Tecnico Superiore per le infrastrutture e i sistemi IT: Network, Cloud e Virtualizzazione

ITS Network and Cloud Specialist

Biennio 2024-26

Sistemi di sicurezza nell'IT aziendale

Giacomo Garoffoli

Assunto con contratto di Apprendistato di Alta Formazione e Ricerca

ai sensi dell'art 45 del D.Lgs. 81/2015 dall'Azienda

Sinapto S.r.l

"Definizione degli standard formativi dell'apprendistato e criteri generali

per la realizzazione dei percorsi di apprendistato, in attuazione dell'articolo 46,

comma 1, del decreto legislativo 15 giugno 2015, n. 81"

Indice

Introduzione

Presentazione personale

Mi chiamo Giacomo Garoffoli, ho 22 anni e vivo a Rovato, un comune situato nella provincia di Brescia.

Fin da piccolo sono sempre stato affascinato dal mondo della tecnologia e dell'informatica. Questa passione, coltivata nel corso degli anni, ha influenzato profondamente il mio percorso formativo e le mie aspirazioni professionali.

Proprio per questo motivo ho deciso di intraprendere un percorso di studi in ambito informatico presso l'Istituto Tecnico Industriale Benedetto Castelli di Brescia. Durante gli anni delle scuole superiori ho acquisito le prime competenze tecniche e di approfondire argomenti legati ai sistemi informatici e alle reti, consolidando ulteriormente il mio interesse per il settore.

Dopo aver completato gli studi superiori, ho deciso inizialmente di intraprendere un percorso universitario. Tuttavia, dopo alcuni mesi, ho compreso che l'approccio didattico proposto non rispondeva pienamente alle mie esigenze formative e alle mie aspettative professionali.

Per questo motivo ho scelto di proseguire il mio percorso presso l'ITS Angelo Rizzoli, una realtà che mi ha permesso di approfondire le mie competenze attraverso un approccio maggiormente orientato alla pratica e al mondo del lavoro.

Grazie a questa esperienza ho potuto confrontarmi con professionisti del settore e acquisire competenze tecniche spendibili in contesti lavorativi reali.

Nel corso del percorso formativo ho avuto inoltre la possibilità di conseguire alcune certificazioni professionali che mi hanno permesso di consolidare e ampliare le competenze acquisite durante le lezioni e l'esperienza lavorativa in azienda.

In particolare, ho ottenuto la certificazione Microsoft AZ-900 (*Microsoft Azure Fundamentals*), che mi ha fornito una panoramica generale sui principali servizi cloud offerti dalla piattaforma Microsoft Azure, approfondendo concetti fondamentali come

Infrastructure as a Service (IaaS), *Platform as a Service* (PaaS) e *Software as a Service* (SaaS).

Successivamente ho conseguito la certificazione Microsoft SC-900 (*Security, Compliance and Identity Fundamentals*), che mi ha consentito di approfondire le tematiche legate alla sicurezza informatica, alla gestione delle identità digitali e alla conformità normativa, aspetti sempre più rilevanti all'interno delle moderne infrastrutture IT.

Ho inoltre ottenuto la certificazione *AWS Certified Cloud Practitioner* (CLF-C02), attraverso la quale ho acquisito una conoscenza generale dei servizi cloud offerti da *Amazon Web Services* (AWS), delle architetture cloud e dei principi fondamentali di sicurezza e gestione delle risorse in ambienti cloud.

Queste certificazioni hanno rappresentato un'importante integrazione al percorso di studi e mi hanno permesso di sviluppare una visione più ampia delle tecnologie utilizzate oggi in ambito professionale, con particolare attenzione agli aspetti legati al cloud computing e alla sicurezza informatica.

Presentazione dell’azienda

Ho svolto l'apprendistato presso Sinapto, un'azienda italiana operante nel settore dell'IT e specializzata nella fornitura di servizi informatici e consulenza tecnologica per le imprese.

L'azienda è stata fondata nel 2000 da un gruppo di giovani professionisti accomunati dalla passione per Internet e per le nuove tecnologie. Nel corso degli anni Sinapto ha consolidato la propria esperienza nel settore IT, affiancando aziende di differenti dimensioni nei processi di innovazione tecnologica e trasformazione digitale.

Il nome "Sinapto" deriva dal termine greco συναπτω, che significa "collego", "unisco" e "aiuto". Questa scelta riflette la filosofia aziendale, basata sulla collaborazione tra competenze diverse e sulla creazione di relazioni durature con clienti e partner. L'obiettivo dell'azienda è infatti quello di creare valore attraverso l'integrazione tra persone, processi e tecnologie.

Grazie a oltre vent'anni di esperienza, Sinapto supporta le aziende nell'analisi, progettazione e gestione delle infrastrutture informatiche, offrendo soluzioni personalizzate in base alle esigenze operative e strategiche di ciascun cliente. L'approccio adottato prevede una fase iniziale di analisi delle necessità aziendali, seguita dalla progettazione e dall'implementazione delle soluzioni tecnologiche più adatte.

Durante il mio percorso di apprendistato sono entrato a far parte di un ambiente dinamico e altamente specializzato, confrontandomi quotidianamente con attività di supporto tecnico, gestione degli endpoint e sicurezza informatica, acquisendo competenze pratiche fondamentali per la mia crescita professionale.

Servizi offerti

Sinapto offre un ampio portafoglio di servizi IT, progettati per supportare le aziende nella gestione, nell'evoluzione e nella protezione delle proprie infrastrutture informatiche. Grazie ad un approccio consulenziale e ad una consolidata esperienza nel settore, l'azienda è in grado di fornire soluzioni personalizzate in base alle esigenze operative dei clienti.

Assistenza Sistemistica

Uno dei principali servizi offerti da Sinapto è l'assistenza sistemistica in modalità outsourcing. Attraverso il *Service Desk*, l'azienda fornisce supporto tecnico agli utenti, gestisce le richieste di assistenza e interviene nella risoluzione delle problematiche legate

a postazioni di lavoro, server, reti e applicazioni aziendali. Le attività possono essere svolte sia da remoto che direttamente presso la sede del cliente.

Sistemi e Infrastrutture

Sinapto si occupa della progettazione, implementazione e gestione di infrastrutture IT. Questo comprende server fisici e virtuali, sistemi di storage, apparati di rete e ambienti cloud. L'obiettivo è garantire infrastrutture affidabili, scalabili e adeguate alle esigenze operative delle aziende.

Modern Workplace

L'azienda propone soluzioni orientate al concetto di *Modern Workplace*, con particolare attenzione agli strumenti di collaborazione e produttività basati sull'ecosistema Microsoft 365. Queste soluzioni permettono agli utenti di lavorare in modo sicuro ed efficiente, sia in presenza che da remoto, favorendo la collaborazione tra gruppi e la condivisione delle informazioni.

Sicurezza Informatica

La sicurezza informatica rappresenta uno degli ambiti più importanti dell'offerta di Sinapto. L'azienda supporta i clienti nell'implementazione di soluzioni dedicate alla protezione degli endpoint, al monitoraggio degli eventi di sicurezza, alla gestione delle vulnerabilità e alla protezione delle infrastrutture aziendali dalle minacce informatiche. Le attività comprendono inoltre verifiche di sicurezza, analisi della conformità e implementazione di strumenti avanzati di difesa informatica.

Cloud & Data Center

Sinapto affianca le aziende nella scelta e nell'implementazione delle migliori soluzioni cloud disponibili sul mercato, integrandole con infrastrutture tradizionali e servizi di *Data*

Center. Questo approccio consente di realizzare ambienti ibridi in grado di garantire elevati livelli di disponibilità, sicurezza e continuità operativa.

L'ampiezza dei servizi offerti permette all'azienda di rispondere alle diverse esigenze tecnologiche dei propri clienti, fornendo supporto sia nella gestione quotidiana dell'infrastruttura IT sia nei progetti di evoluzione e innovazione tecnologica.

