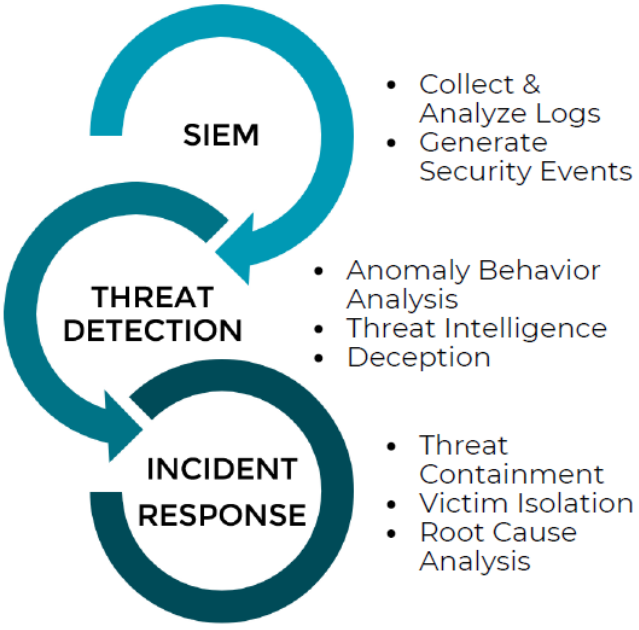
BLUE TEAM HACKING DEFENSE

IN-SIGHT | INCIDENT, DETECTION & RESPONSE



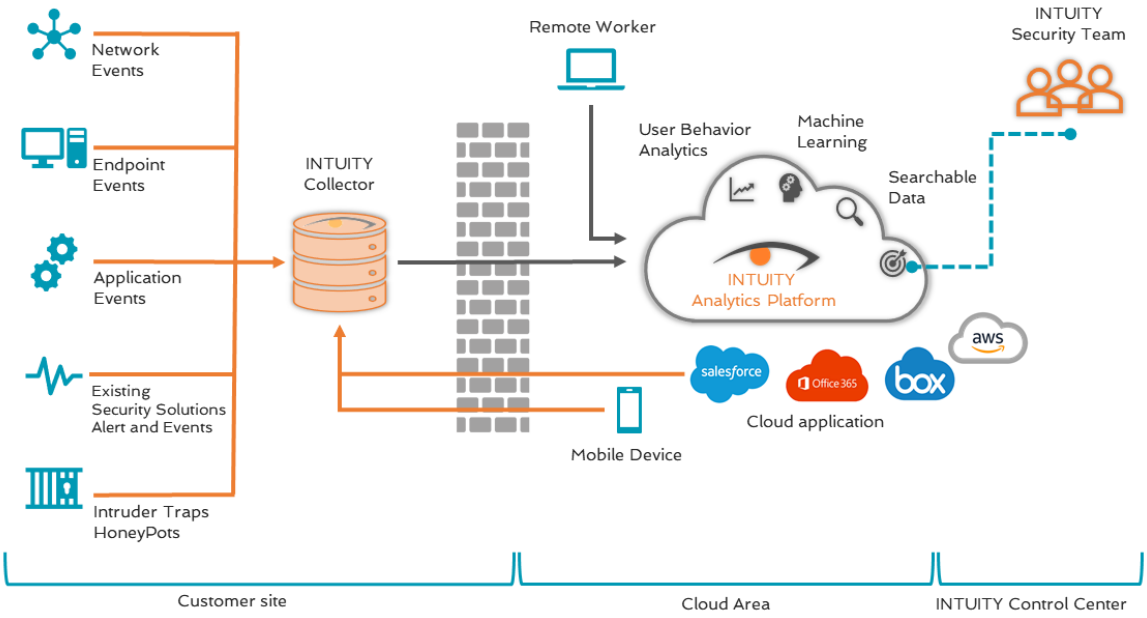
Per aumentare la capacità di rilevazione di un attacco in corso e reagire nel più breve tempo possibile, è possibile attivare funzionalità di **Deception** quali: Honeypot, Honeyfile, Honeyuser, Honeycredential.

Il servizio INTUITY IN.SIGHT nasce dalla consapevolezza, maturata nell'erogazione di servizi Red Team, di quali sono i metodi, gli strumenti e le procedure usati durante un attacco informatico e, di conseguenza, quali siano le strategie più efficaci per rilevarlo e bloccarlo. Per questo motivo il servizio IN.SIGHT è erogato sia da analisti che da Ethical Hacker.

Il servizio è rivolto alle aziende che vogliono dotarsi di un servizio per la rilevazione e la gestione di incidenti informatici o che desiderino estendere la copertura di servizi esistenti includendo visibilità su quanto accade a livello di Endpoint (PC e Server), sui dispositivi in mobilità (Laptop, Smartphone e Tablet) o sui sistemi Cloud (AWS, Google, Microsoft e altri).

Il servizio consente di aumentare la visibilità ed il controllo su quanto accade in azienda, consentendo di reagire tempestivamente, prevenire un danno e rispettare la compliance agli standard di sicurezza più comuni quali: ISO27001, GDPR, PCI DSS.

ARCHITETTURA



Powered by RAPID7

L'architettura del servizio prevede l'installazione di uno o più collettori presso la sede cliente, la distribuzione di un agente su PC, Server, Mobile device e l'interfacciamento con i servizi Cloud di interesse.

Le funzionalità di correlazione sono svolte da una piattaforma in cloud (nel rispetto della normativa GDPR), mentre l'analisi e la comunicazione con il cliente è garantita dal team di specialisti. Il servizio è in grado di garantire risultati sin dalla sua attivazione in quanto, grazie agli agenti distribuiti, riconosce immediatamente le principali minacce e qualunque anomalia sia riconducibile a metodologie di attacco note.

DELIVERABLE

- Technical Report: settimanale
- Executive Report: mensile
- In caso di allarme critico "Alarm", il Security Team prende in carico il problema ed inizia l'analisi, applicando le azioni di contenimento previste. È possibile definire delle azioni automatiche in modo da bloccare la minaccia appena questa viene rilevata. Il Security Team ed il cliente saranno in contatto continuo fino a chiusura dell'incidente.
- In caso di segnalazioni importanti "Notable Behavior", il Security Team inizierà l'analisi entro il giorno lavorativo successivo fino a determinare la più appropriata azione da intraprendere. Il cliente è avvisato dell'analisi in corso e viene aggiornato sui suoi sviluppi, fino alla chiusura dell'incidente.
- Open link con INTUITY Red Team per consulenza e supporto.

USE CASE

- Security Operation and Competence Center per PMI ed Enterprise.
- Add-On per servizi SOC esistenti: visibilità aumentata verso Endpoint, Cloud e Utenti mobili.
- Integrazione con altri strumenti già implementati (Network Analyzer, Advanced Threat Protection System).