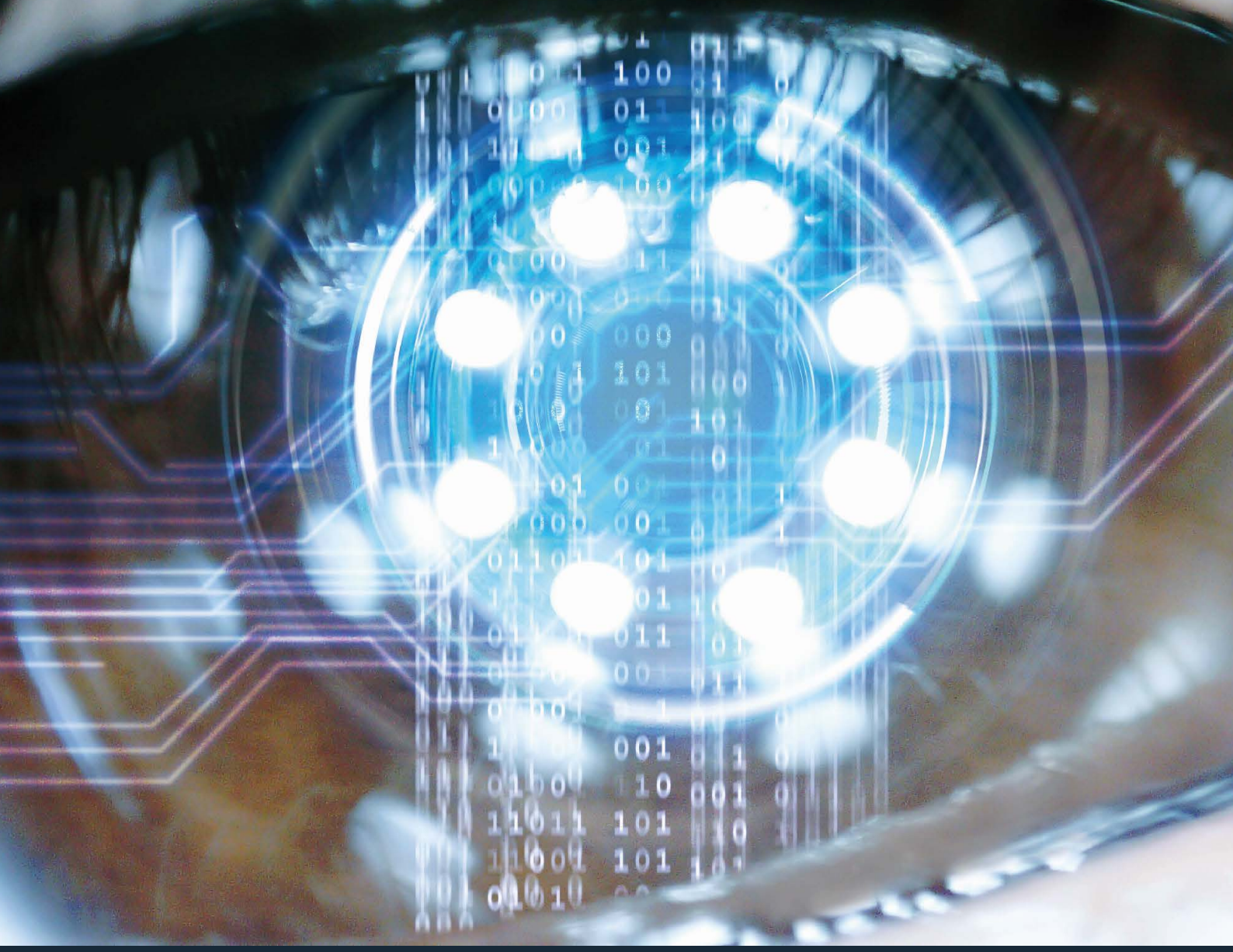


LEONARDO CYBER & SECURITY SOLUTIONS

CYBER SITUATIONAL AWARENESS SYSTEM

LEONARDO

In un'economia digitale in cui istituzioni e aziende si aprono sempre più a uno scambio continuo di comunicazioni con l'esterno, i tradizionali approcci alla cyber security risultano spesso inadeguati per rispondere efficacemente alle minacce cibernetiche con velocità e copertura tali da minimizzarne l'impatto sulla continuità operativa delle organizzazioni. Si tratta infatti spesso di approcci di natura tecnologica, avulsi dai processi operativi e di business dell'organizzazione, in quanto elaborano separatamente le informazioni provenienti da sistemi eterogenei.

