КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ИТОГИ

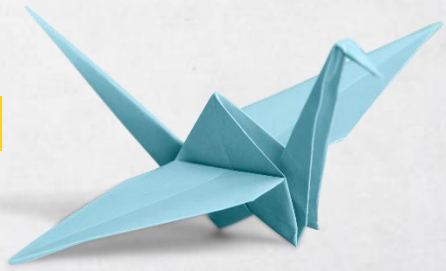
КОД ИБ ИТОГИ 2023

МОСКВА

07 ДЕКАБРЯ 2023

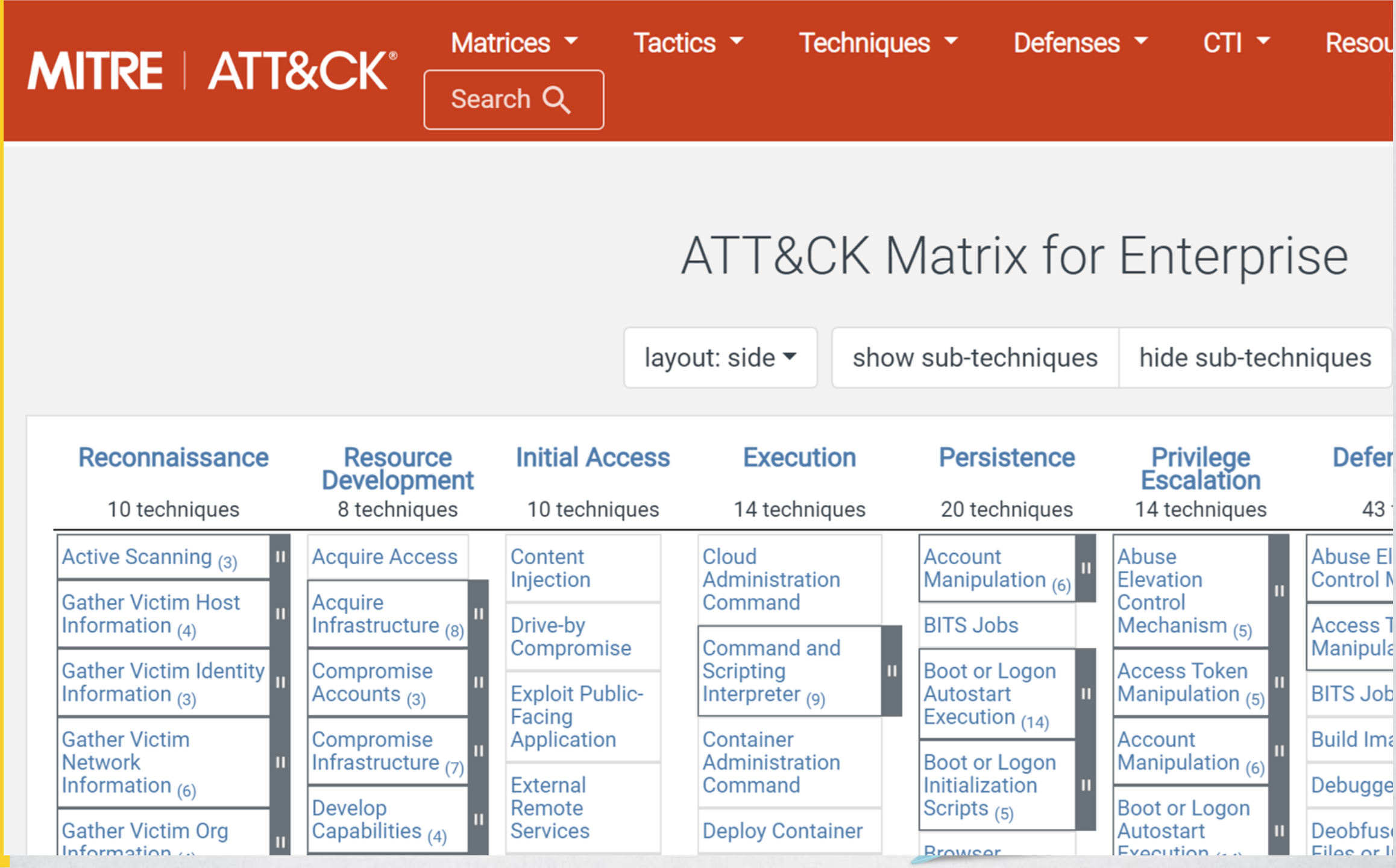
ПАЛЬМИРА БИЗНЕС КЛУБ

Как собирать обучение под задачи кибербезопасности



KILL 1SCOGS

в образовательных продуктах


MITRE | ATT&CK®
Matrices
Tactics
Techniques
Defenses
CTI
Resou
Search
ATT&CK Matrix for Enterprise
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
10 techniques
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (8)
Compromise Accounts (3)
Compromise Infrastructure (7)
Develop Capabilities (4)
Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (9)
Container Administration Command
Deploy Container
Persistence
20 techniques
Account Manipulation (6)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (5)
Access Token Manipulation (5)
Account Manipulation (6)
Boot or Logon Autostart
Defer
43
Abuse El
Control M
Access T
Manipula
BITS Job
Build Ima
Debugge
Deobfusc

Специализация	Модуль/Стенд (на выбор)	Техника/Занятие
SOC 1/2	Обнаружение злоумышленника на периметре (сервисы)	Синтаксис регулярных выражений
		Анализ логов Веб приложения (Apache2, nginx, IIS)
		Анализ логов сетевых средств защиты (WAF / NGFW / IDS). Синтаксис Suricata/Snort сигнатур.

СИНХРОННЫЙ ФОРМАТ

1. Базовый трек
2. Профессиональный трек
3. Курс

1. Базовый трек
2. Профессиональный трек
3. Курс
4. Консультация
5. Оценка уровня подготовки в ИБ
6. Диагностика ИБ-контекста

B2C

B2B

1. Техника / Технология (Микрокурс)
2. Аттестация
3. Менторинг

1. Техника / Технология (Микрокурс)
2. Аттестация
3. CTF
4. Киберполигон
5. Менторинг

АСИНХРОННЫЙ ФОРМАТ