TD SYNNEX

IPS-IDS

Quando la decryption ricopre un ruolo fondamentale per l’analisi del traffico

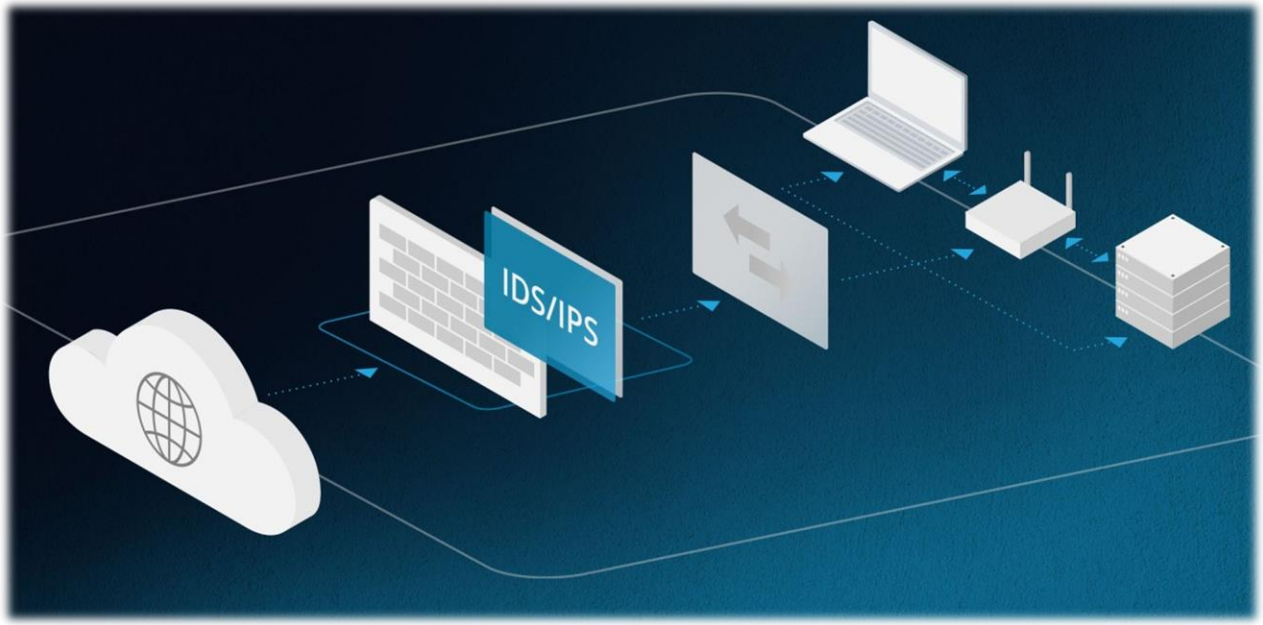
18 Ottobre 2024

Webinar

Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

Cos’è sono IDS e IPS

I sistemi IPS (Intrusion Prevention System) e IDS (Intrusion Detection System) monitorano il traffico, i pacchetti di rete e i loro contenuti in tempo reale, rilevando attività anomale e sospette.
Se il sistema IDS si limita ad avvisare, il sistema IPS blocca l'attacco.
Questa tecnologia fornisce una protezione contro gli attacchi basati sulle vulnerabilità dei protocolli di rete.



