
KASPERSKY lab
17:25:41
Centro operativo
di sicurezza
Kaspersky Lab
www.kaspersky.it

Mentre le aziende affinano le proprie strategie di protezione, i cybercriminali ideano tecniche sempre più sofisticate per penetrare i muri di sicurezza da esse eretti. Sempre più autori di minacce vanno alla ricerca di falle nei sistemi di sicurezza, attratti dalle impareggiabili opportunità di guadagno offerte dagli attacchi informatici.

Per risolvere i problemi di sicurezza nel momento stesso in cui insorgono, fornendo risposte e soluzioni rapide, stanno nascendo sempre più centri operativi di sicurezza.

"I centri operativi di sicurezza (SOC) devono essere strutturati per l'intelligence e comprendere un'architettura adattiva di sicurezza che tenga conto del contesto e si basi sull'intelligence. I responsabili della sicurezza devono comprendere in che modo i SOC basati sull'intelligence usino strumenti, processi e strategie per proteggersi dalle minacce moderne".

Gartner, "The Five Characteristics of an Intelligence-Driven Security Operations Center" (Le cinque caratteristiche di un centro operativo di sicurezza basato sull'intelligence), novembre 2015

IL CENTRO OPERATIVO DI SICUREZZA È UNA FUNZIONE CENTRALIZZATA PER IL MONITORAGGIO E L'ANALISI COSTANTE DELLE MINACCE, PER LA MITIGAZIONE E LA PREVENZIONE DEGLI INCIDENTI DI CYBERSECURITY

Un sondaggio condotto di recente da B2B International (in pubblicazione alla fine del 2016) su oltre 4000 aziende in 25 paesi, ha rilevato che:

- Il **38%** degli intervistati ha riscontrato **gravi problemi con virus e malware** nei 12 mesi precedenti, con conseguente perdita di produttività.
- Il **21%** ha subito **perdita/esposizione dei dati a causa di attacchi mirati**.
- Circa il 40% degli intervistati ha definito tali sfide un problema specifico.
- Il **17%** delle aziende ha subito un **attacco DDoS** nei 12 mesi precedenti, spesso più di una volta.
- Il **42%** di tutti gli intervistati che hanno subito **attacchi di phishing** è rappresentato da aziende.
- Il **26%** di tutti i problemi di sicurezza **è rimasto non rilevato** per settimane o periodi più estesi ed è stato scoperto solo a seguito di controlli di sicurezza esterni.
- Per una grande azienda che subisce almeno una violazione dei dati, **l'impatto finanziario medio** si è rivelato pari a **891 mila $** (che comprendono stipendi per personale interno aggiuntivo, danni ai rating del credito/premi assicurativi, affari mancati, pubbliche relazioni extra per la riparazione dei danni all'immagine del marchio e assunzione di consulenti esterni).
- Le cifre dell'**impatto** per le grandi aziende **variano da 393 mila $ a 1,1 milioni di $**, a seconda del momento in cui la violazione viene rilevata. Un rilevamento rapido si traduce in costi minori per l'azienda.
- Il numero totale di informazioni sensibili di clienti/dipendenti compromesse dipende inoltre dal tempo: da 9 mila con rilevamento virtualmente immediato (sistemi di rilevamento in azione) a 240 mila quando la violazione rimane non rilevata per oltre un anno.

Secondo il modello di architettura adattiva di sicurezza proposto da Gartner, per combattere il cybercrimine in un ambiente di minaccia in piena attività, i team del SOC devono essere in grado di:

- PREVEDERE
- RILEVARE
- PREVENIRE
- RISPONDERE

Gartner, "Designing an Adaptive Security Architecture for Protection From Advanced Attacks" (Progettazione di un'architettura adattiva di sicurezza per la protezione dagli attacchi avanzati), febbraio 2014, Foundational January 2016

QUATTRO ELEMENTI CHIAVE

Al fine di adottare questo approccio riconosciuto a livello di settore, è necessario introdurre quattro elementi chiave, insieme a processi definiti in modo chiaro e alle tecnologie pertinenti. I quattro elementi sono:

- **GESTIONE DELLE CONOSCENZE.** Per essere in grado di prevenire e rispondere in modo vincente ad attacchi sempre più sofisticati, il personale (i membri del team SOC) deve essere adeguatamente formato su analisi forense, analisi del malware e risposta agli incidenti.
- **THREAT INTELLIGENCE.** Raccolta da numerose fonti diverse (quanto più varie possibile), è essenziale per rilevare tempestivamente le minacce emerse:
  1. Dati interni sulla minaccia
  2. Intelligence da fonti open-source (OSINT)
  3. CERT del settore
  4. Fornitori globali di soluzioni anti-malware
- **THREAT HUNTING.** Per cercare in modo proattivo le minacce che i sistemi di sicurezza tradizionali quali firewall, IPS/IDS, SIEM e così via, non sono in grado di rilevare.
- **PANORAMA DELLE RISPOSTE AGLI INCIDENTI.** Applicato per limitare i danni e ridurre i costi di correzione.

Ognuno di questi elementi è ugualmente importante e merita una considerazione separata.

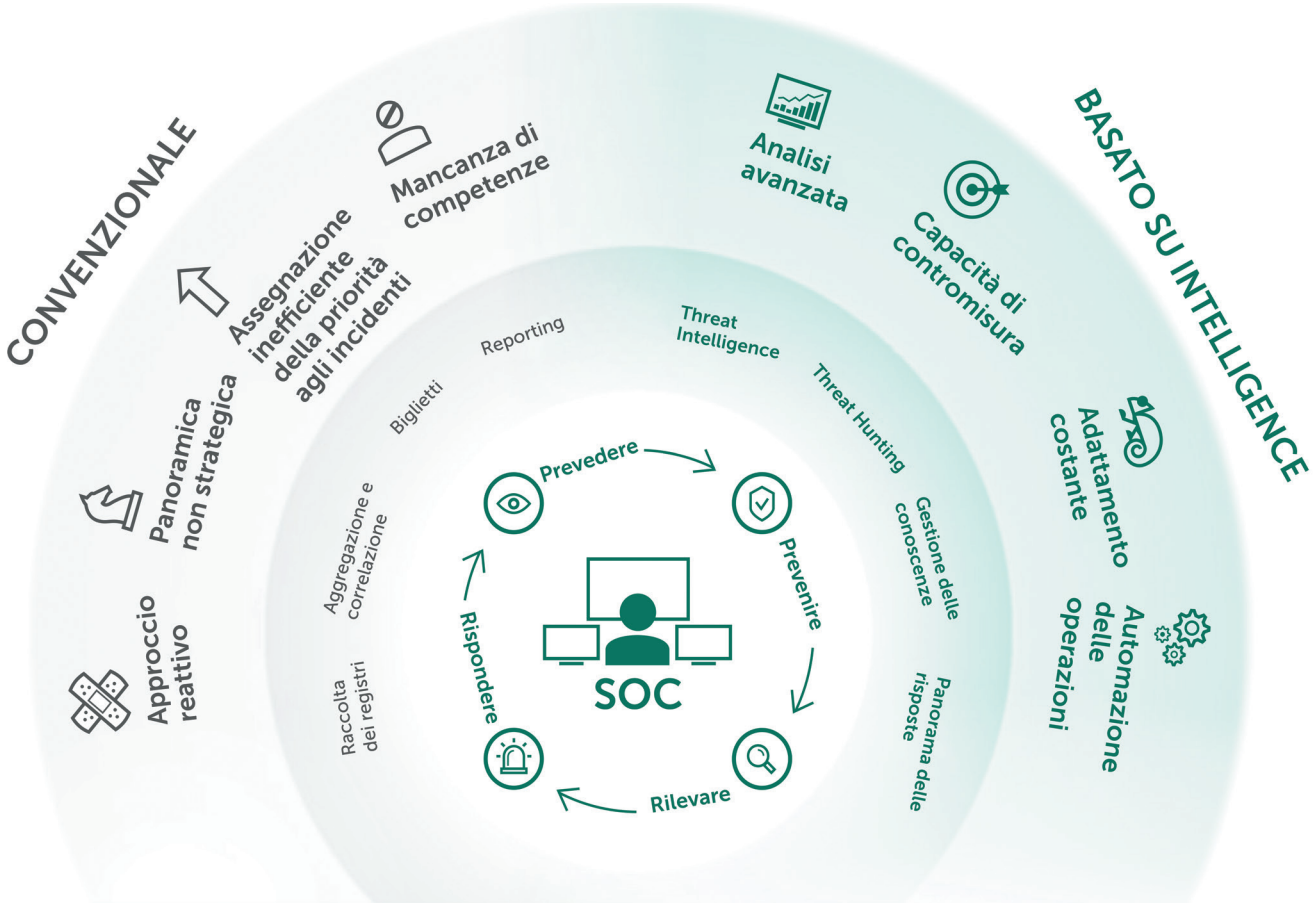


Figura 1:
I quattro elementi chiave del SOC

GESTIONE DELLE CONOSCENZE

Il SOC deve garantire un pool di competenze pratiche ed esperienza sufficiente per analizzare un'enorme quantità di dati e per valutare quando sono richieste ulteriori indagini.

Un budget limitato pone difficoltà al reclutamento del personale per il team SOC.

Attualmente, il mercato è carente di esperti in cybersecurity con una formazione adeguata. Ciò causa un aumento dei costi per reclutamento e assunzione.

