GLOSSARIO
CYBER SECURITY

I T

C S

"Glossario di Cybersecurity"
Realizzato da
Oplon Networks
Anno di pubblicazione:
Luglio 2025
Scaricabile da:
www.oplon.net/glossary_cybersecurity

INDICE

1. INTRODUZIONE

La cybersecurity è un universo in continua espansione. Ogni giorno nascono nuove tecnologie, approcci, minacce e, di conseguenza, anche nuove sigle. Il linguaggio della sicurezza informatica si nutre di acronimi che, per chi lavora nel settore o si affaccia per la prima volta a questo mondo, possono sembrare quasi un'altra lingua.

Conoscere il significato di queste sigle non è solo una questione di "glossario tecnico": è un vero e proprio strumento di orientamento. Le sigle rappresentano concetti, approcci e soluzioni fondamentali per capire dove sta andando il settore, quali sono le priorità, e come si costruiscono ambienti digitali più sicuri.

Il problema è che questo linguaggio evolve alla stessa velocità delle minacce. Oggi esce una nuova tecnologia, domani nasce un nuovo acronimo per descriverla. Ecco perché restare aggiornati è indispensabile: per non perdere il passo, per parlare la stessa lingua dei colleghi e degli esperti, e soprattutto per essere dei professionisti consapevoli e competenti.

Questo e-book nasce proprio con questo obiettivo: aiutarti a fare chiarezza, a non perderti tra le sigle, e a rimanere al passo con un mondo che cambia ogni giorno. È pensato per chi lavora nella cybersecurity, per chi ci sta entrando ora, ma anche per chi vuole semplicemente capirci qualcosa in più.

Sfoglialo, consultalo, tienilo a portata di mano. Perché nel mondo della sicurezza digitale, le parole contano. E spesso iniziano tutte con una sigla.

2. GESTIONE DELLE IDENTITÀ E DEGLI ACCESSI

IAM Identity & Access Management

Insieme di politiche, processi e tecnologie che permettono di creare, gestire e controllare le identità digitali degli utenti e di regolare i loro accessi a risorse, applicazioni e sistemi aziendali. Include autenticazione, autorizzazione, gestione delle credenziali e audit per garantire che solo gli utenti autorizzati possano accedere alle risorse corrette.

IDaaS Identity as a Service

IDaaS è un servizio cloud che fornisce funzionalità di gestione delle identità e degli accessi (IAM) senza la necessità di infrastrutture on-premise. Offre autenticazione, autorizzazione, Single Sign-On (SSO), gestione delle password e provisioning degli utenti in modo scalabile e centralizzato, integrandosi con applicazioni cloud e on-premise.

SSO Single Sign-On

SSO è una tecnologia di autenticazione che permette agli utenti di accedere a più applicazioni o sistemi con un'unica autenticazione iniziale, eliminando la necessità di effettuare il login separatamente per ciascun servizio. Migliora la sicurezza e l'usabilità riducendo la gestione di password multiple e facilitando il controllo degli accessi.

PAM Privileged Access Management

PAM è una tecnologia e un insieme di pratiche per gestire e controllare l'accesso degli utenti con privilegi elevati (amministratori, superuser) ai sistemi critici. Include l'autenticazione forte, la gestione delle credenziali, il monitoraggio delle sessioni e il controllo delle attività per prevenire abusi e violazioni.

PIM Identity Governance and Administration

Il PIM è un sistema che consente di gestire, monitorare e controllare gli accessi degli utenti con privilegi elevati (amministratori di sistema, superuser, ecc.). Include funzionalità come la concessione temporanea dei privilegi, la registrazione delle attività, l'audit degli accessi e la gestione delle password privilegiate. L'obiettivo è ridurre i rischi legati all'abuso di account privilegiati e migliorare la sicurezza complessiva.

CIAM Customer Identity and Access Management

Il CIAM è una soluzione specializzata di gestione delle identità e degli accessi dedicata agli utenti esterni, cioè ai clienti di un'azienda. Include funzionalità come registrazione self-service, autenticazione sicura (spesso con MFA), gestione del consenso e privacy, personalizzazione dell'esperienza utente, e compliance con normative come il GDPR. CIAM consente alle aziende di offrire un accesso sicuro, fluido e scalabile ai propri servizi digitali.

IGA Identity Governance and Administration

L'IGA è un insieme di processi, tecnologie e policy che permettono di gestire e controllare le identità digitali e i relativi accessi all'interno di un'organizzazione. Include attività come la creazione, modifica e disattivazione degli account utente, la gestione dei ruoli, la revisione periodica degli accessi (access certification) e la conformità normativa. Le soluzioni IGA aiutano a garantire che gli utenti abbiano solo i permessi necessari, riducendo i rischi di accessi non autorizzati.

