Вимоги до тренінгу

Вимоги до учасників

У тренінгу беруть участь 250 осіб, які розподіляються на 15 синіх команд, що складаються зі спеціалізованих підкоманд/фахівців, залежно від досвіду учасника. Бажано, щоб кожен учасник володів наступними навичками:

- Вміння швидко навчатися та адаптуватися до нових ситуацій.
- Вміння працювати під тиском і дотримуватися встановлених термінів.
- Вміння критично мислити та вирішувати проблеми.
- Вміння працювати самостійно та в команді.

Бажано, щоб у кожній синій команді були розподілені наступні ролі між членами команди: Керівник команди, експерт з мережевого захисту, експерт із захисту Windows, експерт із захисту Linux, експерт з реагування на інциденти, експерт з безпеки та моніторингу. Розподіл ролей є рекомендаційним, і один член команди може виконувати декілька ролей. Команди можуть вільно розподіляти ролі, змінювати їх або модифікувати так, як вони вважають за потрібне.

Колективно команда повинна володіти такими навичками, як:

Керівник команди
▪ Вміння приймати рішення під тиском ▪ Сильні комунікативні та міжособистісні навички ▪ Вміння керувати та мотивувати команду ▪ Вміння мислити стратегічно і тактично ▪ Знання принципів та найкращих практик з кібербезпеки
Експерт з мережевого захисту
▪ Глибоке розуміння вразливостей мережевої безпеки та способів їх використання ▪ Досвід роботи з інструментами та технологіями мережевої безпеки, такими як брандмауери, системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS) ▪ Знання найкращих практик з мережевої безпеки ▪ Вміння розробляти, впроваджувати та підтримувати політики мережевої безпеки ▪ Вміння здійснювати моніторинг мережевого трафіку на предмет підозрілої активності ▪ Вміння впроваджувати та застосовувати інструменти та технології мережевої безпеки ▪ Вміння розслідувати та реагувати на інциденти безпеки, націлені на мережу ▪ Досвід роботи або знання: OPNSense, VyOS, MikroTik
Експерт із захисту Windows
▪ Глибоке розуміння вразливостей безпеки Windows і способів їх використання ▪ Досвід роботи з такими інструментами та технологіями безпеки Windows, як Windows Defender, System Center Endpoint Protection та Azure Defender ▪ Знання найкращих практик з безпеки Windows ▪ Вміння захищати системи Windows від атак ▪ Вміння впроваджувати та застосовувати політики безпеки Windows ▪ Вміння здійснювати моніторинг систем і мереж Windows на предмет підозрілої активності ▪ Вміння досліджувати та реагувати на інциденти безпеки, спрямовані на системи та мережі Windows

Експерт із захисту Linux
▪ Глибоке розуміння вразливостей безпеки Linux та способів їх використання ▪ Досвід роботи з інструментами та технологіями безпеки Linux ▪ Знання найкращих практик з безпеки Linux ▪ Вміння захищати системи Linux від атак ▪ Вміння впроваджувати та застосовувати політики безпеки Linux ▪ Вміння здійснювати моніторинг систем і мереж Linux на предмет підозрілої активності ▪ Вміння досліджувати та реагувати на інциденти безпеки, спрямовані на системи та мережі Linux
Експерт з реагування на інциденти, експерт з безпеки та моніторингу
▪ Відмінні письмові та усні комунікативні навички ▪ Вміння доносити складну технічну інформацію до нетехнічної аудиторії ▪ Вміння працювати в команді з іншими ▪ Вміння дотримуватись встановлених термінів та працювати самостійно ▪ Знання процедур реагування на інциденти кібербезпеки ▪ Глибоке розуміння комп'ютерних систем та мереж ▪ Вміння усувати несправності та вирішувати технічні проблеми ▪ Досвід роботи з системами виявлення та запобігання вторгнень ▪ Досвід роботи з інструментами управління інцидентами та подіями безпеки (SIEM) з відкритим вихідним кодом ▪ Знання найкращих практик кібербезпеки для системного та мережевого адміністрування

Вимоги до ноутбука

Для участі у тренінгу учасники використовуватимуть власні комп'ютери. Можна використовувати будь-які сучасні комп'ютери з поширеними операційними системами, такими як Windows, Linux і macOS. Бажано, щоб учасники мали повний адміністративний доступ до операційної системи своєї робочої станції. Якщо адміністративний доступ неможливий, то робоча станція синьої команди має відповідати наступним мінімальним вимогам:

- Можливість використовувати кабельне з'єднання RJ45 та WiFi для доступу до Інтернету.
- Можливість встановити та запустити Cisco AnyConnect SSL VPN клієнт та підключення до шлюзу Cyber Range VPN, розміщеного в Інтернеті.
- Можливість використовувати робочу станцію без активних підключень до корпоративної мережі (завжди включено VPN, Windows Active Directory, веб-проксі і т.д.) – мережа 10.0.0.0/8 буде перенаправлена на кіберполігон
- Можливість використовувати веб-браузер Chrome або Firefox
- Можливість приймати самостійно підписані SSL-сертифікати
- Можливість підключатися з веб-браузерами до нестандартних портів
- Мати встановлене програмне забезпечення SSH та SCP
- Мати встановлене клієнтське програмне забезпечення протоколу віддаленого робочого столу (RDP)