08.05.2024

Pierwsze kroki w cyberbezpieczeństwie: czyli jak sobie odpowiedzieć na jedno ważne pytanie?

O mnie:

„W swoim życiu przeczytałem dwie książki…”

Miłosz Jaworski

CyberSecurity Consultant & Trener
(ISC)2 Authorized Instructor

mj@compendium.pl

https://www.linkedin.com/in/milojawo

Dziś na lekcji:

1. ***Znaczenie cyberbezpieczeństwa:***
   Czyli, jak rosnąca liczba cyberataków wpływa na gospodarki i społeczeństwa na całym świecie, dlaczego branża ta jest uznawana za kluczową dla naszej przyszłości.

2. ***Pierwsze kroki w karierze w cyberbezpieczeństwie:***
   Czyli konkretne zasoby edukacyjne, kursy i certyfikaty, które mogą pomóc zdobyć niezbędne umiejętności i wiedzę.

3. ***Obecne role w cyberbezpieczeństwie oraz zawody przyszłości:***
   Czyli omówienie różnych ról i specjalizacji w branży, od etycznego hakowania po analizę zagrożeń i zarządzanie bezpieczeństwem informacji.

4. ***15% z 6000 / 3 min = ???***

Znaczenie cyberbezpieczeństwa:

„Polska jest jednym z najbardziej zagrożonych działalnością cyberprzestępczą krajów na świecie. Jak podaje Microsoft Digital Defense Report, ***znajdujemy się na 4.*** *miejscu wśród najczęściej atakowanych państw europejskich, zaraz po Ukrainie, Wielkiej Brytanii i Francji.”*

„Postępująca cyfryzacja gospodarki i rosnące zagrożenie cyberatakami sprawiają, że zapotrzebowanie na specjalistów ds. bezpieczeństwa cyfrowego rośnie w Polsce szybciej niż w innych krajach Europy.

Jak wskazuje najnowszy raport OECD „Building a Skilled Cyber Security Workforce in Europe” tempo, w jakim przybywa w Internecie ofert pracy w obszarze cyberbezpieczeństwa przewyższa średni wzrost liczby ofert dla innych zawodów”

https://news.microsoft.com/pl-pl/2024/03/18/oecd-polska-pilnie-szuka-specjalistow-od-cyberbezpieczenstwa/

Znaczenie cyberbezpieczeństwa:

„Jak wskazuje raport OECD, rodzimi pracodawcy często wymagają od potencjalnych kandydatów znajomości technologii chmurowych. Jest to zgodne z analizami przeprowadzonymi przez Międzynarodowe Konsorcjum Certyfikacji Bezpieczeństwa Systemów Informatycznych.

ISC2 umiejscawia zabezpieczanie ***technologii chmurowych*** *wśród najistotniejszych kwalifikacji specjalistów ds. cyberbezpieczeństwa.*

W Polsce najbardziej poszukiwane umiejętności dotyczą takich obszarów jak sprzęt sieciowy ICT, wdrażanie wirtualnych sieci prywatnych i programowanie stron internetowych.

Jest to zgodne z dominującym zapotrzebowaniem na architektów i inżynierów w tej dziedzinie, którzy stanowili średnio 45 proc. ofert pracy związanych z cyberprzestrzenią w okresie od stycznia 2018 r. do czerwca 2023 r. Trend ten odzwierciedla również nacisk polskich pracodawców na biegłość techniczną i zarządzanie infrastrukturą w dziedzinie cyberbezpieczeństwa.”

https://news.microsoft.com/pl-pl/2024/03/18/oecd-polska-pilnie-szuka-specjalistow-od-cyberbezpieczenstwa/

Znaczenie cyberbezpieczeństwa:

Wpływ na gospodarkę:

- *Koszty finansowe*
- *Zakłócenia w działalności*
- *Zaangażowanie zasobów*

Wpływ na społeczeństwo:

- *Prywatność i ochrona danych osobowych*
- *Zaufanie do technologii*
- *Wpływ na politykę i regulacje*

Dlaczego branża jest kluczowa dla przyszłości:

- *Wzrost zależności od technologii cyfrowych*
- *Innowacje technologiczne*
- *Strategiczne znaczenie dla narodowego bezpieczeństwa*

„niezależnie czy zainwestujesz w cyberbezpieczeństwo, czy tego nie zrobisz i tak stracisz pieniądze”
Zygmunt G.

Pierwsze kroki w cyberbezpieczeństwie:

„Musisz odpowiedzieć sobie na jedno zajebiście, ale to zajebiście ważne pytanie.
Co lubisz robić? A potem zacznij to robić.”

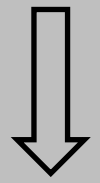
Pierwsze kroki w budowie kompetencji:

1. ***Communication and Network Security***
2. ***IAM*** *(Identity Access Management)*
3. ***Security Architecture and Engineering***
   - *Cloud / SysOps*
   - *ICS / OT / IoT*
   - *Asset Security*
4. ***Security and Risk Management***
   - *GRC (Governance, risk management and compliance)*
5. ***Security Assessment and Testing***
6. ***Software Security***
7. ***Security Operations***
   - *Forensics*
   - *Incident Handling*
   - *Penetration Testing*
   - *Exploitation*

Pierwsze kroki w budowie kompetencji:

Wybór szkolenia:

- *Domena*
- *Poziom*
- *Autoryzowane lub nie*
- *Typ szkolenia*
- *Program*
- *Laby*
- *Materiały*



- *Egzamin*
- *Certyfikacja i jej utrzymanie!*

Pierwsze kroki w certyfikacjach CyberSec:

1. ***Parter - Entry-Level:***

   - *ISC2 CC - Certified in CyberSecurity (free)*
   - *GIAC Information Security Fundamentals (GISF)*
   - *Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)*
   - *Mile2 C)SP Certified Security Principles*
   - *Mile2 C)VA - Certified Vulnerability Assessor*
   - *OffSec - Network Penetration Testing Essentials (PEN-100)*
   - *OffSec - Security Operations Essentials (SOC-100)*
   - *CompTIA Network+*
   - *CompTIA Security+*
   - *ISC2 SSCP - Systems Security Certified Practitioner*
   - *GIAC Security Essentials (GSEC)*
   - *CISCO / ChcekPoint / Palo Alto / Fortinet NSE 1-3*

O kocie w worku:

CompTIA Security+

- *Fundamental Security Concepts*
- *Threat Types*
- *Cryptographic Solutions*
- *Identity and Access Management*
- *Secure Enterprise Network Architecture*
- *Secure Cloud Network Architecture*
- *Resiliency and Site Security Concepts*
- *Vulnerability Management*
- *Network Security Capabilities*
- *Endpoint Security Capabilities*
- *Application Security Capabilities*
- *Incident Response and Monitoring Concepts*

Quiz:

CompTIA Security+

1. *Cryptographic Solutions:*

The Advanced Encryption Standard (AES) is a symmetric stream cipher?

