certego

Your partner against cybercrimes

INTELLIGENCE DRIVEN DETECTION AND RESPONSE

SERVIZI GESTITI DI CYBER SECURITY

L'ATTUALE CONTESTO DELLA CYBER SECURITY

Indipendentemente dalla dimensione e dal settore merceologico di riferimento, **oggi ogni organizzazione può essere target di attività di cyber crime.**

La criminalità informatica ha assunto un carattere globale di industria ben organizzata, con una specializzazione e una divisione dei compiti molto spinta che permette a questo ecosistema di generare profitti consistenti derivanti dalla monetizzazione di tutti gli asset coinvolti (dati finanziari e personali, informazioni sensibili, sistemi e dispositivi violati utilizzati per attività illecite, etc.).

L'utilizzo di tecnologie tradizionali, come ad esempio firewall, antivirus, log management e SIEM, rappresenta una buona prima linea di difesa ma non è più sufficiente per proteggere adeguatamente un'organizzazione da tutte le minacce in ambito cyber.

Oggi, una organizzazione che intenda proteggersi efficacemente da questo tipo di minacce deve comprendere, oltre alla capacità di prevenzione, anche le funzioni di **Rilevamento** e **Risposta** agli incidenti.

certego

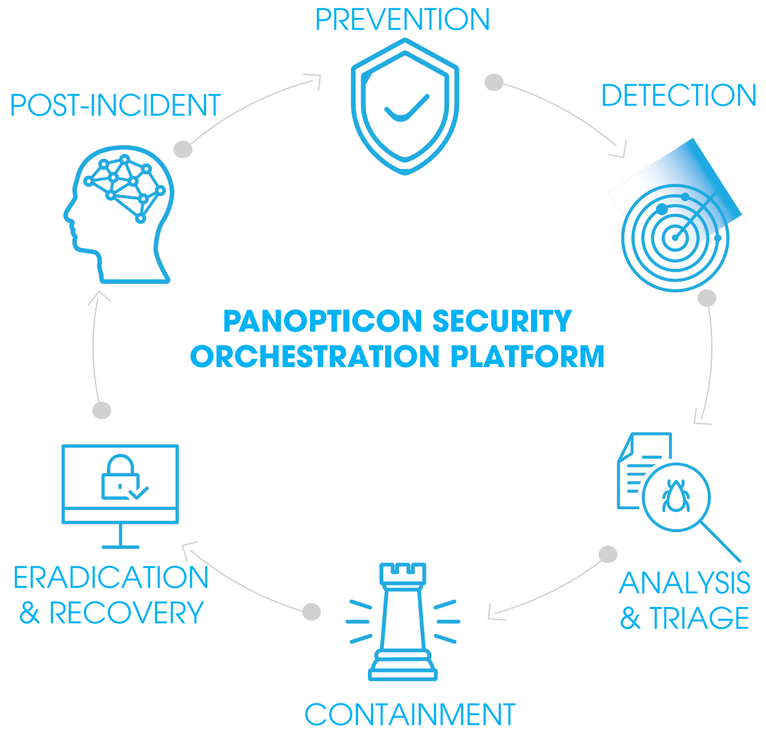
CYBER SECURITY SERVICES CERTEGO

La suite di servizi Certego di **Managed Detection & Response** è composta da un insieme di soluzioni che permettono il monitoraggio, l'identificazione e la gestione di condizioni di rischio legate ad attacchi e ad attività di cyber crime.

Certego ha sviluppato una piattaforma proprietaria di **Security Orchestration, Automation and Response** denominata Certego **PanOptikon®**, che risulta abilitante e a supporto dei processi di raccolta e analisi degli eventi, identificazione e investigazione di possibili condizioni di anomalia e di gestione di eventuali incidenti di sicurezza identificati a seguito di analisi approfondite.

I servizi Certego si basano sulle funzioni di **Computer Security Incident Response Team (CSIRT)** erogate in modalità as-a-service.

Il CSIRT Certego è composto da un team di risorse altamente specializzate e dedicate al rilevamento proattivo di minacce e alla risposta agli incidenti di sicurezza.



Opera 24/7/365 con l'obiettivo di tradurre la complessità di un problema di Information Security in attività sistemistiche che l'organizzazione IT del cliente sia in grado di comprendere e gestire, prevenendo impatti sul business.