Il membro ideale per il team SOC deve avere:
- Una mente curiosa, in grado di creare un quadro integrato complessivo da frammenti di dati sparsi.
- La capacità di mantenere concentrazione costante, resistendo a livelli elevati di stress.
- Una buona competenza generale nel settore IT e della cybersecurity, preferibilmente con notevole esperienza pratica.

Se l'azienda è alla ricerca di risorse per i ruoli SOC, che sia tramite reclutamento esterno o promozione interna, trovare membri del team con le competenze desiderate già acquisite non è semplice. Si renderà necessaria una formazione continua, non solo per colmare i vuoti tra le competenze già acquisite e quelle richieste, ma anche per preparare i membri del team ad affrontare tecnologie di sicurezza in continuo cambiamento e ambienti di minacce in costante evoluzione.

Risposta agli incidenti, analisi forense e analisi del malware sono competenze indispensabili.

RISPOSTA AGLI INCIDENTI E ANALISI FORENSE	ANALISI DEL MALWARE
• Risposta agli incidenti tempestiva ed accurata • Analisi delle prove (immagini del disco rigido, dati estratti dalla memoria, tracce di attività sulla rete) e ricostruzione della cronologia e della logica dell'incidente • Scoperta delle fonti presunte dell'attacco e degli altri sistemi potenzialmente compromessi (se possibile) • Comprensione della causa alla radice dell'incidente per prevenire il verificarsi di incidenti simili	• Ottenimento e comprensione del campione di software dannoso e delle sue capacità • Individuazione del malware, qualora di questo si tratti • Determinazione dell'impatto potenziale del campione sui sistemi compromessi all'interno dell'organizzazione • Creazione di un piano di correzione completo, basato sul comportamento del malware rilevato

Kaspersky Lab offre:
Servizi di formazione sulla cybersecurity

Da oltre 17 anni, l'esperienza di Kaspersky Lab in materia di cybersecurity, che include rilevamento delle minacce, ricerca del malware, reverse engineering e analisi forense, si evolve e avanza continuamente. I nostri esperti sanno come gestire al meglio le minacce poste dai 325.000 tipi di malware con cui ogni giorno ci interfacciamo e in che modo impartire tale conoscenza ed esperienza pratica alle organizzazioni nel momento in cui devono affrontare i nuovi pericoli posti dalla realtà informatica contemporanea.

Il nostro programma di formazione sulla sicurezza è stato progettato e sviluppato da autorità del settore che hanno contribuito alla creazione dei laboratori anti-virus di Kaspersky e che oggi ispirano e fungono da mentori per la nuova generazione di esperti in tutto il mondo.

I corsi prevedono sia lezioni teoriche che laboratori pratici. Al completamento di ogni corso, gli studenti sono invitati a convalidare le loro conoscenze sostenendo una valutazione.

I corsi di formazione sono indirizzati a professionisti del settore IT in possesso di competenze, avanzate o generali, di programmazione e gestione dei sistemi. Tutti i corsi sono erogati in classe, su richiesta del cliente, o presso uffici locali di Kaspersky Lab, se disponibili.

DESCRIZIONE DEL PROGRAMMA

ARGOMENTI	DURATA	COMPETENZE ACQUISITE
ANALISI FORENSE		
• Introduzione all'analisi forense • Acquisizione di prove e risposta live • Elementi interni di Windows Registry • Analisi degli elementi di Windows • Analisi dei browser • Analisi delle email	5 giorni	• Creare un laboratorio di analisi forense • Raccogliere prove digitali e gestirle correttamente • Ricostruire un incidente e utilizzare indicatori orari • Individuare tracce di intrusione negli elementi del sistema operativo Windows • Trovare e analizzare la cronologia dei browser e delle email • Applicare con fiducia strumenti e tecniche di analisi forense
ANALISI DEL MALWARE E REVERSE ENGINEERING		
• Obiettivi e tecniche di analisi del malware e reverse engineering • Elementi interni di Windows, file eseguibili, assembler x86 • Tecniche di analisi statica di base (estrazione di stringhe, analisi delle importazioni, punti di ingresso PE immediati, decompressione automatica, ecc.) • Tecniche di analisi dinamica di base (debugging, strumenti di monitoraggio, intercettazione del traffico, ecc.) • Analisi dei file .NET, Visual Basic, Win64 • Tecniche di analisi basate su script e non PE (file batch, AutoIt, Python, JScript, JavaScript, VBS)	5 giorni	• Creare un ambiente protetto per l'analisi del malware: implementazione di strumenti di sandbox e di tutti gli strumenti necessari • Comprendere i principi dell'esecuzione dei programmi di Windows • Decomprimere, eseguire il debugging e analizzare oggetti dannosi e identificarne le funzioni • Rilevare siti dannosi attraverso l'analisi del malware basata su script • Condurre una rapida analisi del malware

ARGOMENTI	DURATA	COMPETENZE ACQUISITE
ANALISI FORENSE AVANZATA		
• Analisi di Windows approfondita • Recupero dei dati • Analisi di rete e cloud • Analisi della memoria • Analisi della tempistica • Esempi pratici per l'analisi di attacchi mirati nel mondo reale	5 giorni	• Essere in grado di eseguire un'analisi approfondita del file system • Essere in grado di recuperare file eliminati • Essere in grado di analizzare il traffico di rete • Rivelare attività dannose da immagini della memoria • Ricostruire la tempistica dell'incidente
ANALISI DEL MALWARE AVANZATA E REVERSE ENGINEERING		
• Tecniche avanzate di analisi statica (analisi statica del codice della shell, analisi dell'intestazione PE, TEB, PEB, funzioni di caricamento tramite riversi algoritmi di hash) • Tecniche avanzate di analisi dinamica (struttura PE, decompressione manuale e avanzata, decompressione di sistemi di compressione dannosi che archiviano l'eseguibile completo in forma crittografata) • Reverse engineering delle APT (uno scenario di attacco APT, che parte da e-mail di phishing per introdursi quanto più in profondità possibile) • Analisi del protocollo (analisi del protocollo di comunicazione C2 crittografato, metodi di decrittografia del traffico) • Analisi di rootkit e bootkit (debug del settore di avvio tramite le tecniche di debug Ida, VMWare e Kernel utilizzando 2 macchine virtuali, analisi di campioni di rootkit)	5 giorni	• Essere in grado di attenersi alle best practice del reverse engineering, riconoscendo i trucchi di anti-reverse engineering (offuscamento, anti-debugging) • Essere in grado di applicare l'analisi avanzata del malware a dissezioni di rootkit/bootkit • Essere in grado di analizzare il codice della shell degli exploit incorporato nei diversi tipi di file e il malware non Windows
RISPOSTA AGLI INCIDENTI		
• Introduzione alla risposta agli incidenti • Rilevamento e analisi primaria • Analisi digitale • Creazione di regole di rilevamento (YARA, Snort, Bro)	5 giorni	• Differenziare le APT da altre minacce • Comprendere le diverse tecniche dei cybercriminali e l'anatomia degli attacchi mirati • Applicare metodi specifici per monitoraggio e rilevamento • Seguire il flusso di lavoro per la risposta agli incidenti • Ricostruire la cronologia e la logica dell'incidente • Creare regole di rilevamento e generare report

Gli strumenti cambiano nel tempo, ma le nozioni di base e i metodi di lavoro rimangono costanti. I partecipanti non riceveranno solo un insieme di strumenti e istruzioni, ma conoscenze dei principi e delle funzionalità di base. Tutte le attività pratiche sono basate su casi reali, laddove possibile nel rispetto della riservatezza dei clienti.

THREAT INTELLIGENCE E THREAT HUNTING

Il SOC è stato originariamente istituito per offrire:

- Gestione dei dispositivi di sicurezza, manutenzione perimetrale e tecnologie di sicurezza preventiva quali IPS/IDS, firewall, proxy, ecc.
- Monitoraggio degli eventi di sicurezza tramite sistemi SIEM (Security Information and Event Management).
- Analisi forense degli incidenti e correzione.
- Conformità interna e alle normative (ad es. PCI-DSS).

Molte organizzazioni intendono ottenere maggiore visibilità, istituendo SOC privati. Tuttavia, alcune delle organizzazioni che hanno già istituito un SOC, continuano a riscontrare numerosi dei problemi del passato.
Diverse sono le ragioni che spiegano questo fenomeno:

- Assegnazione non corretta delle priorità, che comporta che le minacce reali vengono sommerse tra migliaia di avvisi di sicurezza insignificanti ricevuti e analizzati ogni giorno.
- Correzione degli incidenti senza una comprensione adeguata delle tattiche, delle tecniche e delle procedure (TTP) associate agli attori della minaccia, tale che gli attacchi avanzati passano inosservati.
- Falsi negativi causati dalla mancanza di dati sulla minaccia corrispondente.
- Un approccio agli incidenti reattivo piuttosto che un metodo proattivo, che "scova" le minacce rimaste non scoperte ma attive all'interno dell'organizzazione.
- Mancanza di una visione strategica del panorama esistente delle minacce, della consapevolezza sugli attacchi sferrati ad aziende simili, nonché delle contromisure disponibili.