ISPM Identity Security Posture Management

ISPM è una disciplina e insieme di tecnologie che monitorano, analizzano e migliorano la postura di sicurezza delle identità digitali all'interno di un'organizzazione. Si concentra sulla valutazione continua dei rischi associati agli account utente, privilegi, configurazioni di accesso e policy di sicurezza, per identificare vulnerabilità, comportamenti anomali o esposizioni che potrebbero essere sfruttate da attaccanti. ISPM aiuta a mantenere l'ecosistema di identità sicuro, conforme e resiliente.

ITDR Identity Threat Detection & Response

ITDR è una disciplina e una tecnologia focalizzata sul monitoraggio, rilevamento e risposta agli attacchi e alle minacce che coinvolgono le identità digitali. Include l'analisi dei comportamenti anomali degli utenti, la rilevazione di accessi sospetti, tentativi di compromissione di account privilegiati e la gestione degli incidenti legati agli accessi. L'obiettivo è proteggere l'identità come punto critico di sicurezza e rispondere rapidamente a qualsiasi minaccia che possa compromettere le credenziali o i privilegi degli utenti.

JIT Just-In-Time (Access)

Just-In-Time (JIT) access è una metodologia di sicurezza che concede privilegi o accessi solo quando sono necessari e per un tempo limitato, riducendo la finestra di esposizione agli attacchi. Spesso usata in combinazione con sistemi di gestione privilegiata (PAM/PIM), JIT prevede la richiesta e l'approvazione dinamica degli accessi elevati solo per la durata strettamente necessaria.

ABAC Attribute-Based Access Control

ABAC è un modello di controllo degli accessi in cui le decisioni vengono prese in base a attributi (o proprietà) dell'utente, della risorsa, dell'ambiente e dell'azione. Gli attributi possono includere ruolo, posizione geografica, orario, livello di rischio, tipo di dispositivo, ecc. Questo approccio consente una gestione degli accessi dinamica, granulare e contestuale, ideale per ambienti Zero Trust.

RBAC Role-Based Access Control

RBAC è un modello di controllo degli accessi in cui i permessi sono assegnati a ruoli specifici all'interno di un'organizzazione, e gli utenti ottengono quei permessi in base al ruolo a cui sono assegnati. Questo facilita la gestione centralizzata delle autorizzazioni, riducendo errori e garantendo che gli utenti abbiano accesso solo alle risorse necessarie per le loro mansioni.

IdP Identiy Provider

Un IDP Proxy è un componente che funge da intermediario tra un service provider (applicazione o servizio) e un Identity Provider (IdP). Facilita l'autenticazione degli utenti, semplificando l'integrazione con diversi sistemi di identità e permettendo di centralizzare e consolidare i flussi di autenticazione (es. SAML, OAuth, OpenID Connect). Spesso usato per supportare l'accesso single sign-on (SSO) e migliorare la gestione delle identità in ambienti complessi o multi-cloud.

IdP Proxy Identity Provider Proxy

Un IDP Proxy è un componente che funge da intermediario tra un service provider (applicazione o servizio) e un Identity Provider (IdP). Facilita l'autenticazione degli utenti, semplificando l'integrazione con diversi sistemi di identità e permettendo di centralizzare e consolidare i flussi di autenticazione (es. SAML, OAuth, OpenID Connect). Spesso usato per supportare l'accesso single sign-on (SSO) e migliorare la gestione delle identità in ambienti complessi o multi-cloud.

Identity Broker

L'Identity Broker è un componente o servizio che funge da intermediario tra diversi Identity Provider (IdP) e service provider (applicazioni, servizi). Aggrega e gestisce varie fonti di identità, facilitando l'autenticazione e l'autorizzazione attraverso protocolli standard come SAML, OAuth o OpenID Connect. Consente agli utenti di utilizzare un'unica identità digitale per accedere a molteplici risorse, anche se distribuite su sistemi differenti o cloud diversi.

UAA User Account and Authentication

UAA è un sistema che gestisce autenticazione e autorizzazione degli utenti. Viene spesso usato come componente in ambienti cloud-native (es. Cloud Foundry) per gestire identità, emettere token di accesso (OAuth2), gestire permessi e collegarsi a Identity Provider esterni. Supporta Single Sign-On (SSO), federazione delle identità, e controlli granulari degli accessi.

EAM Enterprise Access Management

EAM è un insieme di tecnologie e processi pr re l'accesso degli utenti alle risorse aziendali (applicazioni, sistemi, dati). Si focalizza sulla gestione centralizzata dei diritti di accesso (entitlements) per garantire che solo gli utenti autorizzati possano accedere a specifiche risorse in base a regole, ruoli o attributi. Spesso è integrato con sistemi IAM, PAM e policy di sicurezza come RBAC o ABAC.

SCIM System for Cross-domain Identity Management

EAM è un insieme di tecnologie e processi progettati per gestire, controllare e monitorare l'accesso degli utenti alle risorse aziendali (applicazioni, sistemi, dati). Si focalizza sulla gestione centralizzata dei diritti di accesso (entitlements) per garantire che solo gli utenti autorizzati possano accedere a specifiche risorse in base a regole, ruoli o attributi. Spesso è integrato con sistemi IAM, PAM e policy di sicurezza come RBAC o ABAC.

