КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КОД ИБ | КАЗАНЬ

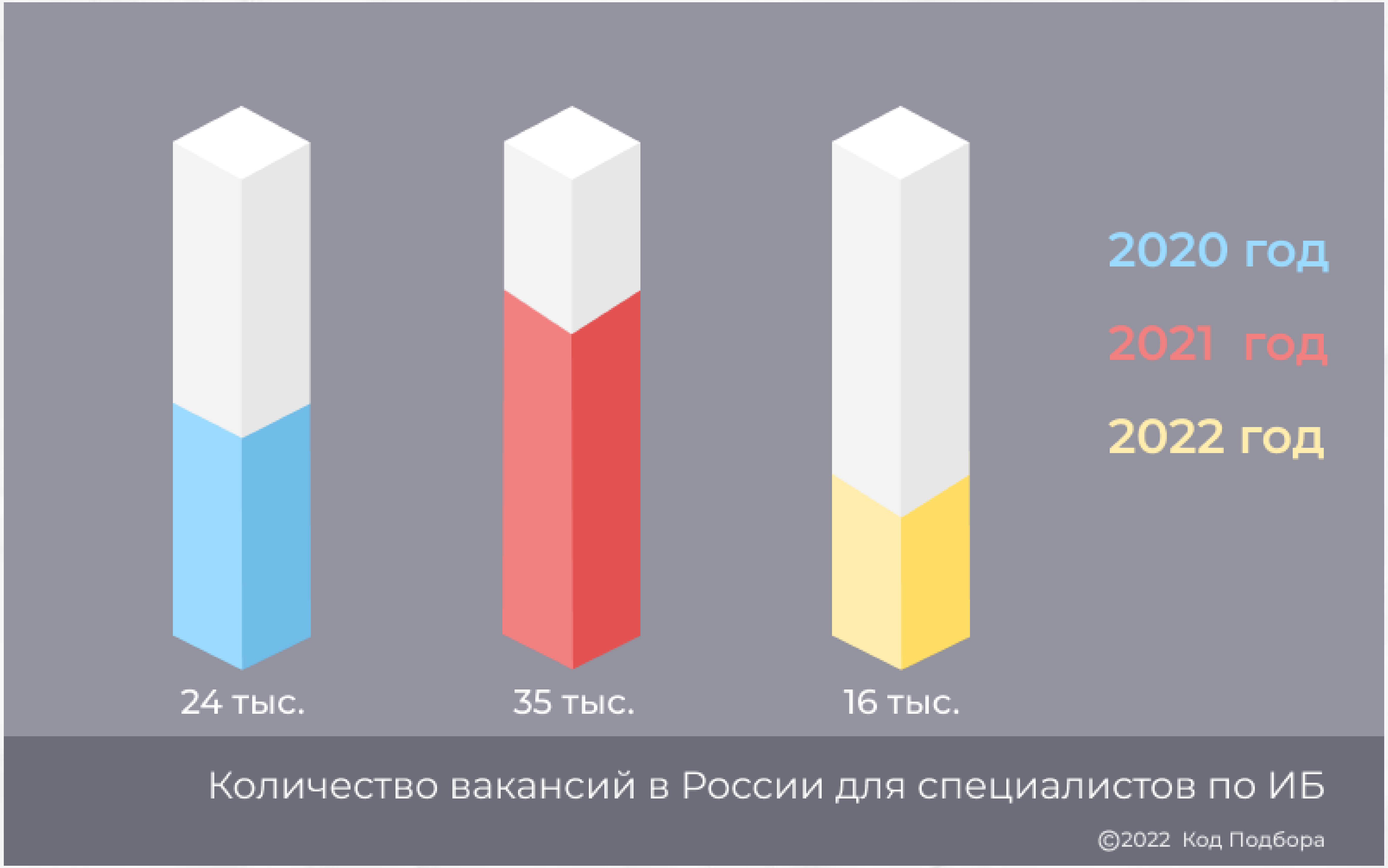
13.10.2022

НИКИТА КОРМИЛЬЦЕВ

- КНИТУ-КАИ им. А. Н. Туполева, специалитет «Информационная безопасность телекоммуникационных систем»
- КНИТУ-КАИ им. А. Н. Туполева, аспирантура «Методы и системы защиты информации, информационная безопасность», аспирант
- АНО ВО «Университет Иннополис», магистратура «Security System and Network Engineering», студент
- MTCNA, MTCRE, MTCSWE, MTCWE, MTCSE
- специалист по ИБ Центра информационной безопасности АНО ВО «Университет Иннополис»

