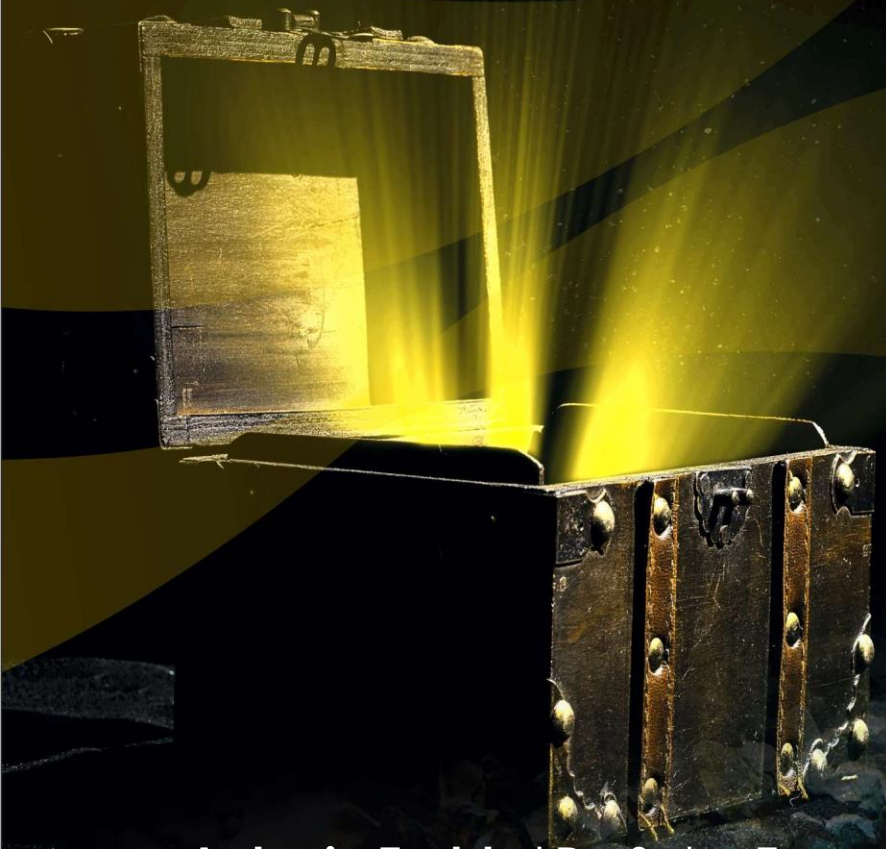
Cybersecurity & SOC: Soluzioni in evoluzione

ETÆRIA
a WIIT Company



PARTNER KICK-OFF 2022

Antonio Tedde | PreSales Team Leader

CHECK POINT™

Linee guida per la sicurezza informatica

ETÆRIA

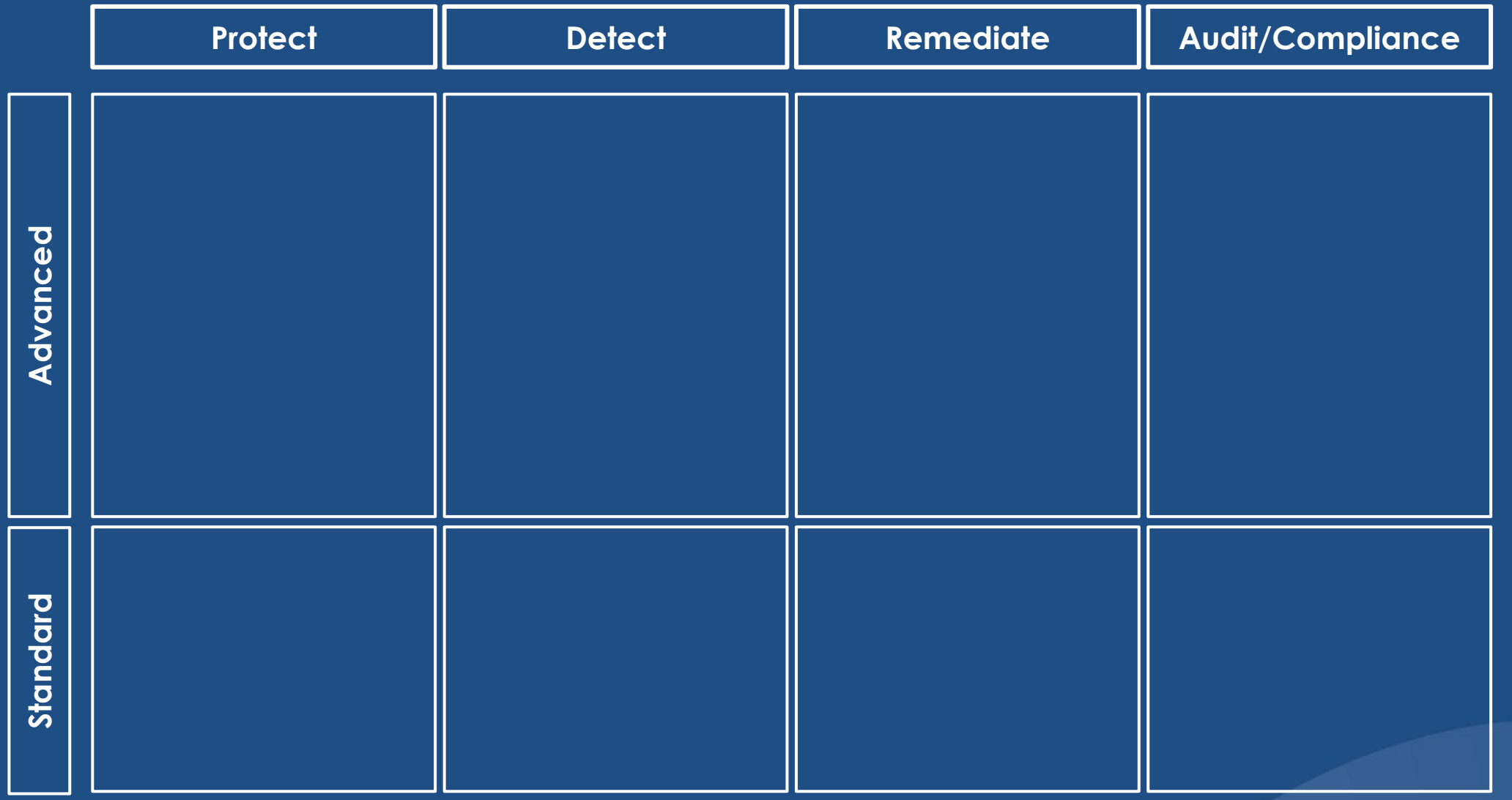
a WIIT Company

Piano Strategico di Risposta agli attacchi informatici:

1) Determinare gli «Stakeholders» chiave e il loro ruolo
2) Identificare gli asset critici
3) Identificare processi e azioni di risposta
4) Implementare le tecnologie di protezione e di investigazione
5) Svolgere attività di «tuning» per perfezionare i processi
6) Verificare di avere sempre la massima visibilità
7) Implementare il controllo degli accessi
8) Condurre attività di informazione e formazione interna
9) Eseguire simulazioni di attacchi e test interni
10) Implementare o aggiornare il BCP/DRP con le azioni di Ripristino