Quiz:

CompTIA Security+

2. Threat Types:

Pharming is a passive means of redirecting users from a legitimate website to a malicious one?

Quiz:

CompTIA Security+

3. Identity and Access Management:

Permissions - The type of access an object is given.
Common permissions include read, write, modify, delete, and execute?

Kolejne kroki w certyfikacjach CyberSec:

2. ***Pierwsze piętro - Intermediate:***

- *Programming Language – Python, Ruby, C++*
- *Fortinet NSE 4-6 / ChcekPoint / Palo Alto*
- *Mile2 C)ISRM - Certified Information Systems Risk Manager*
- *EC-Council CEH & CEH Practical (Certified Ethical Hacker)*
- *ISACA - Certified in the Governance of Enterprise IT*
- *ISACA CRISC - Certified in Risk and Information Systems Control*
- *ISACA CISA - Certified Information Systems Auditor*
- *GIAC GPCS - Public Cloud Security*
- *ISACA CISM - Certified Information Security Manager*
- *Cisco Certified Network Professional (CCNP) Security*
- *CompTIA CASP+ - Advanced Security Practitioner*
- *Mile2 C)PTE - Certified Penetration Testing Engineer*
- *OffSec OSCP - PEN-200: Penetration Testing with Kali Linux*
- *ISC2 CCSP - Certified Cloud Security Professional*
- *GIAC GCIH - Certified Incident Handler*

Co w trawie piszczy?:

EC-Council CEH & CEH Practical (Certified Ethical Hacker)

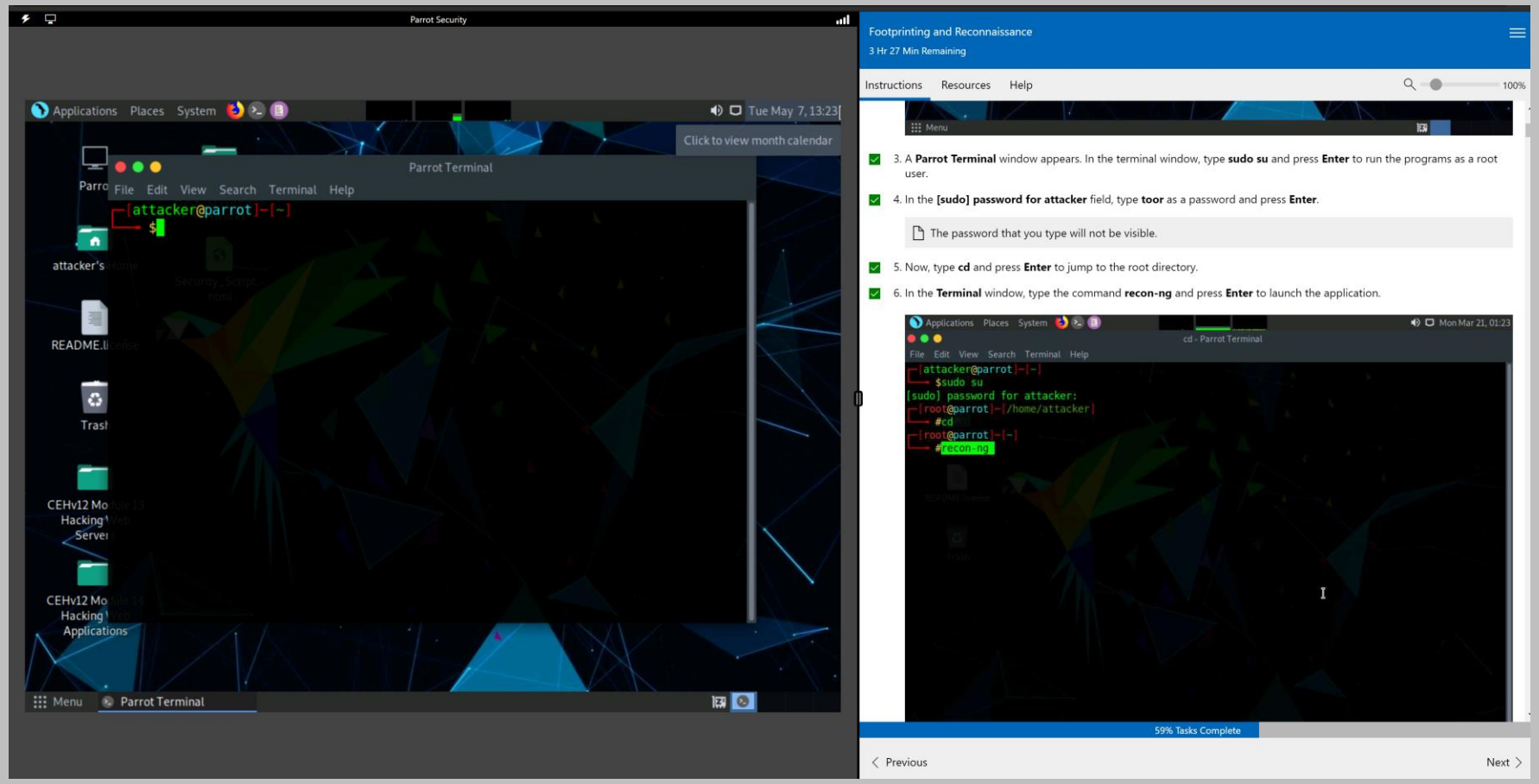
- *Steve, a pen tester, used the Ethical Hacker-2 machine and successfully performed a pen test on a Windows machine. He then obtained its SAM hashes using the responder tool. These hashes are stored in a log file, which can be found at the default location of the responder tool in the Ethical Hacker-2 machine. Crack the password hash and enter the cleartext password in the answer field below.*

