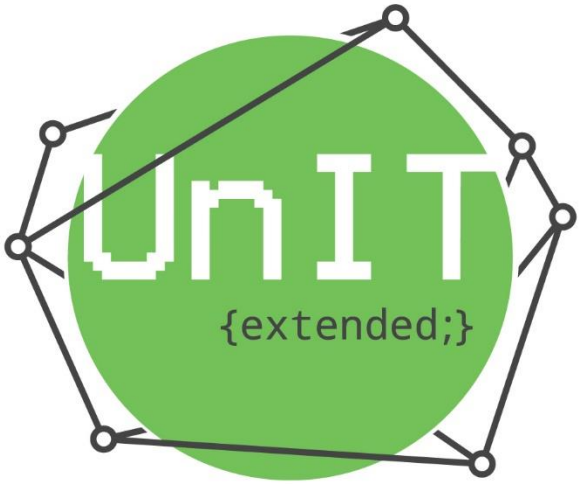


BigData analysis

ŠKODA

Existuje dokonalý IT zločin? Dokážeš se změnit z bezmocné oběti v úspěšného lovce?

Předmluva

IT moderní společnosti vyžaduje neustálou dostupnost a flexibilitu služeb. V důsledku toho jsou informační systémy a jejich role předmětem neustálé změny. Tradiční pojetí bezpečnosti, stojící na přesně definovaných a neměnných pravidlech, selhává a škrtí produktivitu. Dnes je nepostradatelné průběžné monitorování a vyhodnocování. Množství dat je ohromné a manuální analýza je náročná a nákladná. Kdo nedokáže automatizovat, nepřežije.

Abstrakt

Čeká vás korporátní síť plná různorodých událostí. Zvládnete analyzovat big data? Udržte kontrolu nad svěřenou sítí a odhalte útočníka.

Potřebné znalosti

- Schopnost tvorby SQL dotazů
- Základy architektury podnikových sítí
- Přehled o typech a struktuře log záznamů
- Metodologie a techniky penetračního testování
- Azure BI
- Principy detekce anomálií
- Vlastní počítače s sebou!

Technické informace

Team bude mit k dispozici virtualni server na Microsoft AZURE Cloudu na který se může přihlásit pomocí RDP. Spojení je limitováno na 2 současně pracující uživatele. Podmínkou je tedy RDP klient.

Konfigurace serveru
WinServer 2016, Standard D4s v3 (4 vcpus, 16 GB memory)

Dostupné nástroje – Databáze
SQL Server 15.0.1400.75
Microsoft SQL Server Management Studio 18

Předinstalované (doporučené) jazyky
R, Python, JAVA

Dostupné nástroje – Analytika
Jupyter Notebook 5.7.4 dostupný přes Anaconda Navigator
R Studio
Visual Studio Code (lze spouštět všechny možné jazyky – R, Python, JAVA, .NET, …)

Dostupné nástroje – Vizualizace
Microsoft Power BI Desktop

Na virtuálním serveru lze doinstalovat nástroje, knihovny atd., z prostředí AZURE je funkční připojení na internet. Záleží na teamu, co dalšího budou chtít používat.

Kritéria hodnocení

- (25 %) Inovativní přístup (tzn. detekce událostí, které nejsou běžné a dobře popsané v dostupných materiálech)
- (25 %) Využitelnost navržených use-case v bezpečnosti
- (20 %) Kvalita dokumentace algoritmů
- (15 %) Kvalita a výsledky testování prototypů
- (15 %) Prezentace výsledků
- (+10 %) bonus za detekci nejobtížnější události

K dispozici studenti dostanou

- Formulář pro popis detekce bezpečnostní události
- Power BI klient s přístupem k testovacím datům

Tvůrci zadání

Tomáš Trávníček

Absolvent oboru Informační systémy a technologie na Vysoké škole ekonomické v Praze se zkušeností z auditů bezpečnosti informační systémů, řízení IT rizik a vývoje informačních systémů, které získal na projektech v České republice i zahraničí.

Aktuálně má na starosti zajištění informační bezpečnosti u connected car projektů. Pokud netráví čas s rodinou, tak se účastní outdoorových závodů (orientační běh, adventure race).

Vlastislav Cháb

Svým založením praktik, který vystudoval vědu použitelnou i v normálním životě. Od vědecké dráhy přešel k praktické správě IT ve všech jeho vrstvách.

Odzkoušel si pozici IT auditora a forenzního analytika, aby skončil jako koordinátor SOC centra u domácího výrobce automobilů. Ve volném čase se nechá inspirovat přírodou, které rozumí od samotného jádra a obdivuje její dokonalost ve fungující komplexnosti.

Hana Antošová

Absolventka MFF UK. Pracovala na pozicích vývojáře SW i vedoucí IT oddělení, především v oblasti ERP systémů a SAP. Má zkušenosti z vedení velkých mezinárodních implementačních projektů systémů SAP, navrhování podnikových IT strategií v oblasti ERP i projektového řízení. Volný čas tráví nejraději na kole, nebo na lyžích.