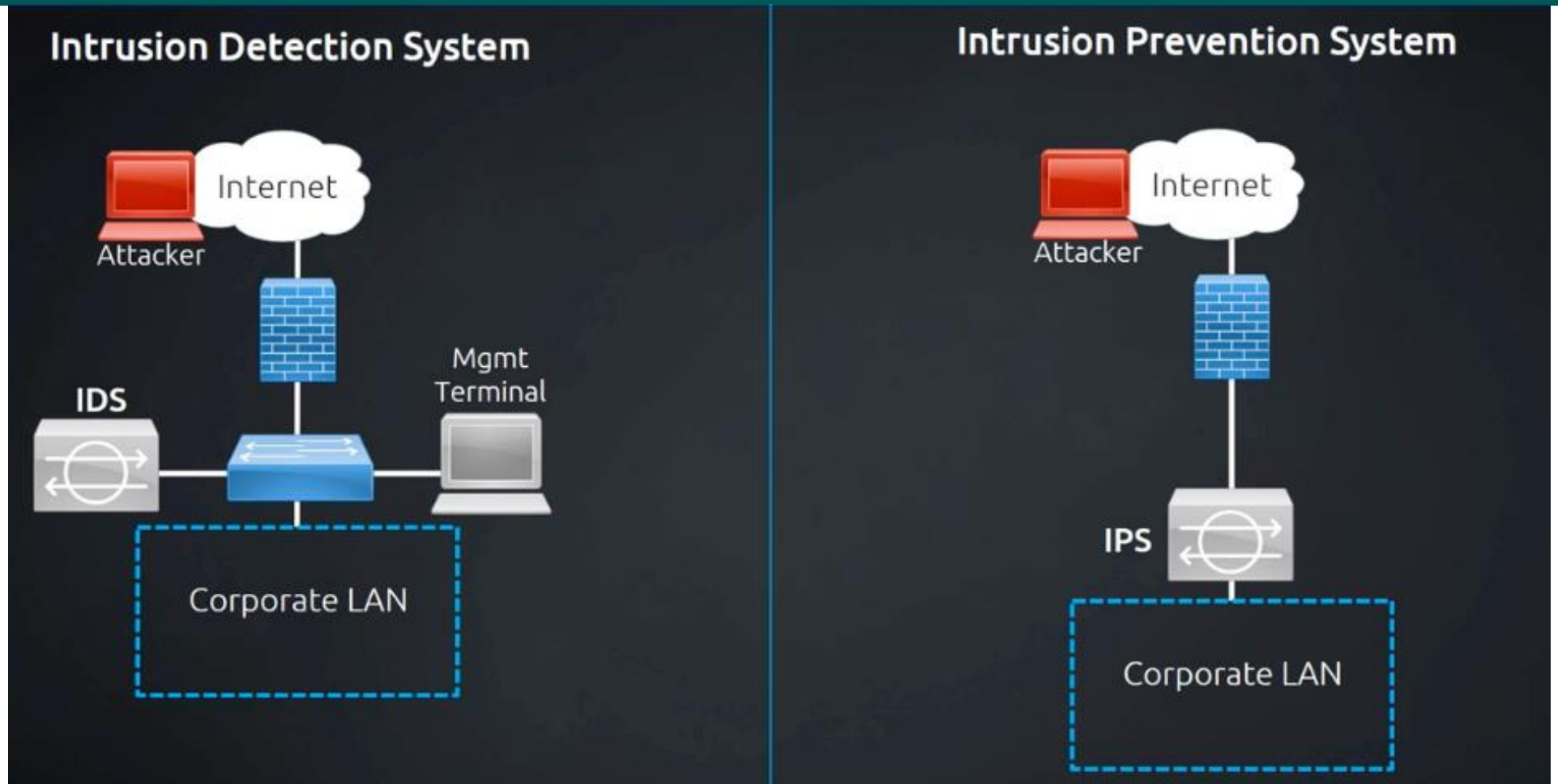
IDS vs IPS

IDS vs. IPS

Most organizations have either an IDS or an IPS, and many have both as part of their security information and event management framework.

