**Príloha č. 4 Opis predmetu zákazky**

## Všeobecné požiadavky na školenia bezpečnostných administrátorov pri správe prevádzkovaných bezpečnostných produktov a aplikácií

**Školenia v oblastiach:**

- Vybudovanie SOC teamu
- Riešenie bezpečnostných incidentov
- Forenzná analýza
- Zabezpečenie systémov Windows
- Zabezpečenie systémov Linux
- Penetračné testovanie webových aplikácií
- Penetračné testovanie interného prostredia

| Školenia | Popis | Časový rozsah |
|---|---|---|
| Vybudovanie SOC teamu | • Vybudovanie reakčného tímu<br>• Definovanie hlavného reakčného tímu<br>• Systémové nástroje<br>• Identifikácia (zadefinovanie incidentu, detekcia a reakcia na prípadnú vnútornú hrozbu)<br>• Ukladanie (Stratégia dokumentácie: video a audio, ukladanie a karanténa, izolácia od prevereného prostredia)<br>• Vyradenie z prevádzky (Posúdenie, či je ohrozené zálohovanie, úplná prestavba operačného systému, zmena architektúry)<br>• Vylepšenia ( monitorovanie systému, očakávanie zvýšenia počtu útokov)<br>• Špecifické akcie na reakcie na rôzne incidenty (špionáž, zneužitie)<br>• Uskladnenie záznamu z incidentu (Formuláre, právna prípustnosť)<br>• Monitoring incidentov (zmena procesov na základe skúseností) | 5 dní |
| Riešenie bezpečnostných incidentov | Riešenie bezpečnostných incidentov minimálne v rozsahu:<br>• prijímanie opatrení na ochranu systémov a sietí postihnutých alebo ohrozených rušivou činnosťou<br>• poskytnutie riešení a poskytnutie stratégií na základe príslušných odborných rád alebo výstrah<br>• pátranie po činnosti narušiteľov na iných častiach siete filtrovanie prevádzky na sieti<br>• systémy prestavby<br>• systémy zaplátania alebo opráv<br>• vypracovanie iných stratégií reakcie alebo stratégií dočasných opravných balíčkov (workarounds).<br>• Reakcie na bezpečnostné incidenty na mieste<br>• Podpora reakcie na bezpečnostné incidenty<br>• Koordinácia reakcií na bezpečnostné incidenty<br>• Analýza bezpečnostného incidentu<br>• Zhromažďovanie dôkazov | 5 dní |
| Forenzná analýza | Forenzné analýzy v rozsahu:<br>1. forenzný proces a analýza - 0,5 dňa<br>2. Forenzná akvizícia a právny/legálny vstup - 1 deň<br>a. Forenzná akvizícia desktopov, serverov, úložných zariadení, virtualizácie, Cloud-u<br>3. Forenzná analýza artefaktov Windows - 1,5 dňa | 8 dní |

| | | |
|---|---|---|
| | a. dôkaz o vykonaní<br>b. dôkaz o otvorení<br>c. dôkaz o prístupe<br>4. Forenzná analýza linuxových artefaktov - 0,5 dňa<br>a. dôkaz o vykonaní<br>b. dôkaz o otvorení<br>c. dôkaz o prístupe<br>5. Forenzná analýza aktívnych zariadení - 0,5 dňa<br>6. Forenzná analýza pamäte - 1 deň<br>7. Forenzná analýza sieťovej komunikácie - 1 deň<br>8. Úvodná analýza škodlivého softvéru - 2 dni | |
| Zabezpečenie systémov Windows | Zabezpečenie a OnPrem a cloudových riešení Windows - AD, podporné služby, O365 a pod<br>• komplexné zabezpečenie O365 v súlade s odporúčaniami MS a best practices - 1 deň<br>• komplexné zabezpečenie Azure v súlade s odporúčaniami MS a best practices - 1 deň<br>• Komplexné zabezpečenie Windows Active Directory v súlade s odporúčaniami Center for Information Security úroveň 2 - 3 dni | 5 dní |
| Zabezpečenie systémov Linux | Zabezpečenia systémov na platforme Linux:<br>• Architektúra a bezpečnostné prvky Linuxu - 0,5 dňa<br>• Hardening Linuxu podľa CIS Lvl2 - 3 dni<br>• Reakcia na incidenty s Linuxom - 0,5 dňa | 4 dni |
| Penetračné testovanie webových aplikácií | Penetračné testovanie webových aplikácií v rozsahu OWASP - Úvod a ciele :<br>• Realizovať odhalenie a prieskum vyhľadávača na účely úniku informácií<br>• Vypočítať aplikácie na webovom serveri<br>• Preskúmať komentáre a metadáta webových stránok kvôli úniku informácií<br>• Identifikovať vstupné body aplikácií<br>Testovanie riadenia konfigurácie a nasadenia - nesprávna konfigurácia zabezpečenia<br>• Testovanie konfigurácie siete/infraštruktúry<br>• Testovanie konfigurácie aplikačnej platformy<br>• Testovanie manipulácie s príponami súborov pre citlivé informácie<br>• Preskúmanie citlivých informácii v starých, záložných a nereferencovaných súborov<br>• Testovanie zabezpečenia HTTP Strict Transport<br>Testovanie správy identít:<br>• Test definícií rolí<br>• Testovanie procesu registrácie používateľa<br>• Testovanie procesu poskytovania/vytvárania účtov<br>• Testovanie výčtu účtov a hádateľného používateľského účtu<br>• Testovanie slabej alebo nevykonávanej politiky pre používateľské mená<br>Testovanie overovania:<br>• Testovanie poverení prenášaných cez šifrovaný kanál<br>• Testovanie predvolených poverení<br>• Testovanie funkčnosti zapamätania hesla<br>• Testovanie politiky hesiel T | 5 dní |

