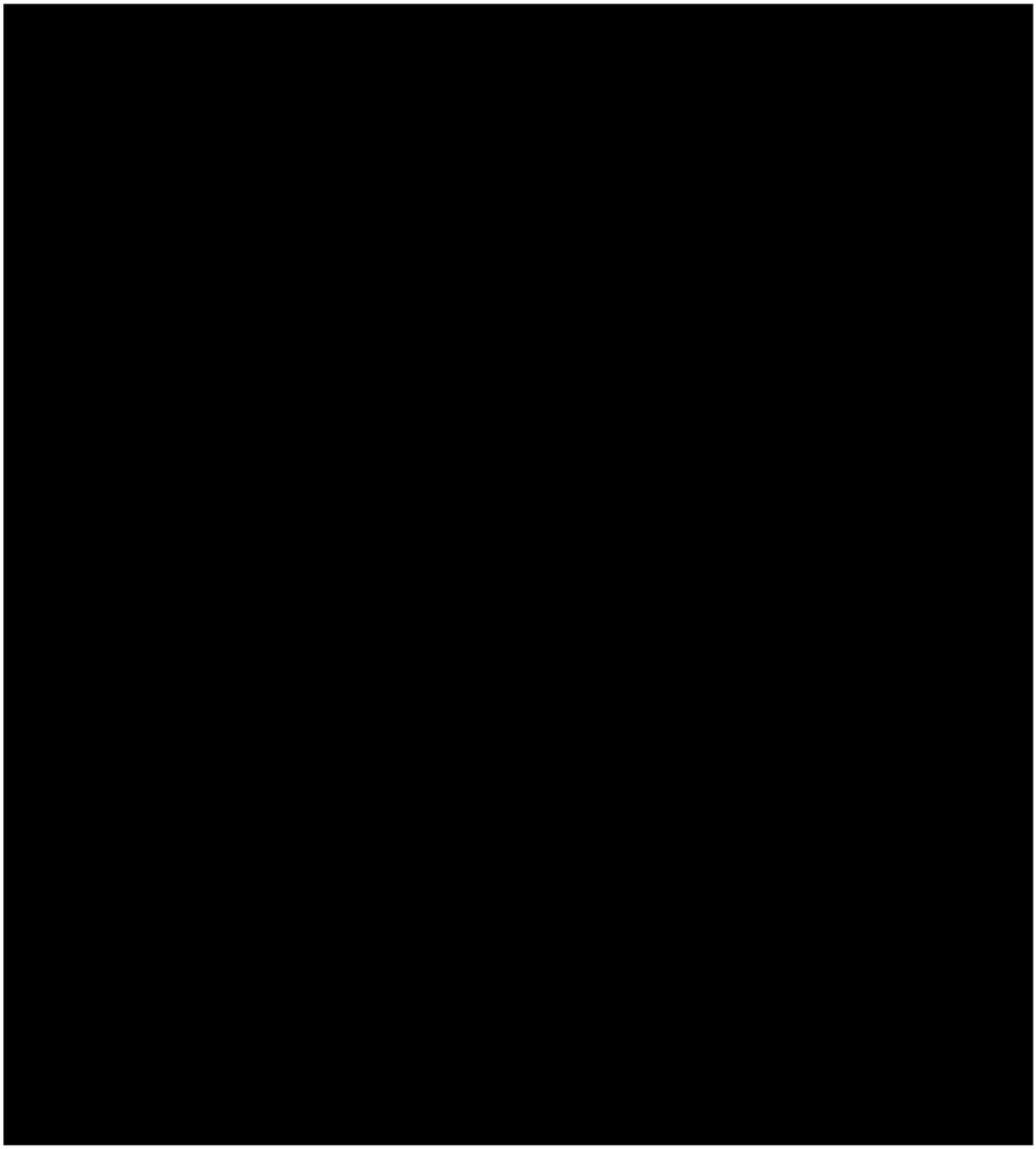
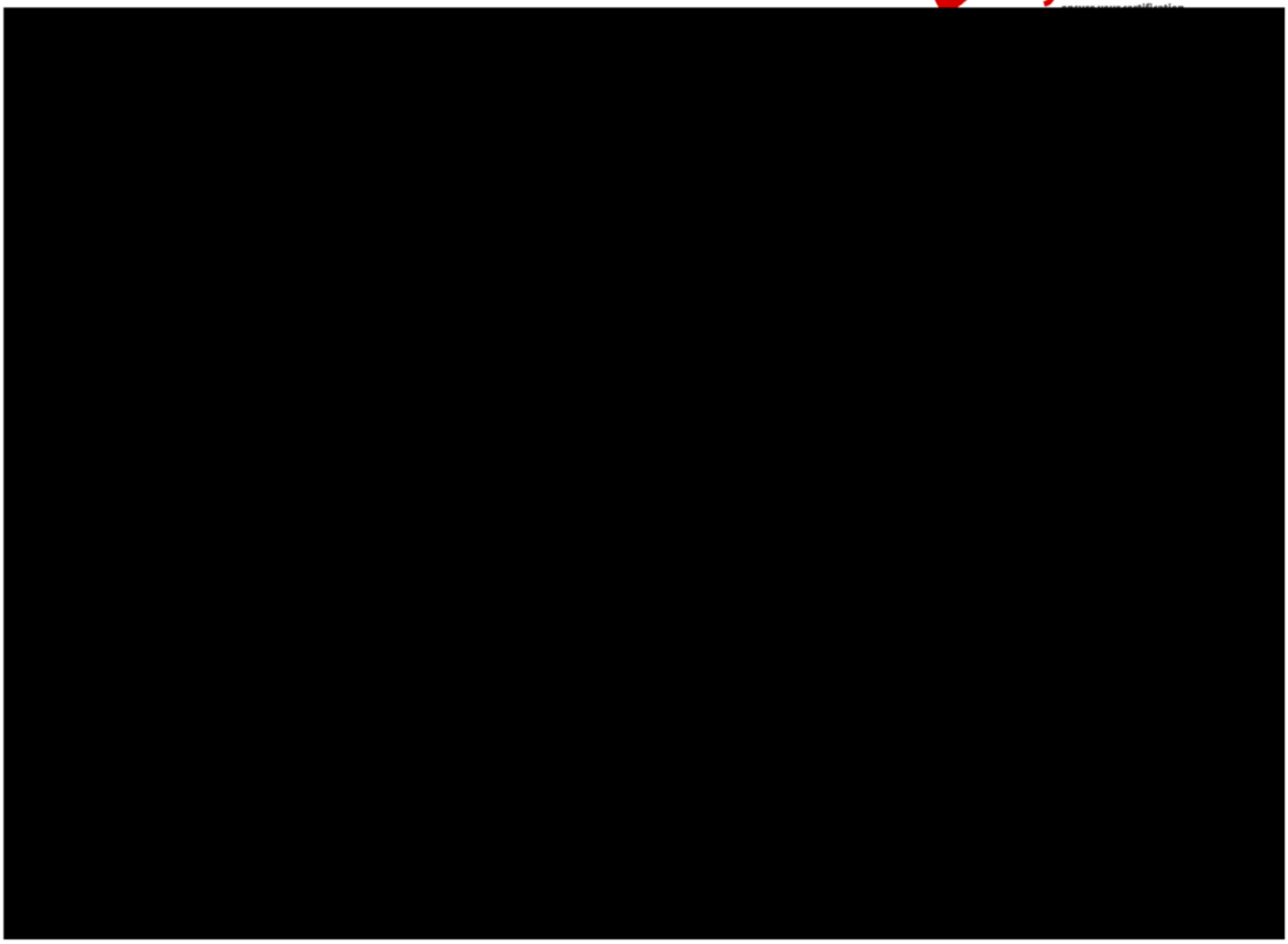
Příloha k objednávce