НЕОБХОДИМЫЕ ХАРД И СОФТ СКИЛЫ СПЕЦИАЛИСТА ПО ИБ

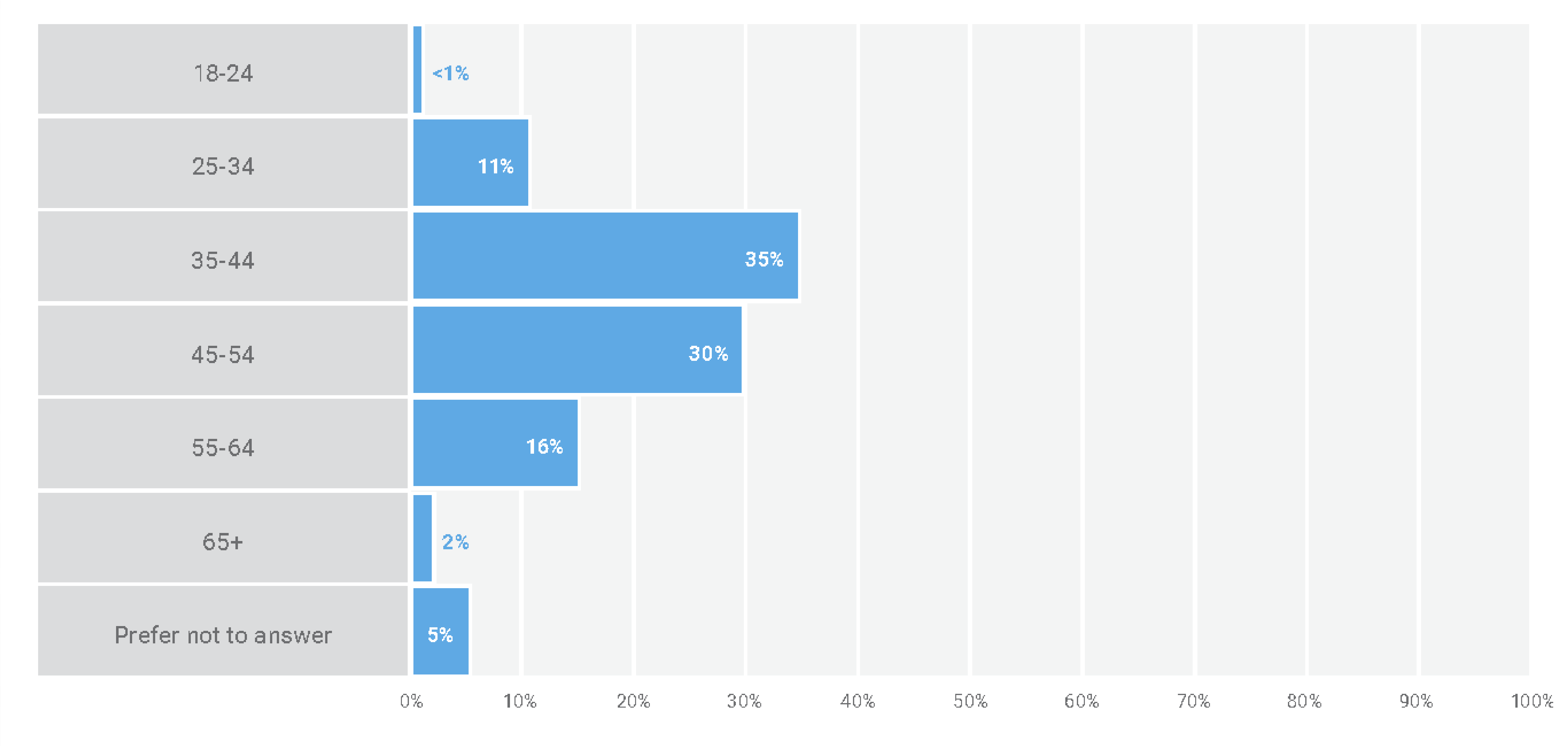
Немного о вакансиях



Количество вакансий в России для специалистов по ИБ

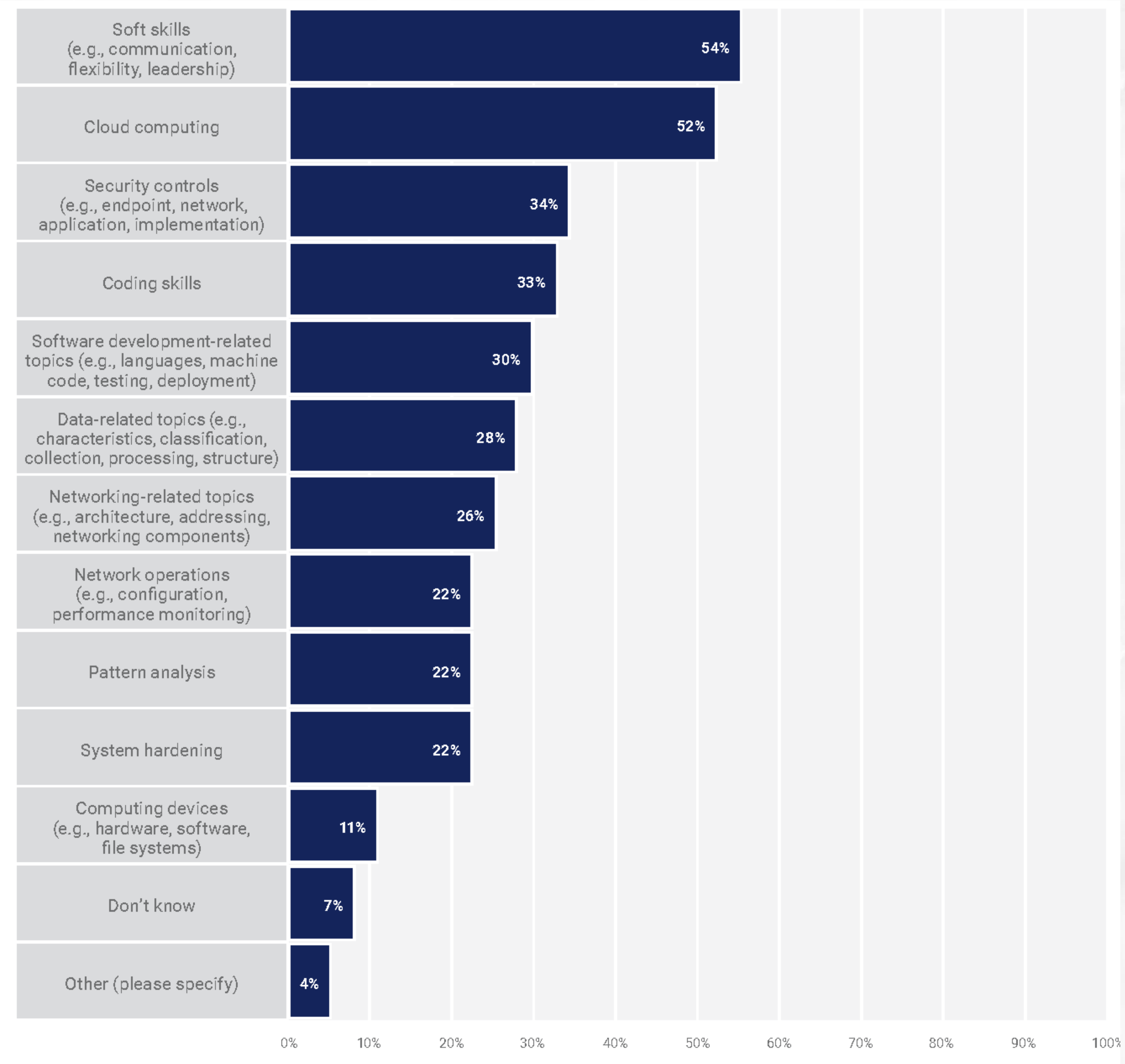
©2022 Код Подбора

Немного о возрасте



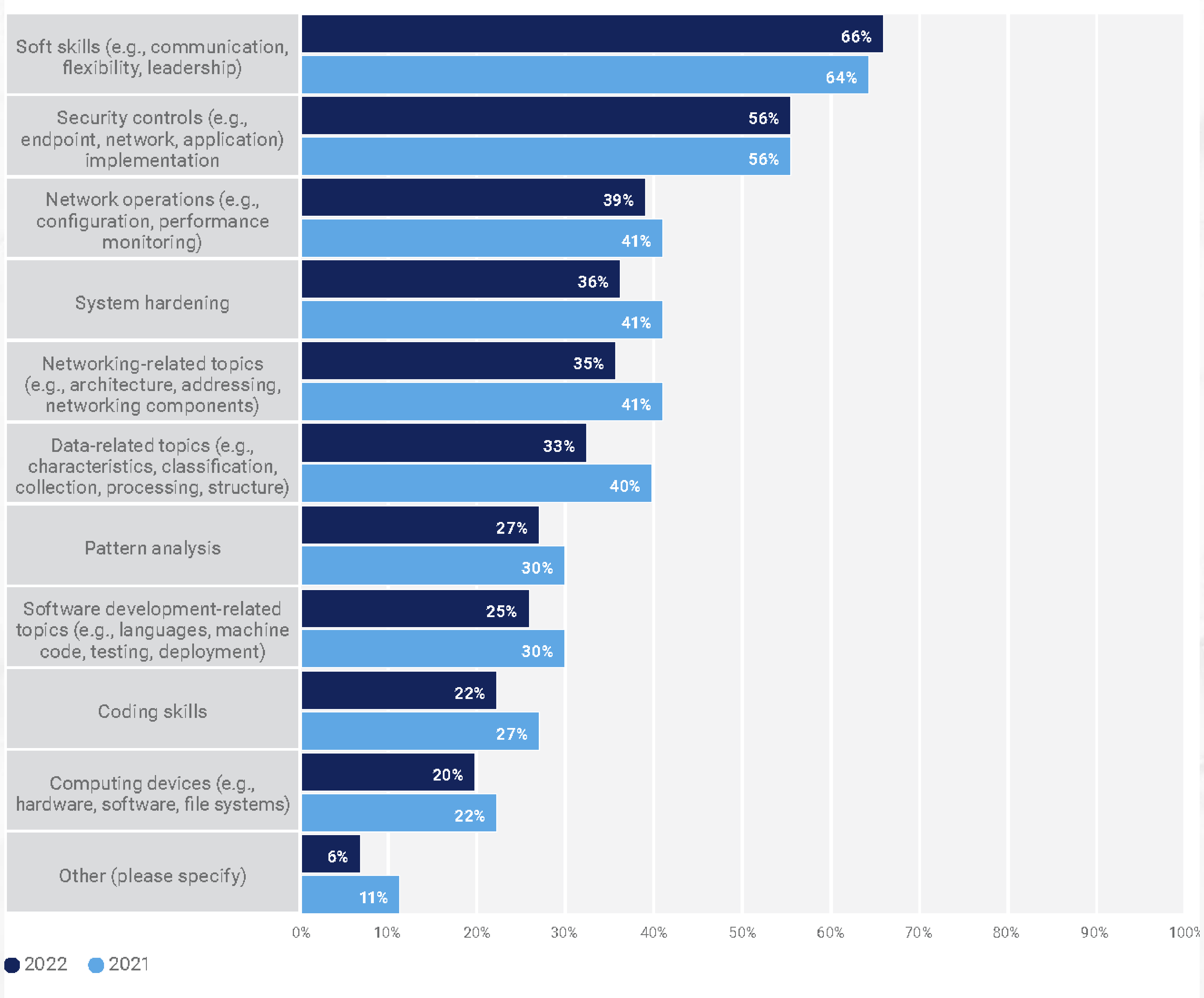