OIDC OpenID Connect

OpenID Connect (OIDC) è un protocollo di autenticazione basato su OAuth 2.0 che consente ai client (app o siti web) di verificare l'identità dell'utente tramite un Identity Provider (IdP) e di ottenere informazioni sull'utente (claim) in modo sicuro. OIDC semplifica l'implementazione del Single Sign-On (SSO) e supporta flussi di autenticazione moderni, inclusi mobile e API.

OAuth Open Authorization

OAuth è un protocollo aperto che permette a un'applicazione di ottenere accesso limitato alle risorse protette di un utente su un altro servizio, senza condividere le credenziali (come la password). Utilizza token di accesso temporanei per delegare permessi in modo sicuro, molto usato per autorizzare accessi a API, app web e mobile.

CIE Carta d'Identità Elettronica

La Carta d'Identità Elettronica (CIE) è un documento di identità digitale rilasciato dallo Stato italiano, che consente l'autenticazione online dell'utente tramite un Identity Provider pubblico (Ministero dell'Interno). La CIE può essere usata per accedere in modo sicuro ai servizi della Pubblica Amministrazione e privati abilitati, tramite protocolli di autenticazione come SAML e OIDC. Supporta anche l'uso su dispositivi mobile tramite NFC e app dedicate.

SPID Sistema Pubblico di Identità Digitale

Il Sistema Pubblico di Identità Digitale (SPID) è un sistema di autenticazione federata che consente ai cittadini italiani di accedere a servizi online tramite credenziali fornite da Identity Provider accreditati. Basato su standard di sicurezza come SAML 2.0 (e OIDC in alcune evoluzioni), SPID garantisce l'identità digitale dell'utente e abilita il Single Sign-On (SSO) verso le piattaforme pubbliche e private che aderiscono al sistema.

WebAuthn Web Authentication

WebAuthn è uno standard di autenticazione sviluppato dal W3C e dalla FIDO Alliance che consente agli utenti di accedere a siti web e applicazioni in modo sicuro e senza password, utilizzando dispositivi come: impronte digitali (biometria);riconoscimento facciale;chiavi di sicurezza hardware (es. YubiKey);PIN o autenticazione del dispositivo. WebAuthn si basa su autenticazione a chiave pubblica: al momento della registrazione, il dispositivo dell'utente crea una coppia di chiavi (pubblica/privata) e invia solo la chiave pubblica al server. Durante l'accesso, l'utente conferma la propria identità localmente (es. con impronta), e il dispositivo firma una sfida usando la chiave privata.

JWT JSON Web Token

JWT è uno standard aperto (RFC 7519) che definisce un formato compatto e auto-contenuto per trasmettere in modo sicuro informazioni tra le parti come oggetti JSON. I JWT vengono firmati digitalmente (usando algoritmi come HMAC o RSA) per garantire l'integrità e, in alcuni casi, la riservatezza. Sono ampiamente utilizzati per autenticazione, autorizzazione e scambio sicuro di dati in ambienti web e API.

BYOI Bring Your Own Identity

BYOI è un modello di autenticazione che consente agli utenti di accedere a servizi digitali utilizzando identità già esistenti fornite da terze parti, come Google, Facebook, Apple, o altri Identity Provider (IdP) federati. Questo approccio semplifica l'onboarding, riduce la gestione delle credenziali da parte delle aziende e migliora l'esperienza utente, mantenendo il controllo degli accessi tramite protocolli standard (es. OAuth, OIDC, SAML).

FS Federated Services

Federated Services si riferisce a un insieme di meccanismi che permettono a più domini o organizzazioni di condividere l'autenticazione e l'autorizzazione degli utenti in modo sicuro e controllato. Grazie a protocolli come SAML, OAuth e OIDC, un utente può accedere a servizi di terze parti utilizzando le proprie credenziali di origine (Identity Provider). Questo è alla base della federazione delle identità e dell'integrazione tra sistemi eterogenei.

FIDO Fast IDentity Online

La FIDO Alliance è un'organizzazione industriale internazionale fondata nel 2012 con l'obiettivo di eliminare l'uso delle password e promuovere standard di autenticazione forti, sicuri e facili da usare. L'obiettivo è creare un ecosistema di autenticazione che sia: più sicuro delle password tradizionali; più semplice per gli utenti; standardizzato e interoperabile tra dispositivi e servizi. Attraverso lo sviluppo di standard aperti per l'autenticazione a due fattori (2FA), l'autenticazione senza password e l'autenticazione biometrica. I principali standard FIDO includono: FIDO U2F (Universal 2nd Factor) – autenticazione con chiavi fisiche (es. YubiKey); FIDO UAF (Universal Authentication Framework) – autenticazione biometrica (impronta, volto); FIDO2 – combina WebAuthn (del W3C) e CTAP (Client to Authenticator Protocol) per login passwordless.