Certego è in grado di fornire al cliente un supporto qualificato e competente per **rilevare** e **contenere** la propagazione di un attacco, **ripristinare** i sistemi coinvolti e **identificare** le "root-cause" degli eventi fornendo indicazioni specifiche, con l'obiettivo di **aumentare la resilienza** dell'infrastruttura a minacce della stessa tipologia.

certego

RILEVAMENTO

Il **monitoraggio continuo** del traffico di rete e degli eventi di sicurezza viene effettuato tramite soluzioni tecnologiche che, utilizzando intelligenza artificiale e logiche di correlazione proprietarie, monitorano e notificano potenziali condizioni di anomalia.

Il monitoraggio coinvolge poi l'attività costante di **analisti di cyber security** Certego altamente specializzati e con comprovate competenze in ambito Security Operation Center.

L'IRT Certego può essere coinvolto 24/7/365 a seguito di rilevazione di particolari di anomalia.

ANALISI

La capacità di rilevare in tempo le minacce di sicurezza e i tentativi di intrusione rappresenta un vantaggio enorme per qualunque tipo di organizzazione.

Questo è uno degli obiettivi principali del servizio di **MDR** Certego: essere quindi in grado di identificare un attacco in corso che ha già oltrepassato eventuali sistemi di prevention e **predisporre eventuali meccanismi di risposta ih tempi rapidi**, prima che la minaccia possa causare dei danni al business dell'organizzazione.

Avere **evidenze chiare di ciò che sta succedendo all'interno** dell'infrastruttura e possedere competenze tecniche specifiche per affrontare queste condizioni, rappresentano i requisiti fondamentali per essere in grado di reagire nel modo migliore.

certego

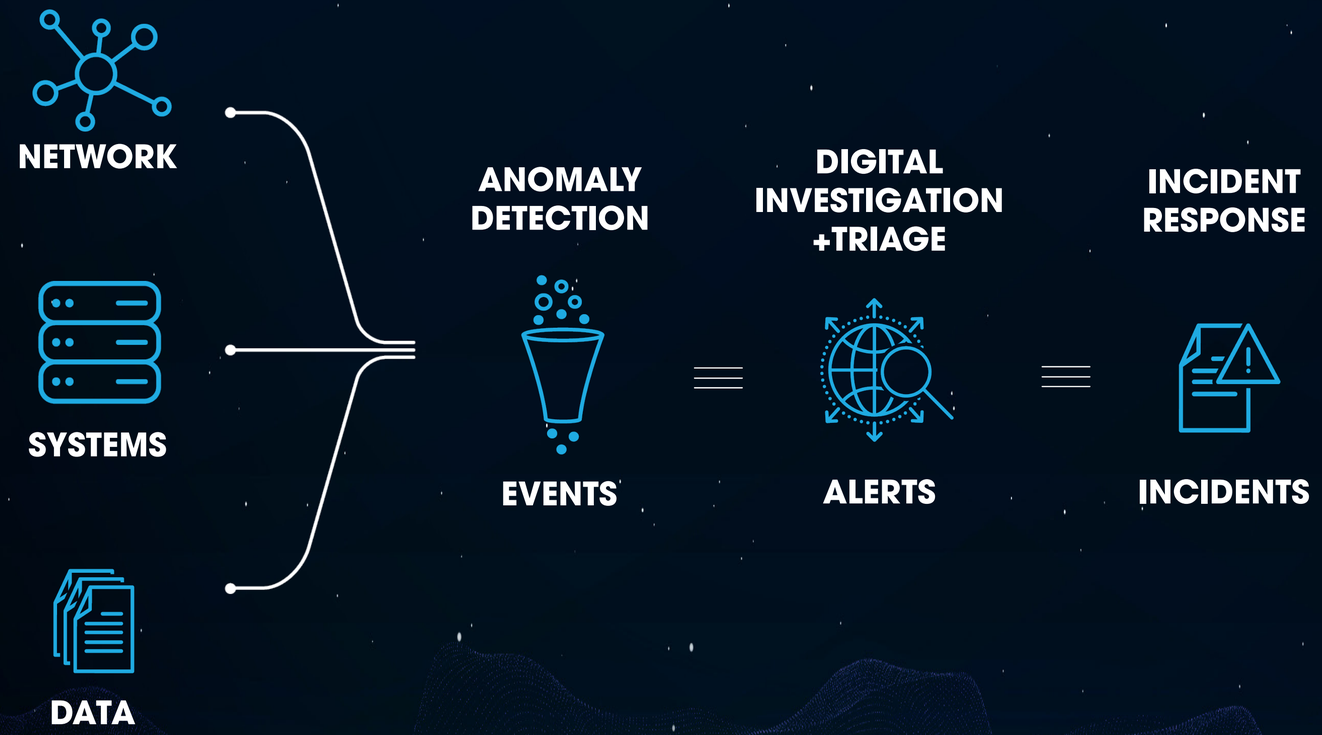
RISPOSTA

L’attività di Incident Response a seguito di un cyber attacco richiede una forte preparazione tecnico organizzativa e una esperienza approfondita nella gestione di situazioni che possono risultare molto critiche per le organizzazioni che devono affrontarle.