Ruolo durante l'apprendistato

Durante il periodo di apprendistato presso Sinapto ho ricoperto il ruolo di *IT Support Engineer* all'interno del *Service Desk* aziendale. Questa esperienza mi ha permesso di operare in diversi ambiti dell'infrastruttura IT, acquisendo competenze sia tecniche che organizzative attraverso il contatto diretto con clienti e colleghi.

Le attività svolte hanno riguardato principalmente il supporto tecnico di primo e secondo livello agli utenti, la gestione delle postazioni di lavoro, il monitoraggio dei sistemi informatici e la risoluzione delle problematiche segnalate tramite il sistema di *ticketing* aziendale.

Nel corso dell'apprendistato ho partecipato ad attività legate alla gestione degli *endpoint* aziendali, alla configurazione di software e servizi, all'amministrazione di ambienti Microsoft 365 e alla verifica delle procedure di backup e continuità operativa.

Una parte significativa del mio percorso è stata dedicata alle attività di sicurezza informatica, partecipando a progetti finalizzati alla protezione degli *endpoint* e alla gestione delle soluzioni utilizzate dai clienti. Queste esperienze mi hanno consentito di approfondire tematiche sempre più rilevanti nel panorama IT moderno, come il monitoraggio delle minacce informatiche, la gestione centralizzata dei dispositivi e l'automazione delle attività operative.

Le attività sono state svolte prevalentemente da remoto attraverso gli strumenti di gestione e monitoraggio utilizzati dall'azienda, ma ho avuto anche l'opportunità di partecipare a interventi presso le sedi dei clienti, acquisendo una visione più completa delle esigenze operative e delle infrastrutture presenti nei diversi contesti aziendali.

Mansioni quotidiane

Durante il mio percorso di apprendistato presso Sinapto ho svolto attività principalmente legate al *Service Desk* e al supporto sistemistico. Le mansioni quotidiane erano molto varie e mi hanno permesso di confrontarmi con differenti tecnologie e realtà aziendali.

Una parte significativa del lavoro consisteva nella gestione delle richieste di assistenza provenienti dai clienti tramite il sistema di *ticketing* aziendale. Le problematiche affrontate riguardavano principalmente le postazioni di lavoro degli utenti, configurazioni software, problemi di accesso ai servizi aziendali, gestione delle credenziali e attività di risoluzioni di problematiche generali.

Tra le attività svolte rientravano inoltre la gestione degli ambienti Microsoft 365, il supporto agli utenti per applicazioni e servizi cloud, la configurazione di nuovi dispositivi e l'assistenza relativa ai sistemi di posta elettronica e collaborazione aziendale.

Ho partecipato anche alle attività di monitoraggio e gestione degli *endpoint* attraverso piattaforme di *Remote Monitoring and Management* (RMM), utilizzate per verificare lo stato dei dispositivi, distribuire software, effettuare aggiornamenti, eseguire *script* da remoto e individuare eventuali anomalie che potessero compromettere il corretto funzionamento dei sistemi.

Un'altra attività importante riguardava il controllo e la verifica dei backup aziendali attraverso le piattaforme utilizzate dall'azienda, con l'obiettivo di garantire la disponibilità dei dati e la continuità operativa dei clienti in caso di problemi o incidenti informatici.

Nel corso dell'apprendistato ho collaborato a progetti di gestione e sicurezza degli *endpoint*, partecipando ad attività di installazione, configurazione e monitoraggio di soluzioni di protezione avanzata. Queste esperienze mi hanno permesso di approfondire le tecnologie utilizzate per la difesa delle infrastrutture informatiche e di acquisire una maggiore consapevolezza dell'importanza della sicurezza nel contesto aziendale moderno.

La varietà delle attività svolte mi ha consentito di sviluppare non solo competenze tecniche, ma anche capacità organizzative, di *problem solving* e di gestione delle priorità, aspetti fondamentali per operare efficacemente nel settore dell'IT.

Progetti e strumenti utilizzati

Durante il periodo di apprendistato ho utilizzato quotidianamente diversi strumenti fondamentali per la gestione e il supporto delle infrastrutture informatiche. L'utilizzo di queste piattaforme mi ha permesso di acquisire competenze pratiche nella gestione degli *endpoint*, nel monitoraggio dei sistemi e nell'assistenza agli utenti.

OTOBO – Sistema di Ticketing

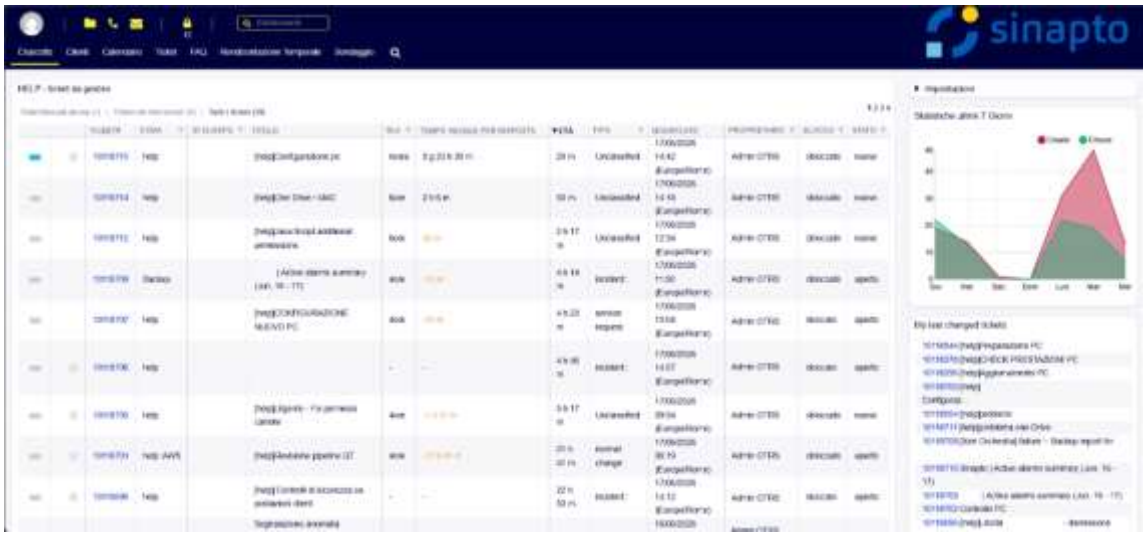


Figura 1. Interfaccia principale di Otobo

OTOBO è una piattaforma open source di *Service Management* e *Ticketing* utilizzata per la gestione delle richieste di assistenza e delle attività interne. Attraverso questo sistema vengono registrati, assegnati e monitorati tutti i *ticket* aperti dai clienti, consentendo di mantenere una tracciabilità completa delle attività svolte.

NinjaOne – Remote Monitoring and Management (RMM)

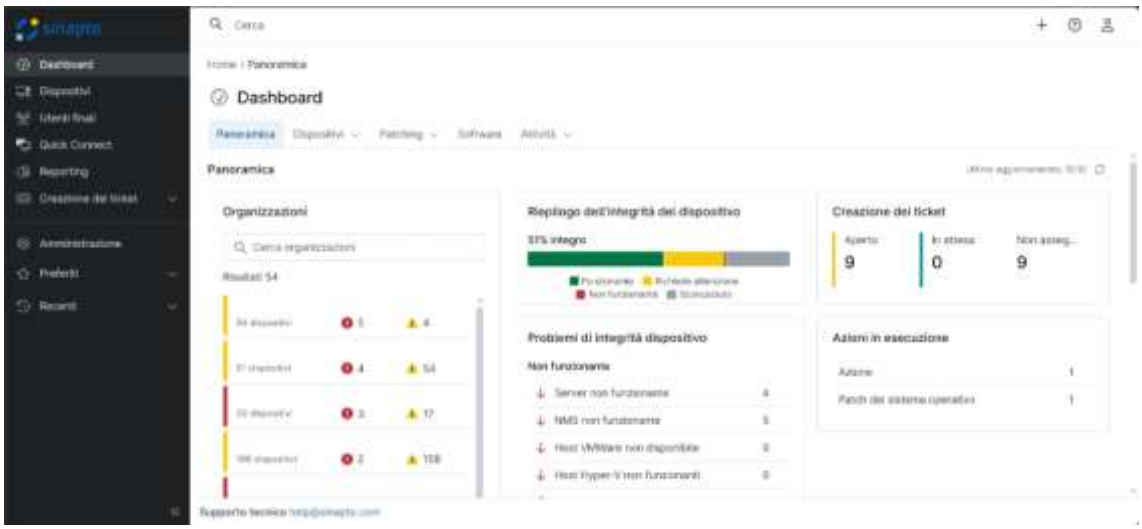


Figura 2. Interfaccia principale di NinjaOne

NinjaOne è la piattaforma di *Remote Monitoring and Management* (RMM) utilizzata da Sinapto per la gestione centralizzata degli *endpoint* dei clienti.

