Catalogo Servizi SOC di Exprivia

Migliorare consapevolezza e competenza per ridurre il rischio di un incidente di CyberSecurity e limitarne i danni conseguenti

future. perfect. simple.

Sommario

Prefazione

La digitalizzazione dei servizi, l'interconnessione degli stessi, l'irreversibilità del processo di trasformazione ed infine la sproporzione tra chi attacca e chi difende suggerisce la necessità di **investire in cybersecurity a garanzia di una crescita sostenibile**.
Il mondo della cybersecurity è al tempo stesso estremamente diversificato e richiede investimenti ottimizzati e costanti nel tempo ed ottimizzati al fine di ridurre il rischio complessivo.
Exprivia offre ai suoi clienti la possibilità di scegliere il modello di delivery più opportuno, lasciando al cliente la possibilità di decidere se utilizzare il servizio on-premises o erogato dal Security Operation Center situato a Molfetta.

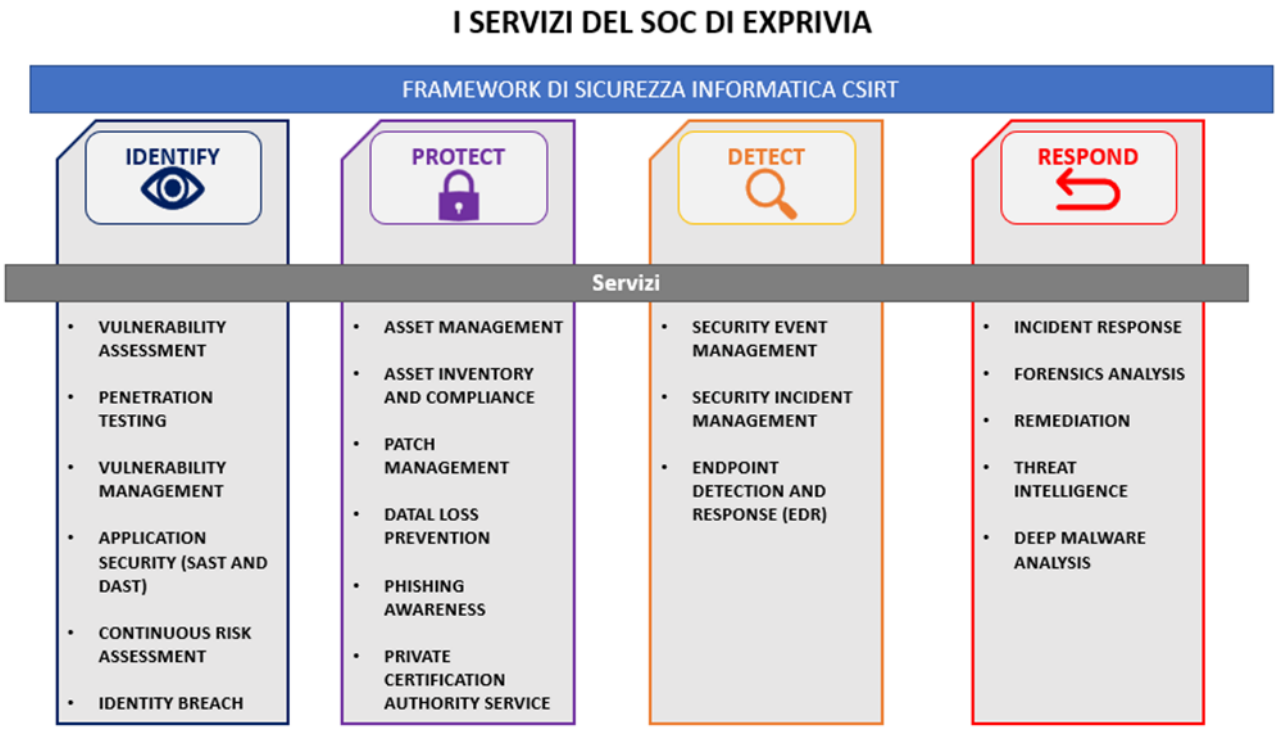
Figura 1- SOC di Exprivia - Molfetta

Certificazioni

Exprivia è certificata **ISO 27001** dal 2012 perciò anche i servizi che eroga, come nel nostro caso il Security Operation Center, sono certificati.
Inoltre, Exprivia nel 2020 ha esteso le certificazioni alle line guida **ISO 27017 e ISO 27018** per i servizi erogati in cloud in modalità Software as a service (SaaS).
Quindi, anche la modalità di erogazione SOC-as-Service è certificata. Nel 2022 il Cloud Security Alliance (CSA) ha processato e approvato il Security Self-Assessment da Exprivia sottoposto, ottenendone la certificazione del proprio SOC **CSA STAR Level One.**
Inoltre, grazie al suo programma di formazione, il Gruppo Exprivia ha già ottenuto più di 2500 certificazioni professionali in diversi domini e tecnologie, come CISCO, SAP, ORACLE, MICROSOFT, CyberArk, ITIL, Scrum Agile, IBM, SOPHOS, CY4GATE, RADIFLOW, HCL Appscan, Guardicore, Certified Ethical Hacker (CEH) e CISP.

Servizi erogati dal SOC

I servizi offerti di identify, protect, detect e respond si basano sul **Computer Security Incident Response Team (CSIRT) framework.**



Security Monitoring

Il servizio di Security Monitoring fornisce una sicurezza interna e perimetrale efficiente 24 ore su 24 con monitoraggio in tempo reale, correlazione degli eventi e analisi dell'infrastruttura del cliente e delle applicazioni critiche per garantire che la minaccia informatica sia gestita in modo proattivo e gli attacchi mitigati.
Il servizio comprende:

- **SECURITY EVENT MANAGEMENT:** con questa attività offriamo la gestione degli eventi di sicurezza (SEM) cioè il processo di identificazione, raccolta, monitoraggio e segnalazione degli eventi relativi alla sicurezza in un software, sistema o ambiente IT. Effettuiamo, quindi, la registrazione e la valutazione degli eventi aiutando gli amministratori di sicurezza o di sistema ad analizzare, regolare e gestire l'architettura, le politiche e le procedure di sicurezza delle informazioni.

- **MONITORING, DETECTION and EVENT ANALYSIS:** questa attività ci consente di eseguire la scansione della rete 24 ore su 24, 7 giorni su 7 per segnalare eventuali anomalie o attività sospette. Il monitoraggio della rete permette al nostro SOC di essere immediatamente informato delle minacce emergenti, offrendo le migliori possibilità di prevenire o mitigare i danni. Gli strumenti di monitoraggio possono includere un SIEM o un EDR. Gli eventi raccolti vengono poi analizzati e correlati al fine di generare degli alert al team di livello 1 del SOC.

- **SECURITY INCIDENT MANAGEMENT:** al livello 2 del SOC svolgiamo le operazioni di Incident Response (IR) in cui sono coinvolti analisti di sicurezza; i membri di questo team, sono responsabili di analizzare le segnalazioni del livello 1 e organizzare le operazioni di remediation.

- **SECURITY INCIDENTS ANALYSIS:** prendiamo carico di svolgere l'analisi di un eventuale incidente. In primo luogo è svolta dal team SOC di livello 1 che riceve un primo feedback di un incidente avvenuto, ed esso deciderà se occuparsi in prima persona della gestione della problematica o dirottare la richiesta verso il team di livello 2 al fine di collaborare alla risoluzione dell'incidente.

Security Assessment

Per adattarsi a molteplici esigenze, l'attività di Security Assessment è composta dai seguenti moduli:

- **VULNERABILITY MANANGEMENT:** garantiamo l'attività ciclica e completamente automatizzata mirata a identificare, classificare, dare priorità, rimediare e mitigare le vulnerabilità. Questa attività ciclica garantisce un continuo controllo sul sistema in maniera che una vulnerabilità, una volta risolta, non possa ripresentarsi nuovamente.

- **VULNERABILITY ASSESSMENT:** fa riferimento all'attività di sicurezza rivolta ad individuare tutte le eventuali vulnerabilità dei sistemi e delle applicazioni di una rete, attraverso una loro identificazione e valutazione che tenga in considerazione gli obiettivi di business e che non infici alla continuità delle operazioni. L'attività di Vulnerability Assessment può essere eseguita sia dall'interno che dall'esterno della rete aziendale, consentendo di simulare diversi scenari che potrebbero verificarsi in un'azienda. Output dell'attività è il report finale contenente le vulnerabilità individuate con relative azioni rimediali, che se opportunamente implementate, garantiscono una sicurezza maggiore e un sistema più sicuro.