https://www.isaca.org/resources/infographics/state-of-cybersecurity-2022-infographic

Пробелы в навыках у специалистов ИБ



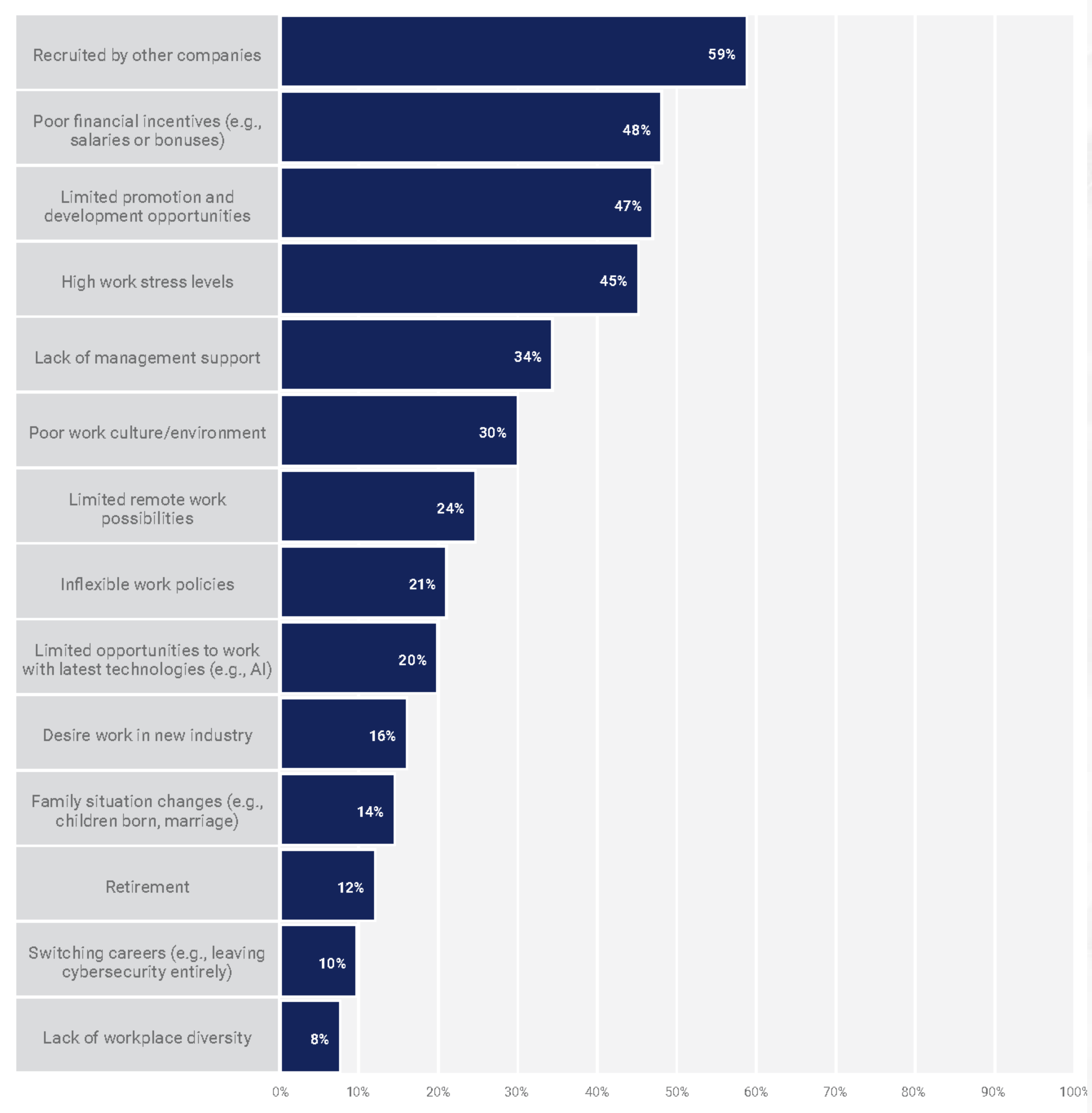
https://www.isaca.org/resources/infographics/state-of-cybersecurity-2022-infographic