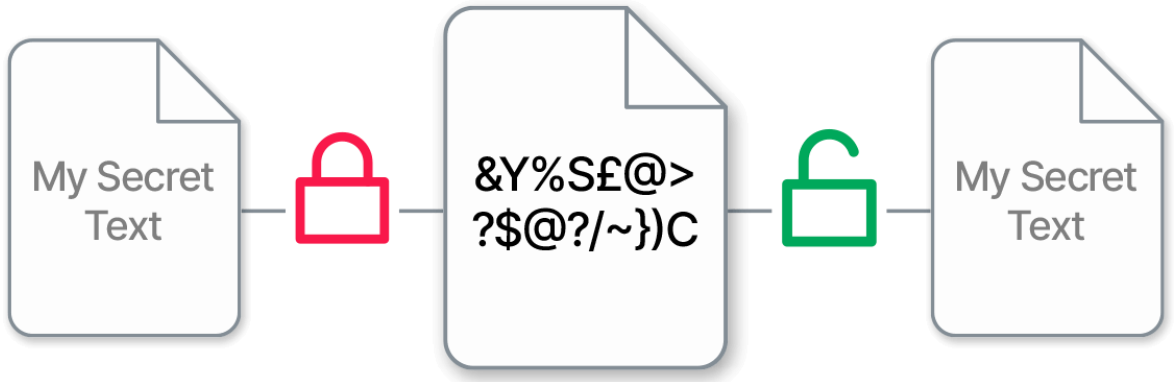
	IDS	IPS
NAME	Intrusion detection system	Intrusion prevention system
DESCRIPTION	A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.	A system that monitors network traffic and alerts for suspicious activity, like an IDS, but also takes preventative action against suspicious activity.
LOCATION	A host-based intrusion detection system is installed on the client computer. A network-based intrusion detection system resides on the network.	Located between a company's firewall and the rest of its network.
USE	Warns of suspicious activity taking place, but it doesn't prevent it.	Warns of suspicious activity taking place and prevents it.
FALSE POSITIVE	IDS false positives are usually just a minor inconvenience. Although the IDS incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.	IPS false positives can be more serious. When an IPS mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which could impact any part of the organization, not just the IT team.

Deployment di rete



Network and Data Encryption

La crittografia di rete, innanzitutto, stabilisce un canale sicuro tra due dispositivi utilizzando protocolli come TLS o VPN. Durante questo processo, gli algoritmi di crittografia e le chiavi crittografiche vengono concordati e scambiati in modo sicuro. I pacchetti di dati vengono trasmessi attraverso la rete crittografata, garantendo che i dati intercettati non possano essere letti senza la chiave di decrittografia. Il dispositivo ricevente decifra i dati, rendendoli utilizzabili. La crittografia di rete garantisce l'integrità e l'autenticità dei dati.



Certificati

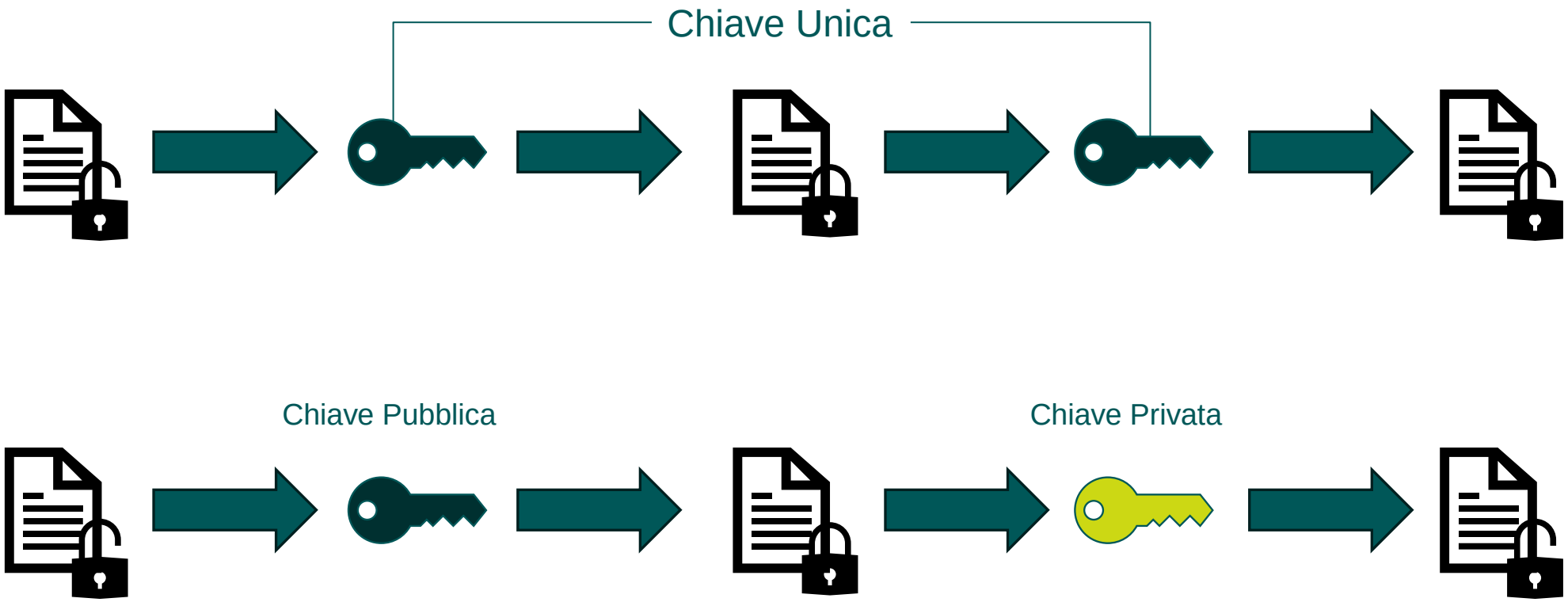
Un certificato SSL/TLS è un oggetto digitale che consente ai sistemi di verificare l'identità e successivamente stabilire una connessione di rete crittografata a un altro sistema utilizzando il protocollo Secure Sockets Layer/Transport Layer Security (SSL/TLS).