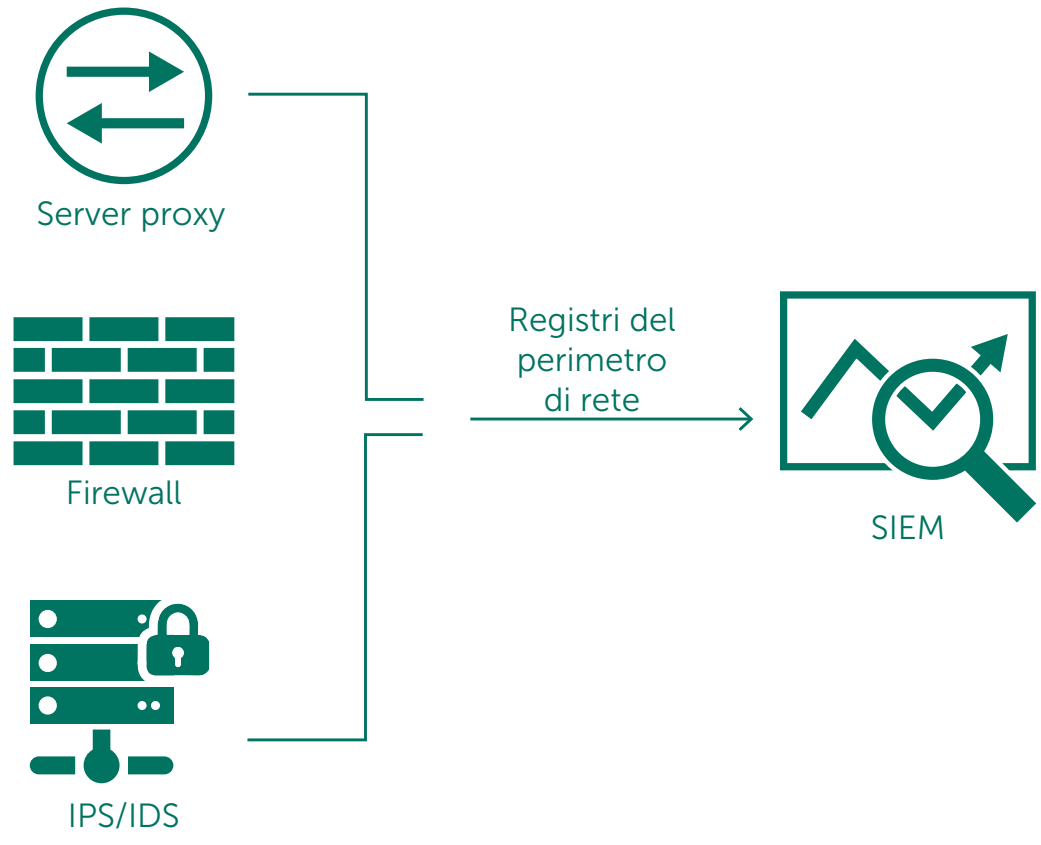


Figura 2:
SOC tradizionale

- Problemi che richiedono investimenti interni adeguati per tecnologie di sicurezza specifiche, a causa delle difficoltà di comunicazione ai dirigenti del consiglio di amministrazione, privi di competenze tecniche, dei rischi associati ai processi aziendali in caso di violazioni della sicurezza.

Gartner definisce la threat intelligence come segue:
"Conoscenza basata sulle prove, inclusi contesto, meccanismi, indicatori, implicazioni e consigli applicabili, relativa a una minaccia esistente o emergente o a un pericolo per le risorse, che può essere utilizzata per prendere decisioni informate sulla risposta del soggetto a tale minaccia o pericolo".

Gartner, How Gartner Defines Threat Intelligence (Come Gartner definisce la Threat Intelligence), febbraio 2016

Sulla base di queste considerazioni, si consiglia ai responsabili della sicurezza di adottare per il SOC un approccio che sia basato sull'intelligence. Per garantire efficienza al SOC, è indispensabile che esso si adatti continuamente alle nuove tecnologie e ai controlli in linea con i notevoli cambiamenti nell'ambiente delle minacce in corso.

Combinando i dati interni sulla minaccia con le informazioni raccolte da diverse fonti (ad es. OSINT o fornitori globali di soluzioni anti-malware), è possibile ottenere una comprensione delle tecniche dell'attacco e dei relativi indicatori di potenziale. Ciò consente alle organizzazioni di sviluppare efficienti strategie di protezione da commodity e attacchi avanzati indirizzati verso determinate organizzazioni.

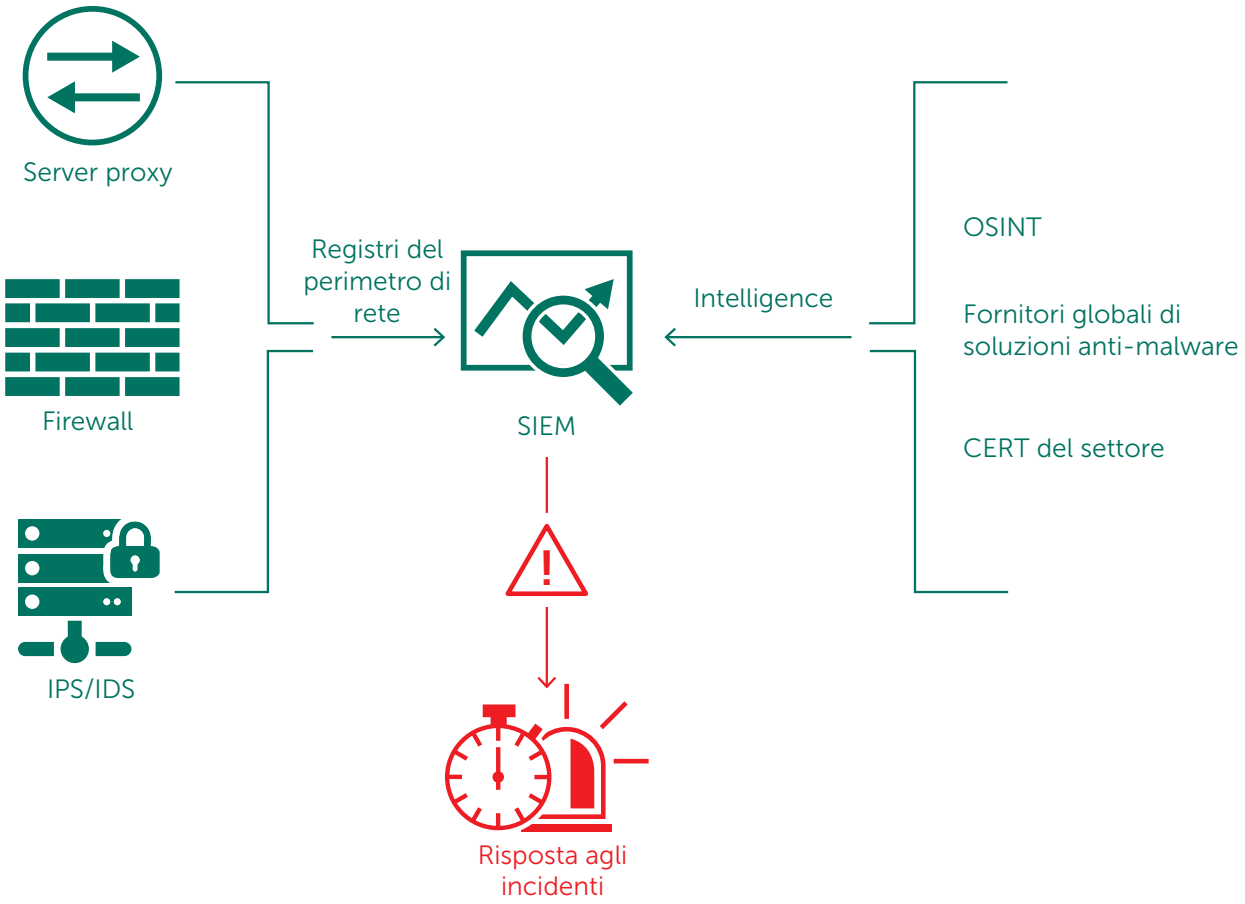


Figura 3:
SOC basato sull'intelligence

Le fonti di intelligence devono essere selezionate accuratamente. Esiste una correlazione diretta tra la qualità dell'intelligence e l'efficacia delle decisioni realizzate sulla base di tale intelligence. Se ci si affida a un'intelligence non pertinente, non accurata o non allineata con il settore o con gli obiettivi dell'azienda, o nel caso in cui i dati sulla minaccia non vengano ricevuti in modo tempestivo, la qualità del processo decisionale dell'organizzazione potrebbe venire gravemente compromesso.

I dati non elaborati e senza contesto non offrono l'attinenza necessaria alla massima efficienza dei team SOC. Ad esempio, sapere che un determinato URL è dannoso è notevolmente diverso dal sapere anche che tale URL viene utilizzato per ospitare un exploit o un tipo di malware specifico. Questo livello aggiuntivo di intelligence istruisce gli esperti di sicurezza dell'azienda su cosa cercare durante l'esplorazione di una macchina infetta.

Cosa cercare nelle fonti esterne di threat intelligence:

- Intelligence con portata globale, che garantisca la più ampia visibilità sugli attacchi.
- Un fornitore con comprovato successo nel rilevamento precoce degli indicatori delle nuove minacce.
- Intelligence con contesto e immediatamente applicabile.
- Formati e meccanismi di implementazione che consentano una semplice integrazione con i controlli di sicurezza esistenti.