Пробелы в навыках после выпуска



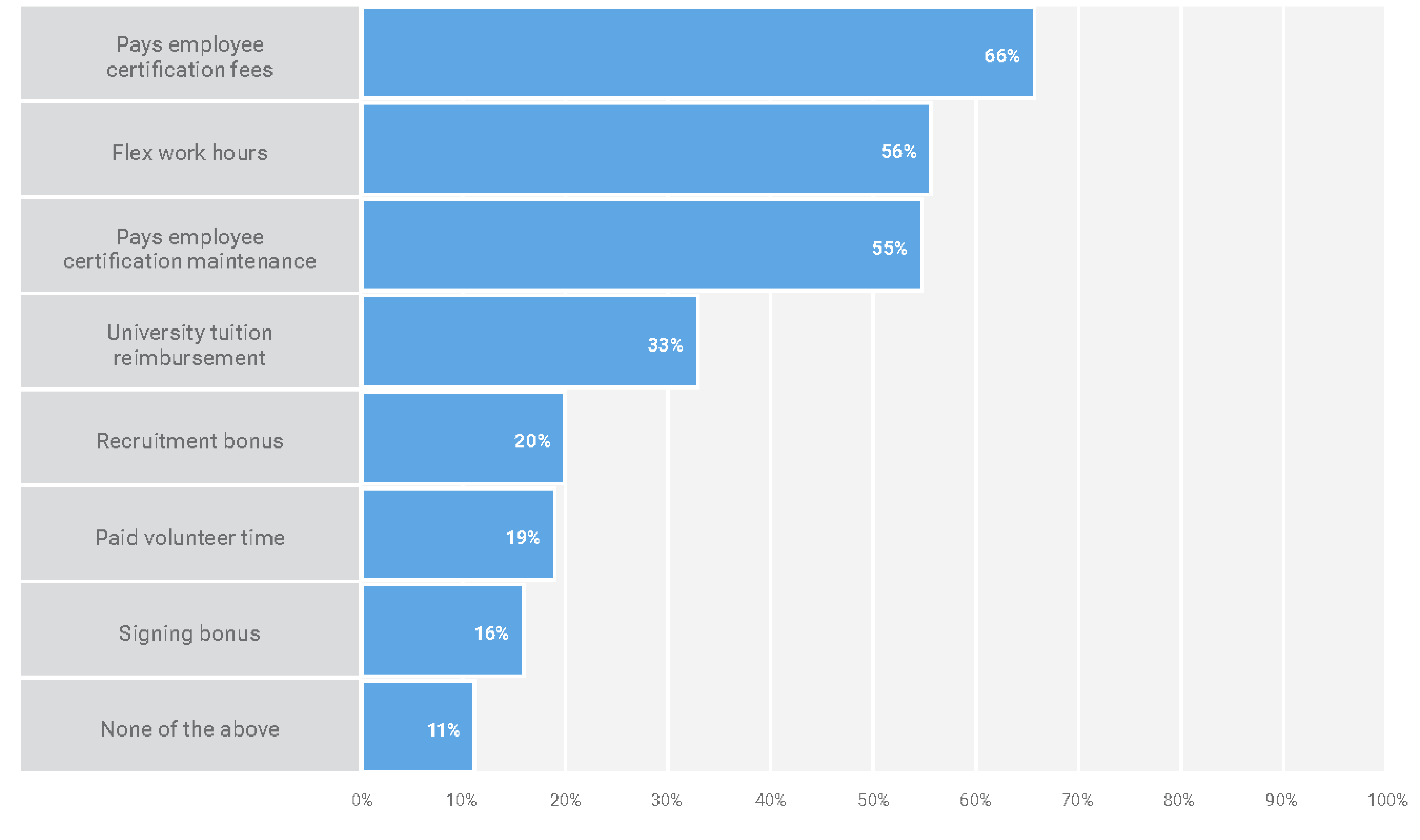
https://www.isaca.org/resources/infographics/state-of-cybersecurity-2022-infographic

Причины увольнений



https://www.isaca.org/resources/infographics/state-of-cybersecurity-2022-infographic