L’Incident Response Team Certego, grazie a una esperienza pluriennale in situazioni di questo tipo, mette a disposizione del cliente una serie di **procedure di risposta ben definite per contenere le minacce** che possono avere impatti sul business.

Laddove ritenuto necessario, per contenere la diffusione di una minaccia estremamente pericolosa, Certego può anche consigliare al cliente di applicare delle procedure di lockdown temporaneo, con l’obiettivo di preservare asset e dati di business esposti a elevato rischio.

*



CERTEGO PANOPTIKON SECURITY ORCHESTRATION, AUTOMATION & RESPONSE PLATFORM

L'erogazione del servizio Certego di Managed Detection & Response avviene attraverso una componente trasversale che è rappresentata dalla piattaforma di Security Orchestration, Automation and Response "Certego **PanOptikon®**" e una serie di **moduli di Detection e di moduli di Response attivabili opzionalmente in base alle specifiche caratteristiche ed esigenze dell'organizzazione** che l'adotta.

La piattaforma è abilitante per l'erogazione di tutti i servizi Certego integrati e permette l'interazione diretta tra IT del cliente e IRT Certego per favorire l'**orchestrazione dei processi e la gestione completa di un incidente di sicurezza** durante tutte le fasi previste.

Certego PanOptikon® dispone inoltre di un **Web Portal** utilizzato per il tracciamento di tutte le attività di analisi e gestione degli incidenti e l'interazione tra il team IT del cliente e l'IRT Certego.

PANOPTIKON SECURITY ORCHESTRATION PLATFORM
(DETECT - VALIDATE - RESPONDE)

I MODULI DI DETECTION PERMETTONO DI OTTENERE LA VISIBILITÀ NECESSARIA ALL'INTERNO DELL'INFRASTRUTTURA DEL CLIENTE, CON LO SCOPO DI IDENTIFICARE EVENTUALI CONDIZIONI DI ANOMALIA E AVVIARE LE PROCEDURE DI INCIDENT RESPONSE.

I MODULI DI RESPONSE CONSENTONO DI AUTOMATIZZARE ALCUNE SPECIFICHE ATTIVITÀ CON L'OBIETTIVO DI RIDURRE AL MASSIMO I TEMPI DI RISPOSTA DURANTE LA FASE DI RESPONSE DI UN INCIDENTE DI SICUREZZA.

certego

Moduli di DETECTION

NETWORK DETECTION MODULE

L'abilitazione e la configurazione di questo modulo permette di effettuare l'**analisi del traffico, tramite l'utilizzo di Network Sensor** (fisici o virtuali) forniti in comodato d'uso da Certego, e la **raccolta e correlazione di log ed eventi** generati da sistemi e apparati di sicurezza presenti nell'infrastruttura del cliente (firewall, antivirus, domain controller, server DNS/DHCP, etc.).

ENDPOINT DETECTION MODULE

L'attivazione di questo modulo, tramite l'installazione di un **agente di telemetria**, permette di ottenere un **livello di visibilità massima sugli endpoint**, consentendo di monitorare le attività di processi e servizi all'interno dei sistemi e identificare particolari condizioni di anomalia grazie anche all'integrazione dei servizi di Threat Intelligence Certego.

CLOUD PROTECTION MODULE

L'abilitazione e la configurazione di questo modulo permette di ottenere le medesime funzionalità del modulo di Network Detection all'interno del perimetro cloud del cliente e permette l'**acquisizione e il processing dei log nativi generati dalle logiche proprietarie delle principali piattaforme Cloud** (Amazon Web Services, Google Cloud Platform, Microsoft Azure).

VULNERABILITY DETECTION MODULE

Questo modulo permette l'abilitazione di un servizio di Continuous Vulnerability Assessment basato sull'utilizzo di scanner specifici, per la **ricerca continuativa di vulnerabilità su sistemi e applicazioni**.
L'attivazione di questo modulo permette di avere una indicazione relativa allo stato di sicurezza dei sistemi e attiva eventuali procedure di incident response, in tempi rapidi, in caso di rilevazione di vulnerabilità particolarmente critiche.

certego

Moduli di RESPONSE

FIREWALL TACTICAL RESPONSE MODULE

L'abilitazione di questo modulo consente l'integrazione tra il Network Sensor Certego e i firewall del cliente, per l'**implementazione automatizzata di regole di blocco che si rendono necessarie a fronte del rilevamento di uno specifico attacco**.