| | | |
|---|---|---|
| | • Testovanie bezpečnostnej otázky/odpovede<br><br>Testovanie autorizácie:<br>• Testovanie prechádzania adresárov/obsahu súborov<br>• Testovanie obchádzania autorizačnej schémy<br>• Testovanie zvýšenia oprávnení<br>• Testovanie nezabezpečených priamych odkazov na objekty<br>Testovanie správy relácií:<br>• Testovanie obchádzania schémy správy relácií<br>• Testovanie na falšovanie krížových požiadaviek na stránky (CSRF)<br>• Testovanie funkčnosti odhlásenia<br>• Testovanie časového limitu relácie<br>Testovanie overovania vstupov:<br>• Analýza chybových kódov<br>• Analýza sledovania zásobníka<br>OWASP Top 10 :<br>• Injekcie<br>• Nefunkčné overovanie a správa relácií<br>• Odhalenie citlivých údajov<br>• Externé entity XML (XXE)<br>• Nefunkčné riadenie prístupu<br>• Nesprávna konfigurácia zabezpečenia<br>• Cross Site Scripting – XSS<br>• Nezabezpečená deserializácia<br>• Používanie komponentu so známymi zraniteľnosťami<br>• Nedostatočné zaznamenávanie a monitorovanie<br>Testovanie na strane klienta/bezpečný kód HTML5:<br>• Testovanie vykonávania JavaScriptu<br>• Testovanie HTML a CSS Injection<br>• Testovanie presmerovania URL na strane klienta<br>• Testovanie manipulácie so zdrojmi na strane klienta<br>• Testovanie zdieľania zdrojov medzi pôvodcami / Cross Origin Resource Sharing<br>• Testovanie Clickjacking<br>• Testovanie lokálneho úložiska | |
| Penetračné testovanie interného prostredia | Penetračné testovanie interného prostredia v rozsahu<br>• Proces etického hackingu - 0,5 dňa<br>• Skenovanie siete a enumerácia - 1 deň<br>• Skenovanie a analýza zraniteľností - 0,5 dňa<br>• Využívanie - používanie a modifikácia verejných exploitov - 1 deň<br>• Post exploitačné techniky a C2 - 1 deň<br>• Útoky na Active directory - 1 deň | 5 dní |