3. SICUREZZA RETE, APPLICATIVA, ACCESSI ZERO TRUST

ZTNA Zero Trust Network Access

Soluzione di accesso sicuro basata sul principio “Zero Trust”: non si fida mai automaticamente di utenti o dispositivi, nemmeno se sono già all’interno della rete aziendale. L’accesso viene concesso solo dopo aver verificato identità, stato del dispositivo e altri fattori di contesto, applicando policy precise per ogni sessione e risorsa.

CASB Cloud Access Security Broker

Il CASB è un punto di controllo situato tra gli utenti e le applicazioni cloud, progettato per monitorare e applicare policy di sicurezza quando si accede ai servizi cloud (come Google Workspace, Microsoft 365, Salesforce, ecc.). Offre visibilità sul traffico cloud, prevenzione della perdita di dati (DLP), rilevamento di attività anomale, crittografia e controllo degli accessi.

SWG Secure Web Gateway

Soluzione di sicurezza che filtra il traffico web in uscita per prevenire accessi a contenuti dannosi o non autorizzati. Controlla le richieste HTTP/ HTTPS, applica policy aziendali (come il blocco di siti pericolosi o inappropriati), rileva malware e protegge da minacce provenienti dal web. Può includere funzioni di URL filtering, sandboxing e Data Loss Prevention (DLP).

FWaaS Firewall as a Service

FWaaS è una soluzione firewall completamente gestita e distribuita tramite cloud, che offre protezione a livello di rete e applicazione senza la necessità di dispositivi fisici. Fornisce funzionalità come filtraggio del traffico, controllo delle applicazioni, prevenzione delle intrusioni (IPS), ispezione SSL/TLS e segmentazione. In un’architettura SASE, FWaaS consente protezione coerente ovunque si trovino utenti e dispositivi.

SSE Security Service Edge

SSE è una componente della più ampia architettura SASE focalizzata esclusivamente sui servizi di sicurezza cloud, come ZTNA, SWG, CASB e Data Loss Prevention (DLP). Fornisce protezione, visibilità e controllo del traffico internet e cloud, separando le funzioni di sicurezza dal networking e offrendo un accesso sicuro e policy-based indipendentemente dalla posizione dell’utente.

SASE Secure Acces Service Edge

SASE è un’architettura cloud-native che unisce funzioni di rete (come SD-WAN) e di sicurezza (come ZTNA, SWG, CASB, FWaaS) in un’unica piattaforma distribuita globalmente. L’obiettivo è fornire accesso sicuro e performante a utenti, dispositivi e applicazioni ovunque si trovino, riducendo la complessità e migliorando visibilità e controllo.

DLP Data Loss Prevention

DLP è una tecnologia e una strategia di sicurezza progettata per prevenire la perdita, la fuoriuscita o il furto di dati sensibili, sia intenzionale che accidentale. Funziona monitorando e controllando i dati in transito, a riposo e in uso, e può bloccare l’invio non autorizzato di informazioni riservate (es. email, upload, stampa, copia). È spesso utilizzata per rispettare normative come GDPR, HIPAA, PCI-DSS.

RBI Remote Browser Isolation

La Remote Browser Isolation è una tecnologia di sicurezza che separa fisicamente o logicamente il processo di navigazione web dal dispositivo dell’utente, eseguendo il rendering delle pagine in un ambiente isolato (cloud o locale) e mostrando all’utente solo una “copia sicura” (ad es. una trasmissione video). In questo modo, eventuali malware o contenuti pericolosi presenti nel sito web non raggiungono mai il dispositivo dell’utente.

Full-Path TLS Inspection

Full-Path TLS Inspection (o SSL Inspection) è una tecnica di sicurezza che consente a un sistema intermediario (es. un firewall, proxy, o SWG) di decrittare, analizzare e poi re-crittare il traffico HTTPS/TLS tra client e server. Questo permette di rilevare minacce nascoste in traffico cifrato, come malware, phishing o fughe di dati. Il termine “full-path” sottolinea che l’ispezione avviene su tutto il percorso, dall’origine alla destinazione, anziché solo in segmenti parziali.

Proactive DDoS Mitigation

Proactive DDoS Mitigation è un insieme di strategie e tecnologie che rilevano e bloccano attacchi DDoS (Distributed Denial of Service) prima che possano impattare i servizi aziendali. A differenza della mitigazione reattiva (che interviene dopo l'inizio dell'attacco), la protezione proattiva utilizza sistemi di analisi del traffico in tempo reale, apprendimento automatico e policy preconfigurate per anticipare e neutralizzare anomalie in modo automatico, mantenendo disponibili le applicazioni e le reti.

CNAPP Cloud-Native Application Protection Platform

CNAPP è una piattaforma unificata che fornisce visibilità, sicurezza e conformità per applicazioni cloud-native lungo tutto il loro ciclo di vita. Combina funzionalità di CSPM (Cloud Security Posture Management), CWPP (Cloud Workload Protection Platform), CIEM (Cloud Infrastructure Entitlement Management) e container/Kubernetes security, offrendo una protezione integrata per codice, infrastruttura e runtime. CNAPP aiuta a rilevare vulnerabilità, configurazioni errate e minacce attive, fornendo anche strumenti per la remediation automatica.