V porotě dále budou:

Jaroslav Rus

Absolvent Univerzity Jana Amose Komenského v Praze. Působí na pozici Security analyst a zabývá se především analýzou bezpečnostních událostí a incidentů, zpracováním návrhů opatření pro zlepšení stavu bezpečnosti a penetračními testy.

Petr Kocmich

Absolvent ČVUT FEL. Pracoval v oblasti administrace podnikových systémů, věnoval se IT bezpečnosti. Má zkušenosti s Incident Managementem, Problem Managementem i ITIL. Ve volném čase rád cestuje a lyžuje.

Lucie Böhmová

Absolventka doktorátu z informatiky a statistiky na VŠE, specializuje se na moderní trendy v ICT. V současnosti pracuje ve ŠKODA AUTO v IT oddělení jako specialistka řízení projektů ve spolupráce s vysokými školami. Má ráda sport a cestování.

Lukáš Bednařík

Vystudoval Teoretickou Fyziku na MFF UK v Praze. Nyní pracuje jako C++ Developer & Researcher v Phonexia s.r.o., která se zabývá analýzou hlasu a hlasovou biometrií.

Marián Pavlík

Více než dva roky vedl IT oddělení v rámci Volkswagen Group Rus. V mladoboleslavské automobilce na vedoucích pozicích pracuje třináct let. Poslední dva roky je ve ŠKODA AUTO zodpovědný za systémové podpory procesů v oblasti prodeje a marketingu. Absolvent brněnského VUT, zde později získal titul doktor filozofie. Hovoří třemi cizími jazyky: anglicky, rusky a polsky. Mezi jeho záliby patří moderní technologie, jízda na kole a práce s lidmi.

Občerstvení

Zajištěno po celou dobu soutěže, obědy máme rezervovány v menze Starý pivovar přímo v areálu, stačí se prokázat nametagem, který dostane každý soutěžící ráno.

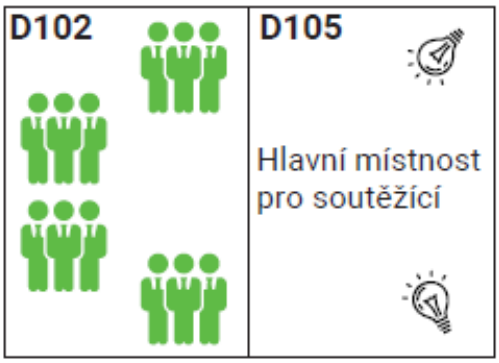
K **večeři** je pizza objednaná dle dotazníku zaslaného před soutěží.

Po celou dobu soutěže je před Místností D0206 v budově D **„food corner“**. Zde budou k dispozici voda, sladké nápoje, káva, čaj i občersvení.

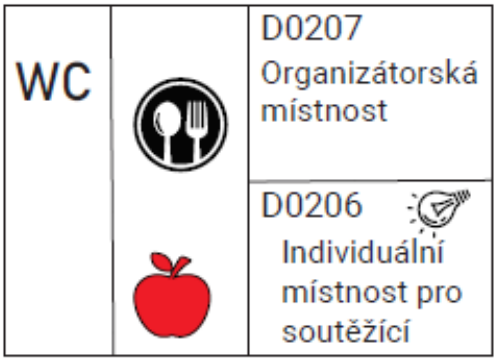
Snídaně bude rovněž nachystaná ve food corneru, na výběr bude sladká i slaná.

Soutěž bude ukončena slavnostním **raut**em ve studentském klubu Kachnička.

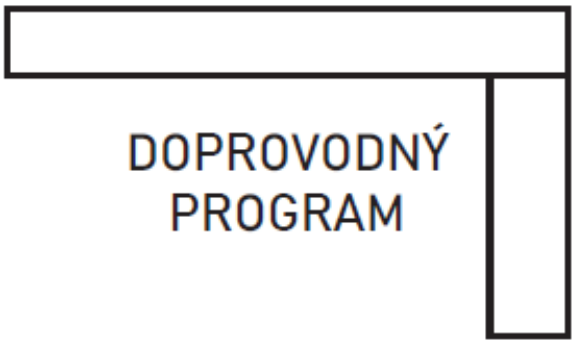
PAVILON D
1. PODLAŽÍ



PAVILON D
2. SUTERÉN



CHODBA C
2. PODLAŽÍ



Zranění

V případě **zranění** je na soutěži přítomná osoba proškolená na první pomoc. Je jí Veronika Koukalová (mob. +420 722 191 554) a Michael Roth (mob. +420 602 211 970)

Všechny zranění prosím hlaste na helpdesku ve vstupu do budovy D.

8:00	začátek registrace
9:00	Oficiální zahájení
9:15	Prezentace zadání
10:00	START
12:30	Obědy (okno 45 min)
18:15	Příjezd pizzy
00:00	Midnight meal
7:30	Snídaně
10:00	KONEC
10:15	Prezentace výsledků
11:45	Vyhodnocení výsledků
12:15	Raut
12:45	Vyhlášení, předání cen
13:15	Foto, ukončení
13:45	Raut

HELPDESK

Se všemi dotazy se neváhejte obrátit na organizátory, které poznáte podle černého trička s nápisem UnIT. Rovněž můžete využít našeho HELPDESKU umístěného ve vstupu do budovy D.