Purple Team per una Information Security più efficace



Il **Purple Team** unisce strumenti e conoscenza del **Blue Team** e **Red Team** in un nuovo approccio collaborativo atto a rispondere alle minacce in continua evoluzione nell'ambito della sicurezza delle informazioni, garantendo protezione, contenimento e reazione, migliorando la security delle organizzazioni.

Le due squadre si fondono per dare vita ad una sicurezza che è al contempo offensiva e difensiva. Se, semplificando al massimo i ruoli, il Red Team è considerato un attaccante e il Blue Team un difensore, Il Purple Team è un difensore che impara dall'attaccante per migliorare e rendere sempre più efficace la sua strategia.

Attacco e difesa si fondono così in una unica visione mirata a garantire la cyber security all'interno di una organizzazione integrando i controlli e la visibilità raggiunta dal Blue Team con le minacce e le vulnerabilità riscontrate dal Red Team.

Il dialogo tra le due squadre è un concetto recente per la sicurezza informatica che fino a qualche anno fa non chiedeva ai due team di comunicare strutturando così un obiettivo comune, mettere in sicurezza l'intera superficie esposta in maniera estremamente reattiva e preventiva.

Red Team: che cos'è, di cosa si occupa

Dalla fine degli anni '80 il Red Team ha risposto all'esigenza delle organizzazioni di testare la propria *security posture* identificando le vulnerabilità nei **PPT (*People, Process and Technology*)**, arrivando a sfidare misure e politiche di

sicurezza messe in atto con il fine di migliorare le contromisure ed anticipare le minacce future, utilizzando strumenti di attacco come Metasploit, Meterpreter, Nmap, exploit etc. emulando gli aggressori nel modo più realistico possibile.

Un componente della squadra rossa non ha come obiettivo quello di rispettare le leggi ma di ragionare fuori dagli schemi e sfidare le regole minando le politiche di sicurezza logica e fisica ricoprendo il ruolo dell'attaccante, vestendo i panni del nemico. Gli attacchi messi in atto dal Red Team hanno il compito di mettere alla prova le capacità del Blue Team, utilizzando le **TTP (*Tactics, Techniques and Procedures*)** dei cyber criminali. Per tale motivo è fondamentale che le due squadre siano ben separate al fine di non creare conflitto d'interesse e abbassare i livelli di competizione.

La squadra rossa si occupa di:

- Offensive Security
- Vulnerability Exploitation
- Penetration Tests
- Social Engineering
- Compromise Credentials
- Black Box Testing
- Web App Scanning
- Threat Emulation
- Attack Simulation
- Custom tools and software development
- Escalate Privileges
- Web App Scanning
- Exploit Development
- Cyber Threat Intelligence
- Move laterally across systems
- Evade protection and protection capabilities

Blu Team: che cos’è, di cosa si occupa

Il Blue Team è una squadra addestrata a **rilevare, rispondere** e **mitigare** i cyber attacchi individuando tentativi di intrusione, movimenti laterali e tutto ciò che rientra nella “**Cyber Kill Chain”** utile a bloccare le minacce informatiche ed evitare i danni al sistema informatico. Un esempio di difensore proattivo è l’analista SOC/MDR che utilizza strumenti di Threat Intelligence, EDR, IPS/IDS, analizza traffico sospetto di rete, dati, log, individua gli *Indicator of Compromise*, mette in atto tutte le fasi dell’Incident Response, si avvale di tutto ciò che può metterlo sulle tracce di un attaccante implementando al contempo l’abilità difensiva dell’organizzazione, migliorandola costantemente.

La squadra blu si occupa di:

- Defensive Security
- Oppose Red Team
- Network Monitoring
- Infrastructure Protection
- Damage Control
- Security Monitoring
- Incident Response
- Operational Security
- Data Analysis
- Threat Hunting
- Threat Detection
- Digital Forensics
- Security Controls
- Implementing Controls
- Proactive Defence
- TTP Based Hunting
- Vulnerability Assessments
- Risk Assessments

Purple Team, evoluzione naturale della sicurezza informatica

Il Purple Team è la **cooperazione, scambio di informazioni e conoscenze** che si crea tra la squadra rossa e quella blu quando lavorano in sinergia. Questa interazione è utile a massimizzare i risultati grazie all'integrazione delle tattiche difensive e di monitoraggio con quelle offensive ponendo come obiettivo comune la protezione dell'infrastruttura.

Dalla dinamica di confronto costante tra i rosso-blu nasce quindi il concetto di viola che ha il compito di proteggere le differenze tra le due squadre mentre garantisce la cooperazione affinché le lezioni apprese dai due team non vadano perse ma costituiscano il valore fondante, l'obiettivo comune, un reciproco vantaggio.

La squadra viola si occupa di:

- Maximize Red Team
- Enhance Blue Team
- Improve Security Posture
- Gap Analysis
- Collaborative Security
- Data Analytics
- System Improvements

La metodologia del Purple Team è fatta di **continui feedback utili a comprendere i livelli di sicurezza e perfezionare le strategie difensive** aumentando le prestazioni e ottimizzando il budget migliorando la cultura collaborativa all'interno dell'azienda al fine di proteggerla dagli attacchi informatici e abbassando i livelli di rischio. Come dichiarato da Riccardo Baldanzi, CEO di 7Layers – azienda specializzata nell'Offensive e Defensive Security – *"Il Purple Team rappresenta il futuro della cyber security poiché in grado di rivoluzionare il modo in cui aziende ed organizzazioni*

prevengono e gestiscono i data breach e i cyber attacchi”.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/purple-team-per-una-information-security-piu-efficace/