CSPM Cloud Security Posture Management

CSPM è una categoria di strumenti e pratiche progettata per identificare e correggere errori di configurazione e vulnerabilità nei servizi cloud (IaaS, PaaS, SaaS). Monitora continuamente gli ambienti cloud alla ricerca di non conformità alle policy di sicurezza, standard (es. NIST, CIS) e normative (es. GDPR, ISO 27001). Aiuta a ridurre il rischio di esposizioni accidentali e attacchi legati a configurazioni errate.

CWPP Cloud Workload Protection Platform

CWPP è una soluzione di sicurezza progettata per proteggere i carichi di lavoro (workload) nei cloud pubblici, privati e ibridi. I carichi di lavoro includono macchine virtuali, container, server fisici, funzioni serverless e altri asset computazionali. CWPP fornisce funzionalità come scansione delle vulnerabilità, monitoraggio del comportamento, protezione runtime, e controlli di integrità, assicurando che ogni workload sia sicuro indipendentemente da dove venga eseguito.

DSPM Data Security Posture Management

DSPM è una soluzione progettata per scoprire, classificare, monitorare e proteggere i dati sensibili (strutturati e non) ovunque si trovino --- in cloud, SaaS, on-premise o ambienti ibridi. Analizza come i dati vengono archiviati, spostati e accessibili, identifica configurazioni errate, accessi eccessivi o dati esposti e aiuta a migliorare la postura di sicurezza dei dati. Spesso si integra con strumenti di DLP, CSPM e IAM.

CAASM Cyber Asset Attack Surface Management

CAASM è una tecnologia che consente alle organizzazioni di ottenere visibilità completa su tutti gli asset IT e cyber (endpoint, applicazioni, dispositivi, identità, cloud, ecc.), correlando informazioni da più fonti per identificare lacune di copertura, configurazioni errate, vulnerabilità e asset esposti. L'obiettivo è mappare e ridurre la superficie d'attacco sfruttabile da potenziali minacce, migliorando la postura di sicurezza complessiva.

4. THREAT DETECTION, SOC & INCIDENT RESPONSE

UEBA User and Entity Behavior Analytics

UEBA utilizza algoritmi avanzati di machine learning e analisi comportamentale per monitorare e analizzare il comportamento di utenti, dispositivi e altre entità all'interno di un sistema IT. L'obiettivo è rilevare attività anomale o sospette che potrebbero indicare minacce interne, compromissioni di account o attacchi avanzati (come insider threat, furto di credenziali, movimenti laterali). UEBA integra dati da molteplici fonti per fornire un contesto approfondito e migliorare la precisione delle rilevazioni.

SIEM Security Information and Event Management

Il SIEM è una piattaforma che raccoglie, normalizza, correla e analizza i log e gli eventi di sicurezza provenienti da vari sistemi IT (firewall, endpoint, server, applicazioni, ecc.). Fornisce visibilità in tempo reale, rilevamento di minacce, alert e supporto alla risposta agli incidenti. Utilizza regole, correlazioni e a volte anche machine learning per identificare comportamenti anomali.

SOAR Security Orchestration, Automation and Response

SOAR è una piattaforma che consente ai team di sicurezza di orchestrare strumenti diversi, automatizzare attività ripetitive e gestire in modo centralizzato i processi di risposta agli incidenti. Si integra con SIEM, EDR, firewall, ticketing e altri sistemi per velocizzare le indagini, ridurre i tempi di reazione e standardizzare le procedure attraverso playbook automatici.

EDR Security Information and Event Management

L'EDR è una soluzione di sicurezza progettata per monitorare, registrare e analizzare continuamente le attività sui dispositivi endpoint (PC, server, laptop) al fine di rilevare, investigare e rispondere rapidamente a minacce avanzate. Utilizza raccolta di dati comportamentali, rilevamento basato su firme e analisi euristica, offrendo capacità di contenimento, isolamento e remediation automatica.

XDR Extended Detection and Response

XDR è una soluzione di sicurezza integrata che combina e correla dati provenienti da diverse fonti --- endpoint, reti, cloud, email, applicazioni --- per fornire una visione unificata delle minacce. Permette di rilevare, analizzare e rispondere in modo più efficace agli attacchi informatici, automatizzando le operazioni di sicurezza e migliorando la capacità di risposta agli incidenti in tutta l'infrastruttura IT.

NDR Network Detection and Response

NDR è una tecnologia di sicurezza che monitora il traffico di rete per identificare attività anomale, minacce e attacchi in corso, anche quelli che sfuggono alle soluzioni tradizionali come firewall o antivirus. Utilizza tecniche avanzate come machine learning, analisi comportamentale e threat intelligence per rilevare comportamenti sospetti, e include funzionalità di risposta per contenere o investigare l'incidente.