Attraverso NinjaOne è possibile monitorare lo stato dei dispositivi, distribuire software, eseguire *script* da remoto, effettuare attività di manutenzione e raccogliere informazioni dettagliate sui sistemi. Lo strumento consente inoltre di automatizzare numerose operazioni riducendo i tempi di intervento e migliorando l'efficienza operativa.

Icinga – Monitoraggio dell'infrastruttura

Figura 3. Dashboard principale di Icinga

Icinga è una piattaforma *open source* dedicata al monitoraggio di server, servizi, apparati di rete e infrastrutture IT.

Attraverso *dashboard* e sistemi di notifica, Icinga permette di rilevare tempestivamente eventuali anomalie o guasti, fornendo informazioni sullo stato di salute dei sistemi monitorati. Questo approccio consente di intervenire rapidamente prima che un problema possa causare un'interruzione del servizio.

Nel contesto aziendale, Icinga veniva utilizzato per il controllo continuo delle infrastrutture gestite e per la generazione di alert in caso di criticità.

VOIspeed – Sistema di telefonia aziendale

Figura 4. Interfaccia iniziale di VOIspeed

VOIspeed è una piattaforma di telefonia VoIP utilizzata per la gestione delle comunicazioni aziendali.

Il sistema permette agli operatori del *Service Desk* di gestire chiamate in entrata e in uscita, consultare rubriche aziendali e interagire con i clienti attraverso un'unica interfaccia centralizzata. Grazie a questa soluzione è possibile garantire una comunicazione rapida ed efficace durante le attività di supporto tecnico.

DokuWiki – Documentazione interna

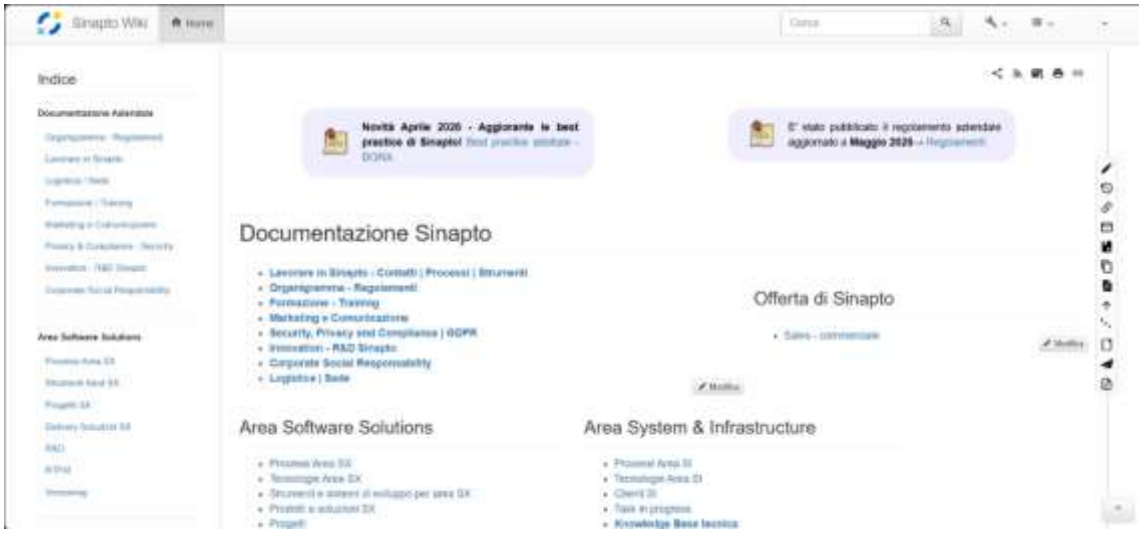


Figura 5. Pagina principale della wiki interna

DokuWiki è una piattaforma *wiki* utilizzata per la gestione della documentazione tecnica interna.

All'interno di questo sistema vengono raccolte procedure operative, configurazioni, guide tecniche e informazioni utili per il supporto ai clienti. La documentazione rappresenta una risorsa fondamentale per garantire uniformità nelle attività svolte e facilitare la condivisione delle conoscenze tra i membri del gruppo.

Durante il mio apprendistato ho consultato frequentemente DokuWiki per reperire informazioni tecniche e procedure operative necessarie alla risoluzione delle problematiche segnalate.

Veeam Backup & Replication

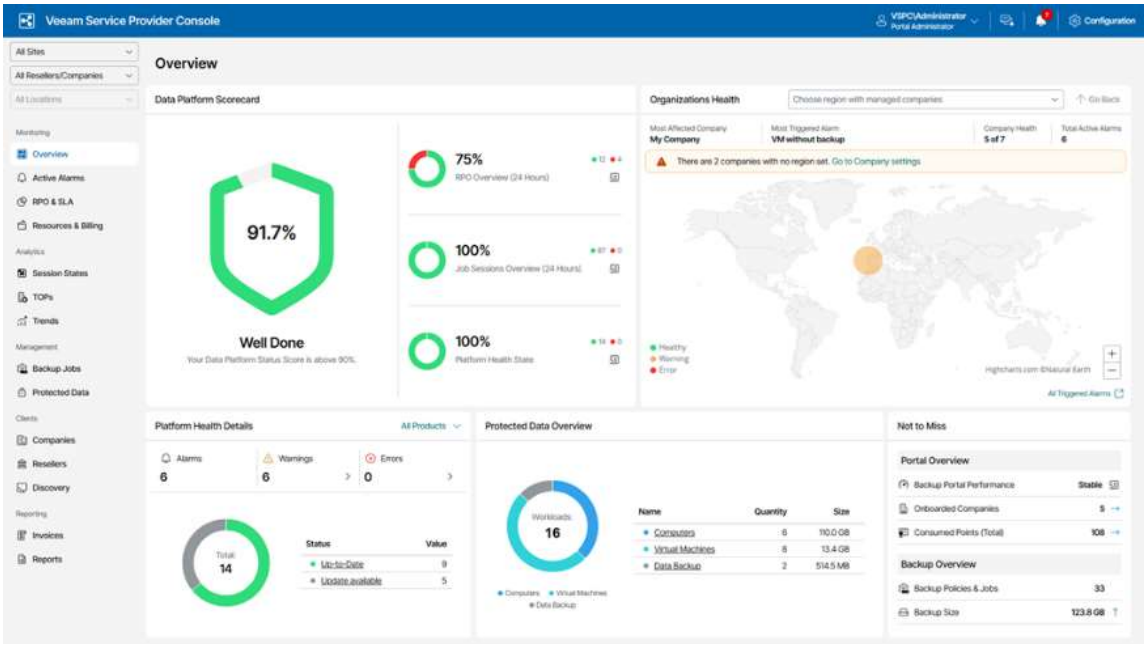


Figura 6. Dashboard principale di Veeam

Veeam Backup & Replication è la soluzione utilizzata per la gestione e il monitoraggio dei backup dei clienti.