ŠKOLENÍ NA MÍRU V OBLASTI KYBERNETICKÉ BEZPEČNOSTI PRO 10 ADMINISTRÁTORŮ A SPECIALISTŮ MO

Nabídka školení pro MO

TAYLLORCOX s.r.o.





Popis vzdělávací aktivity

Navrhujeme realizaci dvoudenního odborného školení v oblasti kybernetické bezpečnosti, které bude přizpůsobeno potřebám účastníků z řad IT administrátorů a specialistů Ministerstva obrany. Školení proběhne v prezenční formě pro 10 osob v prostorách zadavatele v Praze 6.

Školení bude vedeno zkušeným lektorem se silným zázemím v oblasti kybernetické bezpečnosti a s praktickými zkušenostmi s výukou odborných IT témat. Cílem školení je vybavit účastníky jak teoretickými znalostmi, tak především praktickými dovednostmi v oblasti ochrany IT prostředí před současnými hrozbami.

Struktura školení:

1. Úvod do bezpečnosti a hrozeb

– Základní pojmy, přehled aktuálních hrozeb a útoků
– Kybernetická kriminalita, typologie útočníků

2. MITRE ATT&CK v praxi

– Představení rámce a jeho využití v praxi
– Analýza reálných scénářů útoků

3. OSINT (Open Source Intelligence)

– Vyhledávání veřejně dostupných informací
– Praktické ukázky a využití pro ochranu systémů

4. Moderní phishing a e-mailová bezpečnost

– Detekce podvodných e-mailů, ochrana proti phishingu
– Praktické ukázky útoků a obrany

5. Sociální inženýrství a manipulace

– Techniky získávání důvěrných informací
– Obranné strategie, školení zaměstnanců

6. Fyzický redteaming a hardwarové útoky

– Ukázky možných fyzických vektorů útoku
– Ochrana zařízení a přístupových bodů

7. Skenování portů a síťová bezpečnost

– Nmap a další nástroje pro síťovou analýzu
– Detekce a prevence zranitelností

8. Získání přístupu a exploitace

– Základy exploitace, demonstrační scénáře
– Obranné postupy a detekce průniku

9. Bezpečnost mobilních zařízení

– Hrozby pro mobilní systémy (Android/iOS)
– Opatření na úrovni uživatele i správce

10. Tipy, triky a nástroje pro IT administrátory

– Praktické utility a skripty pro správu a zabezpečení
– Automatizace rutinních bezpečnostních kontrol

Harmonogram

	Dopolední blok	Odpolední blok
Den 1	Zahájení školení, seznámení s programem Úvod do bezpečnosti a hrozeb MITRE ATT&CK v praxi	OSINT – techniky, nástroje, praktické ukázky Moderní phishing a e-mailová bezpečnost Shrnutí, dotazy
Den 2	Sociální inženýrství a manipulace Fyzický redteaming a hardwarové útoky Skenování portů a síťová bezpečnost	Získání přístupu a exploatace Bezpečnost mobilních zařízení + Tipy, triky a nástroje pro administrátory Závěrečná diskuse, zpětná vazba