Visura
TINEXTA GROUP

Altri servizi

# Cryptolocker DEFENSE

Soluzioni Cyber Security

Versione 1.0 giugno 2023

www.visura.it

# Sommario

# Cryptolocker Defense

Cryptolocker Defense è un servizio fornito da Swascan, protagonista attiva e parte integrante del nuovo polo nazionale di Cybersecurity costituito da Tinexta. Questo nuovo ruolo, nello scenario Cyber Italiano, la pone come elemento distintivo nel mercato, garantendo un approccio innovativo, efficace ed efficiente. Swascan mette a disposizione a tutti i clienti, privati e pubblici, un supporto strutturato e completo per la Cyber Transformation potendo disporre, non solo delle proprie tecnologie e competenze, ma anche delle migliori soluzioni e protocolli per la difesa dell'identità digitale.

Cryptolocker Defense è un servizio che si snoda su diverse componenti

- EDR – Endpoint Detection Response
- SOC as a service

**EDR (Endpoint Detection & Response)**

Il servizio EDR garantisce la protezione degli asset aziendali definiti dal Cliente (che indicherà il numero di dispositivi su cui vuole attivare la soluzione) grazie all'installazione di Agent di endpoint detection and response.

L'obiettivo è quello di consentire al Team Security di identificare le attività malevole tra il normale comportamento degli utenti. Utilizzando strumenti di analisi basati sull'intelligenza artificiale, le soluzioni EDR sono in grado di identificare modelli e rilevare anomalie.

**SOC as a SERVICE**

Le continue minacce provenienti dal web, come per esempio, ma non limitatamente a *"impersonificazione e furto di identità, furto di dati sensibili (brevetti, carte di credito, fornitori, clienti, dati personali etc.), modifiche non autorizzate, condivisione di materiale non autorizzato ed attacchi alla reputazione aziendale",* spesso vengono realizzate attraverso attacchi mirati ed opportunistici. La soluzione SOC as a Service ha come principale obiettivo quello di difendere attivamente il perimetro informatico aziendale e di offrire un pronto intervento qualora un attacco giungesse a termine.

Riconoscere una reale minaccia richiede un costante studio ed un solido background in reverse engineering, malware writing, malware evasion e communication protocols. Ogni minaccia è differente ed unica per natura; per questa ragione non può possedere lo stesso "peso" in contesti differenti tra loro. Una delle principali caratteristiche della soluzione SOCaaS è la capacità di distinguere le minacce reali in funzione al contesto in cui esse vengono analizzate.

La mitigazione di una minaccia ha un costo implicito compreso nel canone, che è proporzionale al numero di ore necessarie per eseguire la mitigazione stessa e al numero di persone fisiche coinvolte. Il team di analisti conosce molto bene le differenti famiglie di Malware e pone particolare attenzione alla tipologia di azienda cliente e al suo organigramma al fine di eseguire interventi mirati e localizzati per garantire business continuity lean process mitigation. Il team di analisti offre soluzioni di mitigazione e pronto intervento ove ne risulti necessario.
Il servizio è strutturato nelle seguenti attività di Cyber Security che vengono attivate in base o alla tipologia di minaccia o su base temporale:

- Monitoring & Allarme;
- Response;
- Threat Hunting;
- Reporting.

## Benefici

| **Manage & Reduce Risk** | **Compliance&Standard** | **Cost Saving** |
|---|---|---|
| Sicurezza Proattiva<br>• Tecnologie di sicurezza preventiva e proattiva;<br>• Un centro di competenza Cyber dedicato;<br>• 24 ore su 24 e attivo 7 giorni su 7. | *Law Compliance*<br>• GDPR<br>• AGID<br><br>*Standard*<br>• ISO 27001<br>• NIST<br>• NIS<br>• 231<br><br>*Best Practice*<br>• Owasp<br>• OSSTMM | • Efficienza ed efficacia dei sistemi di Cyber Security;<br>• Gestione degli attacchi e degli incidenti cyber aziendali;<br>• Protezione della Business Continuity. |

## Livelli di Servizio

### *Fase1: Monitoring & Allarme*

Attraverso l'attività di monitoring, il team SOCaaS prende in carico tutte le **segnalazioni di allarme** generate dagli agent EDR installati nell'infrastruttura. Ogni allarme è oggetto di un processo di assessment e analisi. Questa fase ha l'obiettivo di determinare se la segnalazione dell'evento rientra in una delle seguenti casistiche:

- Evento malevolo
- Evento anomalo

**Entro 1h (1 ora)** dalla generazione dell'allarme e dalla conferma da parte del team SOCaaS che l'attività è malevola, il Cliente riceve una email con i dettagli preliminari sull'attività monitorata.

### *Fase 2: Response*

In fase di attivazione del servizio, verrà richiesto al Cliente la compilazione di un questionario per determinare le regole d'ingaggio. In casi particolari potrebbe essere richiesta una call di approfondimento.