Attraverso questa piattaforma è possibile verificare il corretto completamento delle attività di backup, controllare eventuali errori e garantire la disponibilità dei dati in caso di necessità di ripristino. Il controllo periodico dei backup rappresenta un'attività essenziale per assicurare la continuità operativa e la protezione delle informazioni aziendali.

L'utilizzo di questi strumenti mi ha permesso di acquisire una visione completa delle attività svolte all'interno di un moderno *Service Desk* e di comprendere l'importanza

dell'automazione, del monitoraggio e della documentazione nella gestione delle infrastrutture informatiche aziendali.

Sicurezza informatica ed EDR

Evoluzione delle minacce informatiche

Negli ultimi anni la sicurezza informatica è diventata un elemento fondamentale per qualsiasi organizzazione che utilizzi sistemi informatici e servizi digitali. La crescente diffusione di dispositivi connessi a Internet, servizi cloud e modalità di lavoro ibride ha aumentato significativamente la superficie di attacco delle infrastrutture aziendali.

In passato le principali minacce informatiche erano rappresentate da virus relativamente semplici, spesso sviluppati con finalità dimostrative o vandaliche. Con l'evoluzione delle tecnologie e la crescente digitalizzazione dei processi aziendali, anche gli attacchi informatici sono diventati più sofisticati e organizzati.

Oggi le aziende devono confrontarsi con minacce avanzate in grado di compromettere sistemi, sottrarre informazioni riservate e interrompere l'operatività aziendale. Tra queste rientrano campagne di *phishing* e *whaling*, *malware* evoluti, *ransomware*, attacchi mirati e attività svolte da gruppi criminali organizzati che operano a livello internazionale.

L'obiettivo degli attaccanti non è più soltanto causare danni ai sistemi informatici, ma anche ottenere vantaggi economici attraverso il furto di dati, l'estorsione o la compromissione delle infrastrutture aziendali. Per questo motivo le organizzazioni sono chiamate a adottare strumenti e strategie di sicurezza sempre più avanzati per proteggere i propri asset digitali.

In questo contesto, i tradizionali antivirus non risultano più sufficienti a garantire una protezione completa, rendendo necessario l'utilizzo di strumenti evoluti in grado di rilevare e analizzare comportamenti sospetti sugli *endpoint* aziendali.

Malware e ransomware

Tra le principali minacce informatiche che colpiscono aziende e privati rientrano i *malware*, ovvero software progettati con l'obiettivo di compromettere la sicurezza, la riservatezza o la disponibilità dei sistemi informatici.

Il termine *malware* deriva dall'unione delle parole inglesi *malicious* e *software* e comprende diverse categorie di minacce, tra cui virus, *worm*, *trojan*, *spyware* e *ransomware*. Questi software malevoli possono diffondersi attraverso allegati e-mail, siti web compromessi, download non sicuri, dispositivi esterni o sfruttando vulnerabilità presenti nei sistemi operativi non aggiornati e nelle applicazioni.

Tra le minacce più diffuse e pericolose degli ultimi anni si distingue il *ransomware*. Questa tipologia di *malware* ha l'obiettivo di impedire l'accesso ai dati della vittima attraverso la cifratura dei file, richiedendo successivamente il pagamento di un riscatto per ottenere la chiave di decrittazione.

Gli attacchi *ransomware* rappresentano una delle principali minacce per le organizzazioni poiché possono causare gravi interruzioni operative, perdita di dati e significativi danni economici. Negli ultimi anni diversi gruppi criminali organizzati hanno sviluppato campagne *ransomware* sempre più sofisticate, colpendo aziende, enti pubblici, strutture sanitarie e infrastrutture critiche.

Un esempio significativo è rappresentato da WannaCry, *ransomware* che nel 2017 ha colpito centinaia di migliaia di sistemi informatici in tutto il mondo sfruttando una vulnerabilità del protocollo SMB di Microsoft Windows. Più recentemente, gruppi come LockBit hanno introdotto tecniche avanzate di doppia estorsione, combinando la cifratura dei dati con il furto di informazioni sensibili, minacciando la loro pubblicazione in caso di mancato pagamento.

Per contrastare efficacemente queste minacce non è sufficiente affidarsi esclusivamente a strumenti di protezione tradizionali. È necessario adottare un approccio multilivello che comprenda aggiornamenti costanti, backup regolari, formazione degli utenti e soluzioni avanzate di monitoraggio e rilevamento delle minacce.

In questo contesto assumono un ruolo sempre più importante le piattaforme EDR (*Endpoint Detection and Response*), progettate per individuare comportamenti sospetti e rispondere rapidamente agli incidenti di sicurezza prima che possano causare danni significativi all'organizzazione.

Limiti degli antivirus tradizionali

Per molti anni gli antivirus tradizionali hanno rappresentato il principale strumento di protezione per i sistemi informatici. Queste soluzioni sono state progettate per individuare e bloccare software dannosi attraverso il confronto con un database di firme conosciute, aggiornato periodicamente dai produttori.

Sebbene questo approccio sia ancora efficace contro numerose minacce note, presenta alcuni limiti significativi di fronte al panorama delle minacce moderne. I cybercriminali sviluppano infatti *malware* sempre più sofisticati, in grado di modificare il proprio comportamento o il proprio codice per evitare il rilevamento da parte delle tradizionali tecnologie basate sulle firme.

Uno dei principali limiti degli antivirus tradizionali riguarda la difficoltà nel rilevare minacce sconosciute, comunemente definite *zero-day*. Questi attacchi sfruttano vulnerabilità non ancora documentate o malware non ancora catalogati dai produttori di sicurezza, risultando spesso invisibili ai sistemi di protezione convenzionali.

Un'altra criticità è rappresentata dalla limitata capacità di analizzare il comportamento dei processi in esecuzione. Un antivirus tradizionale è generalmente progettato per identificare file dannosi, ma può avere difficoltà nel riconoscere attività sospette che non corrispondono a una firma già conosciuta. Questo aspetto diventa particolarmente rilevante nel caso di attacchi avanzati, in cui gli aggressori utilizzano strumenti legittimi del sistema operativo per svolgere attività malevole.

Inoltre, le moderne minacce informatiche non si limitano a un singolo file infetto, ma spesso coinvolgono una sequenza di azioni che possono svilupparsi nel tempo. Un attaccante potrebbe, ad esempio, ottenere l'accesso iniziale tramite una campagna di *phishing*, eseguire movimenti laterali all'interno della rete e successivamente compromettere sistemi critici. Gli antivirus tradizionali non sono progettati per fornire una visione completa di questo tipo di attività.

Per questi motivi le organizzazioni hanno iniziato a adottare soluzioni più evolute, in grado non solo di prevenire le infezioni, ma anche di monitorare costantemente il

comportamento degli *endpoint*, raccogliere informazioni sugli eventi di sicurezza e fornire strumenti di risposta rapida agli incidenti. Da questa esigenza sono nate le piattaforme *Endpoint Detection and Response* (EDR), oggi considerate uno degli elementi fondamentali nella protezione delle infrastrutture informatiche aziendali.

Introduzione agli EDR

Con l'aumento della complessità delle minacce informatiche e dei limiti delle soluzioni antivirus tradizionali, le organizzazioni hanno iniziato ad adottare strumenti di sicurezza più avanzati in grado di fornire una protezione continua degli *endpoint* aziendali.

L'EDR è una soluzione di sicurezza progettata per monitorare costantemente le attività dei dispositivi aziendali, raccogliere informazioni sugli eventi di sicurezza e individuare comportamenti potenzialmente dannosi che potrebbero indicare la presenza di una minaccia.

A differenza degli antivirus tradizionali, che si concentrano principalmente sull'identificazione di file malevoli attraverso firme conosciute, gli EDR analizzano il comportamento dei processi, delle connessioni di rete e delle attività svolte sul sistema. Questo approccio consente di individuare anche minacce sconosciute o tecniche di attacco che non presentano caratteristiche riconducibili a malware già catalogati.