- *You are an aspiring pen tester and have been called for an interview with a renowned organization. As a part of the interview, you are given an assignment where you are presented with a network of multiple machines. The assignment requires you to identify a machine running the FTP service, hack into the machine, and gain access to a file named flag.txt. Enter the code contained in flag.txt as the answer.*

Exam Title: Certified Ethical Hacker (Practical)
Number of Practical Challenges: 20
Duration: 6 hours
Availability: Aspen – iLabs
Test Format: iLabs Cyber Range
Passing Score: 60% to 85%

Co w trawie piszczy?:

EC-Council CEH & CEH Practical (Certified Ethical Hacker)



Sztuka latnia i sztuka spadania:

3. ***Strych - Expert:***

- *GIAC Security Expert (GSE)*
- *ISC2 CISSP - Certified Information Systems Security Professional*
- *ISC2 CISSP concentrations (ISSAP, ISSMP & ISSEP)*
- *Fortinet NSE 7-8 / ChcekPoint / Palo Alto*
- *IACIS CAWFE- Certified Advanced Windows Forensic Examiner*
- *GIAC GNFA - Network Forensic Analyst*
- *GIAC Reverse Engineering Malware Certification (GREM)*
- *OffSec OSED Windows User Mode Exploit Development*
- *OffSec OSWE Advanced Web Attacks and exploitation*
- *OffSec OSEE Advanced Windows Exploitation*
- *GIAC GISP Information Security Professional Certification*
- *AWS Certified Solutions Architect - Professional*
- *Cisco Certified Internetwork Expert (CCIE) Security*

CISSP czyli jak to zagryzać bez popijania?:

ISC2 CISSP

Domain 1 Security and Risk Management

- *CIA triad*
- *Security governance principles*
- *Compliance requirements*
- *Legal and regulatory issues relating to information security*
- *IT policies and procedures*
- *Risk-based management concepts*
- *(ISC)2 Code of Ethics*

Domain 2 Asset Security

- *The classification and ownership of information and assets*
- *Privacy*
- *Asset retention, including EoL (end-of-life) and EoS (end-of-support) processes*
- *Stages of the data lifecycle*
- *Data security controls*
- *Handling requirements*

Quiz:

CISSP

4. CIA triad:

CIANA+PS = Adding nonrepudiation, authenticity, privacy, and safety to CIA?

CISSP czyli jak to zagryzać bez popijania?:

ISC2 CISSP

Domain 3 Security Architecture and Engineering

- *Engineering processes using secure design principles*
- *Fundamental concepts of security models*
- *Security capabilities of information systems*
- *Assessing and mitigating vulnerabilities in systems*
- *Cryptography, including methods of cryptanalytic attacks and key management practices*
- *Security principles as applied to designing sites and facilities*

Domain 4 Communication and Network Security

- *Secure design principles for network architecture*
- *Secure network components*
- *Secure communication channels*
- *OSI (Open System Interconnection) and TCP/IP*

Quiz:

CISSP

5. Security principles as applied to designing sites and facilities:

Crime Prevention through Environmental Design (CPTED), approaches the challenge of creating safer workspaces through passive design elements?

CISSP czyli jak to zagryzać bez popijania?:

ISC2 CISSP

Domain 5 Identity and Access Management (IAM)

- *Physical and logical access to assets*
- *Identification and authentication*
- *Integrating identity as a service and third-party identity services*
- *Authorisation mechanisms*
- *The identity and access provisioning lifecycle*

Domain 6 Security Assessment and Testing

- *Designing and validating assessment and test strategies*
- *Security control testing*
- *Collecting security process data*
- *Test outputs*
- *Internal and third-party security audits*

Quiz:

CISSP

6. Test outputs:

Mutation (Dumb) Fuzzing - Takes previous input values from actual operation of the software and manipulates (or mutates) it to create fuzzed input?

CISSP czyli jak to zagryzać bez popijania?:

ISC2 CISSP

Domain 7 Security Operations

- *Understanding and supporting investigations*
- *Requirements for investigation types*
- *Logging and monitoring activities*
- *Securing the provision of resources*
- *Foundational security operations concepts*
- *Applying resource protection techniques*
- *Incident management*
- *Disaster recovery and Business continuity*
- *Managing physical security*

Domain 8 Software Development Security

- *Security in the software development lifecycle*
- *Security controls in software development ecosystems*
- *The effectiveness of software security*
- *Secure coding guidelines and standards*

Quiz:

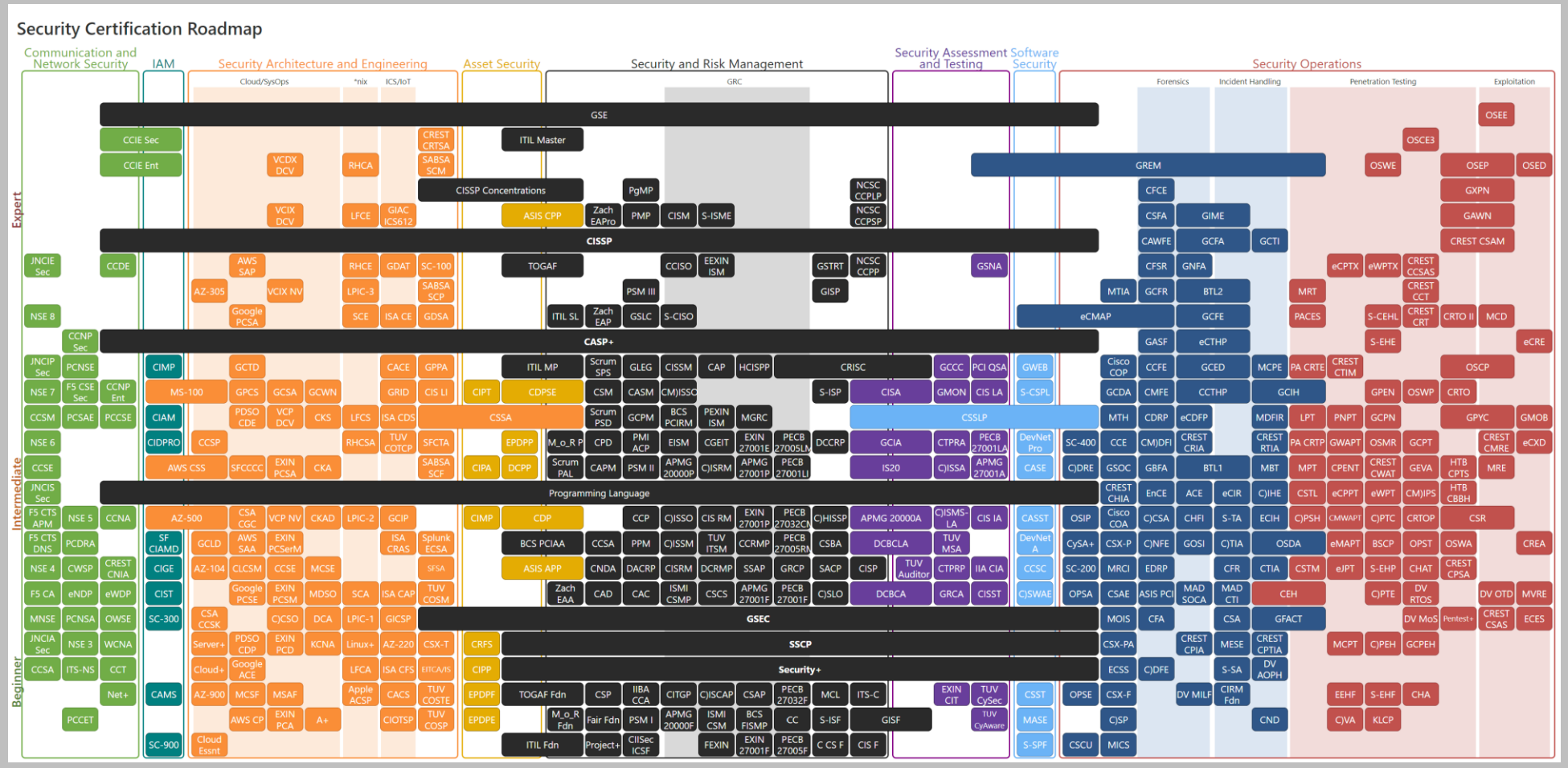
CISSP

7. Disaster recovery and Business continuity:

BCP is the technological aspect of DRP that focuses on IT systems and operations?

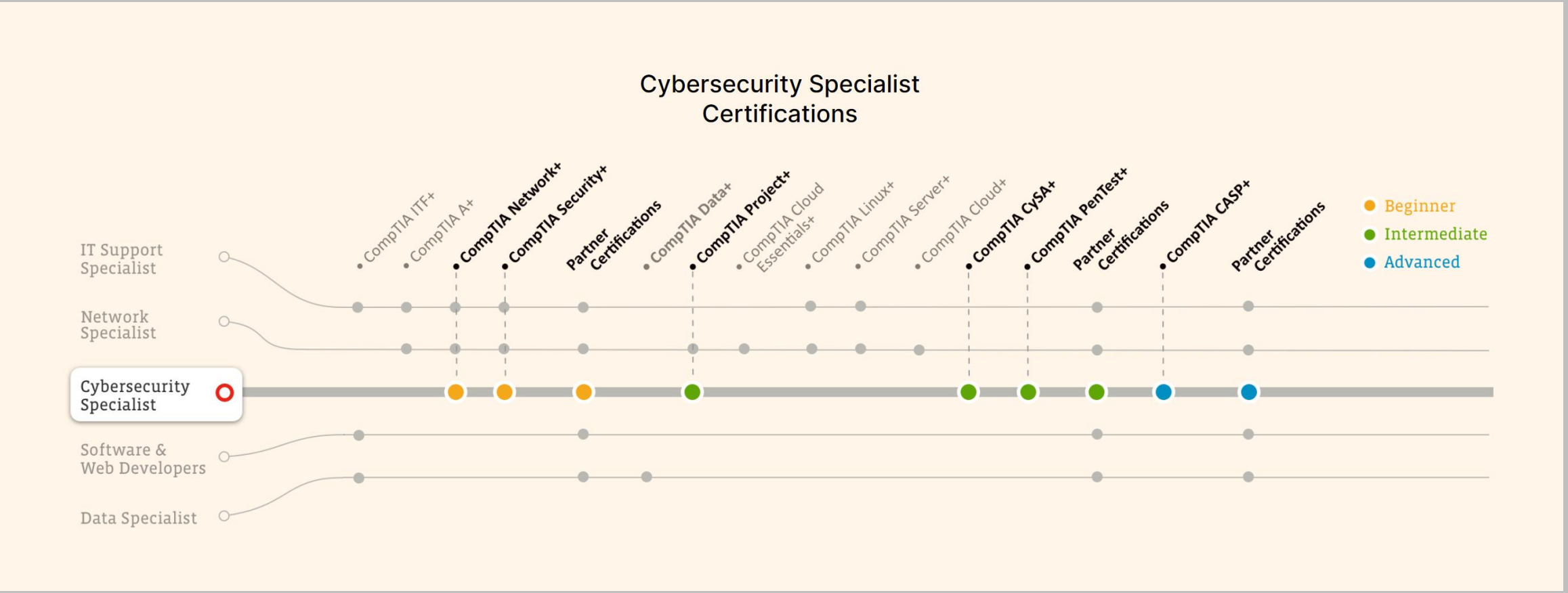
Ewaluacja:

Znalezione w internacie:



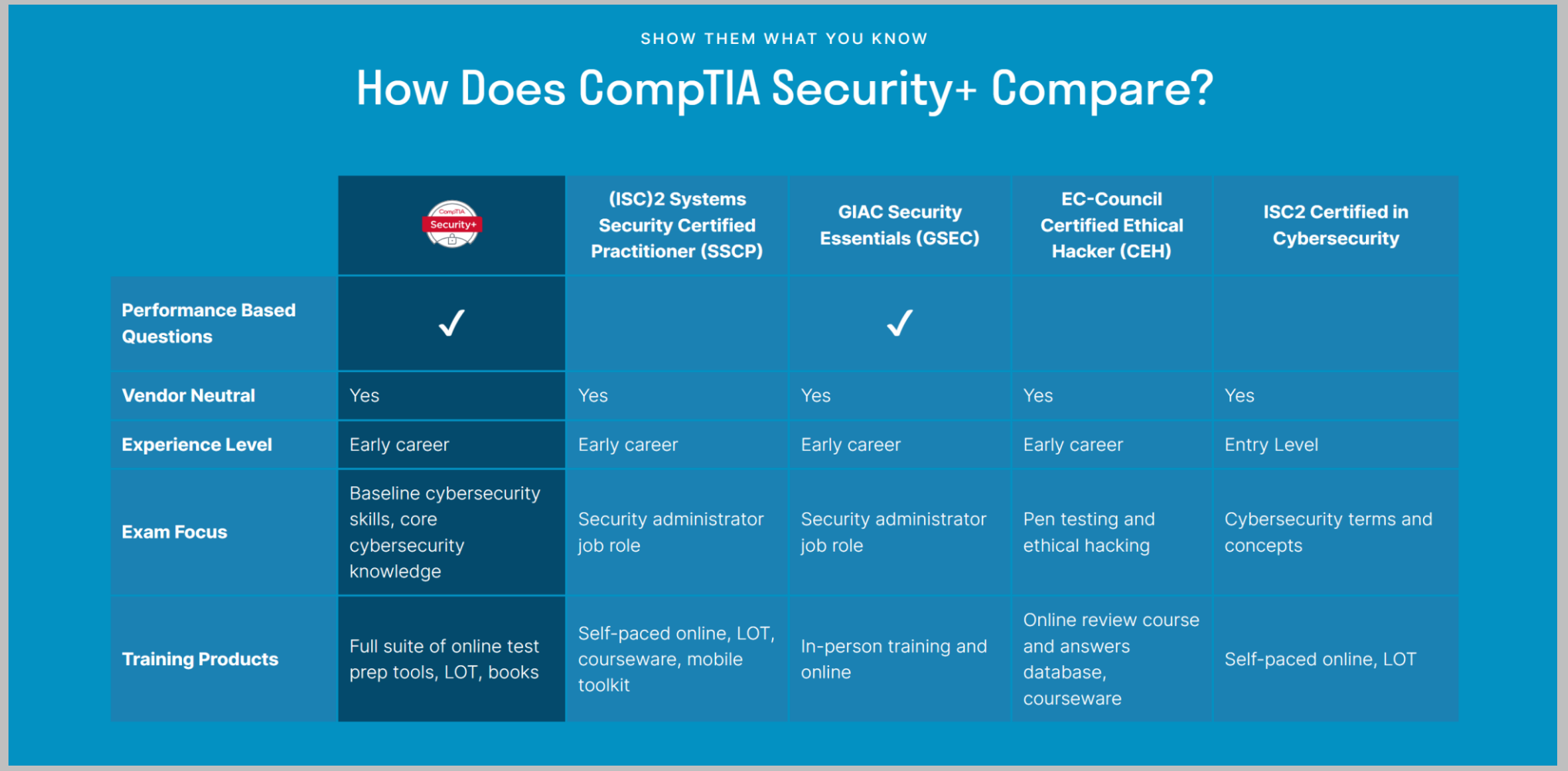
https://pauljerimy.com/security-certification-roadmap/

Znalezione w internacie:



https://www.comptia.org/content/articles/what-is-cybersecurity

Znalezione w internacie:



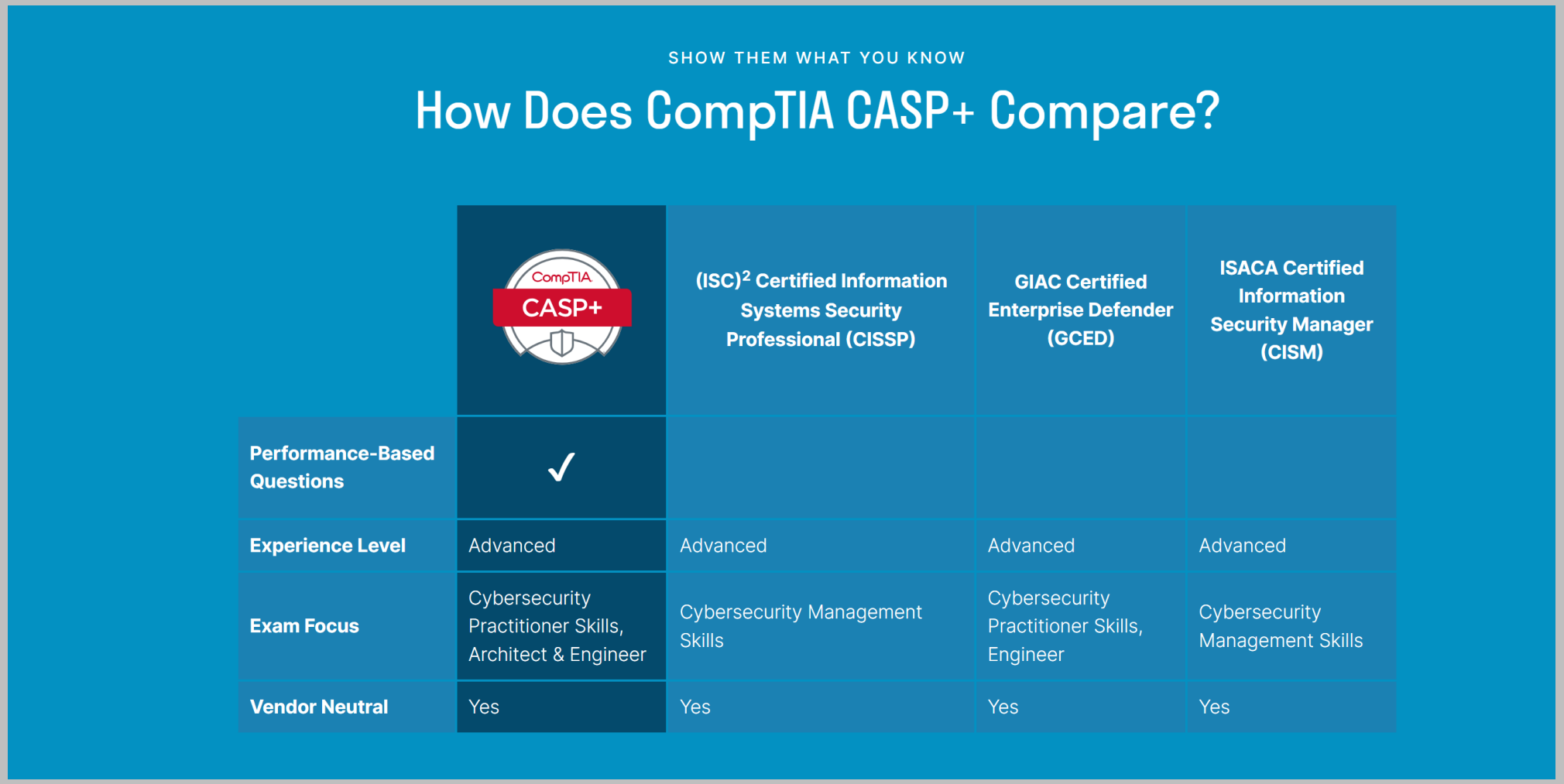
SHOW THEM WHAT YOU KNOW

How Does CompTIA Security+ Compare?

	Security+	(ISC)2 Systems Security Certified Practitioner (SSCP)	GIAC Security Essentials (GSEC)	EC-Council Certified Ethical Hacker (CEH)	ISC2 Certified in Cybersecurity
Performance Based Questions	✓		✓		
Vendor Neutral	Yes	Yes	Yes	Yes	Yes
Experience Level	Early career	Early career	Early career	Early career	Entry Level
Exam Focus	Baseline cybersecurity skills, core cybersecurity knowledge	Security administrator job role	Security administrator job role	Pen testing and ethical hacking	Cybersecurity terms and concepts
Training Products	Full suite of online test prep tools, LOT, books	Self-paced online, LOT, courseware, mobile toolkit	In-person training and online	Online review course and answers database, courseware	Self-paced online, LOT

https://www.comptia.org/content/articles/what-is-cybersecurity

Znalezione w internacie:



SHOW THEM WHAT YOU KNOW

How Does CompTIA CASP+ Compare?

	CompTIA CASP+	(ISC)² Certified Information Systems Security Professional (CISSP)	GIAC Certified Enterprise Defender (GCED)	ISACA Certified Information Security Manager (CISM)
Performance-Based Questions	✓			
Experience Level	Advanced	Advanced	Advanced	Advanced
Exam Focus	Cybersecurity Practitioner Skills, Architect & Engineer	Cybersecurity Management Skills	Cybersecurity Practitioner Skills, Engineer	Cybersecurity Management Skills
Vendor Neutral	Yes	Yes	Yes	Yes

https://www.comptia.org/content/articles/what-is-cybersecurity

Po szkoleniu czyli „bunkrów nie ma ale … ”:

- *Certyfikat uczestnictwa w szkoleniu*
- *Egzaminy i jak się za to zabrać … Computerized Adaptive Testing (CAT)*
- *Doświadczenie zawodowe lub jego brak*
- *Endorsement*

https://www.credly.com/users/sign_in

Po szkoleniu czyli „bunkrów nie ma ale … ”:

Necessary Work Experience:

- *To qualify for this cybersecurity certification,* ***you must pass the exam and have at least five years*** *of cumulative, paid work experience* ***in two or more of the eight domains*** *of the ISC2 CISSP Common Body of Knowledge (CBK).*
- *Learn more about CISSP Experience Requirements and how you may be able to* ***satisfy one year*** *of required work experience with a relevant* ***four-year college degree*** *or if you hold an approved credential.*
- *Don’t have enough experience yet? You can still pass the CISSP exam and* ***become an Associate of ISC2 while you earn the required work experience.***

- *https://www.isc2.org/certifications/cissp#Required%20Work%20Experience*

Jak nie oddać co moje?:

- *Certyfikat i jego ważność*
- *Proces utrzymania certyfikacji czyli Continuing Professional Education (CPE) & $$$*

CISA

You are CISA certified

STATUS: ACTIVE
NUMBER: CISA-20169883
CERTIFICATION DATE: 29 October 2020
CERTIFIED THROUGH: 2024
3-YEAR REPORTING-CYCLE: 2024-2026

REPORT & MANAGE CPE

View/Accept Badges

Print Certificate

CPE PROGRESS*

2024: 0.0 OF 20 CPE HRS EARNED

3 Years: 0.0 OF 120 CPE HRS EARNED

The inner circle shows your current annual CPE progress*
The outer circle shows your 3-year cycle CPE progress*

Need CPE? Learn about CPE Opportunities from ISACA

HIDE CPE SUMMARY –

TIME PERIOD	REQUIRED HRS	EARNED HRS	RECOMMENDED HRS	CPE HRS DUE
2024	20	0.0	40	20.0
2025	20	0.0	40	20.0
2026	20	0.0	40	20.0
3-Year Cycle 2024-2026	120	0.0	120	120.0

Kariera, czyli od zera do bohatera:

1. ***Kompetencje** nabywa się poprzez ogólne wykształcenie, szkolenie, coaching i doświadczenie.*

2. ***Doświadczenie** odnosi się do umiejętności zdobywanych w trakcie wykonywanej pracy, np. planowanie, organizacja pracy, komunikatywność.*