**Školenia pre penetračné testovanie webových aplikácií a interného prostredia minimálne v rozsahu :**

- Rozpoznávanie (Používanie Whois dopredného a spätného vyhľadávania, ARIN, RIPE a APNIC. Získanie systému názvov domén, Zhromažďovanie údajov z pracovných ponúk, webových stránok a vládnych databáz, Identifikácia verejne kompromitovaných účtov, Malta).
- Skenovanie (Lokalizácia a útok na súkromné a firemné siete Wi-Fi, Identifikácia a použitia proprietárnych bezdrôtových systémov. Skenovanie portov: Tradičné, skryté a slepé skenovanie. Aktívne a pasívne metódy fingerprintingu, systémov, Definovanie filtrovania firewallových pravidiel. Vyhľadávanie zraniteľností pomocou programu Nessus a iných nástrojov, Distribúcia skenovania pomocou cloudových agentov s cieľom vyhnúť sa zaradeniu na čiernu listinu)
- Vyhýbanie sa systému detekcie prienikov (IDS) (zmarenie IDS na úrovni aplikácie: Využitie bohatej syntaxe počítačového jazyka (rich computer language syntax), Taktika vyhýbania sa sieťovým útokom IDS, Obchádzanie IDS/IPS pomocou techník obfuscate TCP)
- Vyčíslenie cieľov služby Windows Active Directory (Vyčíslenie Windows Active Directory domén pomocou BloodHound, SharpView, príkazy a ovládanie systému Windows pomocou PowerShell Empire, pripojenie operačného systému z Linux do systému Windows, obrana proti útokom SMB pomocou pokročilých sieťových funkcií systému Windows)
- Útoky na fyzickú vrstvu (využívanie odkrytých USB portov, jednoduché odcudzenie identity v sieti za účelom obnovenia prihlasovacích údajov, krádež knižníc hesiel s nástrojmi na obnovenie systému za studena)
- Zhromažďovanie a analýza paketov (Bettercap, Active Sniffing, LLMNR poisoning, WPAD útoky, DNS cache poisoning: Presmerovanie internetovej prevádzky, Používanie a zneužívanie Netcatu vrátane zadných vrátok a sneaky relays, varianty spoofingu IP, vyhýbanie sa šifrovaniu a útoky na staršie verzie)
- Útoky na operačný systém na úrovni aplikácií (Buffer overflow in depth, Metasploit exploitation framework, AV and application whitelist bypass techniques)
- Netcat (prenos súborov, vytváranie zadných dverí a shell dusting, Netcat relays)
- Obídenie zabezpečenia koncového bodu (Detekcia obídenia pomocou veilu, magic unicorn, spustenie PowerShellu ako nástroja útoku, vyhnutie sa AV pomocou Ghostwritingu, rekonfigurácia nástroja útoku pomocou natívnych binárnych súborov)
- Prelomenie hesla (prelomenie hesla pomocou "" John the Ripper "", Útoky Hashcat Mask, Moderné útoky na systém Windows Pass-the-Hash)
- Útoky na webové aplikácie (Account collection, SQL Injection: Manipulácia s back-endovými databázami, klonovanie relácií: únos relácií iných používateľov, Cross-site scripts)
- Útoky na odmietnutie služby (distribuované odmietnutie služby: Pulse Zombies and Reflected Attacks, Local Denial of Service)
- Udržiavanie prístupu (zadné vrátka: Používanie Poison Ivy, VNC, Ghost RAT a ďalšie, Trojan Horse Backdoors, Rootkits: Nahradenie binárnych spustiteľných súborov podlými variantmi, rootkity na úrovni jadra: útok na srdce operačného systému (Rooty, Avatar a Alureon))
- Skrývanie ciest (skrývanie súborov a adresárov, úprava logov v systémoch Windows a Unix, úprava záznamov v denníku: UTMP, WTMP, história shellu atď., skryté kanály cez HTTP, ICMP, TCP a iné protokoly, analýza útoku z pamäte).
- Praktická analýza (Nmap Port Scanner, Nessus Vulnerability Scanner, Network Mapping, Netcat: File Transfer, Backdoors and Relays, Privilege Escalation)

Každé školenie musí obsahovať:

- Prezentáciu vo forme PowerPoint
- Podrobnú dokumentáciu

- Testovacie prostredie na virtualizačnej platforme, ktoré je použiteľné aj po ukončení školenia a obnoviteľné do pôvodného stavu
- Návod, resp. pracovný zošit pre jednotlivé cvičenia
- Podklady pre školiteľa, aby bolo možné dané školenia opakovať aj s iným trénerom.
- Vytvorenie praktického tréningového scenára pre každý Playbook v rozsahu minimálne 4 hodín