Le piattaforme EDR raccolgono continuamente dati provenienti dagli *endpoint*, generando una telemetria dettagliata che può essere utilizzata per ricostruire gli eventi che hanno portato ad un incidente di sicurezza. In caso di comportamento sospetto, il sistema può generare alert automatici, fornire informazioni dettagliate agli amministratori e, in alcuni casi, eseguire azioni di risposta automatica per limitare i danni. Tra le funzionalità più comuni offerte dalle moderne soluzioni EDR vi sono:

- Monitoraggio continuo degli *endpoint*
- Analisi comportamentale dei processi
- Rilevamento di minacce avanzate e attacchi *zero-day*

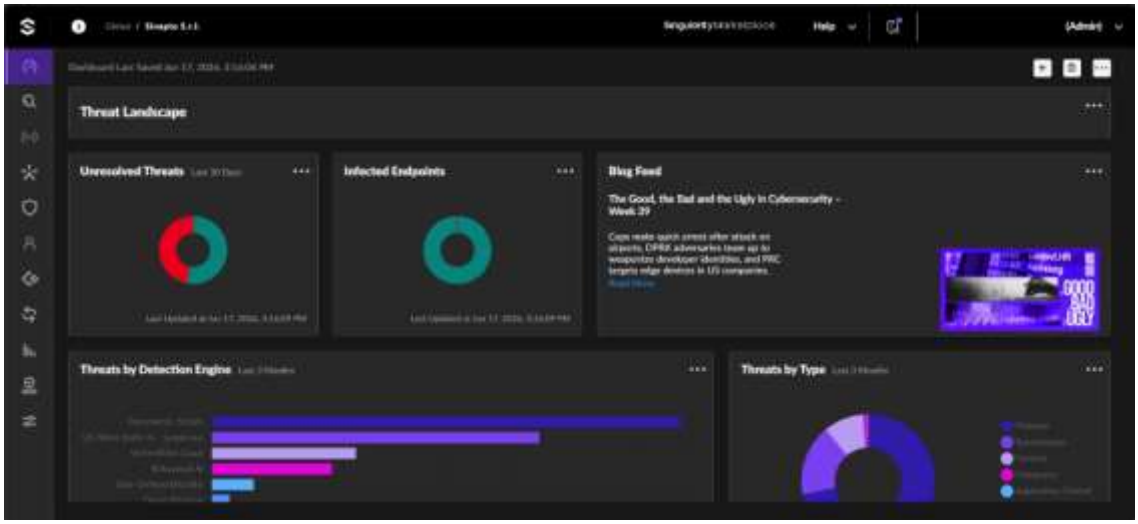
- Raccolta e correlazione degli eventi di sicurezza
- Isolamento dei dispositivi compromessi
- Risposta automatizzata agli incidenti
- Supporto alle attività di investigazione e *threat hunting*

L'adozione di una soluzione EDR consente alle aziende di migliorare significativamente la propria capacità di rilevare e gestire gli incidenti di sicurezza, riducendo il tempo necessario per identificare una minaccia e limitandone l'impatto sull'infrastruttura aziendale.

Nel contesto della mia esperienza lavorativa presso Sinapto, le piattaforme EDR rappresentano uno strumento fondamentale per la protezione degli *endpoint* dei clienti. Per questo motivo, nei capitoli successivi verranno analizzate due delle soluzioni più diffuse in ambito enterprise: SentinelOne e CrowdStrike Falcon.

Piattaforme di sicurezza EDR

SentinelOne



SentinelOne è una piattaforma di sicurezza informatica appartenente alla categoria *Endpoint Protection Platform* (EPP) ed *Endpoint Detection and Response* (EDR), progettata per proteggere gli endpoint aziendali da *malware*, *ransomware* e altre minacce avanzate.

La soluzione utilizza un singolo agente installato sui dispositivi da proteggere, attraverso il quale vengono eseguite attività di monitoraggio continuo, analisi comportamentale e risposta agli incidenti di sicurezza. L'obiettivo principale della piattaforma è individuare e bloccare le minacce prima che possano compromettere i sistemi aziendali.

Uno degli aspetti distintivi di SentinelOne è l'utilizzo di algoritmi di intelligenza artificiale e *machine learning* per analizzare il comportamento dei processi in esecuzione. Grazie a questo approccio, la piattaforma è in grado di identificare attività sospette anche in assenza di firme conosciute, migliorando la capacità di rilevare minacce *zero-day* e attacchi avanzati. La console di gestione centralizzata consente agli amministratori di monitorare in tempo reale lo stato degli *endpoint* protetti, visualizzare gli eventi di sicurezza e analizzare gli incidenti rilevati. Attraverso *dashboard* dedicate è possibile ottenere una panoramica completa della postura di sicurezza dell'organizzazione e intervenire rapidamente in caso di necessità.

Tra le principali funzionalità offerte da SentinelOne si possono evidenziare:

- Protezione antivirus di nuova generazione (NGAV);
- *Endpoint Detection and Response* (EDR);
- Analisi comportamentale dei processi;
- Protezione contro *ransomware*;
- Isolamento automatico degli *endpoint* compromessi;
- Gestione centralizzata degli eventi di sicurezza;
- Funzionalità di *rollback* su sistemi Windows in caso di attacco *ransomware*.

Durante il mio percorso di apprendistato presso Sinapto ho utilizzato frequentemente SentinelOne per il monitoraggio degli *endpoint* dei clienti e per l'analisi degli eventi di sicurezza generati dalla piattaforma. Questa esperienza mi ha permesso di comprendere l'importanza delle soluzioni EDR nella protezione delle infrastrutture informatiche moderne e di acquisire familiarità con gli strumenti di investigazione e risposta agli incidenti messi a disposizione dalla piattaforma.

CrowdStrike Falcon

CrowdStrike Falcon è una piattaforma di sicurezza informatica *cloud-native* appartenente alla categoria *Endpoint Protection Platform* (EPP) ed *Endpoint Detection and Response* (EDR). La soluzione è progettata per proteggere gli *endpoint* aziendali attraverso un'infrastruttura completamente basata sul cloud, eliminando la necessità di server di gestione locali.

La protezione dei dispositivi viene garantita attraverso il *Falcon Sensor*, un agente leggero installato sugli *endpoint* che raccoglie informazioni e telemetria, inviandole alla piattaforma centrale per l'analisi e il rilevamento di eventuali minacce.

Uno degli aspetti distintivi di CrowdStrike Falcon è la forte integrazione con servizi di *threat intelligence* e la capacità di correlare grandi quantità di dati provenienti dagli *endpoint*. Questo consente di individuare rapidamente attività sospette e fornire agli amministratori strumenti avanzati di investigazione e risposta agli incidenti.

La piattaforma include inoltre funzionalità di *Real Time Response* (RTR), che permettono di eseguire operazioni da remoto sugli *endpoint*, raccogliere informazioni diagnostiche ed effettuare attività di *troubleshooting* direttamente dalla console di amministrazione.

Grazie alla sua architettura *cloud-native*, CrowdStrike Falcon risulta particolarmente adatto alla gestione di ambienti distribuiti e organizzazioni con un elevato numero di dispositivi. Questa caratteristica è stata uno degli elementi che hanno reso la piattaforma protagonista del progetto di migrazione descritto nei capitoli successivi.

Confronto tra le soluzioni

SentinelOne e CrowdStrike Falcon sono due delle principali piattaforme EDR presenti sul mercato e condividono numerose funzionalità, tra cui la protezione degli *endpoint*, il monitoraggio continuo delle attività, il rilevamento comportamentale delle minacce e la capacità di risposta agli incidenti di sicurezza.

Entrambe le soluzioni sono progettate per superare i limiti degli antivirus tradizionali, offrendo una maggiore visibilità sugli *endpoint* e consentendo agli amministratori di individuare rapidamente attività sospette o potenziali compromissioni. Grazie all'integrazione di tecnologie avanzate di rilevamento e analisi comportamentale, entrambe le piattaforme rappresentano strumenti efficaci per la protezione delle infrastrutture informatiche moderne.