I team di sicurezza dedicati alla protezione delle infrastrutture informatiche si trovano quindi costretti ad interagire con molteplici strumenti e ad effettuare analisi e correlazioni con dati distribuiti su numerosi applicativi. Ciò rende estremamente complesso ottenere un'indicazione del rischio cibernetico a cui è esposta un'organizzazione, informazione indispensabile per poter rispondere tempestivamente ed efficacemente ad un attacco o ad un incidente informatico, prioritizzando, se necessario, le attività di reazione sulla base degli impatti dell'evento malevolo.

In questo scenario raccogliere le informazioni necessarie per fornire al management delle viste di alto livello che rappresentino, in modo chiaro e sintetico, lo stato generale di sicurezza di un'infrastruttura può essere difficoltoso anche per un team altamente qualificato. Ciò ha impatti sia sulla corretta allocazione degli investimenti in cyber security, ma anche e soprattutto nel momento in cui si verifica un incidente con ripercussioni significative sull'operatività e sulla reputazione dell'organizzazione, che obbligano il top management a prendere decisioni critiche in poco tempo basandosi su informazioni frammentarie.

Cyber Situational Awarness System

CYBER SITUATIONAL AWARENESS SYSTEM

Per innalzare i livelli di cyber awareness di istituzioni e aziende Leonardo ha sviluppato il Cyber Situational Awareness System (CSAS), un ecosistema completo per il monitoraggio informatico e il raggiungimento di elevati livelli di cyber awareness. Il sistema è infatti specificamente progettato per:

- mantenere informati **i team di sicurezza** e i **profili executive** di un'organizzazione su ciò che sta accadendo in termini di cyber security nel proprio contesto operativoattraverso la **raccolta e l'analisi continua di dati;**
- supportare i **processi decisionali e di indagine deglianalisti di sicurezza e del management** fornendo unaccentratore di informazioni che espone dashboard executive e tecnico-operative.

La piattaforma supporta due modelli di erogazione:

• on-premises con installazione del sistema presso il "Cliente";
• as a service, che prevede l'erogazione delle funzionalità della piattaforma da remoto.

L'APPROCCIO PROPOSTO

Dato un insieme di asset da monitorare, il Cyber Situational Awareness System è in grado di interagire con una molteplice varietà di fonti informative al fine di raccogliere dati e informazioni, per poi analizzarle e correlarle. Attraverso funzionalità di data warehousing, il CSAS fornisce un accesso centralizzato ai dati mediante viste dedicate a diversi tipi di utenti con lo scopo di facilitare i processi decisionali di profili tecnici ed executive.

L'approccio proposto prevede una fase di **analisi preliminare** in cui, sulla base delle esigenze e delle tecnologie disponibili presso il Cliente, si definisce la configurazione del sistema, le sorgenti di dati da utilizzare (SIEM, Threat Intelligence, VA, Ticket, CMDB...), vengono selezionate le dashboard desiderate da un catalogo di dashboard predefinito oppure si concordano nuove dashboard da realizzare ad hoc.

La fase di **tuning** dei connettori è propedeutica per alimentare il sistema con i dati eterogenei che popoleranno le viste tecnico-operative e le dashboard executive.

Cyber Situational Awarness System

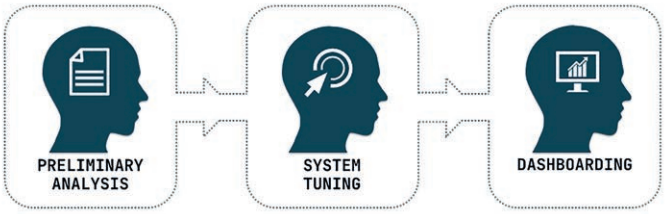
Una volta messi a punto i connettori, nella fase di dashboarding, gli utenti possono accedere a interfacce user-friendly, interattive e filtrabili messe a disposizione dalla piattaforma e alimentate in real time dai sistemi connessi.

Le dashboard contengono informazioni aggregate, statistiche e metriche di performance relative allo stato generale della sicurezza dell'infrastruttura monitorata esono esportabili attraverso report in diversi formati. Possono inoltre essere di tipo executive o operative, a seconda dei profili indirizzati.

Le dashboard **executive** sono di natura strategica in quanto consentono ai top manager di avere una visione d'insieme dell'organizzazione rispetto alle metriche critiche, monitorando l'andamento rispetto ai KPI stabiliti, identificando gli opportuni miglioramenti e le opportunità di espansione.