MDR Managed Detection and Response

MDR è un servizio di sicurezza gestito da terze parti che combina tecnologie avanzate di rilevamento delle minacce (come EDR, SIEM, XDR) con un team di esperti che analizza, indaga e risponde attivamente agli incidenti di sicurezza 24/7. L'obiettivo è fornire una protezione efficace anche alle organizzazioni che non dispongono di un SOC interno o di risorse specializzate.

TIP Threat Intelligence Platform

Una Threat Intelligence Platform (TIP) è una soluzione progettata per aggregare, normalizzare, analizzare e condividere informazioni sulle minacce informatiche provenienti da fonti interne (log, SIEM, incidenti) ed esterne (feed commerciali, open source, comunità, CERT). Aiuta a prioritizzare le minacce, generare indicatori di compromissione (IoC) rilevanti e fornire dati azionabili per soluzioni come SIEM, SOAR, firewall e sistemi EDR/XDR.

FIM File Integrity Monitoring

File Integrity Monitoring (FIM) è un sistema di sicurezza che monitora continuamente file e directory critici (come configurazioni, file di sistema, registri) per rilevare modifiche non autorizzate o anomale. Confronta lo stato attuale dei file con versioni "attese" o baseline sicure, generando alert quando rileva variazioni. È utilizzato per rilevamento delle violazioni, auditing, conformità (es. PCI-DSS, HIPAA, ISO 27001) e risposta agli incidenti.

SOC Security Operations Center

SaaS è un modello di distribuzione del software in cui le applicazioni sono ospitate nel cloud e accessibili via internet, normalmente tramite abbonamento. Gli utenti non devono installare o gestire il software localmente: tutto, dalla manutenzione agli aggiornamenti, è gestito dal fornitore. Esempi comuni: Google Workspace, Microsoft 365, Salesforce.

5. MODELLI E ARCHITETTURE CLOUD

IaaS Infrastructure as a Service

IaaS è un modello cloud che fornisce risorse infrastrutturali virtualizzate (server, storage, rete) via internet. Permette alle aziende di “affittare” l’infrastruttura IT, senza acquistare e gestire hardware fisico. Gli utenti hanno controllo su sistemi operativi, applicazioni e configurazioni, mentre il provider gestisce l’infrastruttura sottostante. Esempi: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

PaaS Platform as a Service

PaaS è un modello cloud che fornisce una piattaforma completa per sviluppo, test,deployment e gestione di applicazioni. Include infrastruttura (come IaaS), sistemi operativi, database, strumenti di sviluppo e servizi middleware. Permette agli sviluppatori di concentrarsi sul codice senza gestire hardware o sistema operativo. Esempi: Google App Engine, Heroku, Azure App Services.

SaaS Software as a Service

SaaS è un modello di distribuzione del software in cui le applicazioni sono ospitate nel cloud e accessibili via internet, normalmente tramite abbonamento. Gli utenti non devono installare o gestire il software localmente: tutto, dalla manutenzione agli aggiornamenti, è gestito dal fornitore. Esempi comuni: Google Workspace, Microsoft 365, Salesforce.

6. SICUREZZA APPLICATIVA (AppSec)

SAST Static Application Security Testing

SAST è una tecnica di analisi della sicurezza del codice sorgente o del binario di un'applicazione senza eseguirla. Identifica vulnerabilità, errori di programmazione e potenziali problemi di sicurezza analizzando staticamente il codice durante la fase di sviluppo. Questo aiuta a correggere le falle prima che il software venga distribuito. È parte integrante delle pratiche di DevSecOps.

DAST Dynamic Application Security Testing

DAST è una tecnica di testing della sicurezza applicativa che analizza un'applicazione durante l'esecuzione, simulando attacchi reali per identificare vulnerabilità come SQL injection, cross-site scripting (XSS) e altri problemi di runtime. Non richiede accesso al codice sorgente, ma verifica la risposta dell'applicazione a input malevoli. È utile per testare applicazioni web e API in ambienti di staging o produzione.

Interactive Application Security Testing

IAST combina elementi di SAST e DAST monitorando il comportamento dell'applicazione durante l'esecuzione in ambienti di test o sviluppo. Usa agenti integrati nel runtime per analizzare il codice in azione, identificando vulnerabilità sia statiche che dinamiche con maggiore precisione e contesto. Questo approccio fornisce un'analisi dettagliata e in tempo reale delle potenziali falle di sicurezza.

RASP Runtime Application Self-Protection

RASP è una tecnologia di sicurezza che si integra direttamente all'interno dell'applicazione per monitorarne il comportamento in tempo reale durante l'esecuzione. Rileva e blocca automaticamente attacchi come iniezioni SQL, cross-site scripting (XSS) e altre minacce, proteggendo l'applicazione dall'interno senza necessità di intervento esterno. Funziona analizzando traffico, chiamate e dati, reagendo immediatamente a comportamenti sospetti.

ASPM Application Security Posture Management

ASPM è una soluzione che fornisce visibilità, valutazione e gestione continua della sicurezza delle applicazioni durante tutto il ciclo di vita, combinando dati da strumenti come SAST, DAST, IAST, RASP e gestione delle vulnerabilità. Aiuta a identificare le lacune di sicurezza, prioritizzare le correzioni e migliorare la postura complessiva dell'applicazione rispetto alle minacce.

