Schneller Aufbau eines Security Operation Centers: mit CySAFA

Experience the commitment®

Security Operation Center (SOC) sind für das Management der Cyber Threat Intelligence unverzichtbar. Informationen aus dem Cyberraum werden im SOC gesammelt, aufbereitet, verarbeitet und analysiert, um eine effiziente Abwehr von Cyberangriffen zu ermöglichen. CySAFA ist ein erfolgreich erprobter, agiler Ansatz, um dem Nutzer in kürzester Zeit ein individuelles SOC zu liefern.

DIE HERAUSFORDERUNG

Ständig wachsende und sich weiterentwickelnde Bedrohungen im Cyberraum erfordern ein effektives und effizientes Management der Cyber Threat Intelligence. Angriffe müssen entdeckt und entsprechende Verteidigungsmaßnahmen eingeleitet werden; idealerweise lassen sich Attacken vorhersagen und entsprechend verhindern.

Hierzu benötigt man ein umfassendes und aktuelles Wissen über die gesamte eigene IT-Landschaft sowie die eigenen Schwachstellen. Diese Informationen zu sammeln, ist schon innerhalb aktueller IT-Systeme aufwändig. Bei bestehenden Legacy-Systemen handelt es sich um eine besondere Herausforderung, weil sie oftmals über keine standardisierten Schnittstellen verfügen.

In allen größeren IT-Organisationen bestehen in der Regel zahlreiche Datenfeeds, Analyse- und Visualisierungstools; viele sind historisch gewachsen und über mehrere Organisationseinheiten und zahlreiche geografische Grenzen hinweg verteilt. Für eine wirksame Cyberabwehr besteht die Anforderung, den Datenimport und die Fusion von allen Daten dynamisch und kostengünstig zu adaptieren. Dabei geht es auch darum, Import und Fusion an zukünftige, noch unbekannte Anforderungen anzupassen.

UNSERE ANTWORT

CGI hat im Auftrag des britischen Verteidigungsministeriums (MOD) die Cyber Situational Awarenes Fusion Architecture (CySAFA) entworfen und aufgebaut. Wir unterstützen das MOD kontinuierlich beim Betrieb und bei laufenden Anpassungen.

CySAFA ermöglicht es, große Datenmengen aus einer Vielzahl von Quellen zu empfangen, zu speichern und zu analysieren: So kann man die Situation optimal einschätzen und die richtigen Entscheidungen zur Abwehr von Cyber-Bedrohungen treffen. Dank der flexiblen Architektur lassen sich die speziellen Anforderungen des deutschen Geheimschutzes problemlos berücksichtigen.

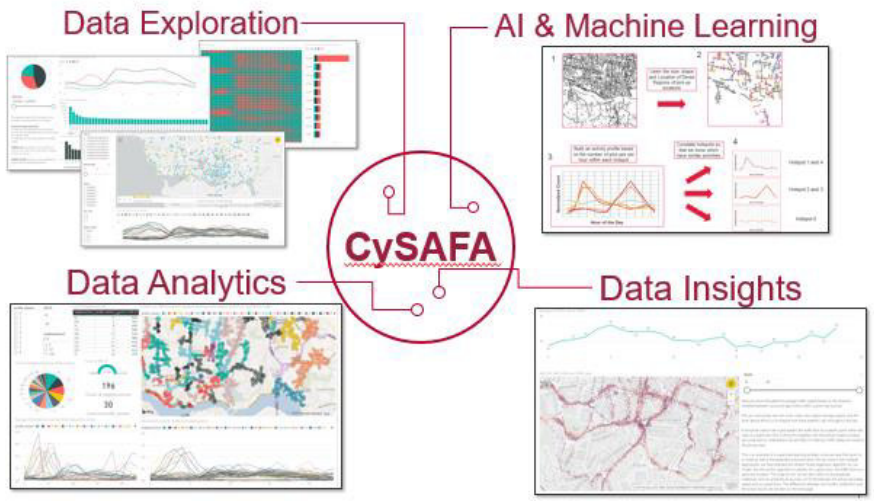
CYSAFA FEATURES

- Skalierbare, modulare Big-Data-Architektur
- Anbinden einer breiten Palette von Analyse- und Visualisierungstools
- Realisieren eines Datenaustausches über alle Sicherheitsebenen hinweg
- Aufheben der „Datensilos“
- Erfüllen der Anforderung des Geheimschutzes durch physische Trennung
- Extraktion mehrerer Daten- und Informationsquellen für jeden Stakeholder, angepasst an die jeweiligen Anforderungen
- Flexibles Anpassen der Import-Schnittstellen sowie der Analyse- und Visualisierungstools

de.cgi.com/cybersecurity

© 2020 CGI DEUTSCHLAND

CySAFA nutzt modulare COTS- und Open-Source-Komponenten und hat mit dem MOD erfolgreich einen agilen Entwicklungs- und Beschaffungsprozess umgesetzt. So können zukünftig benötigte Analysetools und Datenfeeds sehr schnell und effizient integriert werden.



CySAFA versteht sich als „Enabling-Architektur“, die es ermöglicht, das Potenzial künftiger Cyber-Defence-Konzepte zu realisieren. Dies beinhaltet auch das effektive Plug & Play von Datenfeeds und Analysetools bestehender und potenzieller Drittanbieter. CySAFA ist erweiterbar und ermöglicht die schnelle Integration zusätzlicher Fähigkeiten und Dienste, um in Zukunft eine noch bessere Cyber-Resilienz zu erreichen.

WARUM CGI?

Die Grenzen zwischen organisierter Kriminalität, Cyberkriminalität, Terrorismus, konventioneller und unkonventioneller Kriegsführung verschwinden zunehmend. Mit unserem Ansatz „Information Enabled Capability through Digital Transformation“ stellen wir sicher, dass Informationen ein kraftvoller Multiplikator für Tagesbetrieb und Einsatz sind und bleiben.

CGI gehört zu den sechs weltweit am schnellsten wachsenden Unternehmen im Bereich Cybersecurity. Täglich werden durch uns 43 Millionen Cyberattacken auf Militär- und Geheimdienstnetzwerke und -infrastrukturen abgewehrt.

ÜBER CGI

CGI ist ein globaler Dienstleister für IT und Geschäftsprozesse. Wir wurden 1976 gegründet und verfügen heute an 400 Standorten in 40 Ländern über insgesamt 77.500 Mitarbeiter.

Für unsere Kunden sind wir weltweit vor Ort – mit strategischer IT und Business Beratung, Systemintegration, Managed IT, Business Process Services und Intellectual Property auf Top-Niveau.

Wir unterstützen unsere Kunden dabei, laufende Investitionen besser zu nutzen und gleichzeitig neue digitale Technologien und Business-Strategien einzusetzen, durch die sich optimale Lösungen entlang der gesamten Wertschöpfungskette realisieren lassen.

Im Hinblick auf Zeit- und Budgettreue bekommen wir auf Grund unserer strikten Lieferdisziplin regelmäßig Bestnoten. Dazu konnten wir in den Kundenzufriedenheitsanalysen der vergangenen zehn Jahre kontinuierlich mehr als neun von zehn möglichen Punkten erzielen.

Für weitere Informationen kontaktieren Sie uns unter info.de@cgi.com oder besuchen Sie uns auf: de.cgi.com/cybersecurity

de.cgi.com/cybersecurity

© 2020 CGI DEUTSCHLAND