Le dashboard **operative** sono pensate per il monitoraggio e la gestione di processi e attività con un orizzonte temporale più ristretto, un focus più tecnico e una vista più granulare e verticale sulle tematiche di interesse. In entrambi i casi le dashboard costituiscono uno strumento in grado di fornire report informativi periodici con lo scopo di supportare i processi decisionali.

- **Contribuisce a definire il rischio cibernetico,** in quanto i dati informatici tipicamente acquisiti nell'ambito della cyber security non forniscono una misura diretta del rischio impedendo il raggiungimento di una conoscenza completa ed approfondita dello stato di sicurezza (cyber awareness). Le dashboard del CSAS forniscono supporto nel garantire che i controlli di sicurezza adottati siano adeguati ai rischi specifici che a cui un'azienda è esposta.



PRINCIPALI FUNZIONALITÀ

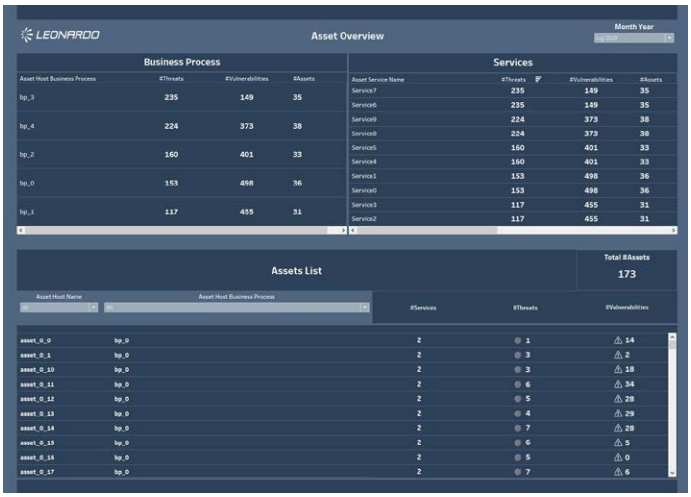
Attraverso il processo precedentemente descritto, il Cyber Situational Awareness System:

- **Supporta i processi di indagine e ricerca** dei team di sicurezza che devono quotidianamente interagire con numerosi strumenti, rendendo spesso difficile effettuare analisi e correlazioni con dati distribuiti su numerosi applicativi. Attraverso l'interazione con sorgenti eterogenee e funzionalità di analisi e correlazione, il CSAS svolge il ruolo di accentratore dei dati ed espone viste tecnico-operative d'insieme per la visualizzazione centralizzata delle informazioni, contribuendo **al miglioramento della produttività dei team di sicurezza e offrendo supporto nel processo di indagine.**

- **Fornisce un dashboarding avanzato,** rispondendo all'esigenza, spesso difficoltosa da indirizzare anche per team di sicurezza qualificati, di raccogliere informazioni per fornire viste di alto livello in grado di rappresentare lo stato di sicurezza complessivo dell'organizzazione ai profili manageriali. Attraverso l'aggregazione di dati e strumenti di Business Intelligence, il CSAS espone delle dashboard, scaricabili come report, che presentano trend e metriche significative, fornendo un accesso immediato a informazioni ad alto valore aggiunto senza la necessità di ricorrere a query e ricerche manuali.

MODELLO LOGICO E TECNOLOGIE

Il CSAS si basa su un **advanced analytic engine** che interagisce con le sorgenti informative ed effettua operazioni di raccolta, normalizzazione, analisi e correlazione dei dati, memorizzandoli in un data warehouse.
Il sistema include inoltre una **knowledge base** che contiene informazioni di threat intelligence, alimentata da fonti eterogenee in quest'ambito.
Al di sopra di questi moduli, il CSAS dispone di layer applicativi che espongono sia le **dashboard tecnico-operative** sia le **dashboard dedicate ai profili executive.**
Il CSAS si avvale di **tecnologie avanzate per l'elaborazione e la visualizzazione di big data** e di **strumenti, competenze ed esperienze evolute nell'ambito della cyber defense** sviluppate da Leonardo nei domini più critici.



BENEFICI

- Maggiore integrazione delle attività di cyber security con le prioritàdel business, le strategie aziendali e i processi vitali per ilfunzionamento dell'organizzazione.
- Migliori capacità analitiche e di indagine di attacchi cibernetici.
- Visione complessiva del perimetro monitorato, attraverso l'accentramento di dati e informazioni eterogenei.
- Capacità di rappresentare le informazioni in base al tipo di utentiche accedono alla piattaforma attraverso dashboard executive etecnico-operative configurabili.

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber & Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

MM09136 11-23

leonardo.com

LEONARDO