I certificati SSL/TLS pertanto funzionano come carte d'identità digitali per proteggere le comunicazioni di rete e stabilire l'identità dei siti Web su Internet e delle risorse su reti private.

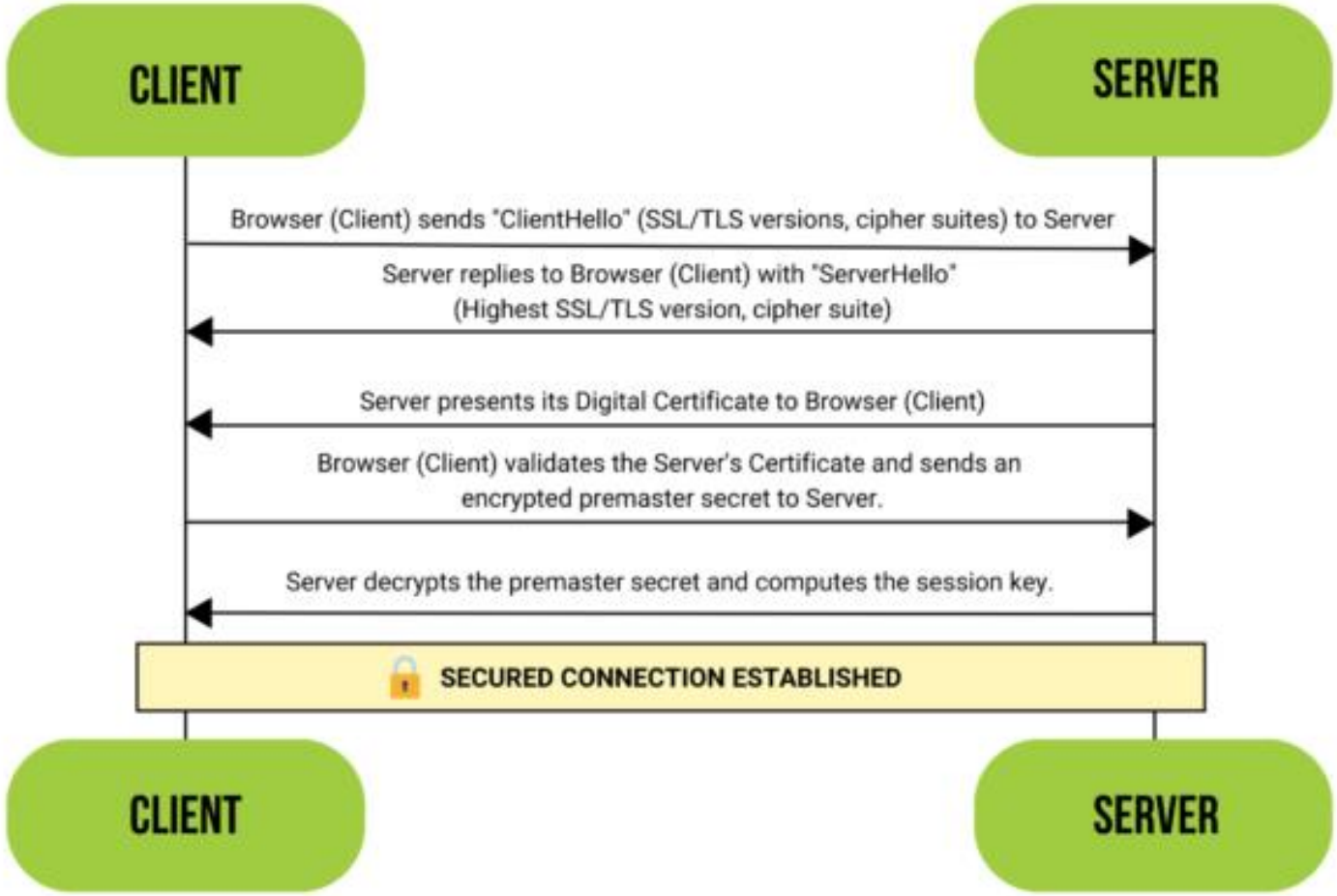
Certificate Authority

Un'autorità di certificazione (CA) è un'entità affidabile che emette certificati Secure Sockets Layer (SSL). Questi certificati digitali sono file di dati utilizzati per collegare crittograficamente un'entità con una chiave pubblica. I browser Web li utilizzano per autenticare i contenuti inviati dai server Web, garantendo la fiducia nei contenuti forniti online.