Nonostante le numerose similitudini, le due soluzioni adottano approcci differenti nella gestione della sicurezza. SentinelOne si distingue per l'elevato livello di automazione e per la capacità di intervenire autonomamente in risposta a determinati eventi di sicurezza. Una delle funzionalità più interessanti è il *rollback* dei file modificati da un attacco *ransomware* su sistemi Windows, che consente di ripristinare rapidamente lo stato precedente del dispositivo riducendo l'impatto dell'incidente.

CrowdStrike Falcon, invece, pone particolare attenzione alla raccolta e all'analisi della telemetria proveniente dagli endpoint, integrando servizi avanzati di *threat intelligence* e strumenti di investigazione. La piattaforma offre funzionalità che permettono agli amministratori di effettuare analisi approfondite sugli eventi di sicurezza e di intervenire da remoto sui dispositivi attraverso la console centralizzata.

Durante il mio percorso di apprendistato ho utilizzato entrambe le soluzioni in contesti operativi reali. SentinelOne è stata la piattaforma con cui ho maturato maggiore esperienza quotidiana, occupandomi principalmente del monitoraggio degli *endpoint* e della gestione degli eventi di sicurezza generati dalla console. CrowdStrike Falcon, invece, è stata la soluzione protagonista del progetto di migrazione descritto nei capitoli successivi, permettendomi di approfondire aspetti legati al *deployment* degli *agent*, alla gestione dei *tenant* e all'amministrazione centralizzata degli *endpoint*.

Progetto di migrazione

Analisi iniziale del cliente

All'inizio del 2025 il cliente è entrato a far parte delle aziende gestite da Sinapto attraverso un contratto di assistenza e gestione dei servizi IT. L'azienda opera nel settore dell'arredamento di alta gamma e dispone di diverse sedi operative distribuite sul territorio nazionale e internazionale.

A seguito dell'avvio della collaborazione, Sinapto ha assunto la gestione dell'infrastruttura informatica del cliente, occupandosi delle attività di supporto agli utenti, della gestione degli *endpoint* aziendali, dei servizi di telefonia e delle principali soluzioni tecnologiche utilizzate dall'organizzazione.

Durante la fase iniziale è stata effettuata un'analisi dell'ambiente esistente al fine di ottenere una visione completa dell'infrastruttura e identificare eventuali criticità. Questa attività ha incluso il censimento dei dispositivi presenti, la verifica delle soluzioni software installate e l'analisi degli strumenti di sicurezza già in uso.

Migrazione del tenant su CrowdStrike Falcon

Tra gli elementi oggetto di particolare attenzione durante la fase di analisi vi era la piattaforma CrowdStrike Falcon utilizzata per la protezione degli *endpoint* aziendali.

L'infrastruttura del cliente era già dotata di una soluzione CrowdStrike Falcon, utilizzata per garantire la protezione dei dispositivi Windows e macOS presenti all'interno dell'organizzazione. Tuttavia, la piattaforma risultava gestita attraverso un *tenant* ospitato negli Stati Uniti e amministrato dal precedente fornitore di servizi IT.

A seguito del passaggio della gestione informatica a Sinapto, è stata valutata la possibilità di migrare l'intera infrastruttura verso un nuovo *tenant* CrowdStrike Falcon ospitato nell'Unione Europea e direttamente gestito dal nuovo gruppo di amministrazione.

La decisione è stata presa tenendo conto di diversi fattori. Uno degli aspetti principali riguardava la conformità alle normative europee in materia di protezione dei dati, con

particolare riferimento al Regolamento Generale sulla Protezione dei Dati (GDPR). L'utilizzo di un *tenant* europeo consentiva infatti una maggiore coerenza con le politiche aziendali relative alla gestione e al trattamento delle informazioni.

La migrazione ha quindi rappresentato un passaggio fondamentale per garantire una gestione più efficiente e uniforme della sicurezza degli *endpoint* aziendali, consentendo al tempo stesso di mantenere elevati standard di protezione durante tutte le fasi del progetto.

Obiettivi della migrazione

Una volta definita la necessità di trasferire la gestione della piattaforma CrowdStrike Falcon verso il nuovo *tenant* europeo, abbiamo dovuto identificare gli obiettivi principali del progetto, sia dal punto di vista tecnico che operativo.

Il primo obiettivo consisteva nella migrazione completa degli *endpoint* aziendali presenti all'interno dell'organizzazione. L'infrastruttura era composta da circa 120 dispositivi tra sistemi Windows e macOS, distribuiti tra diverse sedi e utenti operanti sia in presenza che da remoto.

Un secondo obiettivo riguardava la continuità operativa degli utenti. La migrazione doveva essere eseguita limitando il più possibile eventuali disservizi e garantendo che le normali attività lavorative potessero proseguire senza interruzioni significative.

Dal punto di vista della sicurezza, era fondamentale mantenere costantemente protetti gli *endpoint* durante tutte le fasi del progetto. La rimozione del sensore CrowdStrike esistente e l'installazione del nuovo agente dovevano quindi avvenire in tempi ridotti, evitando che i dispositivi rimanessero privi di una soluzione di protezione per periodi prolungati.

Un ulteriore obiettivo era quello di ridurre al minimo gli interventi manuali attraverso l'utilizzo di strumenti di gestione centralizzata. Considerato il numero elevato di dispositivi coinvolti, una procedura completamente manuale avrebbe richiesto tempi molto lunghi e un notevole impiego di risorse tecniche. Per questo motivo abbiamo deciso di sfruttare la piattaforma NinjaOne per automatizzare gran parte delle attività di distribuzione e installazione.

Infine, il progetto aveva l'obiettivo di garantire una gestione futura più efficiente della piattaforma EDR, consentendo al nostro gruppo di amministrare direttamente gli *endpoint* del cliente attraverso il nuovo tenant CrowdStrike Falcon e di intervenire rapidamente in caso di eventi o incidenti di sicurezza.

Pianificazione e rollout

La migrazione è stata preceduta da una fase di pianificazione accurata volta a ridurre i rischi e garantire la continuità operativa degli utenti.

Prima di procedere con la distribuzione sugli *endpoint* del cliente, abbiamo eseguito diversi test interni per verificare il corretto funzionamento della procedura di migrazione. In questa fase abbiamo utilizzato diverse macchine di laboratorio dedicate, sulle quali è stato possibile simulare l'intero processo di disinstallazione del sensore esistente e installazione del nuovo Falcon Sensor associato al *tenant* europeo.

Una volta verificata l'affidabilità della procedura, i test sono stati fatti a nuovi dispositivi destinati ad essere inseriti nel perimetro del cliente. Questo passaggio ha consentito di verificare ulteriormente il processo in un contesto più vicino all'ambiente di produzione, verificando la corretta registrazione degli *endpoint* all'interno della nuova console CrowdStrike Falcon.

Completata con successo la fase di test, abbiamo eseguito il *rollout* sugli *endpoint* utilizzati quotidianamente dagli utenti. La distribuzione è stata eseguita in modo graduale, monitorando costantemente l'esito delle installazioni e verificando la corretta comunicazione dei dispositivi con il nuovo *tenant*.

Per la gestione delle attività è stata utilizzata la piattaforma NinjaOne, che ci ha permesso di automatizzare gran parte delle operazioni di *deployment* e monitoraggio. Grazie all'utilizzo di *script* e procedure centralizzate è stato possibile ridurre significativamente il numero di interventi manuali su ogni singolo PC.

L'intero progetto si è sviluppato nell'arco di circa tre settimane. Durante questo periodo abbiamo gestito le attività di test, la migrazione degli *endpoint* attivi e la risoluzione delle eventuali problematiche emerse durante il *rollout*.

L'approccio graduale adottato ci ha consentito di individuare eventuali anomalie e di intervenire rapidamente sui dispositivi che richiedevano verifiche aggiuntive, garantendo il completamento della migrazione con un impatto minimo sulle attività lavorative degli utenti.