- **PENETRATION TESTING**: l'attività, rappresenta una vera e propria simulazione di attacco hacker e permette di misurare il livello di sicurezza infrastrutturale, il grado di consapevolezza dei problemi di sicurezza da parte dell'azienda, e il suo livello di Detection & Reaction. Questi tipi di test vengono di solito eseguiti mediante tecnologie manuali o automatizzate con l'obiettivo di compromettere volutamente i sistemi. La loro esecuzione avviene successivamente ad un confronto con il cliente e

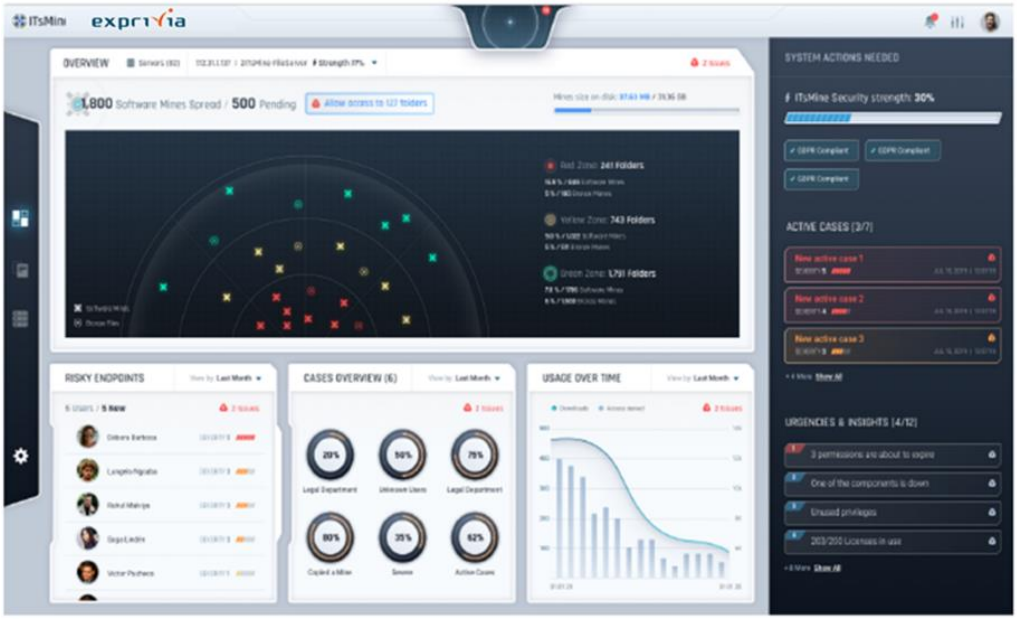
relativa autorizzazione. A seguito del Penetration Test viene consegnato un report che descrive le vulnerabilità identificate e le tecniche utilizzate per violare il sistema, insieme alle azioni rimediali necessarie da implementare per colmare le debolezze individuate.

- **APPLICATION SECURITY (SAST e DAST)**: effettuiamo analisi statica (SAST) e dinamica (DAST) del codice con lo scopo di individuare vulnerabilità. Un'analisi di tipo SAST o Static Application Security Testing è nota come «white box testing». Essa consente agli sviluppatori di individuare le vulnerabilità della sicurezza nel codice sorgente dell'applicazione inizialmente, nel ciclo di vita dello sviluppo del software e quindi prima dell'esecuzione dell'applicazione. L'analisi DAST o Dynamic Application Security Testing è nota anche come «black box testing». Essa può rilevare vulnerabilità e punti deboli di sicurezza in un'applicazione in esecuzione. Vengono impiegate tecniche di injection per identificare vulnerabilità di sicurezza comuni come ad esempio SQL injection e varie tecniche di scripting. A seguito delle scansioni viene consegnato un report che descrive le vulnerabilità identificate e come risolverle.