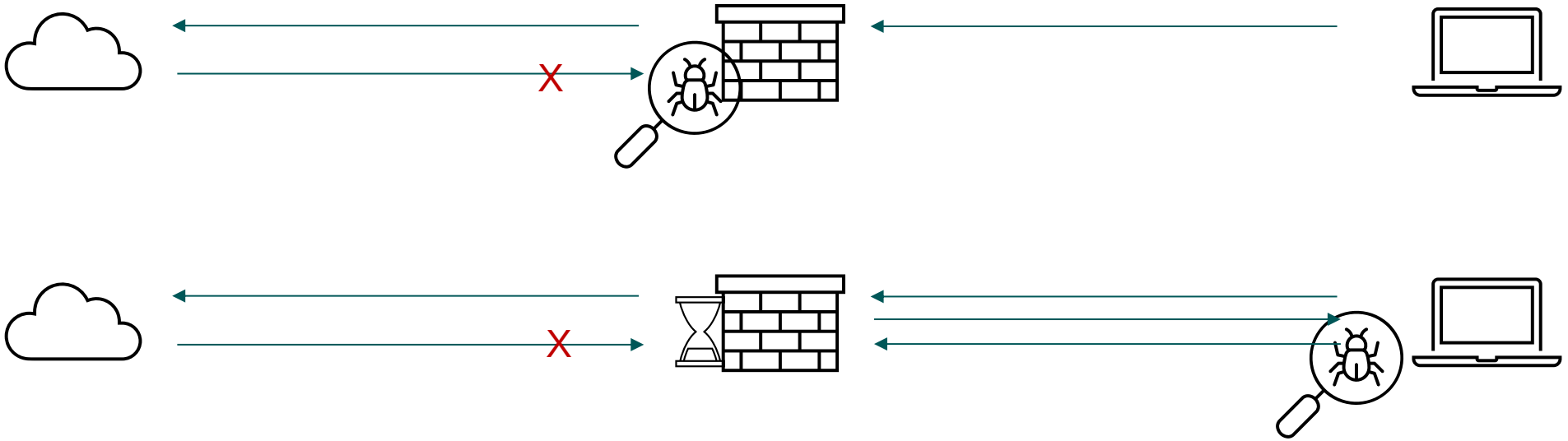
Crittografia simmetrica e asimmetrica



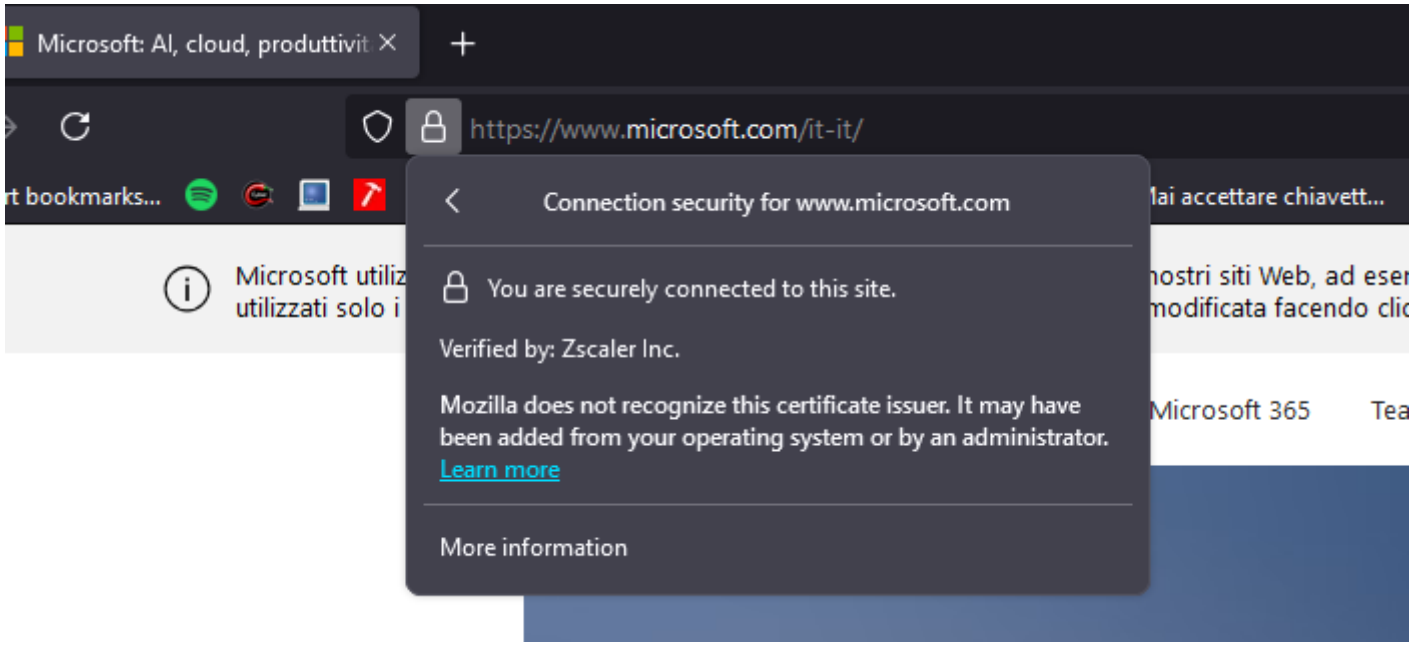
SSL Handshake



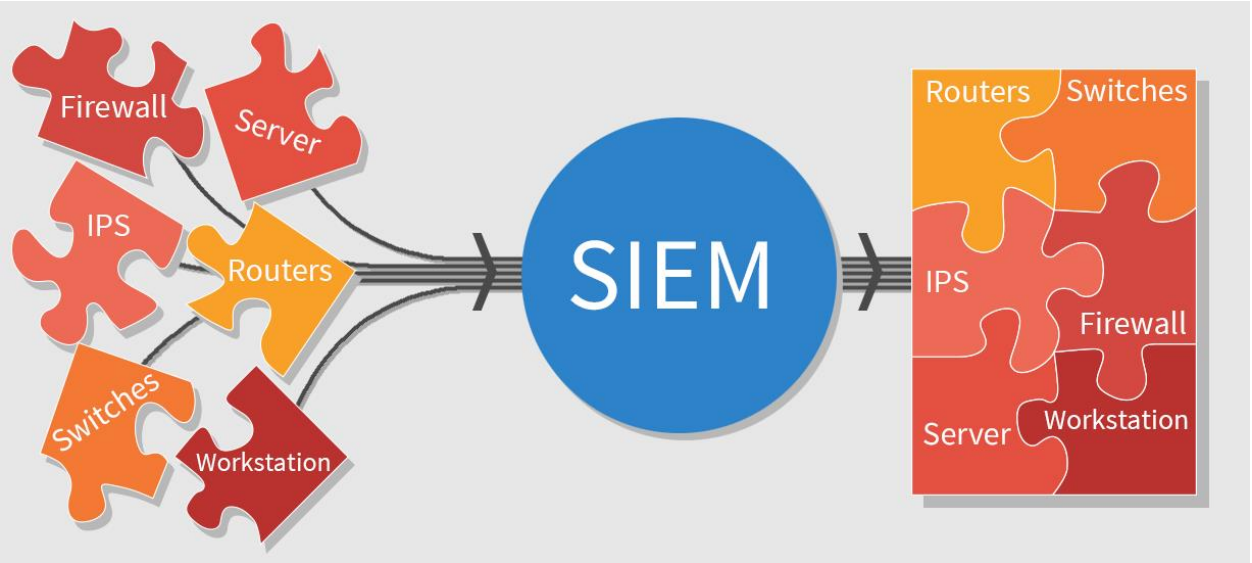
Protezione Perimetrale vs Client Based



Certificati MITM



Log Management



La gestione delle informazioni e degli eventi sulla sicurezza, o SIEM, è una soluzione di sicurezza che aiuta le organizzazioni a riconoscere e affrontare potenziali minacce e vulnerabilità della sicurezza prima che possano interrompere le operazioni di business.

I sistemi SIEM aiutano i team di sicurezza aziendali a rilevare le anomalie del comportamento degli utenti e utilizzano l'intelligenza artificiale (AI) per automatizzare molti dei processi manuali connessi al rilevamento delle minacce e alla risposta agli incidenti.

Response Orchestration