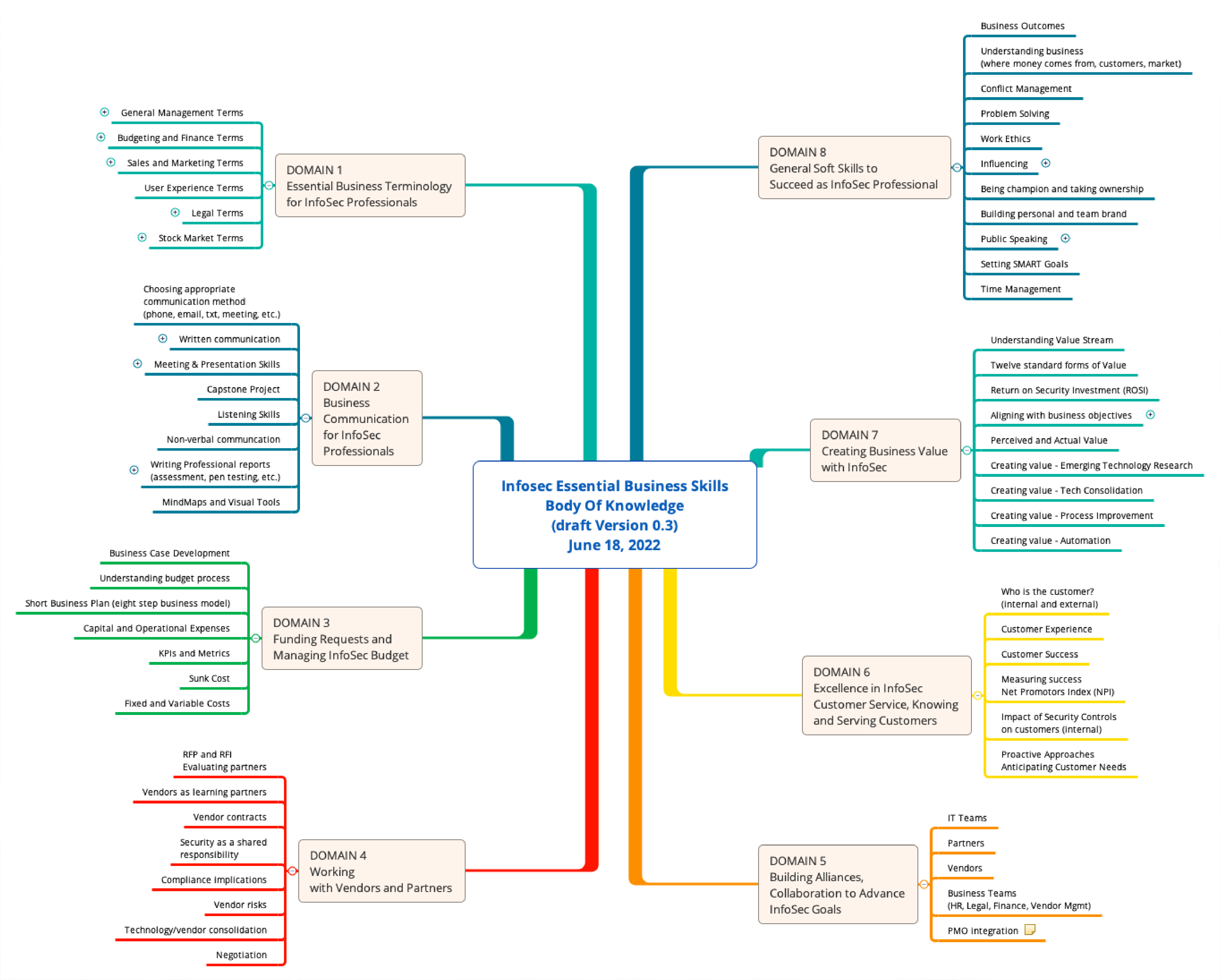
Преимущества работодателей



https://www.isaca.org/resources/infographics/state-of-cybersecurity-2022-infographic

СОФТ СКИЛЫ

Необходимые бизнес скилы



Infosec Essential Business Skills
Body Of Knowledge
(draft Version 0.3)
June 18, 2022

DOMAIN 1
Essential Business Terminology for InfoSec Professionals
- General Management Terms
- Budgeting and Finance Terms
- Sales and Marketing Terms
- User Experience Terms
- Legal Terms
- Stock Market Terms

DOMAIN 2
Business Communication for InfoSec Professionals
- Choosing appropriate communication method (phone, email, txt, meeting, etc.)
- Written communication
- Meeting & Presentation Skills
- Capstone Project
- Listening Skills
- Non-verbal communcation
- Writing Professional reports (assessment, pen testing, etc.)
- MindMaps and Visual Tools

DOMAIN 3
Funding Requests and Managing InfoSec Budget
- Business Case Development
- Understanding budget process
- Short Business Plan (eight step business model)
- Capital and Operational Expenses
- KPIs and Metrics
- Sunk Cost
- Fixed and Variable Costs

DOMAIN 4
Working with Vendors and Partners
- RFP and RFI Evaluating partners
- Vendors as learning partners
- Vendor contracts
- Security as a shared responsibility
- Compliance Implications
- Vendor risks
- Technology/vendor consolidation
- Negotiation

DOMAIN 8
General Soft Skills to Succeed as InfoSec Professional
- Business Outcomes
- Understanding business (where money comes from, customers, market)
- Conflict Management
- Problem Solving
- Work Ethics
- Influencing
- Being champion and taking ownership
- Building personal and team brand
- Public Speaking
- Setting SMART Goals
- Time Management

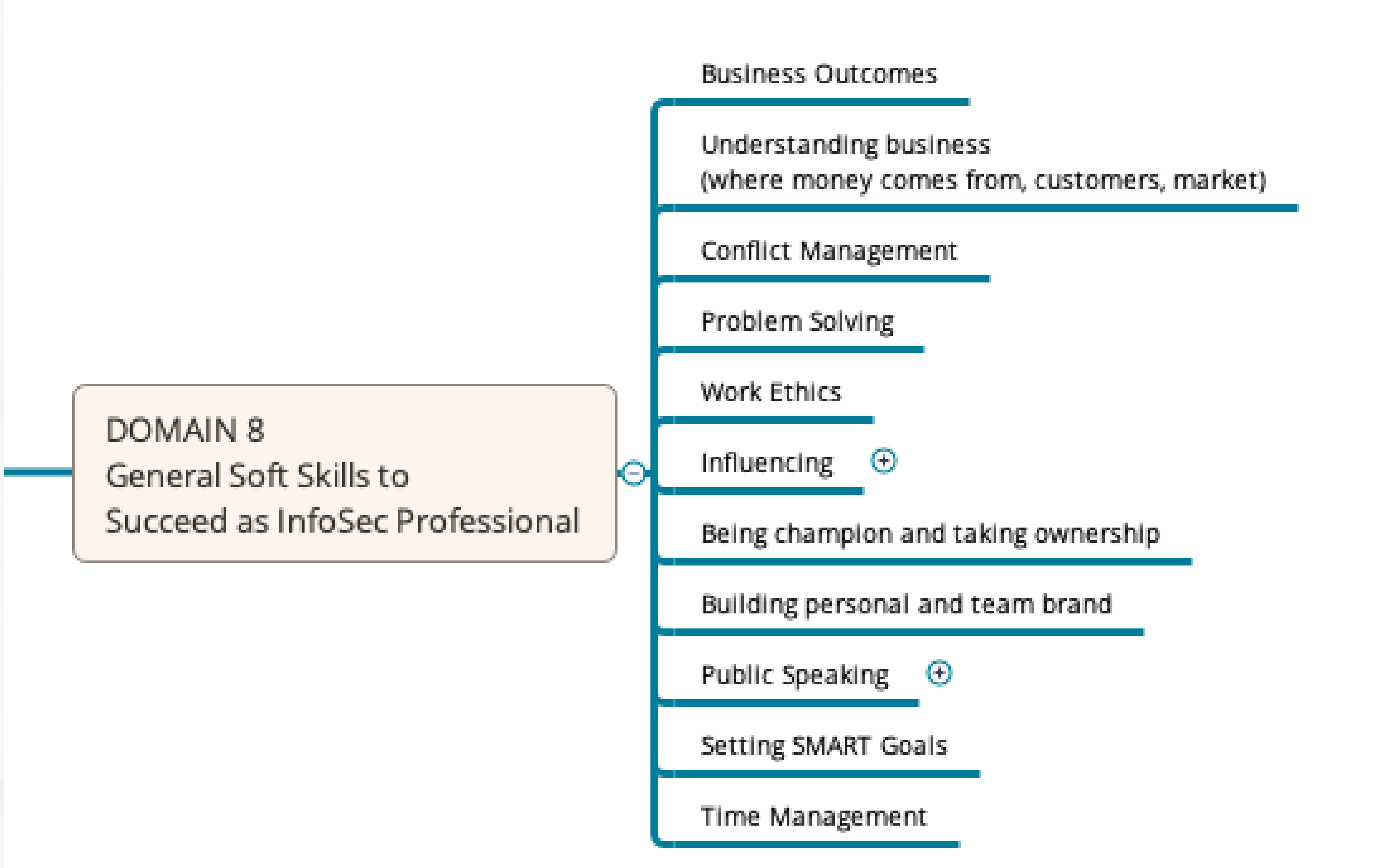
DOMAIN 7
Creating Business Value with InfoSec
- Understanding Value Stream
- Twelve standard forms of Value
- Return on Security Investment (ROSI)
- Aligning with business objectives
- Perceived and Actual Value
- Creating value - Emerging Technology Research
- Creating value - Tech Consolidation
- Creating value - Process Improvement
- Creating value - Automation