Threat Prevention

L'attività di Threat Prevention è l'insieme delle pratiche per cercare di limitare e rendere sicuro il perimetro aziendale che potrebbe risultare in qualche modo vulnerabile. Le attività che forniamo sono:

- **DATA LOSS PREVENTION**: forniamo ai clienti tecniche e sistemi che identificano, monitorano e proteggono i documenti in uso, i documenti in movimento nella rete e quelli a riposo all'interno o all'esterno dell'azienda, con l'obiettivo di individuare e prevenire l'uso illecito di informazioni riservate. La nostra soluzione, oltre ad effettuare l'analisi del comportamento e delle tecniche di inganno, protegge e garantisce lo svolgimento di tutte le fasi dei dati digitali senza richiedere nessun agent endpoint permanente, mantenendo, quindi, inalterata la produttività dei dipendenti.



- **ASSET MANAGEMENT**: è l'attività che si occupa della gestione degli asset aziendali in modo da ottimizzare il rendimento ponderando anche eventuali rischi. Gestiamo, perciò, l'intero ciclo di vita

degli asset IT, dall'installazione alla dismissione garantendo così sistemi sempre all'avanguardia riducendo il rischio di minacce.

- **ASSET INVENTORY, COMPLIANCE E PATCH MANAGEMENT**: sono classificati tutti gli asset e vengono gestite in automatico tutte le patch rilasciate in modo da tenere il sistema sempre aggiornato perciò privo di vulnerabilità note. Quindi, garantiamo la gestione degli endpoint, che consente ai team IT e ai team Security di automatizzare completamente la gestione e la riparazione, sia essa in locale, virtuale o cloud, indipendentemente dal sistema operativo, dalla posizione o dalla connettività. Tutto ciò in tempi molto ridotti e assicurando che tutti gli endpoint siano aggiornati e conformi.

- **PRIVATE CERTIFICATION AUTHORITY SERVICE:** forniamo ai clienti una soluzione PKI completa e totalmente gestita con l'obiettivo di ridurre i problemi associati alla creazione e alla gestione della PKI interna. Inoltre, il nostro servizio permette di mantenere conformità dei certificati senza costi elevati. I certificati che vengono forniti sono per:
    - Siti Intranet;
    - VPN o wireless authentication;
    - Autenticazione del dispositivo;
    - Dispositivi mobile o BYOD;
    - Internet of Things (IoT);
    - Protezione delle comunicazioni tra i servizi interni.

- **EXTENDED DETECTION AND RESPONSE (XDR):** Exprivia XDR Service è gestito da tecniche di Machine Learning per l'assegnazione di priorità agli eventi sospetti. Riesce, pertanto, a rilevare rapidamente e accuratamente ogni minaccia, con una visibilità massima sull'intera organizzazione, dai singoli endpoint al tuo ecosistema cloud. Exprivia XDR Service, utilizza una tecnologia che garantisce un'alta protezione degli endpoint e riesce a bloccare le minacce prima che diventino veri e propri incidenti. Inoltre, il prodotto può essere integrato con piattaforme SIEM di mercato al fine di analizzare in modo più approfondito gli eventi di sicurezza garantendo allo stesso tempo l'individuazione proattiva delle minacce e il potenziamento dello stato generale dei sistemi operativi di IT Security.

- **MANAGED DETECTION & RESPONSE (MDR):** Exprivia offre ai suoi clienti il proprio team di esperti che opera nell'ambito di risposta alle minacce, capace di intercettare e confermare proattivamente la presenza di potenziali minacce e incidenti; utilizzare tutte le informazioni disponibili per determinare il raggio di azione e la gravità delle minacce; applicare il giusto contesto imprenditoriale per le minacce individuate; avviare azioni volte a fermare, contenere e neutralizzare le minacce in remoto ed infine offre consigli pratici per risolvere alla radice il problema degli incidenti ricorrenti.

- **MONITORAGGIO DISPOSITIVI IoT:** forniamo ai clienti non solo un assessment periodico dei dispositivi presenti in rete, ma anche la predisposizione di regole adeguate configurando tutto il sistema e un monitoraggio constante. Viene creata la reportistica che tiene conto di ogni servizio e funzione dei dispositivi.