SCA Software Composition Analysis

SCA è una tecnologia che analizza le componenti di terze parti e le librerie open source all'interno di un'applicazione software per identificare vulnerabilità note, licenze non conformi e rischi associati. Permette di gestire e monitorare continuamente la sicurezza delle dipendenze, assicurando che nessun componente esterno introduca falle o problemi di compliance.

7. NORMATIVE, REGOLAMENTI E STANDARD

GDPR General Data Protection Regulation

Il GDPR è il regolamento europeo (UE 2016/679) entrato in vigore nel 2018 che disciplina il trattamento e la protezione dei dati personali dei cittadini dell'Unione Europea. Stabilisce principi fondamentali (come liceità, trasparenza, minimizzazione dei dati), diritti per gli interessati (es. diritto all'oblio, accesso, portabilità) e obblighi per le organizzazioni, comprese misure di sicurezza, nomina del DPO, gestione dei consensi e notifica delle violazioni.

NIST National Institute of Standards and Technology

Il NIST è un ente governativo statunitense che sviluppa standard, linee guida e best practice per la sicurezza informatica, tra cui il noto framework NIST Cybersecurity Framework (CSF). Questo framework aiuta le organizzazioni a gestire e ridurre i rischi di sicurezza informatica attraverso un approccio strutturato basato su identificazione, protezione, rilevamento, risposta e recupero.

NIS2 Network and Information Security Directive 2

NIS2 è l'aggiornamento della direttiva NIS dell'UE, che rafforza e amplia i requisiti di sicurezza per le reti e i sistemi informativi. Introduce obblighi più stringenti per un maggior numero di settori (compresi i servizi digitali e infrastrutture critiche), aumenta le responsabilità dei vertici aziendali e prevede sanzioni più severe per il mancato rispetto.

DORA Digital Operational Resilience Act

Regolamento dell'Unione Europea che stabilisce requisiti obbligatori per rafforzare la resilienza operativa digitale delle istituzioni finanziarie e degli enti critici. Obbliga a gestire rischi informatici, garantire continuità operativa, monitorare fornitori terzi di servizi ICT e segnalare incidenti di sicurezza in modo standardizzato.

CRA Cyber Resilience Act

Il Cyber Resilience Act è una proposta normativa dell'UE che mira a stabilire requisiti minimi di sicurezza per prodotti con componenti digitali, obbligando i produttori a garantire un livello base di protezione contro vulnerabilità e attacchi informatici durante tutto il ciclo di vita del prodotto.

8. DATI SENSIBILI E PROTEZIONE DELLA PRIVACY

PII Personally Identifiable Information

PII si riferisce a qualsiasi dato che può essere utilizzato, da solo o insieme ad altre informazioni, per identificare in modo univoco una persona fisica. Include elementi come nome, indirizzo, numero di telefono, codice fiscale, email personale, dati biometrici, numeri di documenti o di carte di pagamento. La protezione del PII è regolata da normative come GDPR, HIPAA o CCPA.

9. SICUREZZA RETE, APPLICATIVA, ACCESSI ZERO TRUST

LDAP Lightweight Directory Access Protocol

LDAP è un protocollo standard per interrogare e modificare servizi di directory, che memorizzano informazioni su utenti, gruppi, dispositivi e altre risorse di rete. Viene usato per autenticazione, autorizzazione e gestione centralizzata delle identità in ambienti aziendali, facilitando l'accesso a risorse tramite directory come Active Directory o OpenLDAP.