Implementazione tecnica

Disinstallazione e installazione dell'*agent*

Poiché il nostro nuovo *tenant* europeo utilizzava un differente *Customer ID* (CID), non era possibile trasferire direttamente gli endpoint da una console all'altra. Per questo motivo si è reso necessario procedere con la disinstallazione completa del sensore esistente e la successiva installazione di un nuovo Falcon Sensor associato al *tenant* europeo.

Prima di avviare le attività di migrazione abbiamo effettuato una fase di verifica sugli *endpoint* per accertare la corretta presenza del sensore CrowdStrike e raccogliere informazioni sullo stato dei dispositivi. Questa attività è risultata importante per identificare eventuali *endpoint* offline o sistemi che presentavano problemi già prima dell'inizio del progetto.

La disinstallazione è stata eseguita in modalità centralizzata attraverso la piattaforma NinjaOne, sfruttando *script* e procedure automatizzate distribuite da remoto. Questo approccio ci ha consentito di operare contemporaneamente su un elevato numero di dispositivi riducendo i tempi di intervento rispetto a una gestione manuale.

Durante questa fase abbiamo dovuto verificare il corretto completamento della disinstallazione, poiché eventuali residui del sensore precedente avrebbero potuto compromettere la successiva installazione del nuovo agente. Per questo motivo abbiamo fatto controlli automatizzati aggiuntivi sui servizi installati e sullo stato finale dell'*endpoint* prima di procedere con la fase successiva della migrazione.

Una volta verificata la rimozione del sensore esistente, gli *endpoint* erano pronti per ricevere il nuovo Falcon Sensor associato al *tenant* europeo, garantendo così la continuità della protezione e il corretto inserimento dei dispositivi all'interno della nuova infrastruttura di sicurezza.

Installazione del nuovo agente

Una volta completata la disinstallazione del sensore associato al *tenant* precedente, è stato possibile procedere con l'installazione del nuovo *Falcon Sensor* configurato per il *tenant* europeo.

Per gli *endpoint* Windows è stata adottata una procedura completamente automatizzata attraverso la piattaforma NinjaOne. L'*installer* del *Falcon Sensor* è stato preventivamente distribuito sui dispositivi e successivamente eseguito tramite *script* PowerShell in modalità *silent*, evitando qualsiasi interazione da parte degli utenti finali.

Durante l'installazione veniva specificato il *Customer ID* (CID) del nuovo *tenant* CrowdStrike Falcon tramite appositi parametri di installazione. Questo passaggio risultava fondamentale per consentire la corretta registrazione dell'*endpoint* all'interno della nuova console di gestione.

Al termine dell'installazione venivano effettuate verifiche aggiuntive per accertare che il servizio CrowdStrike fosse correttamente avviato e che il dispositivo risultasse visibile all'interno della *dashboard* del *tenant* europeo.

Per quanto riguarda i sistemi macOS, è stato adottato un approccio differente. Considerato il numero inferiore di dispositivi presenti e alcune particolarità legate alla gestione del sistema operativo Apple, le installazioni sono state eseguite manualmente dai tecnici incaricati.

Anche in questo caso è stato necessario rimuovere preventivamente il sensore associato al *tenant* precedente e procedere successivamente all'installazione del nuovo pacchetto fornito da CrowdStrike. Al termine dell'operazione veniva verificata la corretta registrazione del dispositivo all'interno del nuovo *tenant* e il corretto funzionamento dei servizi di protezione.

L'approccio adottato ha consentito di automatizzare la quasi totalità delle attività sugli *endpoint* Windows, riducendo significativamente i tempi di intervento e garantendo una maggiore uniformità del processo di migrazione. Parallelamente, la gestione manuale dei sistemi macOS ha permesso di affrontare con maggiore flessibilità eventuali problematiche specifiche della piattaforma.

Script utilizzati

Per automatizzare la migrazione degli *endpoint* Windows è stato sviluppato uno *script* PowerShell in grado di eseguire tutte le operazioni necessarie senza richiedere interventi manuali da parte degli utenti.

L'obiettivo principale dello *script* era quello di garantire una procedura standardizzata e ripetibile su tutti i dispositivi coinvolti nel progetto, riducendo il rischio di errori e velocizzando le attività di *deployment*.

La prima fase dello script prevedeva la creazione di una cartella temporanea all'interno del percorso *C:\ProgramData\CSMigration*, utilizzata per ospitare gli strumenti necessari alla migrazione. All'interno di questa *directory* venivano copiati sia il pacchetto di disinstallazione del sensore esistente sia il nuovo installer CrowdStrike Falcon associato al *tenant* europeo.

```powershell
# Modificare questo percorso!!
$folderPath = "C:\ProgramData\CSMigration"
if (-Not (Test-Path -Path $folderPath)) {
    New-Item -ItemType Directory -Path $folderPath -Force | Out-Null
    Write-Host "Cartella creata: $folderPath"
} else {
    Write-Host "La cartella esiste già: $folderPath"
}
```

Una volta preparato l'ambiente di lavoro, lo *script* procedeva con la rimozione del Falcon Sensor precedentemente installato sul dispositivo. Questa operazione rappresentava un passaggio fondamentale, poiché gli *endpoint* dovevano essere completamente scollegati dal *tenant* CrowdStrike esistente prima di poter essere registrati sul nuovo *tenant*.

```powershell
$MaintenanceToken = "c1936e7b97a62b24c8a9bd9d44369f89ce85f6ff23deadcbc0459015f2ebada5"
$UninstallTool = "C:\ProgramData\CSMigration\CsUninstallTool.exe"

$process = Start-Process -FilePath $UninstallTool `
    -ArgumentList "MAINTENANCE_TOKEN=$MaintenanceToken /quiet" `
    -Wait `
    -PassThru

Write-Output "CrowdStrike uninstaller exited with code: $($process.ExitCode)"
exit $process.ExitCode
```

Terminata la disinstallazione, veniva eseguita automaticamente l'installazione del nuovo *Falcon Sensor* in modalità *silent*. Durante questa fase lo *script* passava il *Customer ID* (CID) del *tenant* europeo come parametro di installazione, consentendo al dispositivo di registrarsi correttamente nella nuova console CrowdStrike Falcon.

```powershell
$CID = "D7E7EBB9D20A438E822F20FCC0C9F2FE-AB"
$Installer = "C:\ProgramData\CSMigration\FalconSensor_Windows.exe"

$process = Start-Process -FilePath $Installer `
    -ArgumentList "/install /quiet /norestart CID=$CID" `
    -Wait `
    -PassThru

Write-Output "CrowdStrike installer exited with code: $($process.ExitCode)"
exit $process.ExitCode
```

Al termine della procedura venivano effettuate alcune verifiche per confermare il corretto completamento dell'installazione. Infine, la cartella temporanea utilizzata durante la migrazione veniva eliminata automaticamente, lasciando il sistema pulito e rimuovendo i file non più necessari.

```powershell
# Modificare questo percorso!!
$folderPath = "C:\ProgramData\CSMigration"

Write-Host "Attesa di 20 secondi prima di eliminare la cartella: $folderPath"
Start-Sleep -Seconds 10

if (Test-Path -Path $folderPath) {
    try {
        # Rimozione della cartella e di tutto il contenuto
        Remove-Item -Path $folderPath -Recurse -Force
        Write-Host "Cartella eliminata: $folderPath"
    } catch {
        Write-Host "Errore durante l'eliminazione della cartella: $($_.Exception.Message)"
    }
} else {
    Write-Host "La cartella non esiste: $folderPath"
}
```

L'utilizzo di uno script unico ha consentito di centralizzare tutte le attività della migrazione all'interno di un'unica procedura automatizzata, semplificando la distribuzione tramite NinjaOne e riducendo significativamente i tempi necessari per la gestione degli *endpoint*.

Uso di NinjaOne per la migrazione

Per la gestione operativa della migrazione abbiamo utilizzato NinjaOne, che ci ha consentito di distribuire automaticamente file, *script* e procedure su un elevato numero di dispositivi senza la necessità di interventi manuali da parte degli utenti finali. Questo aspetto si è rivelato particolarmente importante considerando il numero di *endpoint* coinvolti nel progetto e la loro distribuzione geografica.