La tecnologia di orchestrazione, automazione e risposta alla sicurezza (SOAR) aiuta a coordinare, eseguire e automatizzare le attività tra diverse persone e strumenti all'interno di un'unica piattaforma. Ciò consente alle organizzazioni non solo di rispondere rapidamente agli attacchi di cybersecurity, ma anche di osservare, comprendere e prevenire gli incidenti futuri, migliorando così la loro posizione di sicurezza complessiva.

TD SYNNEX

“There’s not a ‘one and done’ solution for cybersecurity, no silver bullet as we like to call it. With cyber, there needs to be continuous care and feeding of the program. It’s a program that requires ongoing improvement. And that’s something very important to explain to the board.”

Zaki Abbas

https://www.techtarget.com/searchsecurity/definition/intrusion-prevention
https://nexgent.com/intrusion-detection-and-intrusion-prevention-systems/
https://aws.amazon.com/it/what-is/ssl-certificate/
https://www.ssl.com/it/articolo/ssl-tls-stretta-di-mano-che-garantisce-interazioni-online-sicure/
https://www.ibm.com/it-it/topics/siem
https://www.hbs.net/blog/benefits-of-log-consolidation-in-a-siem-environment
https://www.paloaltonetworks.com/cyberpedia/what-is-soar

TD SYNNEX

Q&A

Your Opinion Counts!

Scarica la presentazione cliccando sul codice QR

https://forms.office.com/r/B8pN50j9f3

PROSSIMI APPUNTAMENTI

25 OTTOBRE: Palo Alto Networks NGFW

8 NOVEMBRE: Acronis e NIS2

15 NOVEMBRE: Zyxel e Approccio security MSP

https://events.tdsynnex.it/cyber-unit-missione-protezione/

TEAM SECURITY: security.it@tdsynnex.com
SPEAKER: andrea.pezzoni@tdsynnex.com