- **SICUREZZA FISICA:** forniamo ai clienti la tecnologia e il supporto per gestire tutti gli asset e tutti i sistemi a disposizione, ottenendo la gestione e visione integrata delle operazioni per garantire la sicurezza della struttura aziendale. In tal modo, con un unico sistema ed una sola interfaccia, gli operatori delle diverse sale operative possono svolgere con grande efficienza le proprie attività. È possibile gestire sistemi come:

- Telecamere di videosorveglianza.
- Lettura targhe e transiti.
- Controllo accessi.
- Antincendio.
- Antintrusione.
- Intelligenza Artificiale.

Threat Intelligence

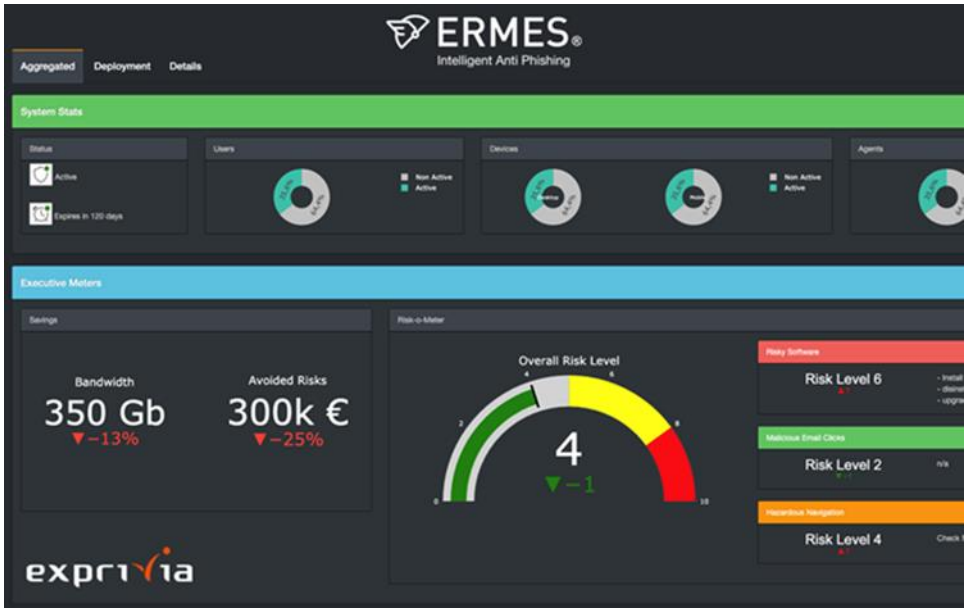
Il servizio di Threat Intelligence è un elemento fondamentale nel campo della sicurezza informatica. Il SOC di Exprivia aggrega un'ampia gamma di feed di intelligence sulle minacce per identificare e bloccare gli attacchi, tra cui:

- Vendor Risk Value: è l'attività che permette di identificare e valutare i potenziali rischi o pericoli associati alle operazioni o ai prodotti di un fornitore e al suo potenziale impatto su tutta l'azienda.
- Analisi dei vettori di attacco scoperti di recente attraverso il nostro Osservatorio, il quale si occupa di individuare nuove minacce nel panorama nazionale ed internazionale e di contestualizzare i risultati delle ricerche con le realtà aziendali.
- Malware analysis: questa attività permette di comprendere il comportamento e lo scopo di un file o URL sospetto. Il risultato dell'analisi aiuta a rilevare e mitigare la potenziale minaccia.
- Sector threat intelligence: è l'attività mirata a individuare le minacce che colpiscono determinati settori all'interno di un'azienda.
- Dark web analysis e leaked credentials monitoring: forniamo un'attività di monitoraggio ad hoc per il cliente del Dark web individuando possibili informazioni sensibili divulgate illecitamente.

Threat Detection

Una serie di servizi per consentire la prevenzione e la remediation proattiva delle frodi:

- Anti Phishing: è un'attività che si focalizza sull'individuazione sulla rilevazione e chiusura di siti clone utilizzati per veicolare campagne di phishing, sull'analisi di transazioni finanziarie fraudolente e sulla risposta a incidenti
- Web threat detection: attività di ricerca real-time delle minacce presenti nel Web da essere sempre pronti a fronteggiare eventuali attacchi.
- Identity breach: controlla se qualsiasi dato sensibile aziendale sia presente nel Web a seguito di un eventuale data breach.