ENDPOINT TACTICAL RESPONSE MODULE

Per alcune tipologie di incidenti informatici, la **rapidità della risposta** (MTTR - Mean Time To Respond) risulta determinante ai fini del contenimento degli impatti e delle conseguenze dell'attacco.
Obiettivo del modulo Endpoint Tactical Response è di **permettere al team IRT Certego, in accordo con il cliente, di intervenire direttamente sugli endpoint**, applicando rapidamente specifiche azioni di contenimento, con l'obiettivo di bloccare o rallentare le attività dell'attaccante.

ITSM INTEGRATION MODULE

Il modulo ITSM permette l'**integrazione bidirezionale della Piattaforma Certego PanOptikon con i principali sistemi di ticketing** presenti sul mercato per facilitare la gestione dell'incidente di sicurezza a tutti gli attori coinvolti nel processo di incident response.

certego


270K
NETWORK SENSORS USED
35K
ENDPOINT SENSORS INSTALLED
1M+
ASSETS MONITORED
ALARMS DETECTED PER YEAR (2022)
110K
10K
INCIDENTS MANAGED PER YEAR (2022)

certego

CHI SIAMO

Certego Srl è la società del Gruppo VEM sistemi specializzata nell'erogazione di servizi di sicurezza IT gestita e di contrasto al cyber crime.

Nata nel maggio 2013, con sede a Modena, Certego è un fornitore innovativo di servizi di Cyber Security, connotato da un modello di business e da un'offerta completamente **unici ed esclusivi nel panorama italiano** e da un team di analisti con esperienza pluriennale nel campo dell'analisi delle frodi online e degli attacchi informatici.

Rispetto all'approccio tradizionale, basato prevalentemente sull'adozione di tecnologie di prevenzione e che oggi non risulta essere di essere più sufficiente per contrastare le minacce cyber, il modello di protezione proposto da Certego permette di **incrementare il livello complessivo di resilienza delle organizzazioni** che lo adottano, integrando competenze specifiche di Incident Response di elevato livello e capacità di identificazione, orchestrazione e gestione delle minacce.

Il servizio di Managed Detection & Response erogato da Certego protegge attualmente 170 clienti presenti in Italia, in Europa e nel resto del Mondo, attivi trasversalmente su tutti i principali settori merceologici.

certego

CERTEGO
INCIDENT RESPONSE TEAM

Tutte le attività di analisi e investigazione degli incidenti sono condotte dal team di specialisti di Incident Response Certegodi Certego con esperienza pluriennale nel campo delle intrusioni e delle frodi informatiche in possesso delle principali certificazioni nel campo della gestione degli incidenti informatici:

- ISC2 Certified Information Systems Security Professional (CISSP)
- GIAC Certified Perimeter Protection Analyst (GPPA)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Reverse Engineering Malware (GREM)
- ISECOM OSSTMM Professional Security Tester (OPST)

Nello svolgimento delle attività di gestione degli incidenti di sicurezza, l'IRT Certego adotta le seguenti raccomandazioni/standard:

- Computer Security Incident Handling Guide, NIST© Special Publication 800-61 Rev. 2
- ISO/IEC 27035 Information technology —Security techniques — Information security incident management
- CMU Handbook for Computer Security Incident
- Response Teams (CSIRTs)

CERTIFICHE E QUALIFICHE

- ISO/IEC 27001:2017ISO/2017 da Febbraio 2018
- ISO/IEC 9001:2015ISO/2015 da Febbraio 2019
- Autorizzati all'uso del marchio " CERTCERT" dal Dicembre 2014
- FIRSTFIRST.ORG: Membro da Novembre 2017
- EC3EC3 Europol Supporting Partner da Aprile 2017
- Trusted IntroducerTrusted Introducer: Listed da Luglio 2016. Accredited da Agosto 2019
- ENISA CSIRTENISA CSIRT Inventory
- Riconosciuti come Regional Player da Gartne nel 2015 e 2017 - Worldwide Threat Intelligence Services Competitive Landscape

CYBERSECURITY™ MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

certego

CERTEGO S.R.L.
Via Ferruccio Lamborghini, 81
41121 Modena (MO) - Italy
certego.net - info@certego.net