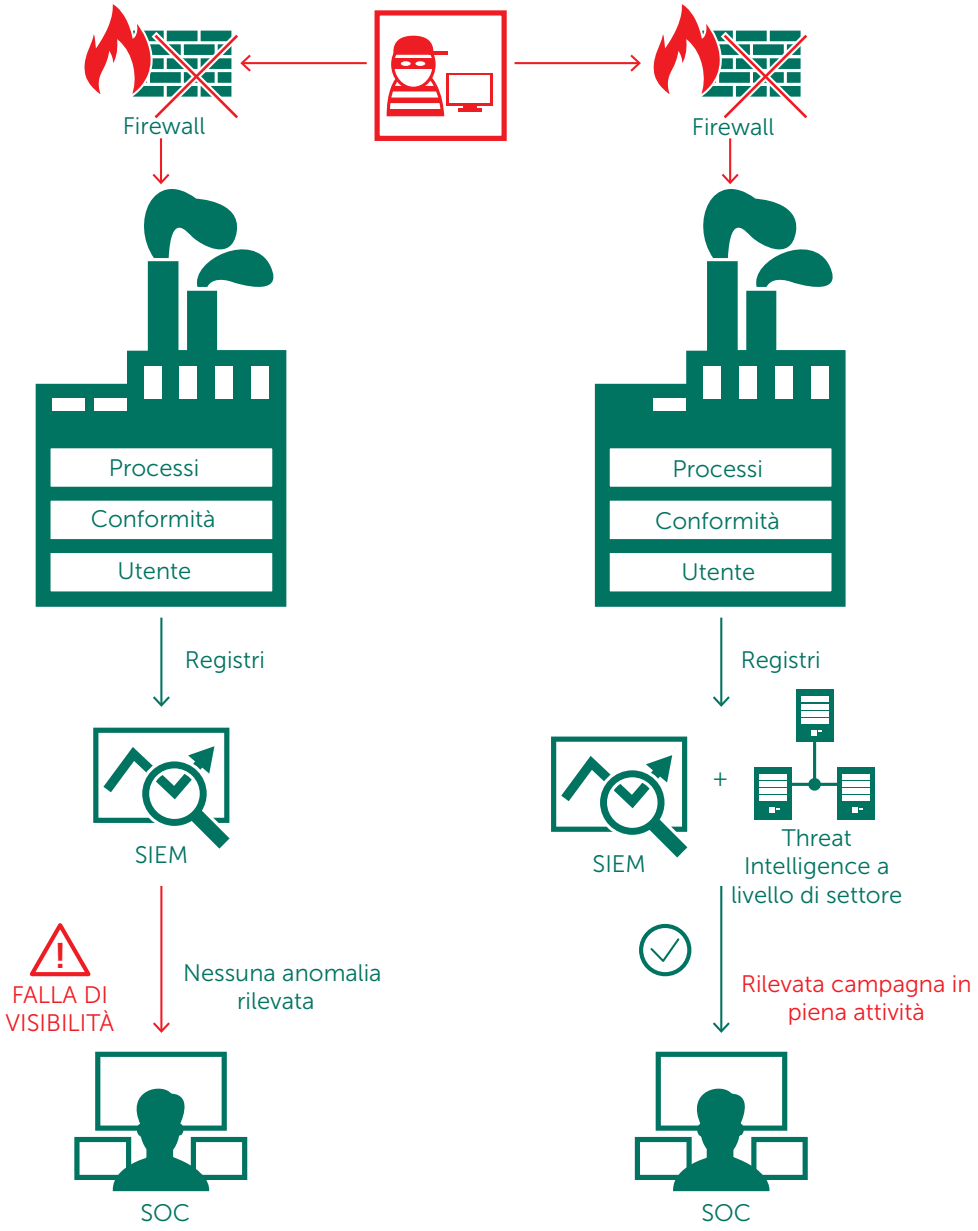


Figura 4:
Modello di threat intelligence

Il Threat Hunting è un altro elemento importante nelle operazioni quotidiane del SOC. Non si tratta di un concetto nuovo. Il rilevamento di minacce avanzate e sconosciute si fonda sull'impegno pratico e scrupoloso degli analisti di sicurezza e non su regole automatizzare o meccanismi di rilevamento basati su firma.

Questo processo implica l'acquisizione e l'applicazione di diverse tecniche (tra cui analisi statistica, apprendimento automatico e visualizzazione) a tutti i dati disponibili, ottenuti da endpoint, reti, controlli di sicurezza implementati, sistemi di autenticazione e così via. L'obiettivo è la conferma di un'ipotesi esistente in merito a una potenziale violazione. Le tecnologie di threat hunting a disposizione degli analisti comprendono alcuni sistemi già menzionati: soluzioni SIEM, OSINT, piattaforme di threat intelligence e altre fonti di dati.

L'analista di threat hunting consulta gli indicatori di compromissione (IOC) ottenuti dall'esterno e applica strumenti specializzati per cercare, negli host dell'organizzazione, tali artefatti (che si presentano sotto forma di indirizzi IP, hash di file, URL, ecc.). Al rilevamento di un chiaro segnale di compromissione della sicurezza, è possibile avviare le procedure di risposta agli incidenti.

Gli esperti altamente qualificati e con grande esperienza sono chiamati a eseguire ricerche approfondite tra volumi di dati enormi al fine di identificare gli artefatti che i sistemi automatizzati non sono riusciti a rilevare.

Kaspersky Lab offre:
Feed di dati sulla threat intelligence

Kaspersky Lab offre aggiornamenti continui dei feed di dati sulla threat intelligence al fine di informare il team SOC delle aziende sui rischi e sulle implicazioni associati alle minacce informatiche e di aiutare l'azienda a mitigare le minacce in modo più efficiente, proteggendosi dagli attacchi ancor prima che vengano sferrati.

DESCRIZIONE DEI FEED

Feed sulla reputazione IP: un set di indirizzi IP con contesto che copre host sospetti e dannosi.

URL nocivi: un set di URL relativi ai siti Web e ai collegamenti più dannosi. Sono disponibili record mascherati e non mascherati.

URL di phishing: un set di URL identificati da Kaspersky Lab come siti di phishing. Sono disponibili record mascherati e non mascherati.

URL dei server di comando e controllo delle botnet: un set di URL dei server di comando e controllo (C&C) delle botnet e oggetti dannosi correlati.

Feed sui dati di whitelisting: un set di hash di file che fornisce soluzioni e servizi di terzi con una conoscenza sistematica del software legittimo.

Feed sull'hash nocivo: per rilevare il malware più pericoloso, diffuso ed emergente.

Feed sull'hash mobile nocivo: un set di hash dei file per il rilevamento di oggetti pericolosi che infettano le piattaforme mobili.

Feed su Trojan P-SMS: un set di hash Trojan con relativo contesto per il rilevamento di Trojan SMS che generano sovrapprezzi per gli utenti di dispositivi mobili, nonché l'attivazione di un autore di attacchi che ruba, elimina e risponde ai messaggi SMS.

URL di comando e controllo delle botnet mobili: un set di URL contestuali che coprono i server di comando e controllo (C&C) delle botnet mobili.

DETTAGLI DEL SERVIZIO

- I feed di dati vengono automaticamente generati in tempo reale, sulla base delle scoperte a livello mondiale (Kaspersky Security Network offre visibilità a una percentuale notevole di tutto il traffico Internet, arrivando a coprire dieci milioni di utenti finali in oltre 200 paesi), e offrono tassi di rilevamento e accuratezza elevati.
- Tutti i record in ogni feed di dati sono completi di contesto di applicabilità (nomi delle minacce, marcature temporali, georilevazione, risoluzione di indirizzi IP di risorse Web infette, hash, popolarità, ecc.). I dati sul contesto consentono di conoscere la situazione generale, favorendo e supportando quindi un ampio uso dei dati. Completi di contesto, i dati possono essere utilizzati più rapidamente per rispondere alle domande su "chi", "cosa", "dove" e "quando", le cui risposte consentono di individuare gli avversari, aiutando le aziende a realizzare decisioni tempestive e ad adottare misure mirate a tutelare l'azienda specifica.
- Formati di diffusione leggeri e semplici (JSON, CSV, OpenIoC, STIX) tramite HTTPS o meccanismi di distribuzione ad-hoc che supportano una semplice integrazione dei feed nelle soluzioni di sicurezza.
- La threat intelligence viene generata e monitorata da un'infrastruttura ad elevata tolleranza di errore, che garantisce disponibilità continua dei dati e prestazioni costanti.
- Integrazione preconfigurata con HP ArcSight, IBM QRadar, Splunk e altri.

Kaspersky Threat Lookup

Kaspersky Threat Lookup fornisce tutte le conoscenze acquisite da Kaspersky Lab sulle cyberminacce e sulle relazioni tra di esse, riunite in un unico e potente servizio Web. L'obiettivo è fornire ai team SOC delle aziende la maggior quantità possibile di dati, per prevenire gli attacchi informatici prima che compromettano l'organizzazione. La piattaforma recupera la threat intelligence più dettagliata e recente su URL, domini, indirizzi IP, hash dei file, nomi delle minacce, dati statistici/analisi comportamentale, dati WHOIS/DNS e così via. Il risultato è la visibilità a livello globale delle minacce nuove ed emergenti, al fine di aiutare i clienti a mettere in sicurezza la propria organizzazione e migliorare la risposta agli incidenti.