**Ďalšie požiadavka na Školenia:**

- vytvorenie a dokumentácie procesov a Playbook-ov riešenia bezpečnostných incidentov minimálne pre :
    - Ransowmare útok
        - Vytvorenie praktických scenárov na virtualizačnej platforme pre Rasnomware (napríklad Case study Conti)"
    - Malware spreading
    - Data Breach
    - DDOS útok
    - Business Email Compromise
    - vytvorenie Playbook-ov pre ohodnocovanie zraniteľností externé
    - vytvorenie Playbook-ov pre ohodnocovanie zraniteľností interné
    - vytvorenie Playbook-ov pre zachytávanie digitálnych stôp
        - sieť
        - pracovné stanice
        - notebooky
        - mobilné zariadenia
        - servery
    - Vytvorenie Playbook-ov pre základnú forenznú analýzu
    - Pre každý Playbook vytvorenie praktického tréningového scenára v rozsahu minimálne 4 hodín
- virtualizačné prostredie
- Step by step Guide pre (môže byt súčasť dodávaných Playbook-ov) :
    - Rozpoznávanie (Používanie Whois dopredného a spätného vyhľadávania, ARIN, RIPE a APNIC, získanie systému názvov domén, zhromažďovanie údajov z pracovných ponúk, webových stránok a vládnych databáz, identifikácia verejne kompromitovaných účtov, Malta).
    - Skenovanie (Lokalizácia a útok na súkromné a firemné siete Wi-Fi, identifikácia a použitia proprietárnych bezdrôtových systémov. Skenovanie portov: Tradičné, skryté a slepé skenovanie, Aktívne a pasívne metódy fingerprintingu, systémov, Definovanie filtrovania firewallových pravidiel, Vyhľadávanie zraniteľností pomocou programu Nessus a iných nástrojov, Distribúcia skenovania pomocou cloudových agentov s cieľom vyhnúť sa zaradeniu na čiernu listinu)
    - Vyhýbanie sa systému detekcie prienikov (IDS) (zmarenie IDS na úrovni aplikácie: Využitie bohatej syntaxe počítačového jazyka (rich computer language syntax), Taktika vyhýbania sa sieťovým útokom IDS, Obchádzanie IDS/IPS pomocou techník obfuskacie TCP)
    - Vyčíslenie cieľov služby Windows Active Directory (Vyčíslenie Windows Active Directory domén pomocou BloodHound, SharpView, príkazy a ovládanie systému Windows pomocou PowerShell Empire, Pripojenie operačného systému z Linux do systému Windows, obrana proti útokom SMB pomocou pokročilých sieťových funkcií systému Windows)
    - Útoky na fyzickú vrstvu (využívanie odkrytých USB portov, jednoduché odcudzenie identity v sieti za účelom obnovenia prihlasovacích údajov, krádež knižníc hesiel s nástrojmi na obnovenie systému za studena)

- Zhromažďovanie a analýza paketov (Bettercap, Active Sniffing, LLMNR poisoning, WPAD útoky, DNS Cache poisoning: Presmerovanie internetovej prevádzky, používanie a zneužívanie Netcatu vrátane zadných vrátok a Sneaky Relays, varianty spoofingu IP, vyhýbanie sa šifrovaniu a útoky na staršie verzie)
- Útoky na operačný systém na úrovni aplikácií (Buffer Overflow in Depth, Metasploit exploitation framework, AV and application whitelist bypass techniques)
- Netcat (prenos súborov, vytváranie zadných dverí a shell dusting, Netcat relays)
- Obídenie zabezpečenia koncového bodu (detekcia obídenia pomocou veilu, magic unicorn, spustenie PowerShellu ako nástroja útoku, Vyhnutie sa AV pomocou Ghostwritingu, rekonfigurácia nástroja útoku pomocou natívnych binárnych súborov)
- Prelomenie hesla (Prelomenie hesla pomocou "" John the Ripper "", Útoky Hashcat Mask, Moderné útoky na systém Windows Pass-the-Hash)
- Útoky na webové aplikácie (Account collection, SQL Injection: Manipulácia s back-endovými databázami, klonovanie relácií: Únos relácií iných používateľov, Cross-site scripts)
- Útoky na odmietnutie služby (distribuované odmietnutie služby: Pulse Zombies and Reflected Attacks, Local Denial of Service)
- Udržiavanie prístupu (zadné vrátka: Používanie Poison Ivy, VNC, Ghost RAT a ďalšie, Trojan Horse Backdoors, Rootkits: Nahradenie binárnych spustiteľných súborov podlými variantmi, Rootkity na úrovni jadra: Útok na srdce operačného systému (Rooty, Avatar a Alureon))
- Skrývanie ciest (skrývanie súborov a adresárov, Úprava logov v systémoch Windows a Unix, úprava záznamov v denníku: UTMP, WTMP, história Shell-u atď., skryté kanály cez HTTP, ICMP, TCP a iné protokoly, analýza útoku z pamäte).
- Praktická analýza (Nmap Port Scanner, Nessus Vulnerability Scanner, Network Mapping, Netcat: File Transfer, Backdoors and Relays, Privilege Escalation)

- Prezentácia
- Podrobná dokumentácia

Dodané materiály budú použité len v rezorte Ministerstva financií SR a organizáciách patriacich pod rezort MF SR.