In base alle regole di ingaggio, Il SOCaaS opererà come segue:

Se il Cliente ha definito, a livello di regole di ingaggio, di bloccare automaticamente gli eventi identificati come malevoli, i sistemi saranno configurati per bloccare i processi e i task oggetto dell'allarme. In questo caso la segnalazione viene considerata chiusa.

In caso contrario, in assenza di indicazioni del cliente, il team SOCaaS continua a monitorare ciascun evento malevolo fino a 5 ore o fino a quando l'attività dell'attaccante non inizia ad espandersi. Questa fase è cruciale per raccogliere tutta la Threat Intelligence e le informazioni su:

- Tattiche;
- Tecniche;
- Procedure e metodologie adottate.

Questi dati vengono utilizzati nelle fasi successive per attivare un Piano di Risposta completo ed efficace, che prevede quali azioni saranno intraprese a seguito dell'analisi dell'accaduto. Le azioni possono essere, ad esempio, il blocco del processo, il download e creazione whitelist in caso di falso positivo oppure la blocklist in caso malevolo.

Nella fase di analisi il team inizierà proattivamente a interrogare l'intera infrastruttura e a acquisire tutti i dati necessari per capire la causa principale dell'attacco e per scoprire qualsiasi altro endpoint potenzialmente compromesso.

Una volta che le fasi di raccolta delle informazioni sulle minacce di threat hunting sono terminate e tutte le prove necessarie sono state raccolte, gli endpoint vengono sanificati e messi in modalità di

remediation, cioè di rimozione del malware e, in casi estremi, di isolamento del dispositivo. Il piano di risposta viene attivato e vengono create tutte le politiche di blocco necessarie. Gli endpoint che non possono essere sanificati per motivi tecnici o per richiesta del cliente vengono isolati se si desidera un'ulteriore analisi.

*Fase 3: Threat Hunting*

Si tratta di un'attività continuativa di ricerca e analisi. Non tutte le minacce possono essere identificate automaticamente; in alcuni casi l'attaccante è in grado di imitare l'attività di un utente reale, come ad esempio nel caso di un certificato rubato o di una password che garantisce l'accesso a un sito VPN od a un servizio interno. In questo caso, le soluzioni EDR non possono fornire informazioni esaurienti e sufficienti (il contesto sull'attività iniziata al di fuori del loro ambito). Per identificare situazioni simili, vengono utilizzate campagne di Threat Hunting.

Il Threat Hunting è un processo che viene eseguito continuamente e sfrutta la conoscenza dell'infrastruttura del Cliente per identificare e isolare potenziali minacce. Questa attività viene svolta sia attraverso la Threat Intelligence interna, come la ricerca di indicatori conosciuti come parte di attori maligni attivi, sia attraverso la ricerca comportamentale avanzata, in cui vengono rilevati comportamenti nuovi o insoliti.

Se viene identificata una potenziale minaccia il Cliente riceve una email con i dettagli della minaccia (**FASE 1**).

*Fase 4: Reporting*

Entro 72 ore tutte le informazioni acquisite durante le attività forensi post-breach e Threat Hunting, vengono raccolte in un report e consegnate al Cliente. Gli Incident Report contengono tutti gli IOC necessari, gli indicatori comportamentali, la ricostruzione del percorso dell'attaccante e tutto ciò che è necessario per comprendere l'evento e fornire informazioni attivabili al fine di permettere al Cliente di rafforzare le proprie difese in quella specifica area.

## Team Impiegato

Di seguito una descrizione di sintesi a titolo esemplificativo:

| Figura Professionale | Job Description |
|---|---|
| **SOC Coordinator** | Oltre 10 anni di esperienza nel campo della Cyber Security. Una esperienza di circa 5 anni come Responsabile SOC di enti Ministeriali e Militari. Ha avuto modo di seguire diverse attività definendo e indirizzando delle linee guida strategiche in merito alla sicurezza delle informazioni, sviluppando politiche di sicurezza, si è inoltre occupato dell'amministrazione e gestione |

| | |
|---|---|
| | dei Firewall di sicurezza perimetrale, e il monitoraggio e la gestione di un sistema di intrusion Prevention System, esecuzione di Pentration Test Vulnerability Assessment sulla rete. Durante la sua carriera ha conseguito diverse certificazioni legate alla sicurezza tra cui: GIAC, Comptia+, GPEN, CCSA R76, CCSE R77, ESFE. |
| **Analista SOC** | Specialista SOC con esperienze in Sicurezza Informatica e delle reti da almeno 3 anni. Gestione firewall ed implementazione policy, esperienze di operatività su sistemi di Intrusion Detection, esperienze nell'utilizzo di apparati SIEM per la correlazione di eventi. Gestione di apparati per la sicurezza email. Gestione di sistemi di Vulnerability Management. Gestione di sistemi EDR. Esperienze in ambito di gestione sistemi e ambienti di virtualizzazione, ambienti Unix/Windows. |