DETTAGLI DEL SERVIZIO

- Intelligence affidabile: una caratteristica chiave di Kaspersky Threat Lookup è l'affidabilità dei dati della threat intelligence, completati dal contesto di applicabilità. I prodotti Kaspersky Lab sono leader nel settore secondo i risultati dei test condotti sulle soluzioni anti-malware[1], grazie a un'impareggiabile intelligence di sicurezza e a tassi di rilevamento più elevati, che garantisco una quantità di falsi positivi quasi pari a zero.
- Livelli elevati di copertura in tempo reale: la threat intelligence viene automaticamente generata in tempo reale, sulla base delle scoperte effettuate in tutto il mondo, ed è supportata da Kaspersky Security Network.
- Threat Hunting: proattività nella prevenzione, nel rilevamento e nella risposta agli incidenti, al fine di ridurre al minimo l'impatto e la frequenza. Monitoraggio e rimozione degli attacchi nel minor tempo possibile. Quanto prima la minaccia viene rilevata, tanto minore sarà il danno causato. Quanto più rapidamente hanno luogo le correzioni, tanto prima le attività di rete possono tornare al normale funzionamento.
- Grande varietà di dati: la threat intelligence offerta da Kaspersky Threat Lookup copre una gamma enorme di tipi differenti di dati, tra cui informazioni relative ad hash, URL, IP, whois, pDNS, GeoIP, attributi dei file, dati statistici e analisi comportamentale, catene di download, marcature temporali e tanto altro. Con il supporto di questi dati, è possibile sondare il variegato panorama delle minacce alla sicurezza che le aziende si trovano ad affrontare.
- Disponibilità continua: la threat intelligence viene generata e monitorata da un'infrastruttura ad elevata tolleranza di errore, che garantisce disponibilità continua dei dati e prestazioni costanti.
- Analisi continua da parte degli esperti di sicurezza: centinaia di esperti, tra cui analisti della sicurezza provenienti da tutto il mondo, esperti di sicurezza di fama mondiale del nostro team GReAT e di team di Ricerca e Sviluppo all'avanguardia, contribuiscono alla creazione di una threat intelligence di valore, basata su situazioni reali.

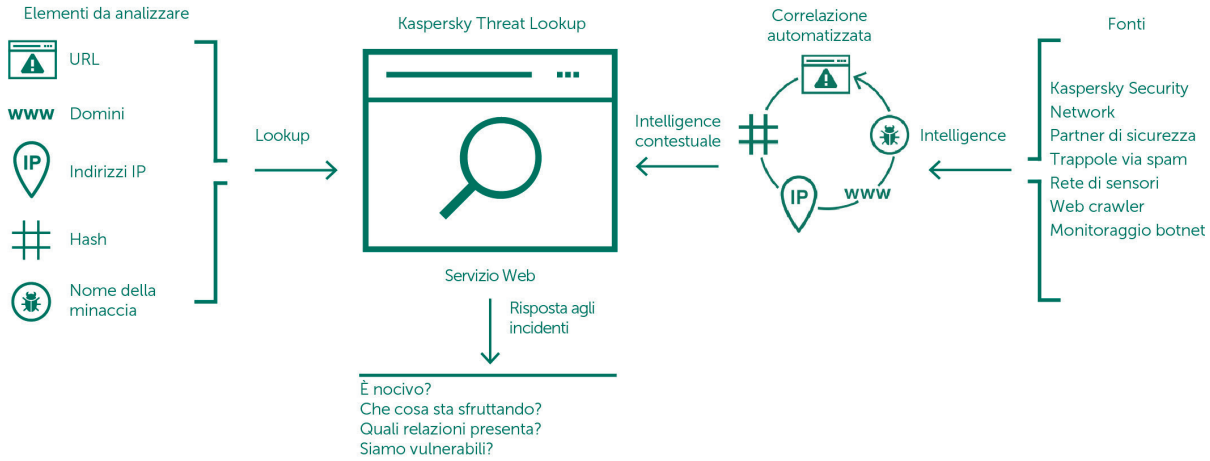
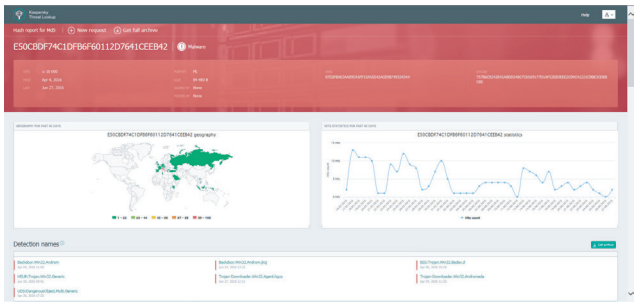
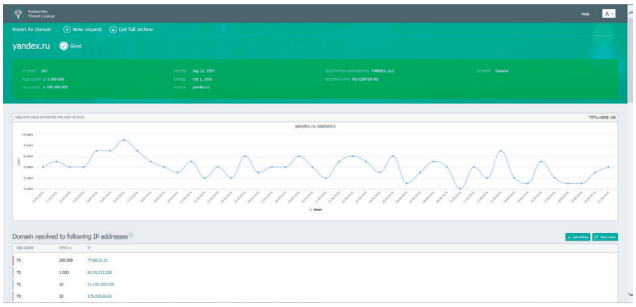


Figura 5:
Kaspersky Threat Lookup

1 http://www.kaspersky.com/top3

- Analisi della sandbox: consente di rilevare le minacce sconosciute eseguendo oggetti sospetti in un ambiente sicuro e analizzando il comportamento completo della minaccia e degli artefatti tramite report intuitivi.
- Ampia gamma di formati di esportazione: è possibile esportare gli indicatori di compromissione (IOC) o il contesto di applicabilità nei formati di condivisione maggiormente utilizzati e organizzati, nonché leggibili dai computer, come STIX, OpenIOC, JSON, Yara, Snort o addirittura CSV, per usufruire di tutti i vantaggi della threat intelligence, per automatizzare il flusso di lavoro operativo o per effettuare l'integrazione con controlli di sicurezza quali SIEM.
- Interfaccia Web o API RESTful di facile utilizzo: consente di utilizzare il servizio in modalità manuale tramite un'interfaccia Web (via browser Web) o di accedervi tramite una semplice API RESTful, a seconda delle preferenze.





Report di intelligence sulle APT

Non tutte le nuove APT (Advanced Persistent Threat) vengono segnalate tempestivamente. La nascita di molte di esse, anzi, non viene mai divulgata. Scegliete di essere i primi a conoscere le nostre ricerche più recenti grazie all'esclusivo report di intelligence sulle APT, contenente informazioni dettagliate e applicabili.

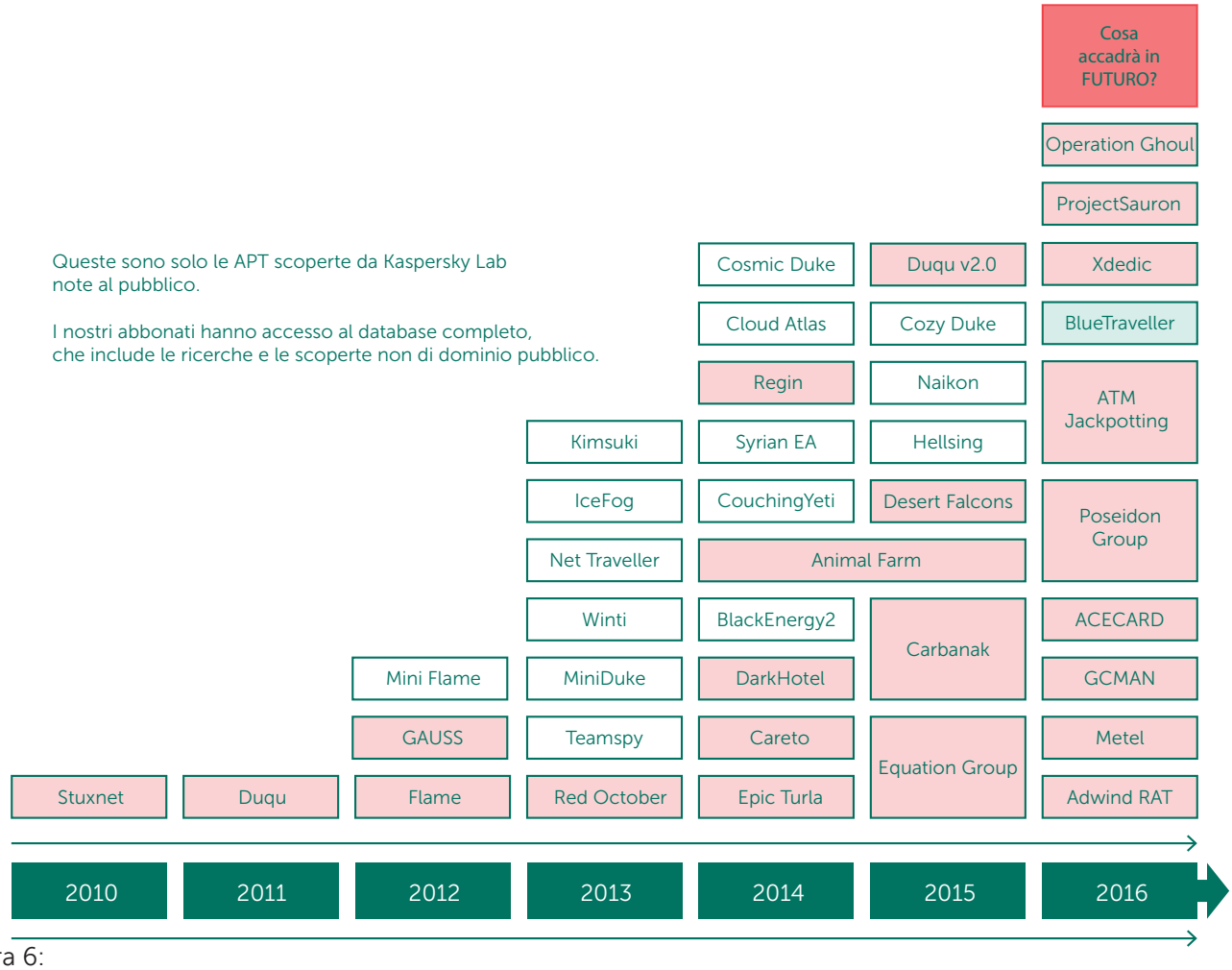


Figura 6:
APT scoperte da Kaspersky Lab

Agli abbonati al servizio di Report di intelligence sulle APT forniamo un utile e costante accesso alle nostre indagini e ai relativi risultati, che comprendono dati tecnici completi in un'ampia gamma di formati su ogni nuova APT scoperta, comprese le minacce che non saranno mai rese pubbliche. I nostri esperti, i più stimati e competenti del settore nella scoperta di nuove APT, vi comunicheranno tempestivamente eventuali cambiamenti rilevati nelle strategie dei gruppi cybercriminali e cyberterroristi. Potrete inoltre usufruire di accesso completo al database dei report sulle APT di Kaspersky Lab, un altro potente strumento di ricerca e analisi che apporta valore aggiunto al vostro arsenale per la sicurezza aziendale.