    - ***Internship time czyli: „Jestem Laska. Z Polski. Jestem synem Króla Sedesów"***

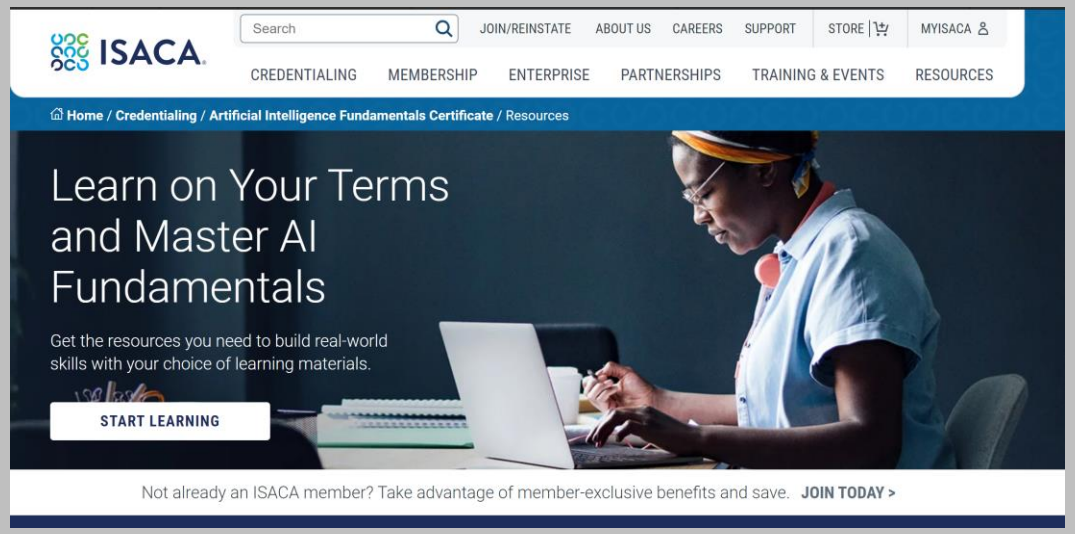
3. ***Zaangażowanie** to połączenie motywacji i wiary w siebie pracownika w odniesieniu do realizacji konkretnego celu lub zadania.*

RBAC w cyberbezpieczeństwie:

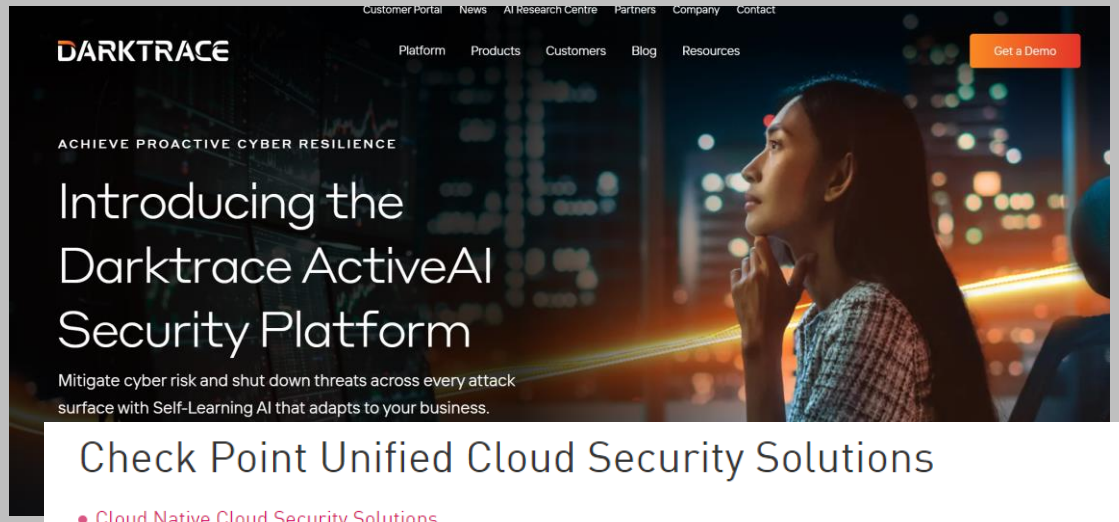
- *Chief information security officer*
- *Chief compliance officer*
- *Information system security officer*
- *Information/privacy risk consultant*
- *Information security manager*
- *IT manager*
- *Operations manager*
- *Information control manager*
- *IT auditor*
- *Compliance analyst/program manager*
- *Risk analyst/program manager*
- *Data protection manager*
- *Security oficer*
- *Vulnerability Analyst / Penetration Tester*
- *Software Developer / Engineer*
- *CyberSecurity Specialist / Technician*
- *Cyber Risk Analyst*
- *Risk manager*
- *Business analyst*
- *Incident response analyst*
- *Security architect*
- *CyberSecurity engineer*
- *Threat hunter*
- *Security operations center (SOC) analyst*
- *Application security analyst*
- *Threat intelligence analyst*
- *CyberSecurity Engineer*
- *CyberSecurity Analyst*
- *Network Engineer / Architect*
- *CyberSecurity Consultant*
- *CyberSecurity Manager / Administrator*
- *Systems Engineer*

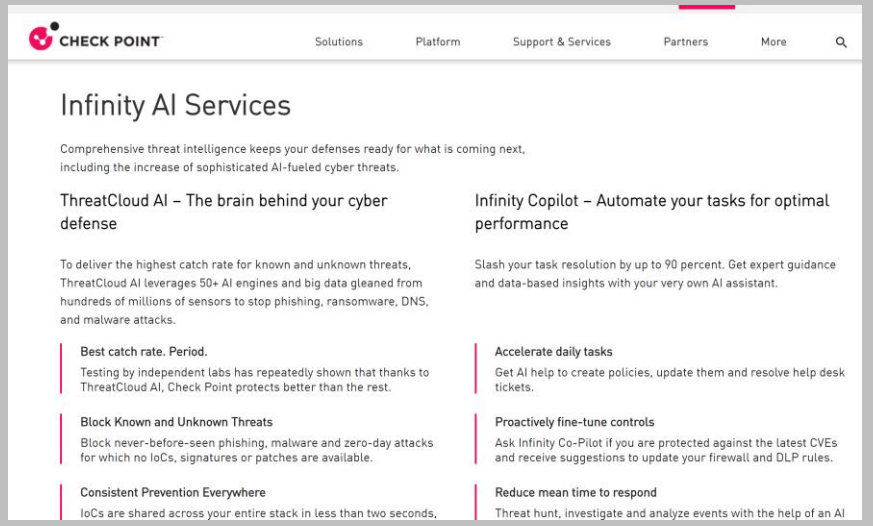
Certyfikacje przyszłości w cyberbezpieczeństwie:

CompTIA Essentials	
AI Essentials	Any occupation
CompTIA Expansions	
Sec AI+	Security Engineers
PenTest AI+	Penetration Testers
CySA AI+	Security Analysts
Data AI+	Data Analysts
AI SysOp+	Systems Operations
AI Scripting+	Tech Support, Network Operations
AI Architect+	AI Systems Architects
AI Prompt+	Prompt Engineers



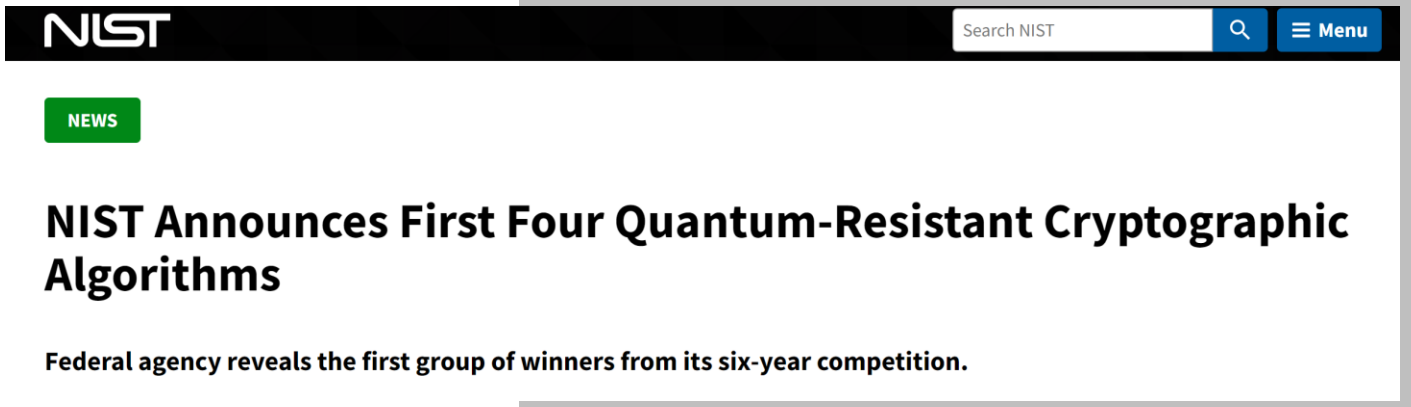
Zawody przyszłości w cyberbezpieczeństwie:





Check Point Unified Cloud Security Solutions

- Cloud Native Cloud Security Solutions
- Cloud Security Posture Management
- Cloud Workload Protection
- Cloud Intelligence and Threat Hunting
- Cloud Network Security
- Serverless Security
- Container Security
- AWS Security
- Azure Security
- GCP Security
- Branch Cloud Security



Compendium CE:

1. *Compendium Centrum Edukacyjne (Compendium CE), założone w roku 2000 (24 lata na rynku), jest firmą specjalizującą się w edukacji.*

2. *Wyłącznym obszarem jej działalności jest świadczenie usług szkoleniowych i usług związanych z przeprowadzaniem egzaminów certyfikacyjnych.*

3. *Obszar działania Compendium CE obejmuje Polskę, jak również regiony CEE i EMEA, w zależności od zawartych umów z dostawcami produktów edukacyjnych.*

Compendium CE to:

- *30 autoryzacji/akredytacji: autoryzacje od renomowanych dostawców, takich jak Check Point, CompTIA, Fortinet, Microsoft, Google Cloud, AWS, ISC2, …*
- *Ponad 1000 kursów w ofercie*
- *Centra egzaminacyjne: Pearson VUE, Kryterion*

https://www.compendium.pl/

Compendium CE:

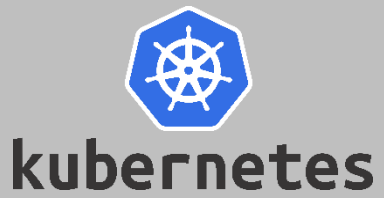
Compendium CE – CyberSecurity:

Vendor-neutral

Vendor-specific

Compendium CE – Cloud:

Vendor-neutral



Vendor-specific

Compendium CE:

Wszystkie szkolenia w ofercie Compendium CE są dostępne w jednej z trzech/czterech form ich dostarczania:*

1. ***Stacjonarnie (ILT)** - szkolenie prowadzone przez instruktora (na żywo w sali)*

2. ***Zdalnie (VILT)** - wirtualne szkolenie prowadzone przez instruktora (na żywo w oparciu o środowisko Microsoft Teams)*

3. ***Hybrydowo (ILT+VILT)** - studenci mają możliwość wyboru, czy uczestniczą w szkoleniu stacjonarnie czy zdalnie (sala szkoleniowa z wykorzystaniem środowiska Microsoft Teams)*

4. ***Blended Learning (ILT/VILT z BL)** - łączy różne elementy, aby stworzyć skuteczne i elastyczne środowisko szkoleniowe:*
   - *to zaplanowane sesje, podczas których uczestnicy wchodzą w interakcję z instruktorem w czasie rzeczywistym*
   - *uczestnicy mogą zadawać pytania, dyskutować na tematy i otrzymywać spersonalizowane wskazówki*
   - *czas trwania tych sesji może się różnić (np. raz w tygodniu, raz na dwa tygodnie lub co miesiąc)*

***Forma dostarczania może być dostosowywana w zależności od specyficznych potrzeb szkoleniowych.**

Dziękuję za uwagę!