ETÆRIA
a WIIT Company

Vista Funzionale

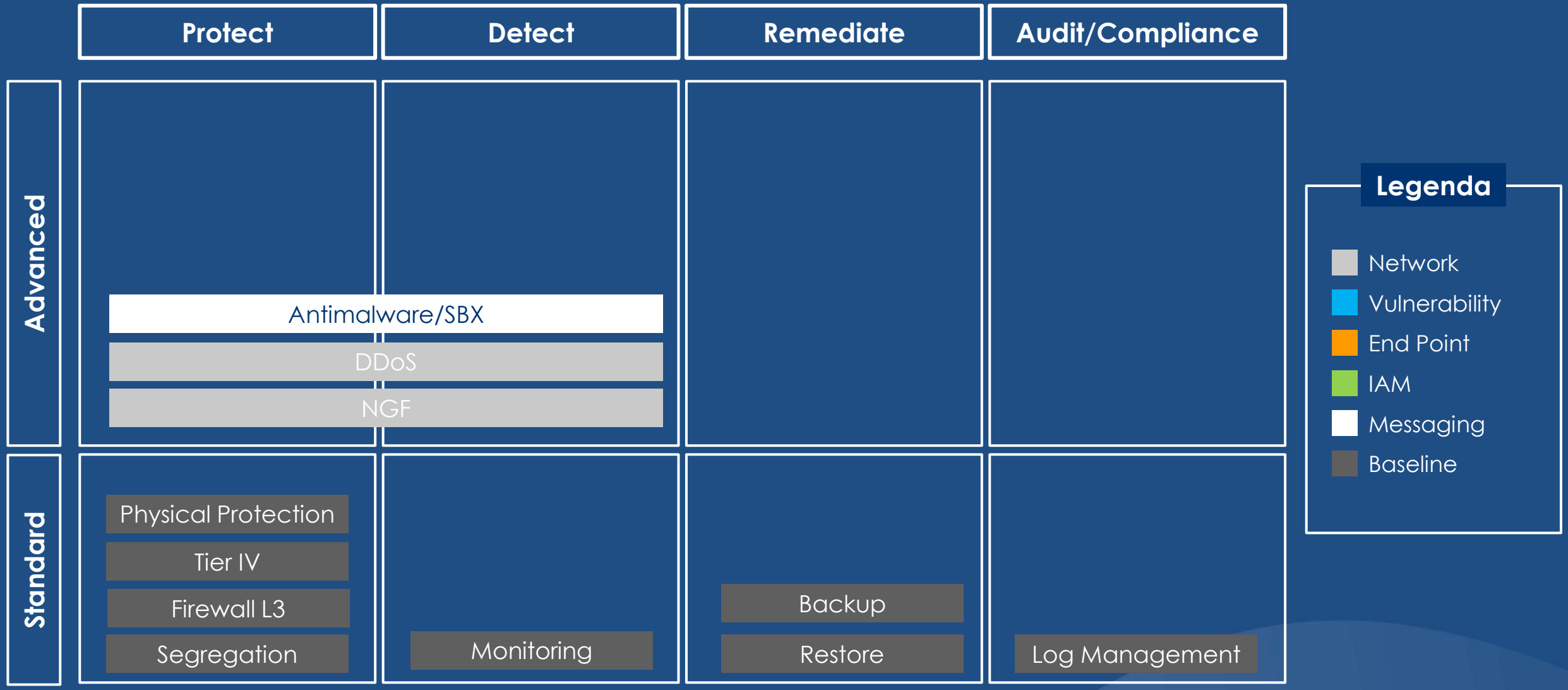


Legenda

- Network
- Vulnerability
- End Point
- IAM
- Messaging
- Baseline

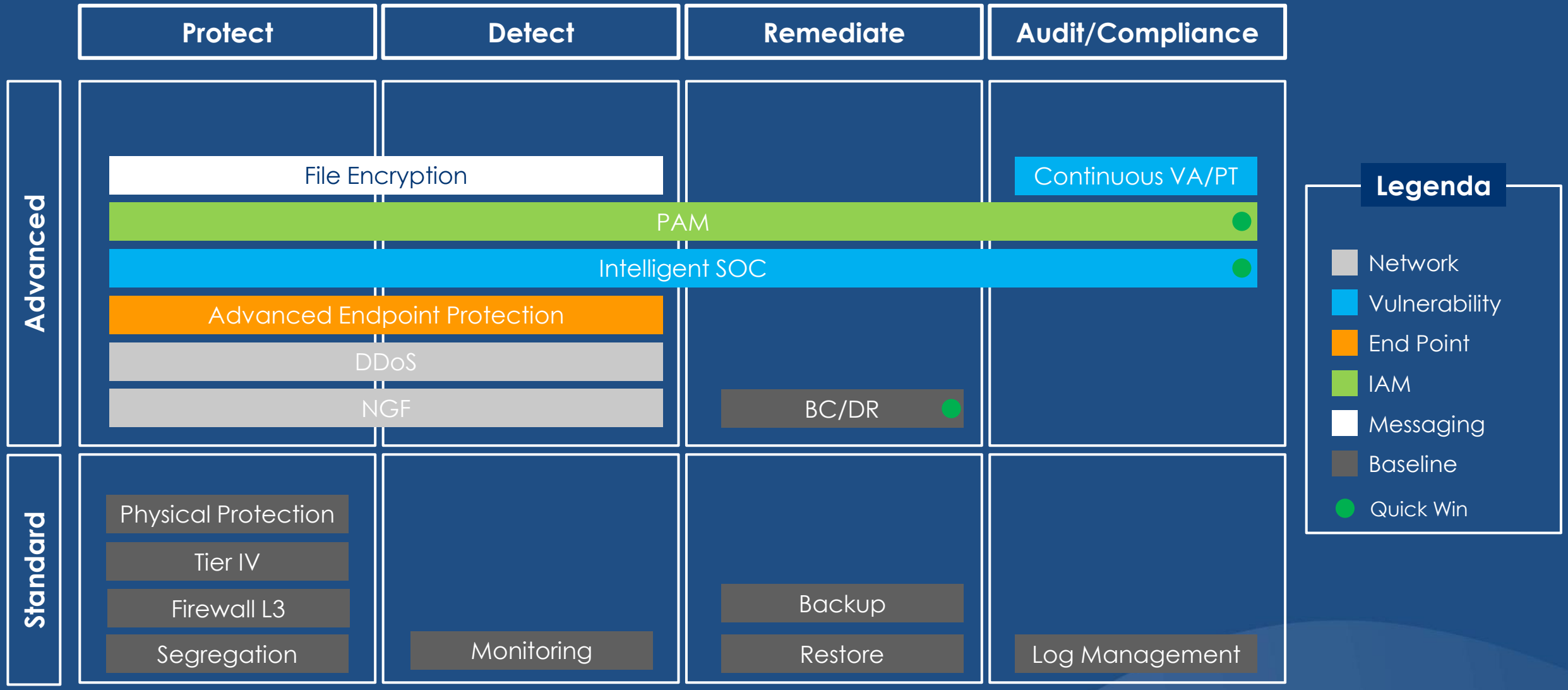
ETÆRIA
a WIIT Company

Vista Funzionale as-is



ETÆRIA
a WIIT Company

Vista Funzionale To-be



ETÆRIA
a WIIT Company

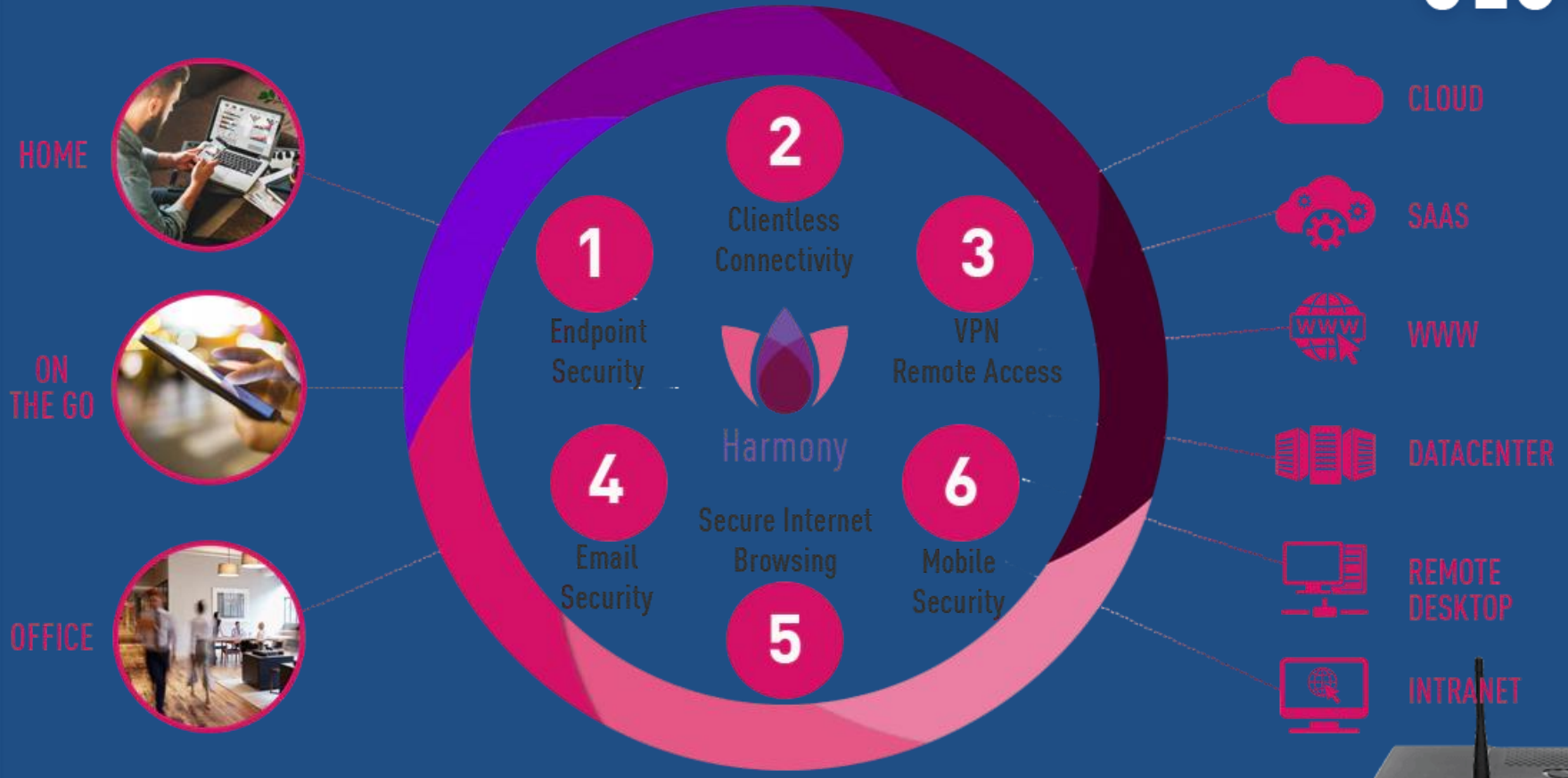
Strumenti di protezione

ETÆRIA

a WIIT Company

CHECKPOINT

CLOUD WITH CONFIDENCE



CHECK POINT
CloudGuard™

ETÆRIA
a WIIT Company

SOC as a Service

SOC as a Service

Perchè

Compliance

Necessità di adempiere a specifici regolamenti di settore o di privacy quali:

- ✓ PCI DSS
- ✓ GDPR
- ✓ NIS
- ✓ HIPPA
- ✓ ISO xxx

Insider Threats and Advanced Detection

Necessità di rilevare proattivamente le minacce anche quelle interne. Sospetti di abuso di accesso privilegiato provenienti da utenti legitimi. Rete accessibile da diverse terze parti (consulenti, suppliers,etc)

Centralized Security Management

Necessità di controlli avanzati di sicurezza e detection centralizzati con visibilità sia dai sistemi in cloud che on premises.

H.24

RealTime Monitoring & Incident Response

Mancanza di risorse, tempo e competenze specifiche per il monitoraggio continuo delle minacce e l'adeguata Risposta agli Incidenti col rispettivo Piano di Remediation.

Come

Gain Compliance

Il SOC implementa attraverso il SIEM specifici controlli che rispondono ai requisiti delle normative. Inoltre è possibile impostare dei report di compliance.

Automate Intelligence

La funzionalità di Behavioral Analysis e di Threat Intelligence del SOC rileva i comportamenti anomali all'interno della rete, incluso quando provengono da utenti legittimi, inoltre applicando IA alla ricerca proattiva delle minacce si può accelerare il processo di circa il 50%

See everything

In una singola console di Security vengono consolidati e correlati i logs, flussi ed eventi provenienti dagli ambienti SaaS, IaaS e on-premise.

Become proactive

La piattaforma d'Intelligence analizza automaticamente flussi di rete e log generando gli alert che vengono gestiti da analisti esperti H24. Il SOC di Etæria coordina la risposta agli incidenti dai 4 livelli di escalation in base alla tipologia dell'incidente.

