Международный центр образования НЦОТ

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Безопасность Active Directory

Продолжительность	Форма получения образования	Стоимость
60 академ. часов	Очная (дневная) с использованием ИКТ	3 100 руб.

Цель программы

Формирование навыков аудита и защиты Active Directory, выявления и устранения уязвимостей, обнаружения атак и усиления безопасности доменной инфраструктуры.

Целевая аудитория

✓Руководители и специалисты подразделений информационной безопасности, центров обеспечения кибербезопасности и реагирования на киберинциденты.

✓Системные и сетевые администраторы; специалисты по администрированию и обеспечению безопасности Active Directory.

✓Специалисты по защите корпоративной информационной инфраструктуры.

Преимущества программы

41 час практических и лабораторных занятий.

BloodHound, PingCastle и NTEC SIEM для анализа безопасности.

Чему вы научитесь

Аудировать Active Directory, выявлять и устранять ошибки конфигурации.

Настраивать мониторинг атак и усиливать защиту доменной инфраструктуры.

ДОКУМЕНТ ПО ИТОГАМ ОБУЧЕНИЯ

Свидетельство о повышении квалификации

государственного образца

Рассрочка для физических лиц

Условия и подробности уточняйте у специалистов центра.

Учебный план

№	Наименование раздела и темы
1.	**ОСНОВЫ ACTIVE DIRECTORY И ГРУППОВЫЕ ПОЛИТИКИ**
1.1.	Кибербезопасность, информационная безопасность, защита информации. Опыт противодействия киберпреступности (на примере Республики Беларусь и Российской Федерации)
1.2.	Архитектура Active Directory
1.3.	DNS, репликация и объекты Active Directory
1.4.	Групповые политики (GPO) и политики безопасности
1.5.	Развёртывание домена corp.local
1.6.	Объекты AD и ввод машин в домен
1.7.	Настройка групповых политик
2.	**МОДЕЛЬ ПРИВИЛЕГИЙ, РАЗВЕДКА И БАЗОВЫЙ HARDENING**
2.1.	Модель прав доступа: Access Token, SID, ACL/ACE
2.2.	MachineAccountQuota, LAPS и gMSA
2.3.	Разведка и аудит домена в BloodHound
2.4.	Поиск и эксплуатация мисконфигураций ACL
2.5.	Базовый hardening и аудит PingCastle
3.	**АТАКИ НА АУТЕНТИФИКАЦИЮ: KERBEROS И NTLM**
3.1.	Протокол Kerberos и атаки на него
3.2.	NTLM, Pass-the-Hash и DCSync
3.3.	Kerberoasting и AS-REP Roasting
3.4.	Pass-the-Hash и обнаружение DCSync
4.	**NTLM RELAY И ИНФРАСТРУКТУРА СЕРТИФИКАТОВ (AD CS)**
4.1.	NTLM Relay и принуждение к аутентификации (Coercion)
4.2.	Инфраструктура сертификатов AD CS и атаки ESC1–ESC8
4.3.	NTLM Relay с принуждением (PetitPotam)
4.4.	Эксплуатация AD CS (ESC1)

Учебный план (продолжение)

№	Наименование раздела и темы
5.	**БОКОВОЕ ПЕРЕМЕЩЕНИЕ И ЗАКРЕПЛЕНИЕ В СИСТЕМЕ**
5.1.	Боковое перемещение (Lateral Movement) и механизмы закрепления (Persistence)
5.2.	Обнаружение бокового перемещения
5.3.	Поиск и устранение механизмов закрепления
6.	**МОНИТОРИНГ (SIEM) И КОМПЛЕКСНЫЙ HARDENING AD**
6.1.	Advanced Audit Policy и ключевые Event ID. SIEM NTEC SIEM для детектирования атак на AD
6.2.	Комплексный hardening Active Directory
6.3.	Мониторинг атак в NTEC SIEM
6.4.	Финальный hardening и контроль PingCastle
7.	**ИТОГОВАЯ ПРАКТИКА**
7.1.	Аудит и hardening «грязной» AD-инфраструктуры