keine Begrenzung der Anzahl der zu überwachenden Produkte
- Durchsuchbare Newsletter in den Formaten HTML, PDF, XML und TXT
- Anpassung der Meldungen/Alarme und Newsletter (Profile, Häufigkeit des E-Mail-Empfangs, Kritikalität der Schwachstellen)
- Integriertes Workflow-Tool
- API-basierte Plattform (Application Programming Interface) zur Interaktion mit anderen Sicherheitstools (SIEM, Ticketing, Scanner)
- Malware-Analyse-Plattform
  - Signaturanalyse durch 47 antivirale Maschinen
  - Statische und Verhaltensanalyse von Malware
  - spezifische Analyse für Business-Master

Reaktion auf Vorfälle

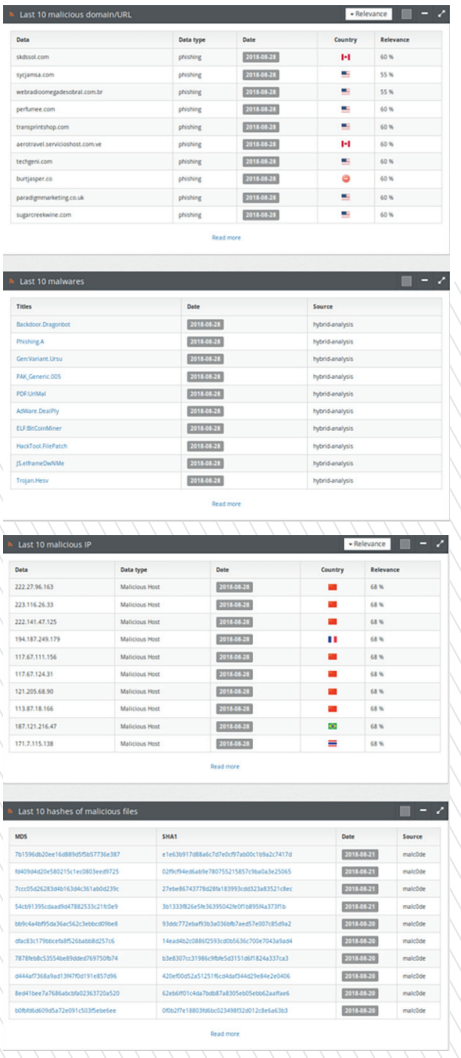
- Krisenmanagement und Unterstützung bei Großangriffen
- Begleitung und Unterstützung bei Sicherheitsvorfällen:
  - durch Viren (Ransomware, Trojaner)
  - durch Social-Engineering
  - durch Informationsleck
  - durch Phishing, Speer-Phishing
  - durch Windows-Intrusion
  - durch Unix-Intrusion
  - durch DDoS
  - durch böswilliges Netzwerkverhalten
  - durch Verunstaltung der Webseite
- Threat Intelligence Modul mit Zugriff auf relevante Kompromitierungsindikatoren (IP, Domains, MD5) und zur Suche nach der Reputation von Domains und IPs. Es werden verschiedenste Quellen hinzugezogen u.a. FIRST Partners, OSINT, etc.

Forensik/Untersuchung

- Forensische Post-mortem-Analyse
- hinsichtlich Betrug, internen Missbrauch
- hinsichtlich Informations-/Kreditkartendiebdiebstahl
- hinsichtlich Herunterladen oder Zugriff auf illegale Medien
- hinsichtlich Identitätsdiebstahl
- hinsichtlich Malware-Infektionen
- Erstellung von rechtlichen und technischen Unterlagen

AXIANS MASSGESCHNEIDERTE ZUSATZLEISTUNGEN MIT ALLIACERT:

- Informationsflüsse über Hackergruppen und Angriffstrends
- Informationen zu ausgefilterten Daten und Forschung zum Darknet
- Erkennung von falschen Anwendungen bei Stores (Google Play, Apple Store, etc.)
- Identifizierung von gezielten Angriffen (Überwachung von Domains, Websites und Client-IPs)
- gTLD und ccTLD Domainüberwachung, Typosquatting/Cybersquatting
- Überwachung sensibler Webseiten gegen die Verunstaltung/Verweigerung von Diensten/ XSS-Angriffen



Axians IT Security GmbH · Arndtstraße 25 · 22085 Hamburg
Tel.: +49 40 271661-0 · Fax: +49 40 271661-44 · E-Mail: info-itsecurity@axians.de · www.axians.de