DOMAIN 6
Excellence in InfoSec Customer Service, Knowing and Serving Customers
- Who is the customer? (internal and external)
- Customer Experience
- Customer Success
- Measuring success Net Promotors Index (NPI)
- Impact of Security Controls on customers (internal)
- Proactive Approaches Anticipating Customer Needs

DOMAIN 5
Building Alliances, Collaboration to Advance InfoSec Goals
- IT Teams
- Partners
- Vendors
- Business Teams (HR, Legal, Finance, Vendor Mgmt)
- PMO integration

https://rafeeqrehman.com/wp-content/uploads/2022/06/infosec-essential-skills-draft-v3-20220618.png

8 домен

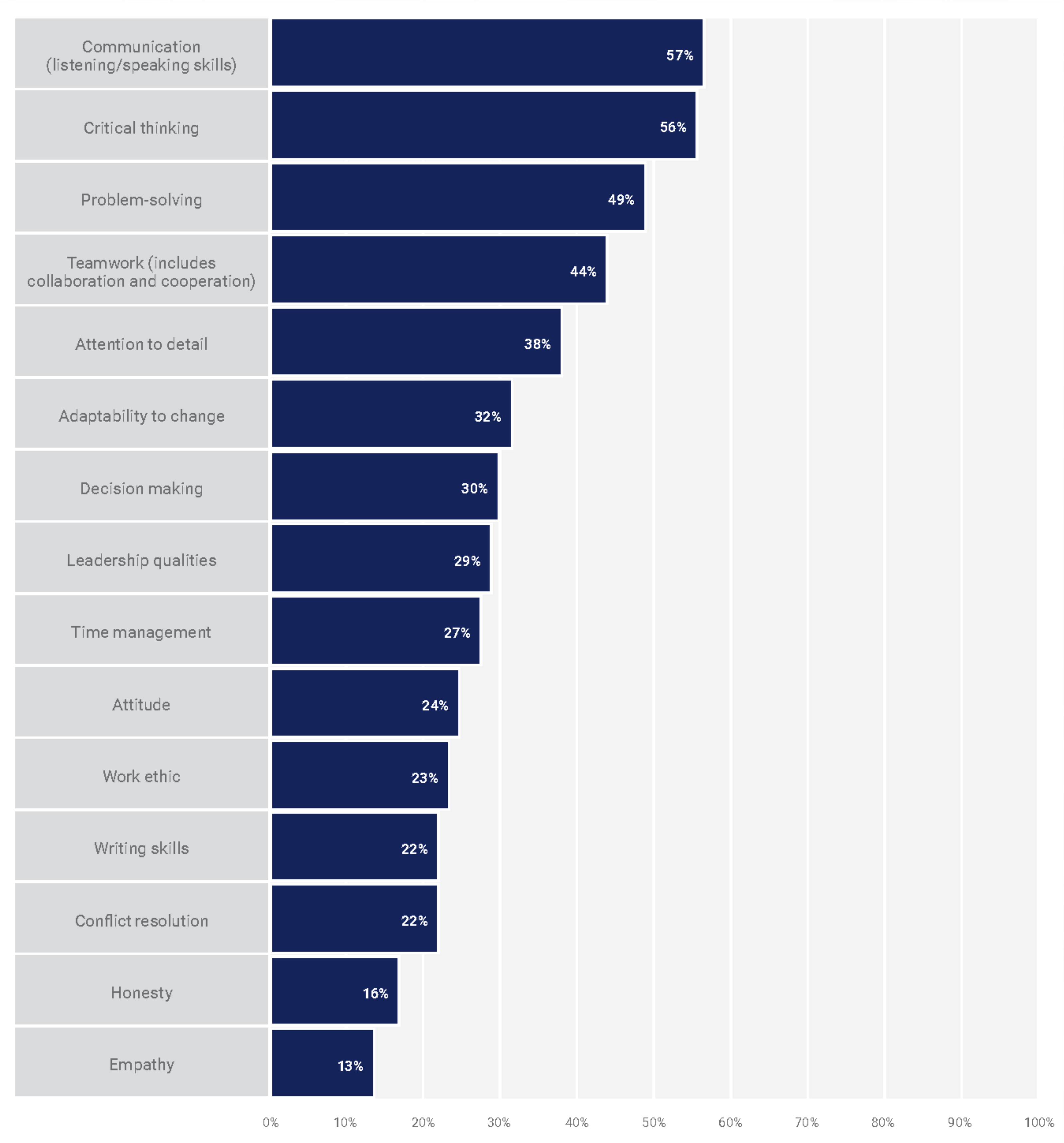


DOMAIN 8
General Soft Skills to
Succeed as InfoSec Professional

- Business Outcomes
- Understanding business
(where money comes from, customers, market)
- Conflict Management
- Problem Solving
- Work Ethics
- Influencing
- Being champion and taking ownership
- Building personal and team brand
- Public Speaking
- Setting SMART Goals
- Time Management

https://rafeeqrehman.com/wp-content/uploads/2022/06/infosec-essential-skills-draft-v3-20220618.png

Топ 5 софт скилов



https://www.isaca.org/resources/infographics/state-of-cybersecurity-2022-infographic

Рекомендации

Harvard Business Review
10 лучших статей
Эффективные коммуникации
альпина паблишер
бизнес