DETTAGLI DEL SERVIZIO

- Accesso esclusivo a descrizioni tecniche sulle minacce più recenti durante le continue indagini, prima della comunicazione pubblica.
- Approfondimenti sulle APT non pubbliche. Non tutte le minacce di alto profilo vengono comunicate pubblicamente. Alcune di esse, a causa delle vittime che vengono colpite, della sensibilità dei dati, della natura delle vulnerabilità relative ai processi di recupero o di attività relative alle forze dell'ordine, non vengono rese pubbliche. Tuttavia, i nostri clienti ne verranno sempre a conoscenza.
- Dati tecnici dettagliati a supporto, campioni e strumenti, tra cui un elenco esteso di Indicatori di compromissione (IOC), disponibile in formato openIOC, e accesso alle nostre norme Yara.
- Monitoraggio continuo delle campagne APT. Accesso a informazioni di intelligence applicabili durante le indagini (informazioni sulla distribuzione delle APT, sugli IOC e sull'infrastruttura di comando e controllo).
- Analisi retrospettive: durante il periodo di validità dell'abbonamento, forniamo accesso all'archivio dei report privati.

Da un punto di vista pratico, gli indicatori di compromissione rappresentano, per gli esperti del SOC, la parte più applicabile del report. Queste informazioni strutturate vengono fornite per il successivo uso con specifici strumenti automatizzati che contribuiscono al rilevamento di segnali di infezione all'interno dell'infrastruttura.

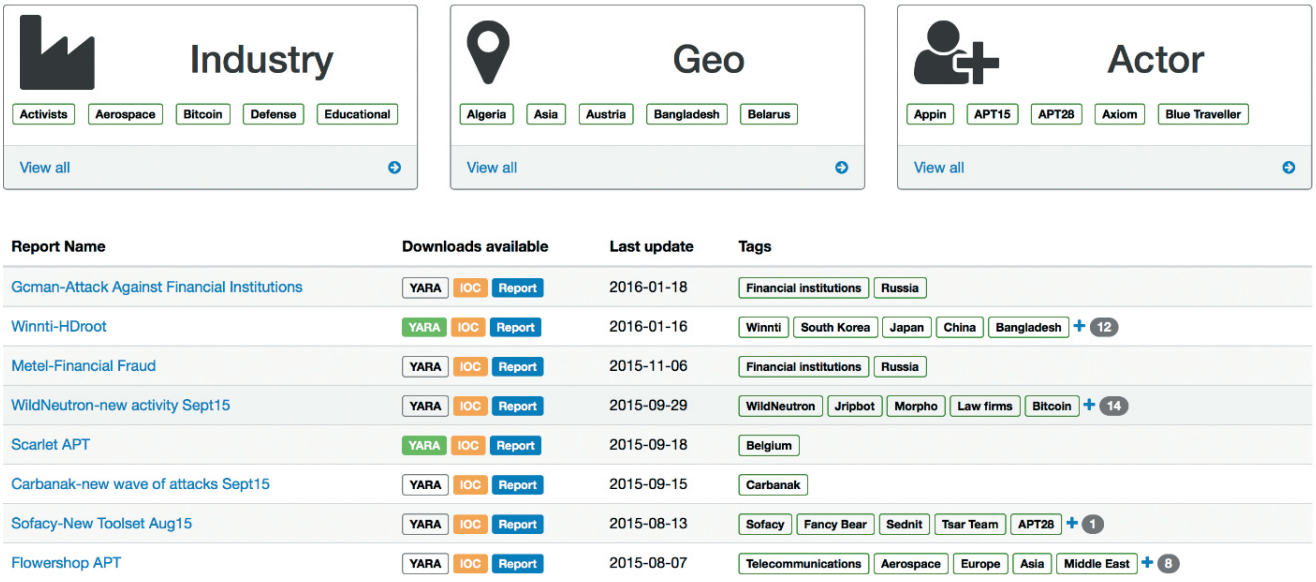


Figura 7:
APT Intelligence Portal

Report su misura per le minacce

Report sulle minacce specifiche di un cliente

Qual è il miglior modo per attaccare un'organizzazione? Quale percorso e quali informazioni sono disponibili ai cybercriminali che intendono attaccare un'azienda? Avete già subito un attacco o siete sotto minaccia?

Il report specifico sulla threat intelligence di un cliente offerto da Kaspersky risponde a queste e a molte altre esigenze. I nostri esperti creano un quadro completo sullo stato dell'attacco in corso, identificando i punti deboli da migliorare e rilevando le prove degli attacchi del passato, di quelli in corso, nonché di quelli pianificati per il futuro.

Supportate da informazioni così dettagliate, le aziende potranno concentrare la strategia di difesa sulle aree maggiormente inclini a subire attacchi dai cybercriminali, adottando misure rapide e precise per respingere gli intrusi e ridurre al minimo il rischio che gli attacchi possano provocare danni.

Sviluppati con sistemi di intelligence open-source (OSINT), analisi approfondite dei database e dei sistemi avanzati di Kaspersky Lab e con la nostra esperienza sulle reti "underground" dei cybercriminali, i report coprono aree quali:

- **Identificazione dei vettori della minaccia**: identificazione e analisi dello stato dei componenti critici esposti all'esterno, tra cui ATM, sistemi di videosorveglianza e altri sistemi che utilizzano tecnologie mobili, i profili dei dipendenti sui social network e gli account email del personale, potenziali obiettivi di un attacco.
- **Analisi sul monitoraggio del malware e dell'attacco informatico**: identificazione, monitoraggio e analisi di un potenziale malware attivo o disattivo indirizzato alla vostra organizzazione, delle attività di botnet passate o in corso e di eventuali attività sospette sulla rete.
- **Attacchi di terzi**: prova dell'attività di botnet o di minaccia indirizzata in modo particolare sui vostri clienti, partner e abbonati, i cui sistemi infetti potrebbero essere utilizzati per un attacco diretto alla vostra azienda.
- **Perdita delle informazioni**: tramite il monitoraggio discreto delle community e dei forum online "underground", siamo in grado di scoprire se gli hacker stanno pianificando un attacco alla vostra azienda o, ad esempio, se un dipendente disonesto sta divulgando informazioni.
- **Stato dell'attacco in corso**: gli attacchi APT possono continuare per anni, senza essere rilevati. Se rileviamo un attacco in corso sull'infrastruttura, forniamo consulenza per consentire all'azienda di risolvere in modo efficiente il problema.

AVVIO RAPIDO – SEMPLICITÀ D'USO – NESSUNA RISORSA NECESSARIA

Una volta stabiliti i parametri e il formato dei dati preferiti (per i report specifici sui clienti), non è necessaria alcuna infrastruttura aggiuntiva per iniziare a usare il servizio di Kaspersky Lab.

Il report sulla Threat Intelligence di Kaspersky non compromette l'integrità e la disponibilità delle risorse, comprese quelle di rete.

Report sulle minacce specifiche del paese

La cybersecurity per un paese comprende la protezione di tutte le principali istituzioni e organizzazioni. Le minacce avanzate persistenti (APT) contro autorità governative possono compromettere la sicurezza nazionale. Gli attacchi informatici contro il settore della produzione, dei trasporti, delle telecomunicazioni, degli istituti finanziari e altri settori cardine possono potenzialmente causare danni significativi a livello statale, tra cui perdite finanziarie, incidenti di produzione, blocco delle comunicazioni di rete e malcontento popolare.

Grazie alla panoramica sulla situazione corrente degli attacchi e sulle tendenze attuali per attacchi di malware e hacker contro il proprio paese, le aziende potranno concentrare la strategia di difesa sulle aree maggiormente inclini a subire attacchi dai cybercriminali, adottando misure rapide e precise per respingere gli intrusi e ridurre al minimo il rischio che gli attacchi possano provocare danni.

