|  |
| --- |
| **Školenie 1** |
| *Kybernetická bezpečnosť v praxi* |
| **Obsah školenia** |
| * Pochopenie riadenia informačnej bezpečnosti
* Popis a zmysel riadenia bezpečnosti informácií
* Základné stavebné kamene ISMS
* Procesy a dokumentácia
* Ekosystém technických nástrojov
* Životný cyklus prístupu k bezpečnosti informácií
* Problematika kybernetických hrozieb
 |
| **Počet zamestnancov, ktorý absolvujú školenie** |
| 4 |
| **Podmienky** |
| * Školenie vykonané online
* Jazyk výuky – slovenčina prípadne čeština/EN
 |

|  |
| --- |
| **Školenie 2** |
| *CompTIA Security +* |
| **Obsah školenia** |
| * Praktické vedomosti informačnej bezpečnosti v procesnej i technickej oblasti v rozsahu postačujúcom pre úspešné zloženie certifikačnej skúšky CompTIA Security+ SY0-601
* Hrozby, útoky a zraniteľnosti
* Technológie a nástroje
* Architektúra a design
* Riadenie identity a prístupu
* Detekcia hrozieb, techniky zamerania rizík
* Základná kryptografia a PKI
 |
| **Počet zamestnancov, ktorý absolvujú školenie** |
|  1 |
| **Podmienky** |
| * Školenie vykonané online
* Jazyk výuky – slovenčina prípadne čeština/EN
 |

|  |
| --- |
| **Školenie 3** |
| *Bezpečnostný monitoring* |
| **Obsah školenia** |
| * Základné teoretické znalosti i praktické skúsenosti nevyhnutné pre zaisťovanie bezpečnostného monitoringu
* Analýzy a reakcie na bezpečnostné incidenty v moderných organizáciách
* Základná klasifikácia bezpečnostných incidentov
* Typy malware
* Základy analýzy e-mailu
* Základy analýzy škodlivého kódu
* Základy analýzy sieťovej prevádzky
* Relevantné štandardy a legislatívne požiadavky (ZKB/VKB, ISO 27 035, NIST SP 800-61, SIM3)
 |
| **Počet zamestnancov, ktorý absolvujú školenie** |
|  1 |
| **Podmienky** |
| * Školenie vykonané online
* Jazyk výuky – slovenčina prípadne čeština/EN
 |

|  |
| --- |
| **Školenie 4** |
| *Threat Hunting* |
| **Obsah školenia** |
| * Princípy threat huntingu a základné prístupy k nemu
* Zasadenie threat huntingu do existujúcich bezpečnostných procesov v rámci organizácie Východiská pre threat hunting
* Modely hrozieb
* Threat intelligence
* Neštandardné sieťové správanie
* Odhaľovanie exfiltrácie dát
* Analýzy záchytov prevádzky Všeobecné odporúčania pre threat hunting
* Metriky pre vyhodnocovanie threat huntingu
 |
| **Počet zamestnancov, ktorý absolvujú školenie** |
| 1 |
| **Podmienky** |
| * Školenie vykonané online
* Jazyk výuky – slovenčina prípadne čeština/EN
 |

|  |
| --- |
| **Školenie 5** |
| *Kybernetický útok a obrana v praxi* |
| **Obsah školenia** |
| Kybernetický útok:* Metodiky a postupy pre penetračné testy
* Footprinting a OSINT
* Skenovanie a enumerácia
* Techniky a nástroje pre prienik do siete
* Základné útoky na webové aplikácie

Kybernetická obrana:* Analýza e-mailových hlavičiek a odhaľovanie podvrhnutých správ
* Analýza skriptov a ďalších spustiteľných súborov, office dokumentov a PDF súborov a súvisiacich nástrojov
* Analýza PCAP súborov z pohľadu bezpečnosti
* Tvorba a použitie vlastných Snort signatúr a súvisiacich nástrojov
* Tvorba a použitie vlastných YARA pravidiel a súvisiacich nástrojov
 |
| **Počet zamestnancov, ktorý absolvujú školenie** |
| 1 |
| **Podmienky** |
| * Školenie vykonané online
* Jazyk výuky – slovenčina prípadne čeština/EN
 |

|  |
| --- |
| **Školenie 6** |
| *Forenzná analýza* |
| **Obsah školenia** |
| * Získať základné informácie o mieste, úlohe a prínosoch forenznej analýzy v systéme reakcií na bezpečnostné incidenty organizácie
* Právne aspekty, pozícia a postavenie analytického pracoviska, nezávislosť a zaradenie,
* Základné technické prostriedky, ich konfigurácia,
* Analytické nástroje, praktické zoznámenie sa s ich princípmi práce, možnosťami a obmedzeniami,
* Praktické cvičenia
 |
| **Počet zamestnancov, ktorý absolvujú školenie** |
| 1 |
| **Podmienky** |
| * Školenie vykonané online
* Jazyk výuky – slovenčina prípadne čeština/EN
 |