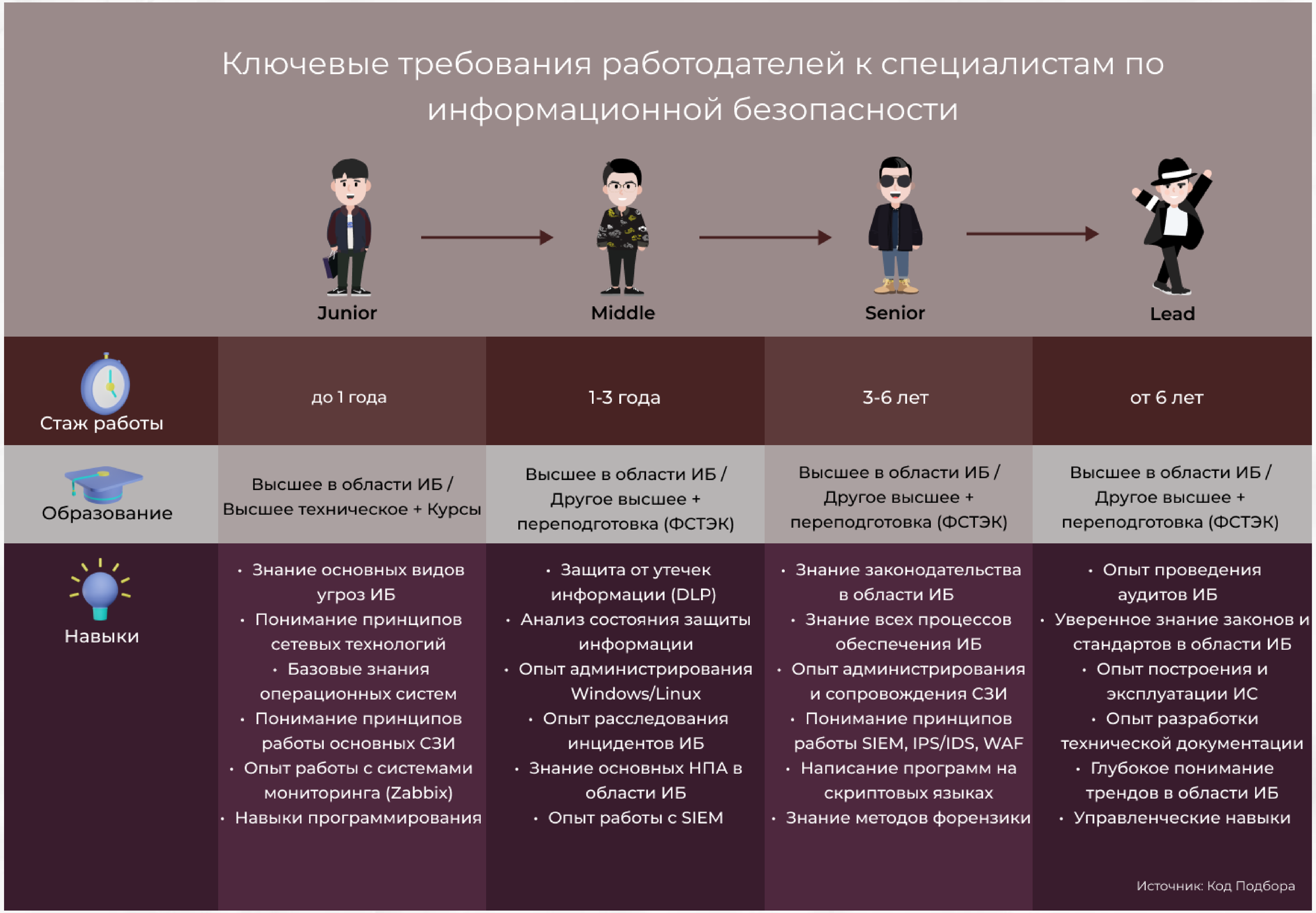
https://www.litres.ru/harvard-business-review-guides/

Harvard Business Review
10 лучших статей
Эмоциональный интеллект
альпина паблишер
бизнес