La procedura di migrazione è stata implementata attraverso una automazione pianificata composta da più attività eseguite in sequenza. Ogni fase del processo veniva avviata automaticamente solo dopo il completamento della fase precedente, garantendo una maggiore affidabilità della procedura e riducendo il rischio di errori durante la migrazione degli *endpoint*.

Tra le principali automazioni configurate erano presenti:

- Trasferimento del pacchetto CrowdStrike Falcon sugli *endpoint*
- Notifica di inizio procedura di migrazione sulla console
- Disinstallazione del sensore associato al *tenant* statunitense
- Installazione del nuovo *Falcon Sensor* associato al *tenant* europeo
- Notifica di completamento della migrazione
- Procedure correttive per la gestione di eventuali anomalie

Grazie alla console NinjaOne è stato inoltre possibile monitorare lo stato di avanzamento delle attività, verificare l'esito delle installazioni e identificare rapidamente eventuali *endpoint* che richiedevano interventi aggiuntivi.

Un ulteriore vantaggio offerto dalla piattaforma è stata la possibilità di eseguire *script* PowerShell da remoto e raccogliere informazioni diagnostiche direttamente dagli *endpoint*. Questa funzionalità si è rivelata particolarmente utile durante le attività di *troubleshooting* e nella gestione dei dispositivi che non completavano correttamente la procedura di migrazione.

Problemi riscontrati e soluzioni

Una delle principali difficoltà è stata rappresentata dalla presenza di *endpoint* offline durante le finestre di migrazione pianificate. Alcuni dispositivi risultavano infatti spenti o non connessi alla rete aziendale, impedendo la corretta esecuzione delle automazioni distribuite tramite NinjaOne. In questi casi è stato necessario monitorare periodicamente lo stato dei dispositivi e attendere che tornassero disponibili per poter completare le attività previste.

Un'ulteriore criticità ha riguardato alcuni *endpoint* sui quali la procedura automatizzata non veniva completata correttamente. In determinate situazioni la disinstallazione del sensore esistente o l'installazione del nuovo *Falcon Sensor* non producevano l'esito previsto, rendendo necessario un intervento supplementare.

La prima attività svolta in questi casi consisteva nel rilanciare l'automazione tramite NinjaOne, verificando successivamente l'esito delle operazioni attraverso i *log* e gli strumenti di monitoraggio disponibili. Nella maggior parte dei casi questa procedura risultava sufficiente per completare correttamente la migrazione.

Per i dispositivi che continuavano a presentare anomalie anche dopo ulteriori tentativi automatici, è stato necessario concordare un intervento diretto con l'utente. Dopo aver verificato la disponibilità della persona interessata, ci si collegava da remoto al dispositivo per eseguire manualmente le operazioni di verifica, disinstallazione e reinstallazione del Falcon Sensor.

Particolare attenzione è stata inoltre dedicata alle verifiche successive alla migrazione. Per ogni *endpoint* è stato controllato il corretto avvio dei servizi CrowdStrike e la corretta registrazione all'interno del nuovo *tenant* europeo. Questo processo ha permesso di identificare tempestivamente eventuali anomalie residue e garantire che tutti i dispositivi risultassero correttamente protetti al termine del progetto.

Nonostante le problematiche riscontrate, l'approccio graduale adottato durante il *rollout* e l'utilizzo degli strumenti di automazione hanno consentito di completare con successo la migrazione dell'intero parco macchine, limitando l'impatto sulle attività quotidiane degli utenti e mantenendo elevati standard di sicurezza durante tutte le fasi del progetto.

Conclusione

Il percorso svolto presso Sinapto durante il biennio ITS ha rappresentato per me un'esperienza estremamente formativa, sia dal punto di vista professionale che personale. Grazie all'apprendistato ho avuto l'opportunità di entrare a contatto con il mondo del lavoro in maniera concreta, confrontandomi quotidianamente con attività, problematiche e responsabilità che caratterizzano il settore informatico.

Nel corso di questi anni ho potuto osservare da vicino il funzionamento di un'azienda che opera nel settore dei servizi IT, comprendendo quanto siano importanti aspetti come l'organizzazione, la collaborazione tra colleghi e la capacità di adattarsi rapidamente alle esigenze dei clienti. Lavorare all'interno del *Service Desk* mi ha permesso di sviluppare non solo competenze tecniche, ma anche capacità relazionali e comunicative fondamentali per interfacciarsi con utenti e professionisti provenienti da contesti differenti.

Le attività svolte durante l'apprendistato mi hanno consentito di approfondire molteplici ambiti dell'informatica, dalla gestione degli endpoint al monitoraggio delle infrastrutture, dall'utilizzo di strumenti di assistenza remota fino alle tematiche legate alla sicurezza informatica. Attraverso l'impiego quotidiano di piattaforme professionali e la partecipazione a progetti reali ho potuto comprendere come le conoscenze teoriche apprese durante il percorso di studi trovino applicazione concreta all'interno delle aziende.

Uno degli aspetti che più mi ha colpito durante questa esperienza è stata l'importanza che la sicurezza informatica ha assunto negli ultimi anni. Le minacce informatiche sono sempre più evolute e complesse e richiedono strumenti e competenze adeguate per essere affrontate efficacemente. Proprio per questo motivo ho scelto di dedicare questa tesina ai sistemi di sicurezza nell'IT aziendale e, in particolare, alle soluzioni EDR, che oggi rappresentano uno degli strumenti più efficaci per la protezione degli *endpoint* e delle infrastrutture aziendali.

Parallelamente all'esperienza lavorativa, il percorso formativo presso l'ITS Angelo Rizzoli ha avuto un ruolo fondamentale nella mia crescita professionale. L'approccio pratico adottato durante le lezioni, il confronto continuo con docenti provenienti dal

mondo del lavoro e la possibilità di applicare immediatamente le conoscenze acquisite durante l'apprendistato hanno contribuito a rendere la formazione particolarmente efficace e orientata alle reali esigenze del mercato del lavoro.

Anche le certificazioni conseguite durante il percorso hanno rappresentato un'importante occasione di approfondimento e crescita, permettendomi di consolidare competenze in ambito cloud, sicurezza e infrastrutture IT. Queste esperienze hanno contribuito ad ampliare la mia visione del settore e a comprendere meglio le tecnologie che caratterizzano l'informatica moderna.

Guardando al futuro, ritengo che il biennio ITS abbia rappresentato una tappa fondamentale del mio percorso formativo e professionale. Le competenze tecniche acquisite, unite all'esperienza maturata sul campo, costituiscono una solida base sulla quale continuare a costruire il mio percorso lavorativo. Sono convinto che quanto appreso durante questi anni mi sarà di grande utilità per affrontare le future sfide del settore informatico, un ambito in continua evoluzione che richiede aggiornamento costante, curiosità e voglia di mettersi continuamente in gioco.

Concludendo, considero questa esperienza estremamente positiva e significativa, non solo per le competenze professionali sviluppate, ma anche per la crescita personale che mi ha permesso di maturare. Il percorso svolto mi ha confermato la passione per il mondo dell'informatica e mi ha fornito gli strumenti necessari per affrontare con maggiore consapevolezza e preparazione il mio futuro professionale.

Bibliografia e sitografia

- Wiki Sinapto wiki.sinapto.net
- Documentazione Crowdstrike https://falcon.crowdstrike.com/documentation
- Documentazione SentinelOne https://www.sentinelone.com/resources
- Documentazione NinjaOne https://www.ninjaone.com/docs
- Documentazione Otobo https://doc.otobo.org
- Documentazione Icinga https://icinga.com/docs
- Linee Guida CyberSecurity https://www.cisa.gov/cybersecurity
- Informazione GDPR https://gdpr-info.eu
- Linee Guida NIST https://www.nist.gov/cyberframework