ETÆRIA
a WIIT Company

DA SICUREZZA GESTITA A SOC as a SERVICE

DIFESA PASSIVA

Tecnologie di difesa e detection, risposta passiva

- Difesa del perimetro, anti-intrusione, Antivirus, rilevamento intelligente delle minacce, sandboxing

Riduce il perimetro attaccabile, rileva parte delle minacce evolute, aumenta i costi di un attacco

DIFESA ATTIVA

Rilevamento completo, risposta immediata

- Monitoraggio continuo, Analisi Intelligente con strumenti appositi, Sincronizzazione e Correlazione di eventi

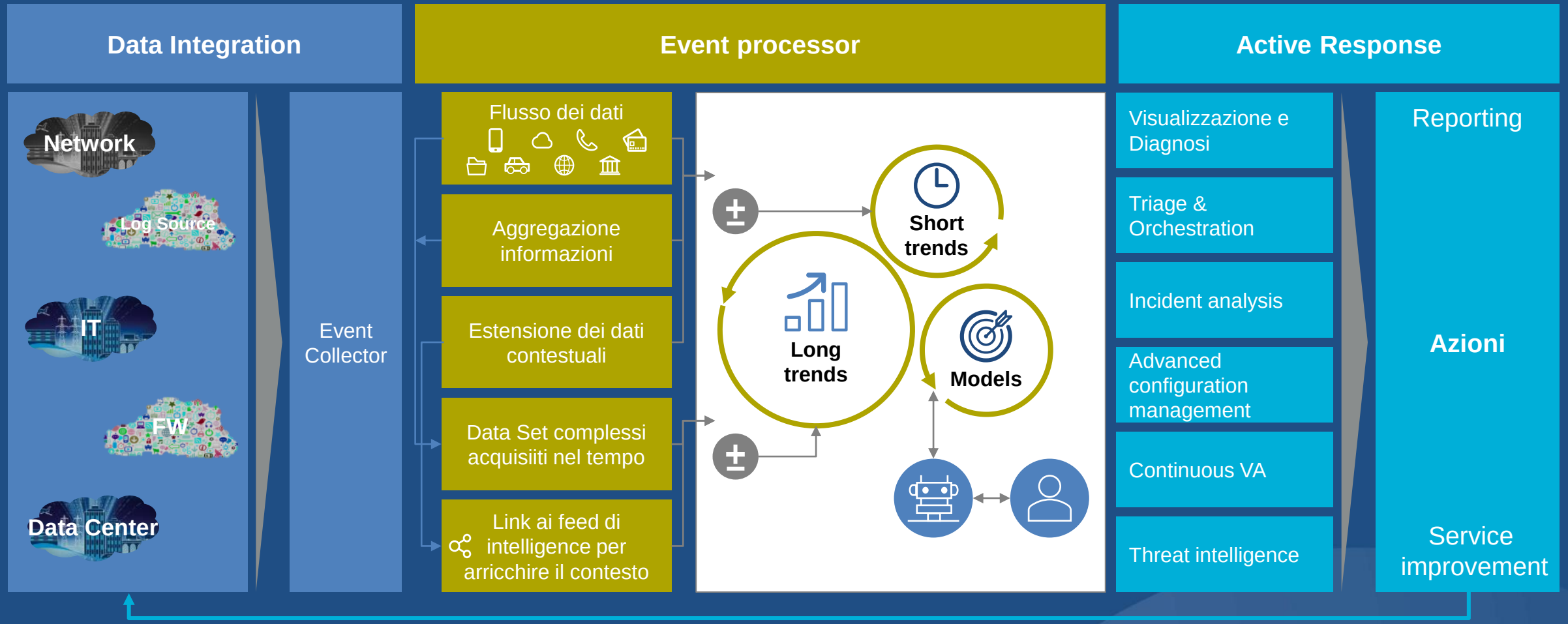
Sincronizza e correla diverse tecnologie di difesa, accorcia i tempi di rilevamento e risposta, impone organizzazione di processo

ETÆRIA
a WIIT Company

Intelligent SOC

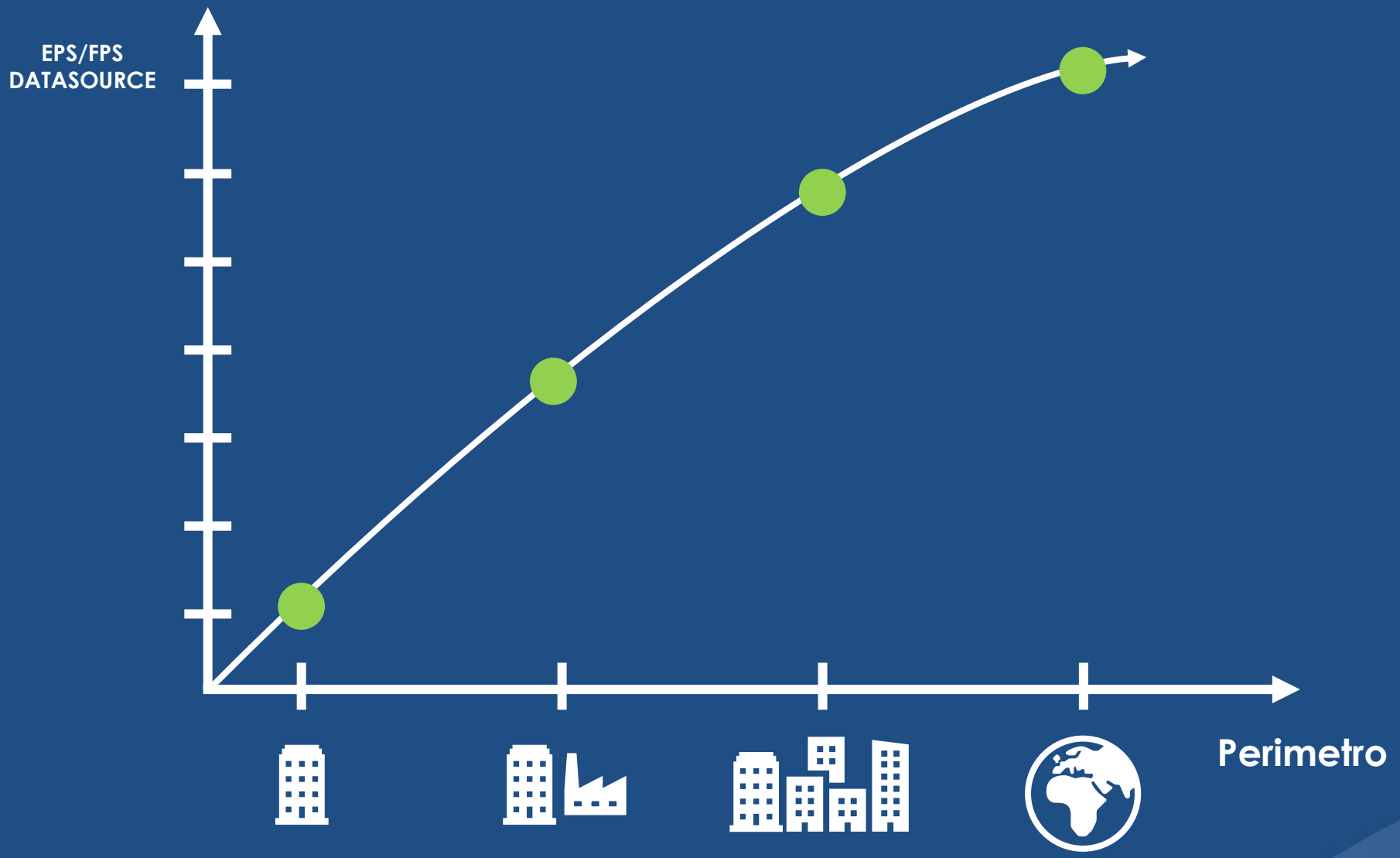
ETÆRIA
a WIIT Company

SOC – TECNOLOGIE E SERVIZI – VISTA INTEGRATA



ETÆRIA
a WIIT Company

Un approccio modulare



Un'offerta modulare che scala in base al perimetro da gestire.

