Servizi inclusi nel SOC di Würth Phoenix

- ✓ Installazione dei log collector NetEye Satellite - Elastic Security for SIEM (versione Platinum)
- ✓ Invio degli eventi all'infrastruttura NetEye Cloud
- ✓ Tempi di onboarding certi
- ✓ Attività di Red Team a chiusura della fase di onboarding
- ✓ Servizio 24/7 gestito da un team di 30 analisti su 3 turni giornalieri
- ✓ Attività di triage svolte sempre da analisti, con l'obiettivo di minimizzare la comunicazione di falsi positivi
- ✓ Servizio di Threat Intelligence basato sulla piattaforma proprietaria SATAYO (https://neteye.guide/next/satayo/satayo.html)
- ✓ Istanza Atlassian Confluence per la documentazione del servizio
- ✓ Istanza Atlassian Jira per la messa a disposizione dei ticket correlati ai servizi
- ✓ Playbooks per la gestione di differenti scenari di Incident Response
- ✓ Vulnerability Assessment mensile sul perimetro pubblico
- ✓ Vulnerability Management
- ✓ Meeting mensili di allineamento
- ✓ Supporto tecnico localizzato in Italia e multilingua (italiano, inglese, tedesco)
- ✓ Report mensile Strategico, Tattico e Operativo
- ✓ Report informativi periodici
- ✓ Report settimanale malicious connections
- ✓ Indicatori di compromissione aggiornati quotidianamente
- ✓ Web Service per la gestione attiva degli IoC e IoA
- ✓ Normalizzazione e indicizzazione di qualsiasi fonte di log
- ✓ Totale libertà da parte del cliente nell'utilizzo ed integrazione nel SOC di qualsiasi tecnologia
- ✓ Scrittura di regole di detection personalizzate
- ✓ Sviluppo di report personalizzati sulla base di necessità di compliance
- ✓ Possibilità di copertura degli endpoint attraverso Elastic Defend
- ✓ Classificazione nella condivisione delle informazioni attraverso TLP (https://www.first.org/tlp/)

Potrai inoltre contare su un team di professionisti che negli anni si è contraddistinto nel panorama della cyber security, attraverso:

- creazione del progetto di condivisione di fonti di Threat Intelligence deepdarkCTI (https://github.com/fastfire/deepdarkCTI)
- presenza nella community Curated Intelligence (https://www.curatedintel.org/)
- accordo di collaborazione con il Centro Operativo per la Sicurezza Cibernetica della Polizia Postale (https://www.wuerth-phoenix.com/news/prevenzione-e-contrasto-dei-crimini-informatici/)
- contributi a decine di progetti open source (tra gli altri: Holehe, Sigma Rules, dnsrecon, OpenCTI...)
- partecipazione come speaker ad alcune tra le più importanti conferenze nazionali ed internazionali