Sviluppati con approcci che variano dall'intelligence open-source (OSINT) alle analisi approfondite dei sistemi e database avanzati di Kaspersky Lab, passando per la nostra esperienza sulle reti "underground" dei cybercriminali, i report sulle minacce specifiche del paese coprono aree quali:

- **Individuazione dei vettori della minaccia**: identificazione e analisi dello stato delle risorse critiche del paese, esposte all'esterno, tra cui applicazioni governative vulnerabili, apparecchiature di telecomunicazione, componenti dei sistemi di controllo industriale (come SCADA, PLC, ecc.), ATM e così via.
- **Analisi sul monitoraggio del malware e dell'attacco informatico**: individuazione e analisi di campagne APT, campioni di malware attivi e disattivi, attività delle botnet correnti o pregresse e altre minacce rilevabili che mirano al paese, sulla base dei dati provenienti dalle nostre eccezionali risorse di monitoraggio interne.
- **Perdita delle informazioni**: tramite il monitoraggio illegale delle community e dei forum online "underground", siamo in grado di scoprire se gli hacker stanno pianificando un attacco a determinate organizzazioni. Inoltre, siamo in grado di rilevare account notevolmente compromessi, che potrebbero costituire un rischio per organizzazioni e istituzioni (ad esempio, gli account che appartengono a dipendenti di agenzie governative con un ruolo nella violazione di Ashley Madison, potenzialmente utilizzabili per estorsioni).

Il report sulla Threat Intelligence di Kaspersky non compromette l'integrità e la disponibilità delle risorse di rete sottoposte a ispezione. Il servizio si basa su metodi di riconoscimento della rete non invadenti e analisi delle informazioni provenienti da fonti open-source e risorse ad accesso limitato.

Al termine del servizio, viene fornito un report contenente la descrizione delle minacce più rilevanti per diversi settori industriali e istituzioni del paese, nonché informazioni aggiuntive sui risultati dettagliati delle analisi tecniche. I report vengono distribuiti tramite messaggi e-mail crittografati.

Il servizio viene fornito come progetto una tantum o su base periodica con abbonamento (ad esempio trimestrale).

Kaspersky Managed Protection

Il servizio Kaspersky Managed Protection offre agli utenti Kaspersky Security for Business e Kaspersky Anti Targeted Attack Platform un'eccezionale combinazione di misure tecniche avanzate per rilevare e prevenire gli attacchi mirati: il servizio comprende il monitoraggio 24 ore su 24 da parte degli esperti di Kaspersky Lab e l'analisi continua dei dati relativi alla cyberminaccia (intelligence sulla cyberminaccia), garantendo in tal modo il rilevamento in tempo reale di campagne, nuove e note, di cyberspionaggio e dei cybercriminali che mirano ai sistemi informativi critici.

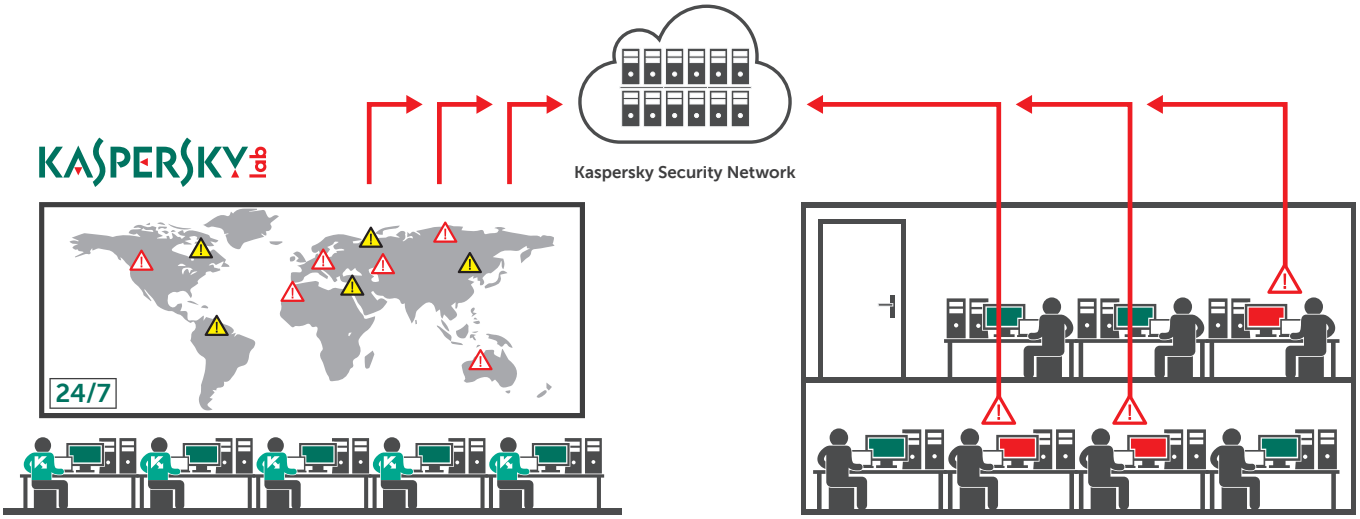


Figura 8:
Kaspersky Managed Protection

DETTAGLI DEL SERVIZIO

- Un elevato livello di protezione da attacchi mirati e malware, con supporto 24 ore al giorno, 7 giorni su 7 da parte degli analisti di Kaspersky Lab.
- Informazioni dettagliate sui cybercriminali, sulle relative motivazioni, su metodi e strumenti utilizzati e sul potenziale danno, favorendo lo sviluppo di una strategia di protezione efficace e completamente informata.
- Rilevamento di attacchi non causati da malware, attacchi che coinvolgono strumenti in precedenza sconosciuti e attacchi che sfruttano le vulnerabilità zero-day.
- Analisi retrospettive dell'incidente e threat hunting.
- Riduzione dei costi totali per la sicurezza con parallelo miglioramento della qualità della protezione. Si tratta di un servizio altamente specializzato, offerto dai leader mondiali in materia di analisi degli attacchi informatici, che includono l'analisi dei metodi e delle tecnologie utilizzati dai cybercriminali. Ottenere tali livelli di informazioni tramite un servizio esterno risulta notevolmente più economico rispetto all'assunzione di specialisti focalizzati sul problema.
- Approccio integrato: la nostra ampia gamma di soluzioni Kaspersky Security for Business integrate ci consente di offrire tutte le tecnologie e i servizi necessari per implementare un ciclo di protezione completo contro gli attacchi mirati: Preparazione - Rilevamento - Indagini - Analisi dei dati - Protezione automatizzata.

VANTAGGI DEL SERVIZIO

- Rilevamento rapido degli incidenti.
- Raccolta di una quantità di informazioni sufficiente per la distinzione tra falsi positivi e rilevamento corretto.
- Determinazione della popolarità degli artefatti, con relativa individuazione del livello di unicità dell'attacco.
- Avvio del processo di risposta agli incidenti di sicurezza della informazioni.
- Avvio di eventuali aggiornamenti necessari sui database antivirus al fine di arrestare la diffusione delle minacce.

Altre informazioni sulle fonti di threat intelligence di Kaspersky

La threat intelligence è un aggregato derivante dalla fusione di fonti eterogenee e ad elevata affidabilità, tra cui Kaspersky Security Network (KSN), Web crawler, servizio di monitoraggio delle botnet (monitoraggio 24 ore al giorno, 7 giorni la settimana, 365 giorni all'anno dei botnet, degli obiettivi e delle attività a essi relativi), trappole via spam, team di ricerca, partner e altri dati storici sugli oggetti dannosi, raccolti da Kaspersky Lab in oltre due decenni. In tempo reale, dunque, tutti i dati aggregati vengono accuratamente ispezionati e perfezionati tramite diverse tecniche di pre-elaborazione, quali criteri statistici, sistemi avanzati di Kaspersky Lab (sandbox, motori di euristica, strumenti per la somiglianza, profiling comportamentale e così via), convalida da parte degli analisti e verifica del whitelisting.

Potendo contare su personale con competenze e formazione adeguate e su una threat intelligence acquisita da fonti attendibili e implementata nei controlli di sicurezza in uso, è ora giunto il momento di considerare la risposta agli incidenti.

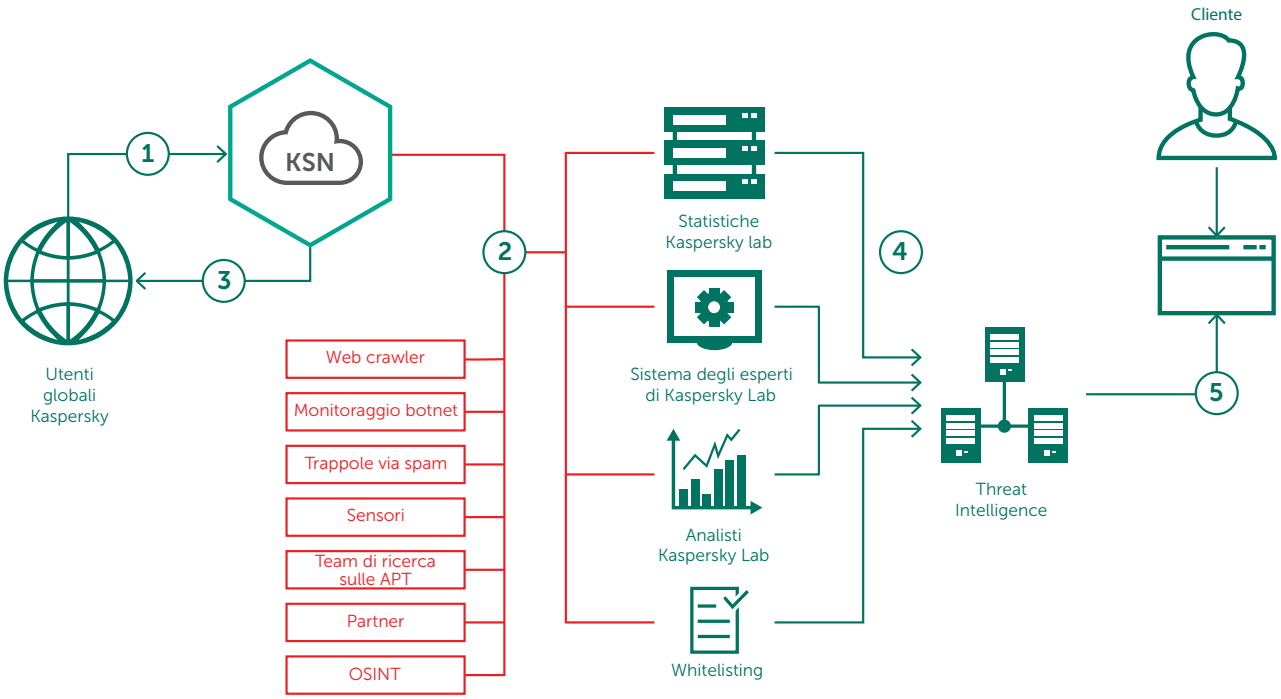


Figura 9:
Fonti di Threat Intelligence di Kaspersky Lab

PANORAMA DELLE RISPOSTE AGLI INCIDENTI

L'analisi forense e la risposta agli incidenti richiedono l'allocazione di un numero notevole di risorse interne in modo graduale o improvviso. Gli esperti, con ampia esperienza pratica nella lotta alle minacce informatiche, dovranno agire in modo rapido per individuare, isolare e bloccare l'attività dannosa. Al fine di ridurre al minimo le conseguenze e i costi per la correzione, la velocità è un fattore cruciale.