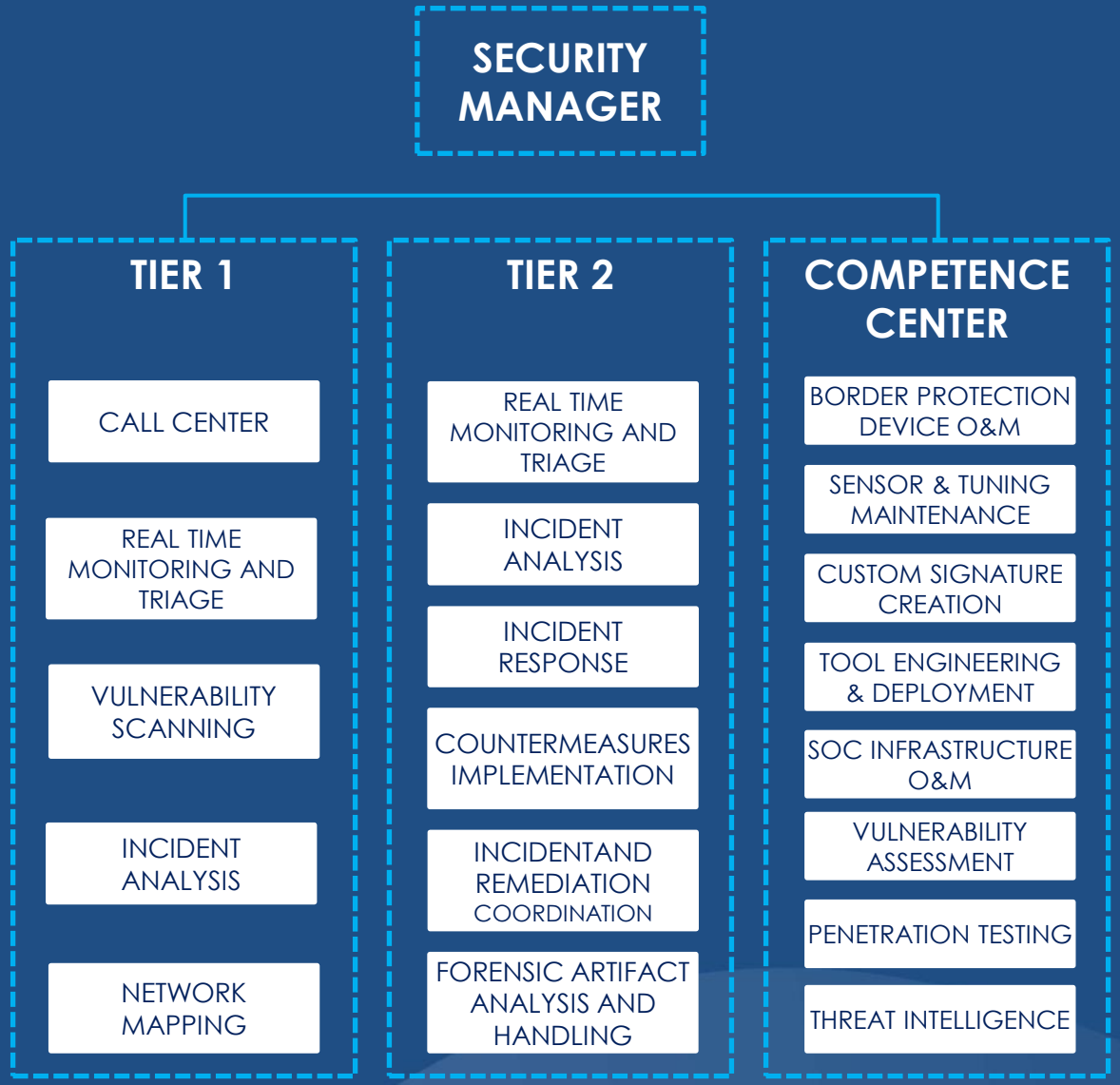
ETÆRIA
a WIIT Company

ORGANIZZAZIONE SOC

Security Manager: è il principale interlocutore del Cliente, avendo una visione completa e la responsabilità dello stato del servizio. È coinvolto in fasi come la gestione degli incidenti e le riunioni di revisione.

Proactive Detection team (Tier 1 and Tier 2): è un team di analisti della sicurezza che si preoccupano di identificare le minacce indirizzate all'infrastruttura IT monitorando continuamente la coda degli avvisi, triage degli avvisi di sicurezza, eseguendo un'analisi approfondita degli incidenti. Il team gestisce gli incidenti di sicurezza, determinando se un sistema o un set di dati critici è stato colpito, occupandosi della riparazione e fornendo supporto per nuovi metodi analitici per il rilevamento delle minacce.

Competence Center: il team possiede una conoscenza approfondita di rete, endpoint, intelligence sulle minacce, analisi forense e reverse engineering del malware, nonché il funzionamento di applicazioni specifiche o dell'infrastruttura IT sottostante; agisce come un "cacciatore" di incidenti; strettamente coinvolto nello sviluppo, messa a punto e implementazione di analisi di rilevamento delle minacce.



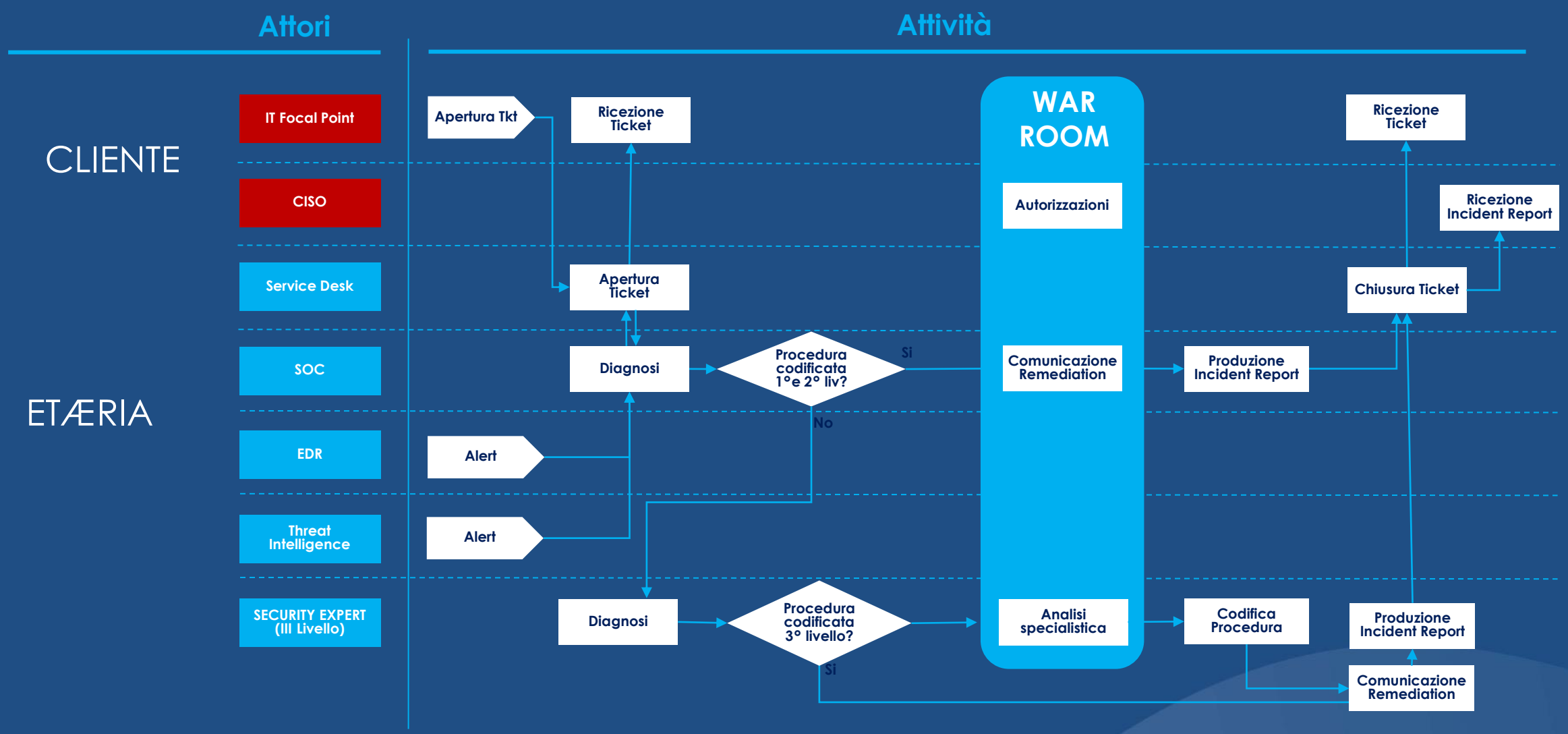
ETÆRIA
a WIIT Company

INCIDENT RESPONSE

In conformità al **NIST Special Publication 800-61**, un processo di risposta agli incidenti contiene quattro fasi principali:

ETÆRIA
a WIIT Company

ESEMPIO PROCESSO DI GESTIONE INCIDENT SICUREZZA



ETÆRIA
a WIIT Company

Dettaglio Servizio Smart SOCaaS

SMART SOCaaS – Caratteristiche funzionali

SERVIZIO SMART SOCaaS STANDARD

Correlazione Eventi
Azioni proattive

Monitoring delle tecnologie

Scansione delle Vulnerabilità

Monitoraggio e reportistica sulla conformità

EDR gestita

Servizi di risposta agli incidenti

Threat hunting gestita

Integrazione con Tecnologie Specializzate

Rilevamento avanzato e proattivo delle minacce

Risposta e Contenimento delle minacce più esteso

SERVIZI DI PREVENZIONE E REMEDIATION

Configurazioni e Segmentazione

Gestione delle tecnologie di sicurezza

Formazione

Penetration Test

Altri servizi gestiti e di assistenza

SERVIZIO SMART SOCaaS EXTENDED

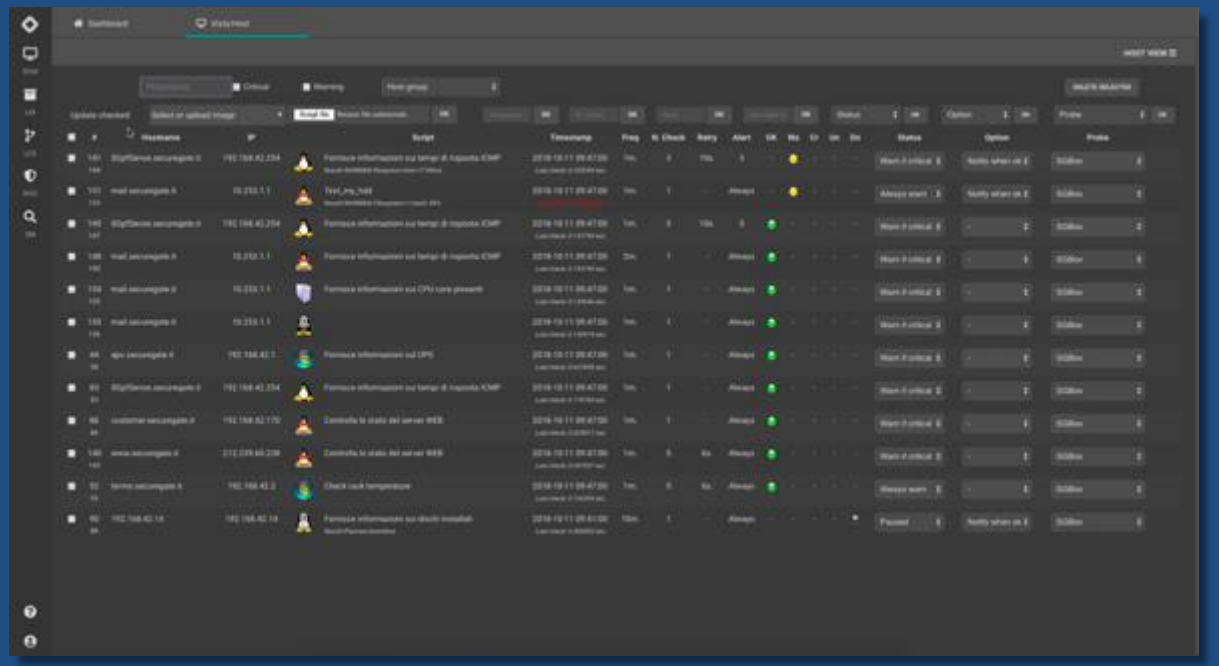
ETÆRIA
a WIIT Company

FUNZIONALITA' DEL SERVIZIO STANDARD

CONTROLLI DI MONITORING

CONTROLLI MONITORING:

- Disponibilità (Uptime) di tutti i sistemi provvisti di Data Source con alert in caso di indisponibilità per + di 4 minuti
- Per i server:
  - monitoring della CPU (Alert se uso della CPU > 95% per + di 14 minuti)
  - monitoring della RAM (Alert se uso delle RAM > del 90% per + di 14 minuti)
  - monitoring dello Storage (Alert se occupazione arriva al 95%)
- Report mensili:
  - % Uptime Sistemi



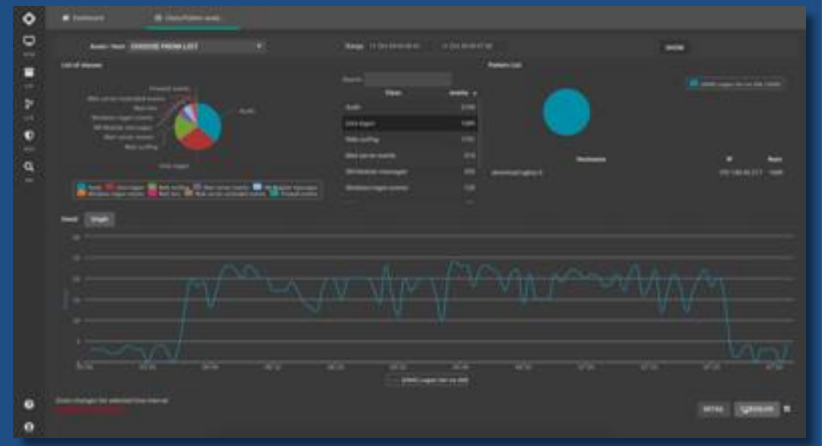
ETÆRIA
a WIIT Company

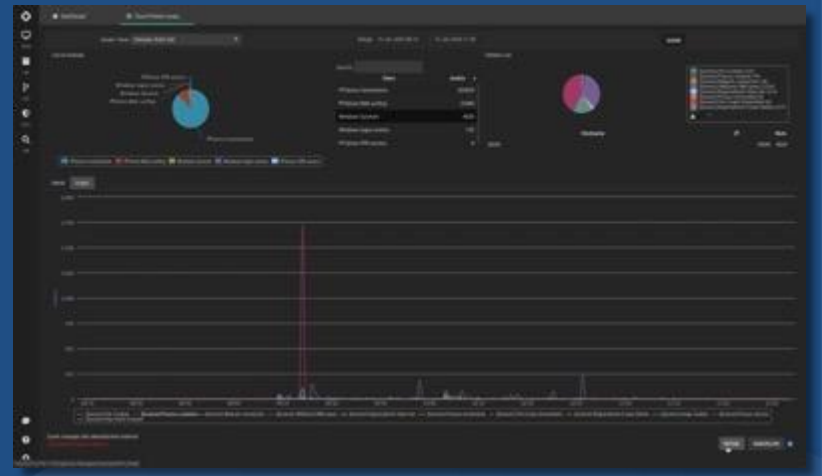
FUNZIONALITA' DEL SERVIZIO STANDARD

SERVIZIO SMART SOCaaS STANDARD

SIEM: Controlli Compresi

- Normalizzazione LOG e Conservazione per 6 mesi in linea e 6 mesi in modalità Backup per:
  - Raccolta LOG Amministratori di Sistema
  - Raccolta LOG Firewall e Access Point
  - Raccolta LOG Server di Posta
  - Raccolta LOG VOIP
  - Raccolta LOG Server
- Controllo Server:
  - Allarme per accesso sospetto (3 tentativi di accesso non andati a buon fine)
  - Allarme in caso di picchi anomali di file cancellati sui «File Server»
  - Allarme in caso di accesso notturno di utenti non autorizzati
- Controllo VPN:
  - Allarme per accesso sospetto (3 tentativi di accesso non andati a buon fine)
  - Registrazione dell'orario di accesso e uscita degli utenti (Smartworking)
  - Report mensile con situazione per ogni utente
- Controllo Minacce End Point Windows:
  - Allarme in caso di minacce rilevate in base a confronto con situazioni di rischio note (MITRE ATT&CK)
- Asset:
  - Rilevamento periodico degli asset presenti sulla rete e segnalazione in caso di asset non autorizzati





ETÆRIA
a WIIT Company

FUNZIONALITA' DEL SERVIZIO STANDARD

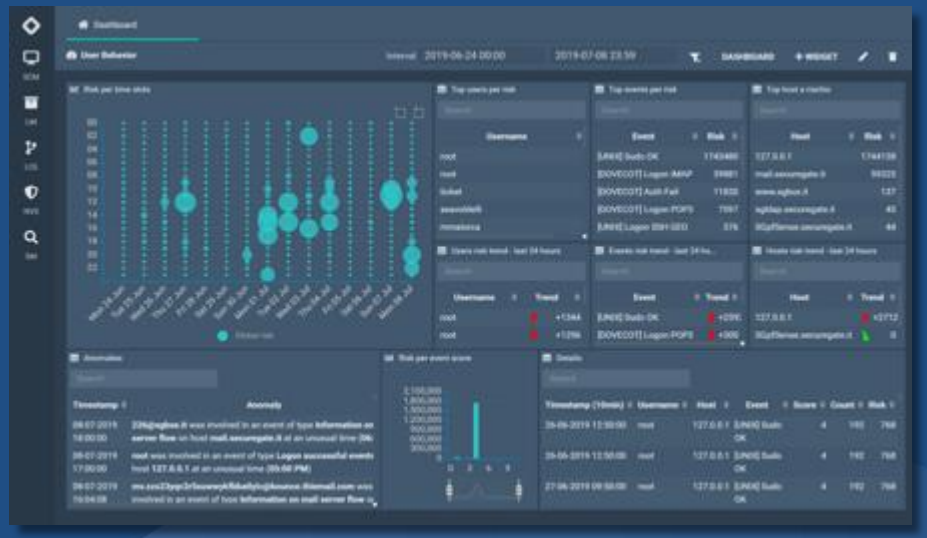
SERVIZIO SMART SOCaaS STANDARD

Vulnerability SCAN: Controlli compresi

- Scansione settimanale delle vulnerabilità dei sistemi con relativo invio report:
  - All'organizzazione tecnica di remediation: Report Tecnico con dettaglio vulnerabilità e rimedi
  - Al Partner/Cliente: Report sintetico con confronto storico
  - Allarme in caso indice di tendenza delle vulnerabilità supera la soglia tollerabile

UBA: controlli compresi con l'estensione FULL SIEM

- Controllo intelligente delle attività degli utenti
  - Sfrutta modulo UBA di SGBOX
  - Analisi del comportamento degli utenti con gestione della categoria di rischio
  - Allarme in caso di superamento dell'indice di rischio



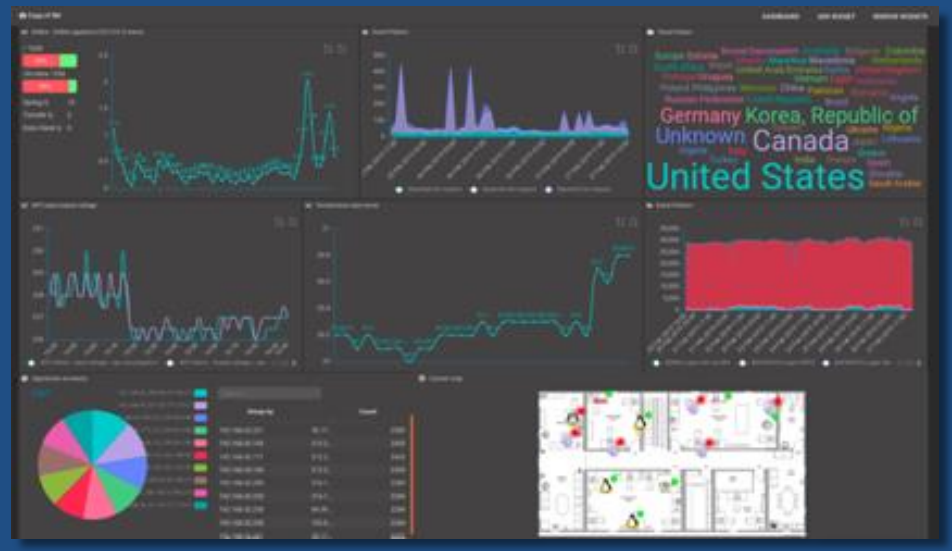
ETÆRIA
a WIIT Company

SLA DEL SOC

- Gli SLA diventano impegnativi a partire dal secondo mese
- Analisi immediata dell'allarme/problema e definizione di un severity code
- Risposta con ingegneria della soluzione e ingaggio III parti

SOC Tier	Descrizione	Severity 1 Critical	Severity 2 High	Severity 3 Medium	Severity 4 Low
SERVIZIO SOC TIER 1	Presa in carico della richiesta di assistenza	Immediata			
	Tempo massimo entro il quale il problema deve essere analizzato, individuata la soluzione e segnalata al Tier 2	2 ore	4 ore	12 ore lavorative	24 ore lavorative
	Modalità di segnalazione	Chiamata telefonica e e-mail	Chiamata telefonica e e-mail	e-mail	e-mail
SERVIZIO SOC TIER 2*	Tempo massimo di identificazione e comunicazione al cliente della prima azione di Remediation o passare a severity code maggiore	8 ore	12 ore	16 ore lavorative	24 ore lavorative