CA Ceritification Authority

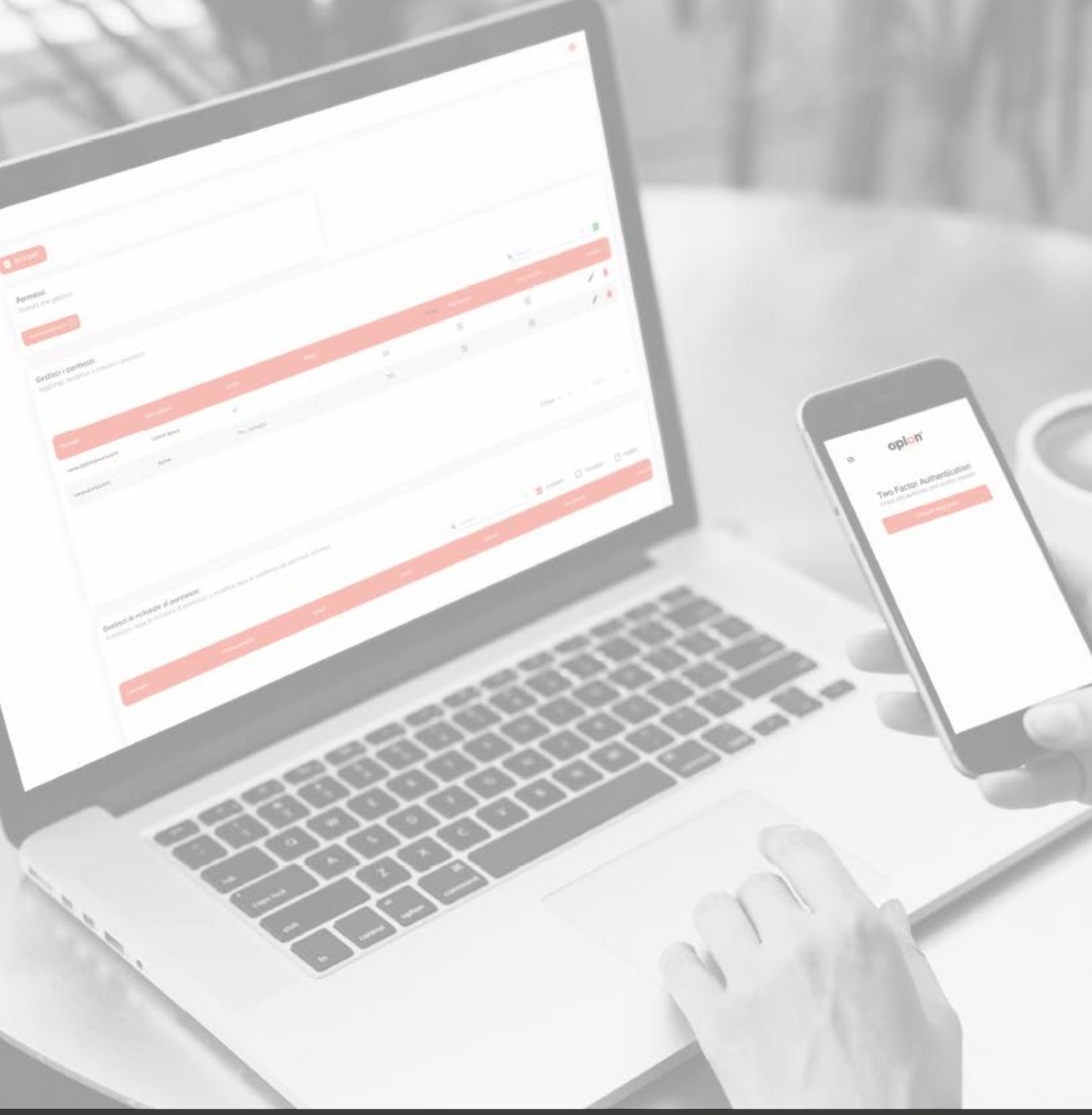
Una Certification Authority (CA) è un ente che emette certificati digitali per garantire l'identità di utenti, dispositivi o servizi in una rete. I certificati digitali sono usati, ad esempio, per abilitare comunicazioni sicure tramite protocolli come HTTPS o TLS. La CA attesta che una chiave pubblica appartiene a un determinato soggetto (utente, server, azienda), firmando digitalmente un certificato (X.509). Una CA può essere anche interna , in questo caso è gestita all'interno di un'organizzazione (es. un'azienda o una PA) e non è riconosciuta pubblicamente, ma è fidata all'interno del perimetro aziendale. Viene usata per Autenticare utenti, server o dispositivi interni come Wi-Fi, posta elettronica, ecc.

BYOD Bring Your Own Device

BYOD è una policy aziendale che consente ai dipendenti di utilizzare i propri dispositivi personali (smartphone, laptop, tablet) per accedere a risorse e dati aziendali. Questo approccio migliora la produttività e la flessibilità, ma introduce anche rischi di sicurezza legati alla gestione dei dati, alla protezione degli endpoint e alla separazione tra ambito personale e lavorativo. Per gestirlo in sicurezza si usano soluzioni come MDM (Mobile Device Management) o EDR (Endpoint Detection and Response).

AD Active Directory

Active Directory è un servizio di directory sviluppato da Microsoft che permette la gestione centralizzata di utenti, gruppi, computer e risorse di rete in ambienti aziendali. Per comunicare e scambiare queste informazioni, Active Directory utilizza un protocollo standard chiamato LDAP (Lightweight Directory Access Protocol). LDAP consente a client e applicazioni di interrogare, autenticare e modificare i dati contenuti nella directory, rendendolo uno strumento fondamentale per l'autenticazione e l'autorizzazione in sistemi centralizzati come Active Directory.



oplon®

Per saperne di più, visita il nostro sito
https://www.oplon.net
o scrivici a info@oplon.net

Oplon Networks è una società di ingegneria informatica nata nel 2010. La mission è creare prodotti e servizi per garantire Alta Affidabilità e sicurezza a livello infrastrutturale nell'erogazione dei servizi, con standard qualitativi straordinari.
L'eccellenza è il nostro primo obiettivo!
Per questo realizziamo strumenti di cybersecurity e soluzioni integrate per presidiare i moderni Data Center, Network, Cloud e Hybrid Cloud.

Dati e caratteristiche possono variare in qualsiasi momento senza alcun obbligo di preavviso.