Gestire tale livello di competenza con breve preavviso può essere difficile anche per un team SOC consolidato. Poche organizzazioni dispongono di risorse interne sufficienti per arrestare un attacco avanzato in corso. Inoltre, potrebbero verificarsi situazioni come, ad esempio, nel caso di minacce sponsorizzate a livello di stati nazionali o di APT, per cui il team SOP non dispone di competenze approfondite sugli approcci e sulle tattiche specifici usati dagli attori APT coinvolti.

In questi casi, per la risposta agli incidenti potrebbe risultare più conveniente e produttivo collaborare con un fornitore o consulente terzo, che sia pronto all'applicazione di una risposta rapida e completamente informata.

Un panorama completo di risposta agli incidenti dovrebbe includere:

- **Individuazione dell'incidente**
  Analisi iniziale dell'incidente e isolamento dei sistemi infetti
- **Acquisizione di prove**
  A seconda del tipo di incidente, sarà necessario ispezionare diversi tipi di risorse per acquisire le prove necessarie
- **Analisi forense (se richiesta)**
  In questa fase, è possibile creare un quadro dettagliato dell'incidente
- **Analisi del malware (se richiesta)**
  Per ottenere una comprensione delle capacità di un dato malware
- **Piano di correzione**
  Sviluppo di un piano finalizzato all'eradicazione della causa alla radice del problema e di tutte le tracce del codice dannoso
- **Nozioni apprese**
  Analisi e aggiornamento dei controlli di sicurezza esistenti per prevenire incidenti simili

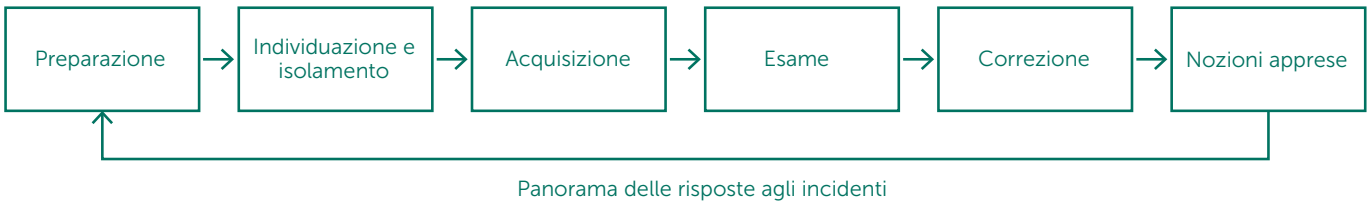


Figura 10:
Panorama delle risposte agli incidenti

Kaspersky Lab offre:
Servizi di risposta agli incidenti

La risposta agli incidenti è il nostro servizio di punta, che copre l'intero ciclo di indagine sull'incidente, dall'acquisizione di prove in loco all'identificazione di indicazioni di compromissione aggiuntive, per giungere alla preparazione di un piano di correzione e alla rimozione completa della minaccia presso l'organizzazione. Le indagini di Kaspersky Lab sono condotte da analisti e investigatori di grande esperienza, specializzati nel rilevamento di intrusioni informatiche. L'intera portata della nostra esperienza nell'analisi forense e del malware, sviluppata a livello globale, può contribuire alla risoluzione degli incidenti di sicurezza presso le aziende.

Durante l'esecuzione del servizio, è necessario raggiungere i seguenti obiettivi:

- Identificazione delle risorse compromesse.
- Isolamento della minaccia.
- Prevenzione della diffusione dell'attacco.
- Ricerca e raccolta delle prove.
- Analisi delle prove e ricostruzione della cronologia e della logica dell'incidente.
- Analisi del malware usato nell'attacco (in caso di rilevamento di malware).
- Scoperta delle fonti dell'attacco e degli altri sistemi potenzialmente compromessi (se possibile).
- Conduzione di analisi, con supporto di strumenti, dell'infrastruttura IT dell'azienda finalizzate al rilevamento di possibili segnali di compromissione.
- Analisi delle connessioni in uscita tra la rete aziendale e le risorse esterne per rilevare eventuali elementi sospetti (ad esempio, possibili server di comando e controllo).
- Rimozione della minaccia.
- Suggerimento di ulteriori azioni di correzione da intraprende.

A seconda che l'azienda disponga o meno di un team di risposta agli incidenti interno, è possibile chiedere ai nostri esperti di eseguire l'intero ciclo di investigazione al fine di individuare in modo semplice e isolare le macchine compromesse, nonché per prevenire la diffusione della minaccia o per condurre analisi forensi o del malware.

ANALISI DEL MALWARE

L'analisi del malware offre una spiegazione completa del comportamento e degli obiettivi degli specifici file di malware che prendono di mira un'organizzazione. Gli esperti di Kaspersky Lab conducono un'analisi approfondita del campione di malware fornito dall'organizzazione, creando un report dettagliato che include:

- Proprietà del campione: una breve descrizione del campione e il verdetto sulla classificazione del malware.
- Descrizione dettagliata del malware: un'analisi approfondita delle funzioni, del comportamento e degli obiettivi della minaccia nel campione del malware, inclusi gli indicatori di compromissione, che fornirà le informazioni necessarie a neutralizzarne le attività.
- Scenario di correzione: il report suggerirà le misure necessarie per proteggere completamente l'organizzazione da questo tipo di minaccia.

ANALISI FORENSE

L'analisi forense può includere anche l'analisi del malware, in caso di rilevamento di un malware durante l'indagine. Gli esperti di Kaspersky Lab mettono assieme le prove per comprendere esattamente quello che sta succedendo, avvalendosi dell'uso di immagini del disco rigido, dati estratti dalla memoria e tracce sulla rete. Il risultato è una spiegazione dettagliata dell'incidente. Il cliente avvia il processo raccogliendo le prove e fornendo una definizione del contesto dell'incidente. Gli esperti di Kaspersky Lab analizzano i sintomi dell'incidente, identificano l'eventuale malware binario e conducono l'analisi del malware per fornire un report dettagliato comprensivo delle necessarie misure di correzione.

OPZIONI DI DISTRIBUZIONE

I servizi di risposta agli incidenti di Kaspersky Lab sono disponibili:

- Su abbonamento
- In risposta a un singolo incidente

Entrambe le opzioni si basano sulla quantità di tempo impiegato dai nostri esperti per porre soluzione all'incidente. Questo aspetto viene negoziato con il cliente prima della firma del contratto. Il cliente potrebbe opzionalmente includere la quantità di ore di lavoro che ritiene necessarie o seguire i consigli dei nostri esperti, adatti ad ogni caso specifico.

PERCHÉ KASPERSKY LAB?

Kaspersky offre:
- Partnership con forze dell'ordine a livello globale, come Interpol e CERT
- Strumenti basati sul Web che monitorano milioni di minacce informatiche in tutto il mondo in tempo reale
- Team globali che analizzano e comprendono le minacce Internet di tutti i tipi

Kaspersky è:
- La più grande azienda indipendente di software per la sicurezza, incentrata sulla threat intelligence e la leadership tecnologica
- Leader indiscussa in più test indipendenti di rilevamento malware rispetto a qualsiasi altro fornitore
- Riconosciuta come Leader da Gartner, Forrester e IDC

Informazioni su Kaspersky Lab

Kaspersky Lab è il maggior fornitore privato di soluzioni per la protezione degli endpoint al mondo. L'azienda è tra i primi quattro fornitori mondiali di prodotti di sicurezza per utenti endpoint. Da più di 18 anni Kaspersky Lab è pioniere della sicurezza IT e offre soluzioni efficaci per la sicurezza digitale ad aziende, piccole e medie imprese e a privati. Con società madre e sede legale nel Regno Unito, Kaspersky Lab è presente in quasi 200 paesi e territori in tutto il mondo e offre soluzioni di protezione a oltre 350 milioni di utenti a livello globale.


Twitter.com/
KasperskyLabIT


Facebook.com/
Kasperskylabitalia


Youtube.com/
KasperskyItalia

Kaspersky Lab, Mosca, Russia
www.kaspersky.it

Tutto sulla sicurezza in Internet:
www.securelist.com

Trovate il partner più vicino:
www.kaspersky.it/buyoffline