*è incluso il coordinamento della Remediation



ETÆRIA
a WIIT Company

Tecnologia SIEM SGBOX

SGBOX Architecture

HARDWARE APPLIANCE VIRTUAL APPLIANCE **MSSP/CLOUD**

Log Management

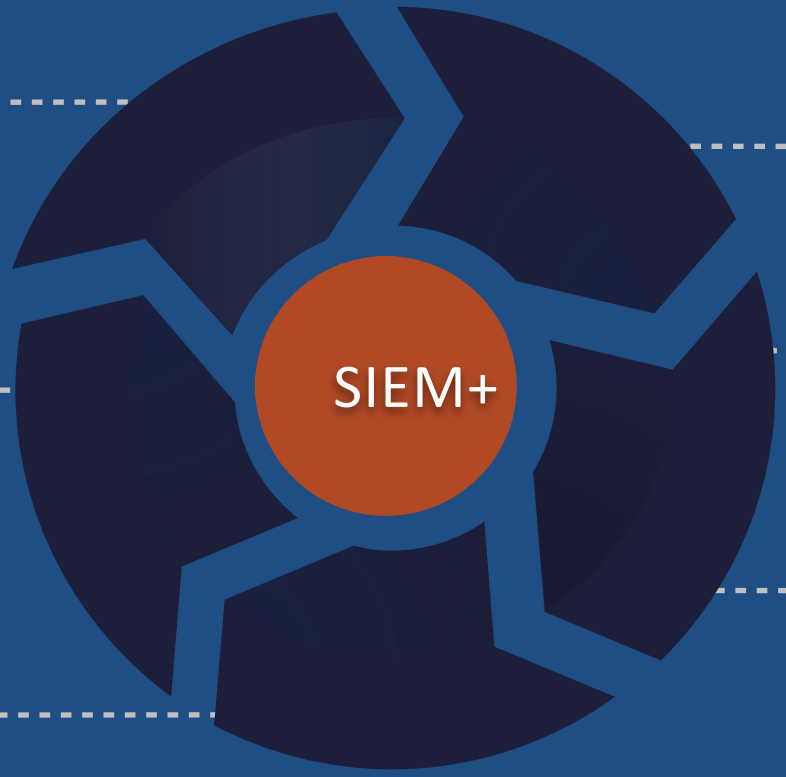
Raccogliere qualsiasi formato di log da qualsiasi tipo di fonte dati. I Log raccolti sono firmati e crittografati al fine di garantire l'integrità dei dati memorizzati.

User Behavior Analytics (UBA)

Tracciamento, raccolta e valutazione dei dati e delle attività degli utenti mediante sistemi di monitoraggio.

System Monitoring

Fornisce informazioni in tempo reale, analizzando le prestazioni e lo stato dei componenti di rete.



Event Correlation

Definire regole di correlazione per rilevare comportamenti anomali attraverso un'interfaccia semplice e intuitiva.

Endpoint Threat Detection & Response (ETD)

Rilevamento e risposta avanzate di anomalie e attacchi.

Vulnerability Management

Scansioni di vulnerabilità automatiche per rilevare vulnerabilità su qualsiasi tipo di host e dispositivi.
Il modulo genera report dettagliati e personalizzati che supportano l'IT per gestire le vulnerabilità e ridurre il rischio di violazione dei dati.

ICT Security

IoT

Big Data

Compliance

Auditing

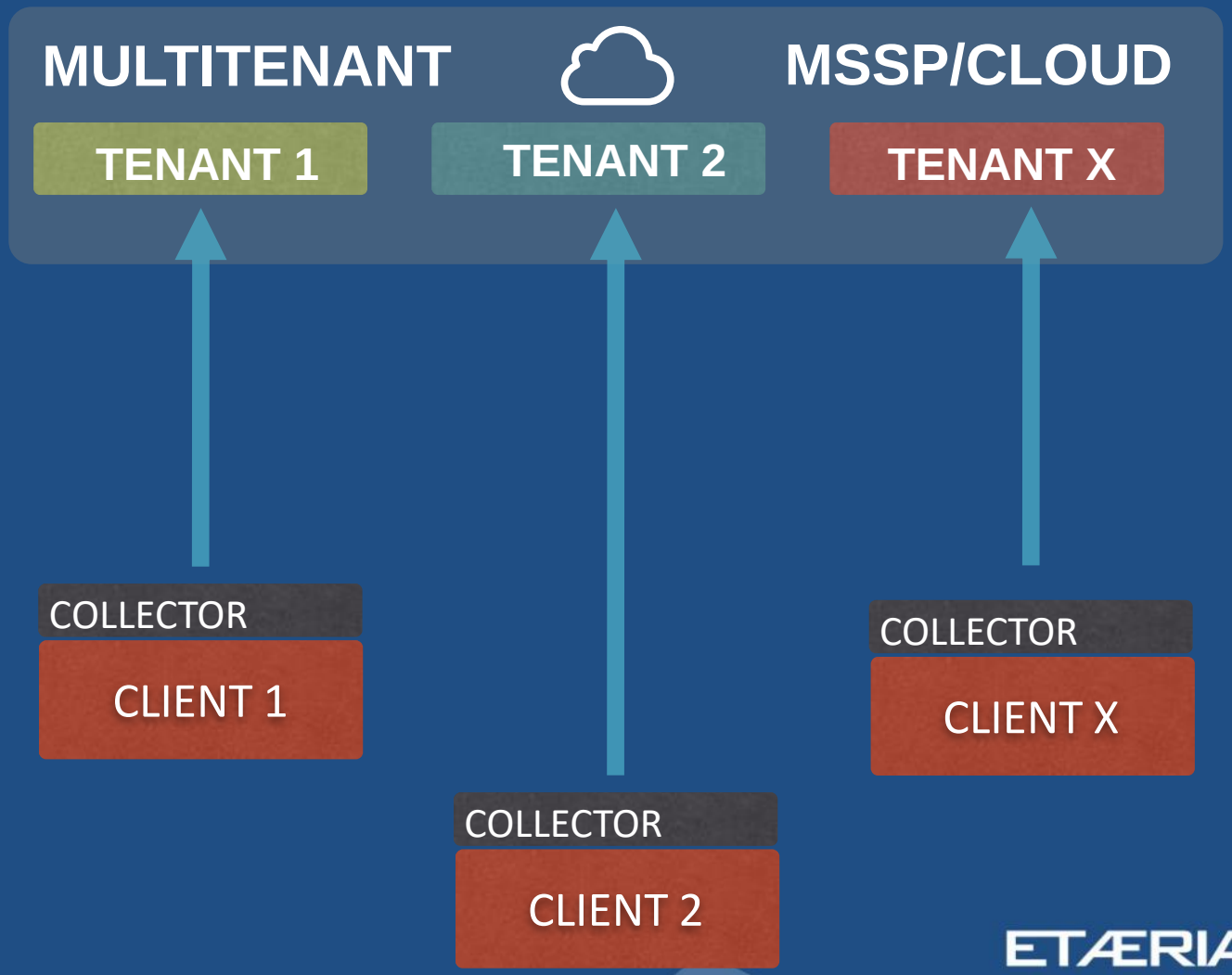
IIoT

Governance

ETÆRIA
a WIIT Company

GDPR

SGBOX Multitenant

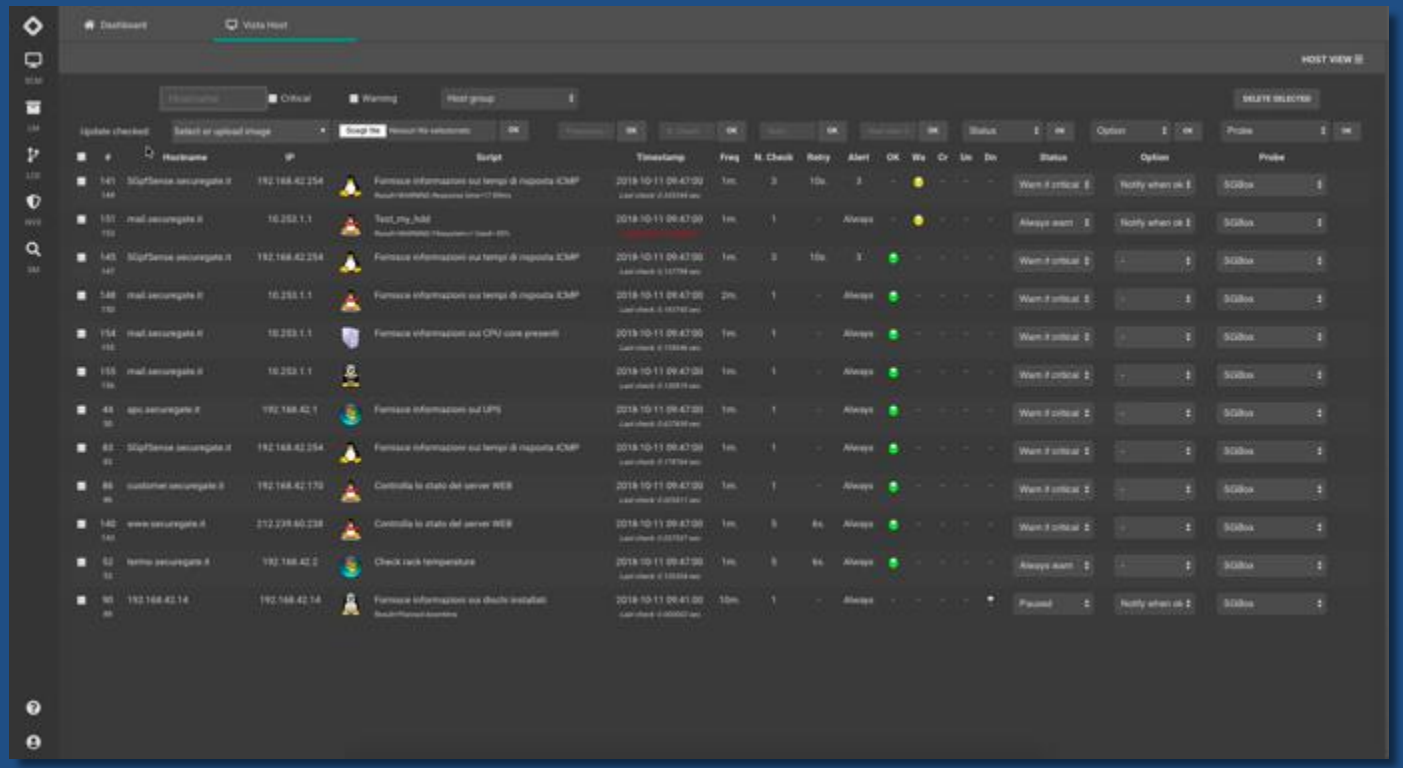


- Implementazione all'interno di un datacenter fisico o virtuale
- Gestione delle istanze tramite la tecnologia Multitenant
- SGbox centralizzato ma con istanze dedicate per ogni singolo cliente
- Possibilità di accesso da parte dell'utente finale e privilegi configurabili
- Collettore virtuale o fisico per la raccolta dei Log