Digital Forensics e Incident Response

I nostri servizi di risposta agli incidenti coprono l'intera fase dalla scoperta alla gestione dall'incidente, servizi forensi e analisi avanzata dei malware per comprendere rapidamente la natura e l'origine dell'attacco:

- I servizi di risposta agli incidenti identificano una strategia rapida ed efficace, riducendo l'impatto sul business e supportando nella fase di remediation e recovery dei sistemi.
- I servizi di threat intelligence raccolgono informazioni sulle nuove ed esistenti minacce che riguardano il Cliente. Assicura che i sistemi del cliente siano sicuri e privi di minacce così da non compromettere i propri.
- I servizi di analisi forense riguardano perizia informatica legale, acquisizione, duplicazione e estrazione di dati con tecniche e metodologie ripetibili, analisi dei sistemi operativi (Windows, Linux e OSX), analisi e individuazione degli accessi abusivi al sistema. Creazione e tutela dell'integrità della catena di custodia delle fonti di prova e delle evidenze digitali.
  Il servizio di digital forensic si estrinseca attraverso specifiche attività, quali raccolta dei log dai sistemi coinvolti, studio del caso, analisi dei log raccolti, analisi dei sistemi coinvolti, relazione tecnica e supporto legale.

Referenze

Il SOC di Exprivia vanta numerose referenze, sia in ambito Pubblica Amministrazione, che in ambito small-medium and enterprise business. Di seguito un elenco delle principali referenze corredate di una breve descrizione dei servizi erogati:

- Acquirente Unico: esercizio e manutenzione dei sistemi, delle reti e della sicurezza, attraverso la gestione della piattaforma SIEM e della piattaforma XDR+MTR.
- Cliente in ambito difesa: servizio di supporto specialistico e fornitura di licenze in ambito SIEM, SOAR, Cloud Security.
- Ente governativo della comunità europea: disegno architetturale ed evoluzione della piattaforma monitoraggio SIEM. Attività di system integration e correlazione eventi della piattaforma SIEM.
- Azienda multinazionale in ambito Manufactoring: Gestione in outsourcing del Security Operations Center (SOC). Servizi di monitoraggio dell'infrastruttura IT e di Sicurezza in tempo reale. Servizi di supporto L1 e L2.
- Cliente della PA locale: gestione in outsourcing del Security Operations Center (SOC). Servizi di monitoraggio dell'infrastruttura IT e di Sicurezza in tempo reale. Servizi di supporto L1 e L2. Gestione piattaforma XDR ed Incident response.
- Cliente enterprise: Servizi professionali in ambito sicurezza, SOC, gestione piattaforma XDR ed Incident response.
- Primari Istituti bancari Italiani: Application Assessment: Application Security Testing. Vulnerabilities identification and classification. Remediation.
- Commissione Europea: realizzazione delle infrastrutture informatiche, in particolare dell'Early Warning System, sistema di rilevamento e divulgazione delle minacce, e di un Federation of Cyber Ranges, ambiente avanzato di simulazione Cyber.
- Pubblica Amministrazione Centrale: gestione del CED del cliente attraverso la configurazione e manutenzione degli apparati di sicurezza multibrand in ambito network security (IPS, IDS, Firewall, WAF e bilanciatori), degli storage, nonché attività di Domain Amministration e virtualizzazione.
- Cliente della PA locale: fornitura e configurazione degli apparati di sicurezza perimetrale. Servizi professionali in ambito sicurezza, gestione piattaforma XDR ed Incident response.
- Azienda multinazionale in ambito Manufactoring Enterprise: fornitura e configurazione piattaforma XDR e servizi di incident response.

Come eroghiamo il servizio

Exprivia offre due tipi di soluzioni:

1. SOC-on-Premise: Installazione, configurazione e messa in opera della soluzione tecnologica presso il cliente. Gestione del servizio erogato dalla Control Room Exprivia o mediante il supporto dei nostri security analyst on Premise (presso le strutture del cliente).
2. SOC-as-Service: Installazione, configurazione e messa in opera della soluzione tecnologica e successiva gestione in modalità SaaS. Gestione del servizio erogato dalla Control Room Exprivia o mediante il supporto dei nostri security analyst on Premise (presso le strutture del cliente).