

ITA



Cyber Threat Hunting

BY CY4GATE

Cos'è la soluzione di Cyber Threat Hunting di CY4GATE?

Tramite approccio proattivo alla *detection* delle minacce, la soluzione di Cyber Threat Hunting di CY4GATE ricerca attivamente e scopre, grazie al motore di intelligenza artificiale comportamentale, eventuali pattern di anomalie che potrebbero indicare la presenza di minacce. Grazie al monitoraggio attivo e in near-real time degli

indicatori di compromissione (IOCs), è infatti possibile rilevare anomalie e inibire l'attaccante, mitigando l'impatto della minaccia. Tale approccio riduce la *time to response*, permettendo al *security analyst* di rispondere e reagire in maniera appropriata con interventi rapidi ed efficaci.

Una soluzione innovativa ad un problema in continua evoluzione

Il problema

 **Minacce** sempre più **frequenti e complesse** rendono fondamentale un approccio proattivo, anziché reattivo, alla loro rilevazione.

 Gli **enormi volumi di log e dati** complicano ulteriormente l'individuazione generando un numero ingestibile di allarmi, spesso falsi positivi.

 La **complessità distribuita** dell'ambiente IT crea la necessità di una visione olistica per poter correlare i dati ed individuare eventuali pattern.

 Eccessivi *dwell time* consentono a loro volta tempi prolungati di accessi non autorizzati, esfiltrazione di dati ed altre attività malevole.

 La **carenza di risorse** qualificate ed i **costi elevati** d'implementazione e manutenzione delle tecnologie rendono necessaria l'offerta di soluzioni *cost-effective* per l'**efficientamento delle risorse**.

La soluzione

 La soluzione di Cyber Threat Hunting by CY4GATE permette la ricerca attiva e la corretta interpretazione di anomalie e **pattern malevoli**, grazie al **motore di intelligenza artificiale comportamentale**.

 Un unico punto di vista per l'analista permette una **navigazione più efficiente**, aiutando a rilevare le entità ed i pattern e prevedere le minacce.

 L'automazione della raccolta dati e dell'analisi delle minacce grazie all'IA ed il ML migliora la **time to response**.

 L'integrazione della **multi-verdict evaluation** e la **rilevazione comportamentale** permettono di usufruire di processi semi-automatizzati che aumentano l'accuratezza della scoperta di minacce, consentendo l'efficientamento delle risorse e la riduzione dei false alert.

Cosa ci distingue dagli altri?

Siamo diversi. Guarda come.



ADVANCED UEBA: Algoritmi di Composite AI basati su profiling, correlation rules, UEBA e ML per **efficientare l'analisi** di grandi volumi di dati



APPROCCIO TIME MACHINE: Possibilità di **navigare flessibilmente** attraverso i dati indietro nel tempo per sfruttare al massimo le potenzialità del Retro Hunting



SCALABILITÀ ED AFFIDABILITÀ: **Approccio cloud-oriented** e modulare della soluzione pensata in ottica **Multi-Tenancy**



VISUALIZZAZIONE DATA EXPLOITATION: Customizzazione di **Dashboard e widgets**, insight e visualizzazione avanzati



MULTIMODAL INTERACTION FOR DATA VISUALIZATION: **Visualizzazione avanzata** basata su consequenzialità su linea temporale, aggregazione su dashboard e relazioni su grafo



COMPLIANCE: La soluzione **risponde ai requisiti** di carattere normativo in ambito compliance (i.e. GDPR)



5 Unique Selling Points per il Cyber Threat Hunting di CY4GATE

E quindi, perché sceglierci?

1. **Facilità di adozione:** breve tempo di ramp-up per l'adozione, facilità d'uso e possibilità di **customizzazione** con integrazione verso tecnologie IT/OT/IoT
2. **Soluzione disponibile per deploy** OnPrem e SaaS
3. **Integrabilità prima di tutto:** una soluzione pensata primariamente per integrarsi in ecosistemi cyber/IT anche complessi, per potenziare le capacità di osservability, detection e response a vantaggio degli analisti.
4. **Verticalizzazione e approccio multi-domain verso OT/IoT:** architettura modulare e capacità use case-specific di finetuning per adattarsi a specifiche esigenze settoriali in ambito OT/IoT
5. **Composite AI:** CY4GATE è riconosciuto da GARTNER® come Representative Vendor in Composite AI grazie al know-how in materia di AI applicata a soluzioni di cyber security e decision intelligence

Una soluzione pensata, progettata e realizzata per rispondere anche alle esigenze dei Security Service Providers

Conosciamo l'importanza del ruolo degli MSSP e MDR nel cyber domain, per questo abbiamo pensato soluzioni e business model per scalare e crescere insieme

Il Cyber Threat Hunting di CY4GATE è pensato per rispondere alle esigenze dei Security Service Providers.

- Multi-Tenancy
- Integrazione prima di tutto: soluzione pensata per integrarsi e non per sostituire tecnologie esistenti, con forte capacità di verticalizzazione in ambito OT/IoT
- Pricing model aggressivo e vantaggioso
- Scalabilità ed affidabilità di una soluzione fruibile On Premise e in SaaS
- Soluzione pensata per l'ottimizzazione delle FTE interne al SOC: efficientamento e riduzione di attività a basso valore aggiunto
- Un Partner Program chiaro multi-level con supporto tecnico dedicato

Prova la soluzione di Cyber Threat Hunting, entra nel mondo Cy4Gate