ETÆRIA
a WIIT Company

System Monitoring (SM)

Verifica delle risorse e dei servizi

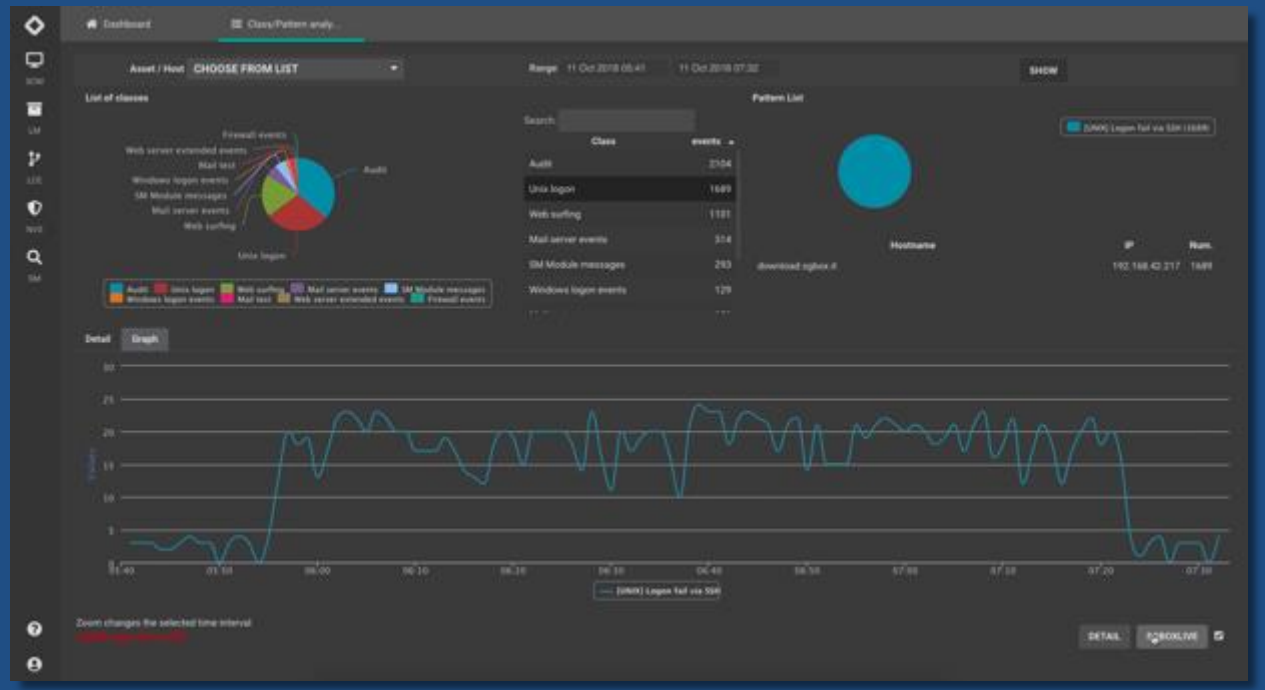


- Verifica, sfruttando diversi protocolli (SNMP), la disponibilità dei servizi
- Indica i tempi di risposta dei servizi
- Fornisce report interattivi su SLA e uptime dei sistemi/servizi
- Definizione di soglie di allarme
- Genera eventi/allarmi in base allo stato dei servizi
- Integrazione Plug-in prodotti di terze parti

ETÆRIA
a WIIT Company

Log Management (LM)

Raccolta e analisi dei Log



Compressi

Cifrati

Verifica Firma

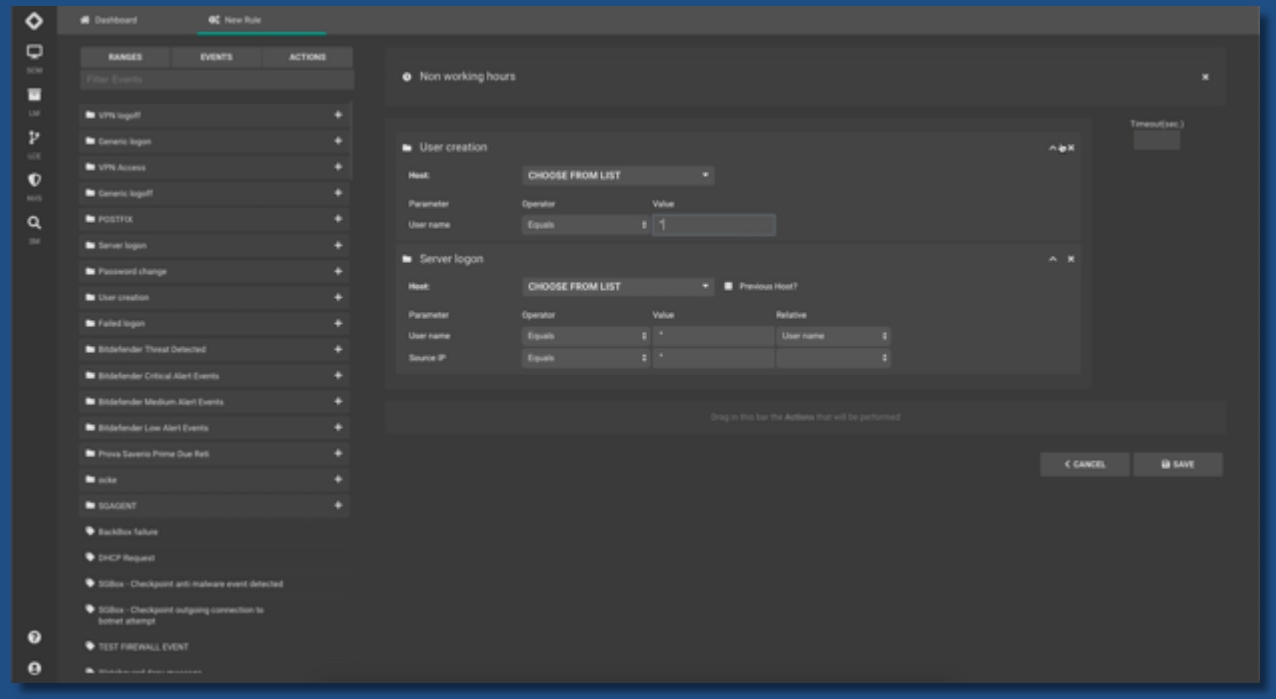
D.Lgs. 196 Obbligo di acquisizione dei log di accesso degli amministratori di sistema e obbligo di conservazione per almeno 6 mesi con modalità che ne garantiscanola completezza, l'inalterabilità e l'integrità.

- Raccolta di LOG da qualsiasi data source
- Agentless o utilizzo di Agent proprietario
- Estrae eventi dalle informazioni raccolte
- Strumento di analisi a fronte di anomalie riscontrate
- Rappresentazione grafica e generazione di report personalizzati su quanto analizzato
- Gestisce elevate quantità di informazioni
- Conservazione per un periodo arbitrario

ETÆRIA
a WIIT Company

log correlation engine (LCE)

correlazione degli eventi



- Analisi degli eventi ricevuti dall'infrastruttura e/o dai moduli di SGBox
- Generazione allarmi Automatici a fronte di una sequenza di eventi non rispetta
- Allarmi generati in varie modalità e verso più utenti
- Regole "standard"
- Semplicità nella creazione di una regola

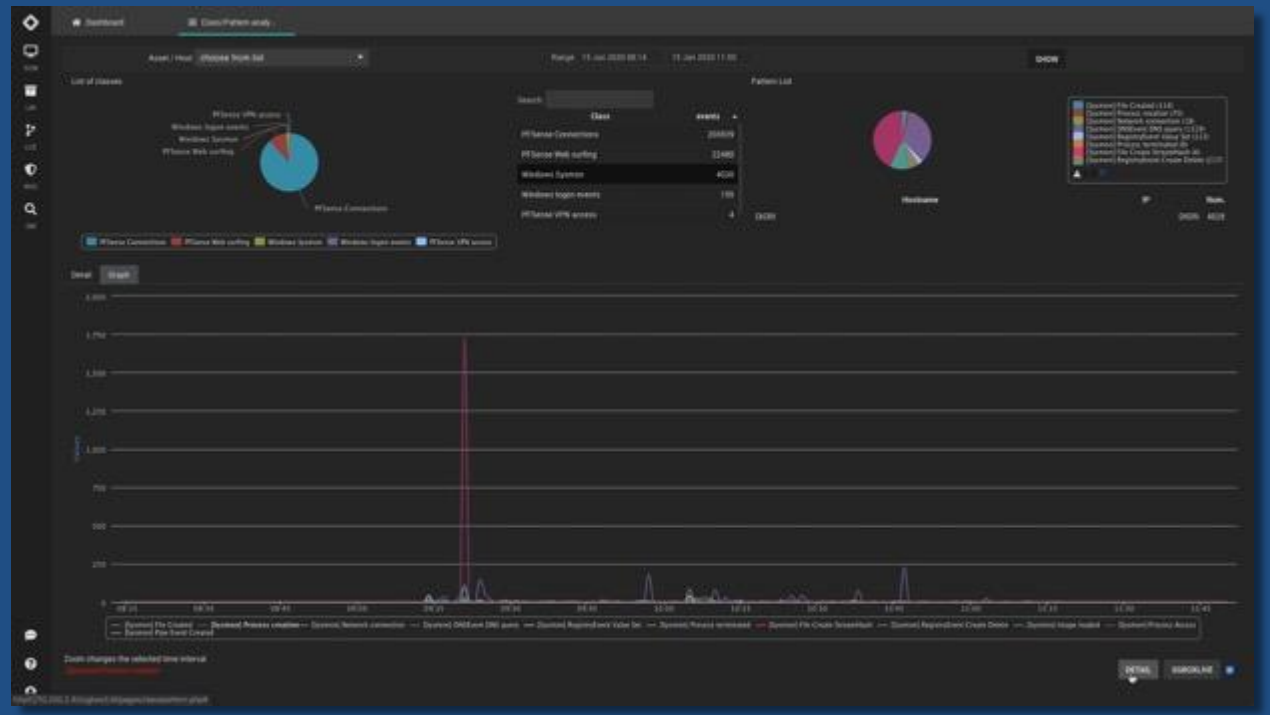
- Esecuzione di SCRIPT automatici
- Esecuzione di APP

Integrazione nativa con tecnologie di terze parti

ETÆRIA
a WIIT Company

Endpoint Threat Detection & Response (ETD)

Rilevamento avanzato di Anomalie e Attacchi ai sistemi Microsoft

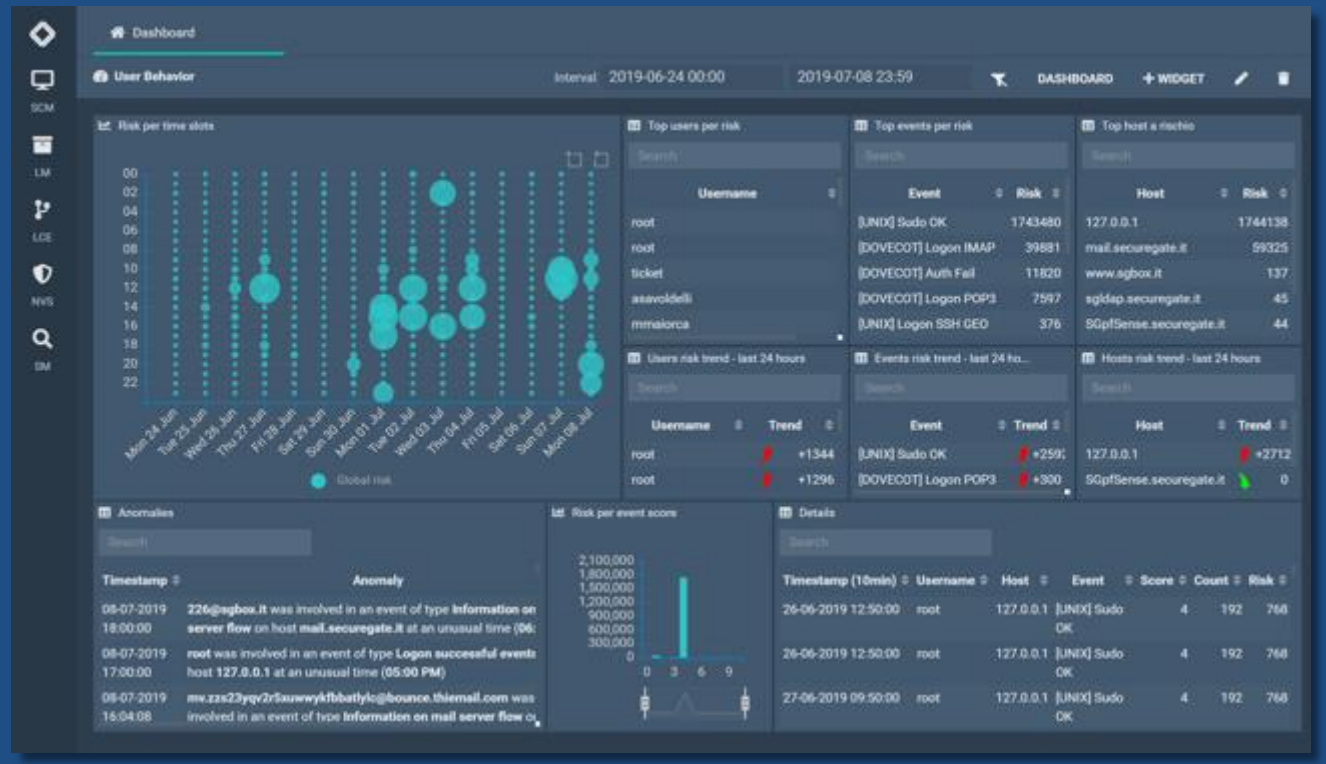


- Funzionalità di Endpoint Detection and Response (EDR) per le piattaforme Microsoft Windows
- Permette l'identificazione degli indicatori di compromissione (IoC) sugli endpoint
- Mappatura degli indicatori con il framework MITRE ATT&CK
- Rappresentazione in dashboard dedicate (processi, connessioni di rete)
- Generazione di allarmi automatici (mail, Telegram, chiamate API)
- Non richiede una licenza commerciale (componente Microsoft gratuita)
- Installabile tramite package SGBox in pochi minuti

ETÆRIA
a WIIT Company

User Behavior Analytics (UBA)

Analisi del comportamento



- Raccolta dati relativa alle attività degli uten
- Identificazione automatica dei comportamenti anomali
- Categoria di rischio associate all'utente
- Allarmi facilmente interpretabili
- Visualizzazioni delle anomalie attraverso le dashboard

ETÆRIA
a WIIT Company

Vulnerability Scanner (NVS)

Gestione e verifica delle vulnerabilità

- Verifica le vulnerabilità dei sistemi, dei servizi e delle applicazioni WEB
- Fornisce una vista d'insieme sullo stato di sicurezza degli asset
- Schedulazione delle scansioni programmabile
- Report differenziali su più livelli e personalizzati
- Report programmati a fronte di scansioni ed indirizzati ai responsabili degli asset
- ISO27001, Auditing PCI-DSS, Misure Minime di Sicurezza ICT…

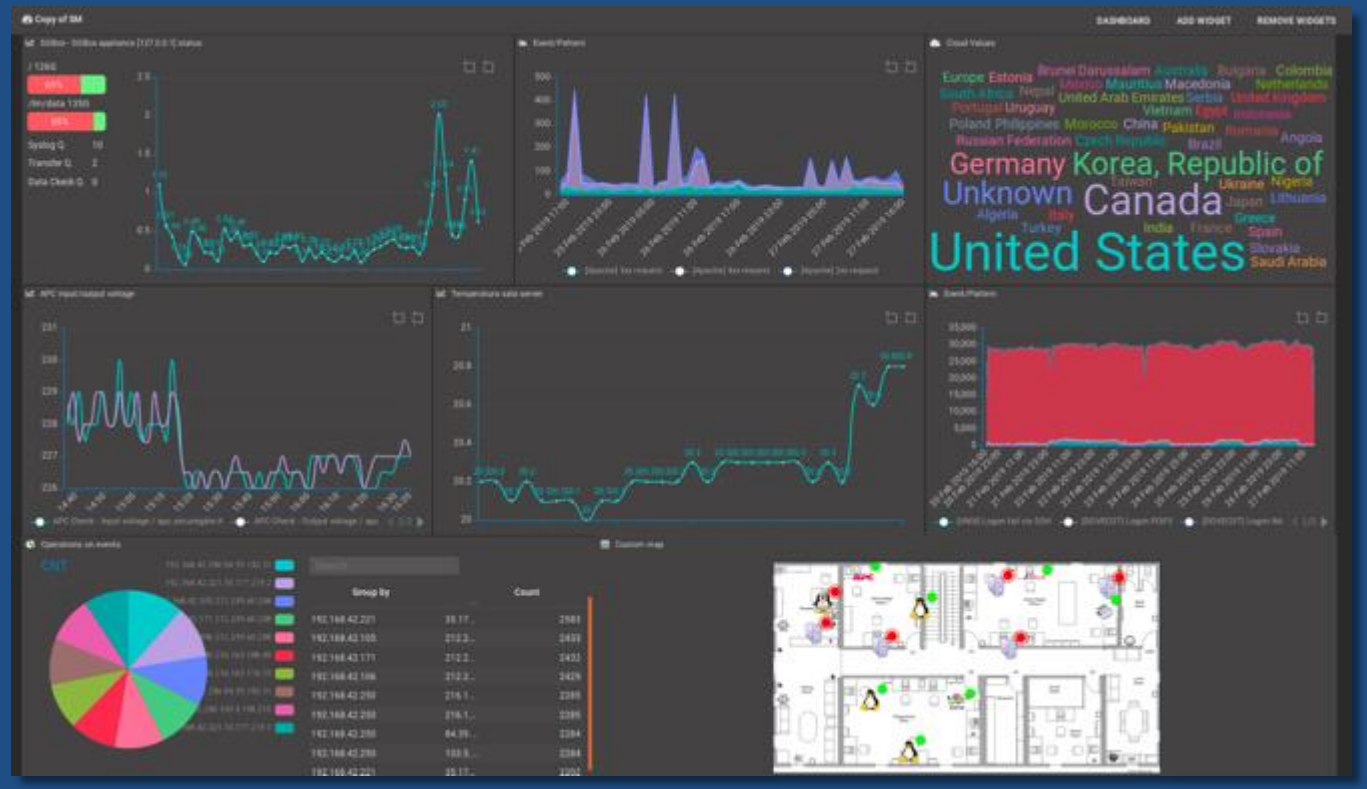
- Indice di vulnerabilità secondo lo standard internazionale CVSS
- Attribuzione di priorità per la fase di "REMEDIATION"

cvss · Agenzia per l'Italia Digitale, Presidenza del Consiglio dei Ministri · PCI Security Standards Council · ISO 27001

ETÆRIA a WIIT Company

Security Control Management (SCM)

CONSOLE CENTRALIZZATA



- Rappresentazione grafica delle informazioni raccolte dai diversi moduli
- Autenticazione su directory esterna (autenticazione unica)
- Assegnazione permessi (granulari) per gruppi utente
- Modificare visibilità degli oggetti per gruppi utenti (profili)

ETÆRIA
a WIIT Company


ETÆRIA
a WIIT Company
partnership
dialogo relazioni
sfide idee
strategia lavoro
obiettivi squadra
opportunità
A TUTTI
UN OTTIMO
2022
CHECK POINT™