https://www.litres.ru/raznoe/effektivnye-kommunikacii/

ХАРД СКИЛЫ

Требования к специалистам ИБ

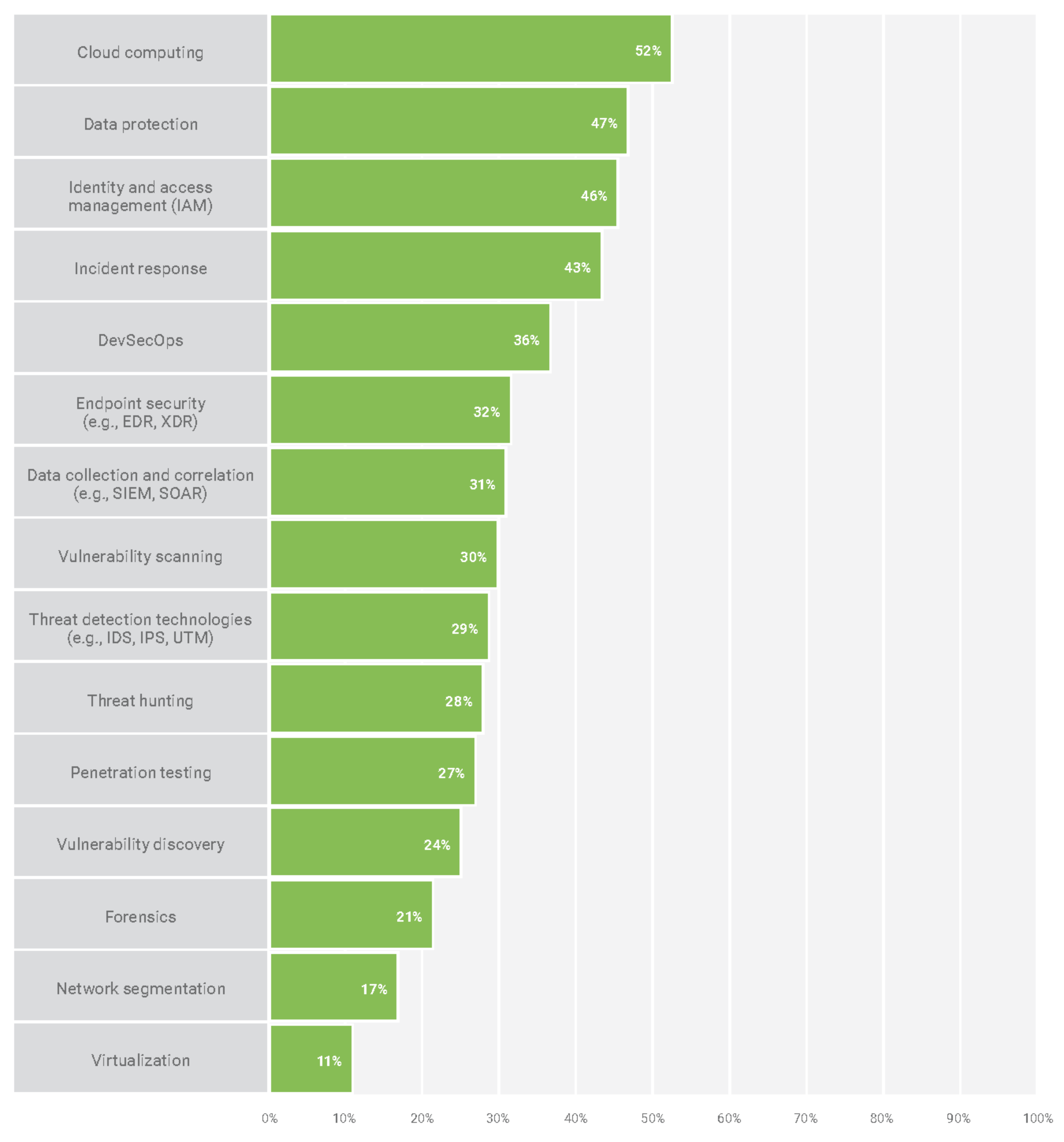


Ключевые требования работодателей к специалистам по информационной безопасности

	Junior	Middle	Senior	Lead
Стаж работы	до 1 года	1-3 года	3-6 лет	от 6 лет
Образование	Высшее в области ИБ / Высшее техническое + Курсы	Высшее в области ИБ / Другое высшее + переподготовка (ФСТЭК)	Высшее в области ИБ / Другое высшее + переподготовка (ФСТЭК)	Высшее в области ИБ / Другое высшее + переподготовка (ФСТЭК)
Навыки	• Знание основных видов угроз ИБ • Понимание принципов сетевых технологий • Базовые знания операционных систем • Понимание принципов работы основных СЗИ • Опыт работы с системами мониторинга (Zabbix) • Навыки программирования	• Защита от утечек информации (DLP) • Анализ состояния защиты информации • Опыт администрирования Windows/Linux • Опыт расследования инцидентов ИБ • Знание основных НПА в области ИБ • Опыт работы с SIEM	• Знание законодательства в области ИБ • Знание всех процессов обеспечения ИБ • Опыт администрирования и сопровождения СЗИ • Понимание принципов работы SIEM, IPS/IDS, WAF • Написание программ на скриптовых языках • Знание методов форензики	• Опыт проведения аудитов ИБ • Уверенное знание законов и стандартов в области ИБ • Опыт построения и эксплуатации ИС • Опыт разработки технической документации • Глубокое понимание трендов в области ИБ • Управленческие навыки

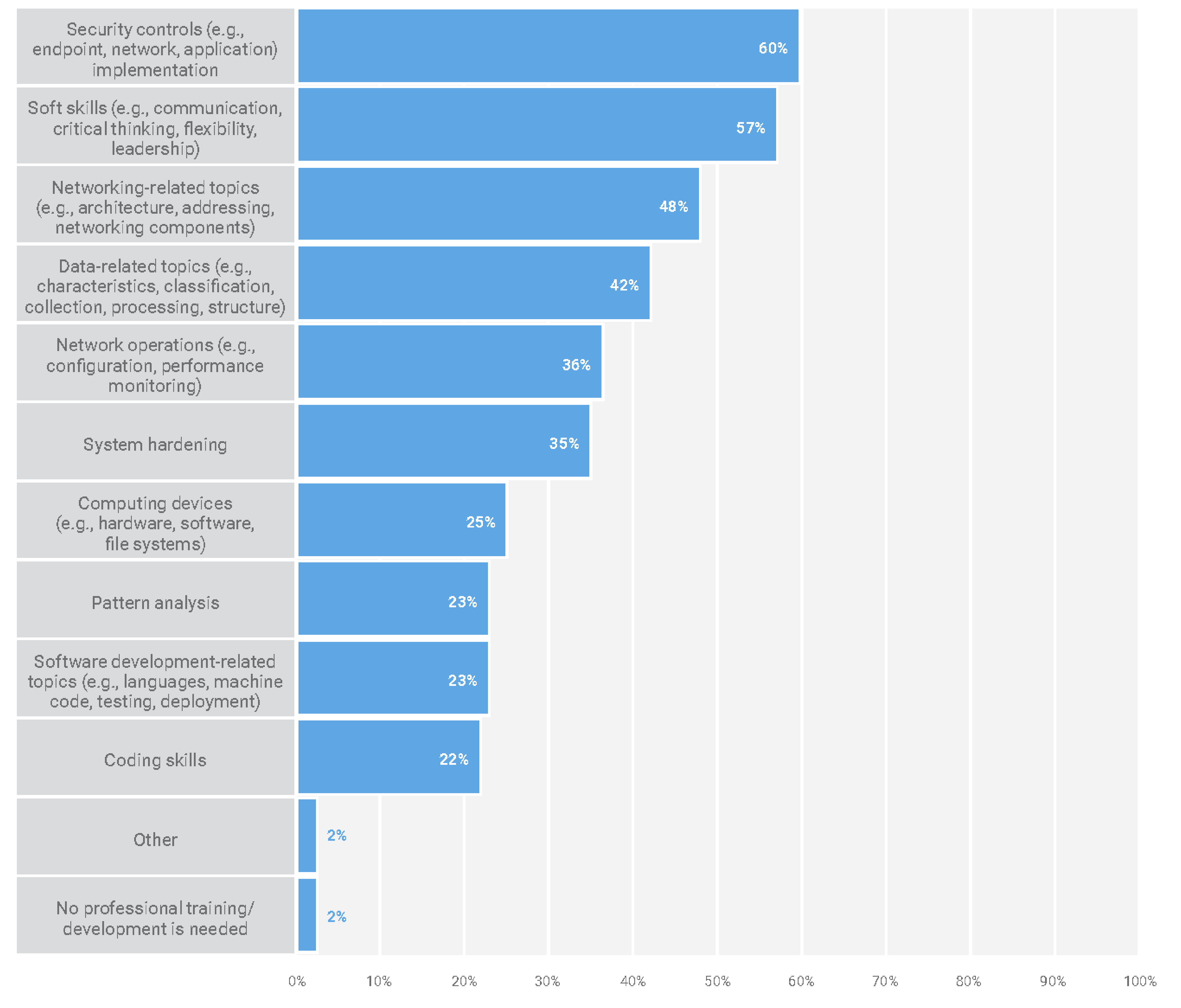
Источник: Код Подбора

Топ 5 хард скилов



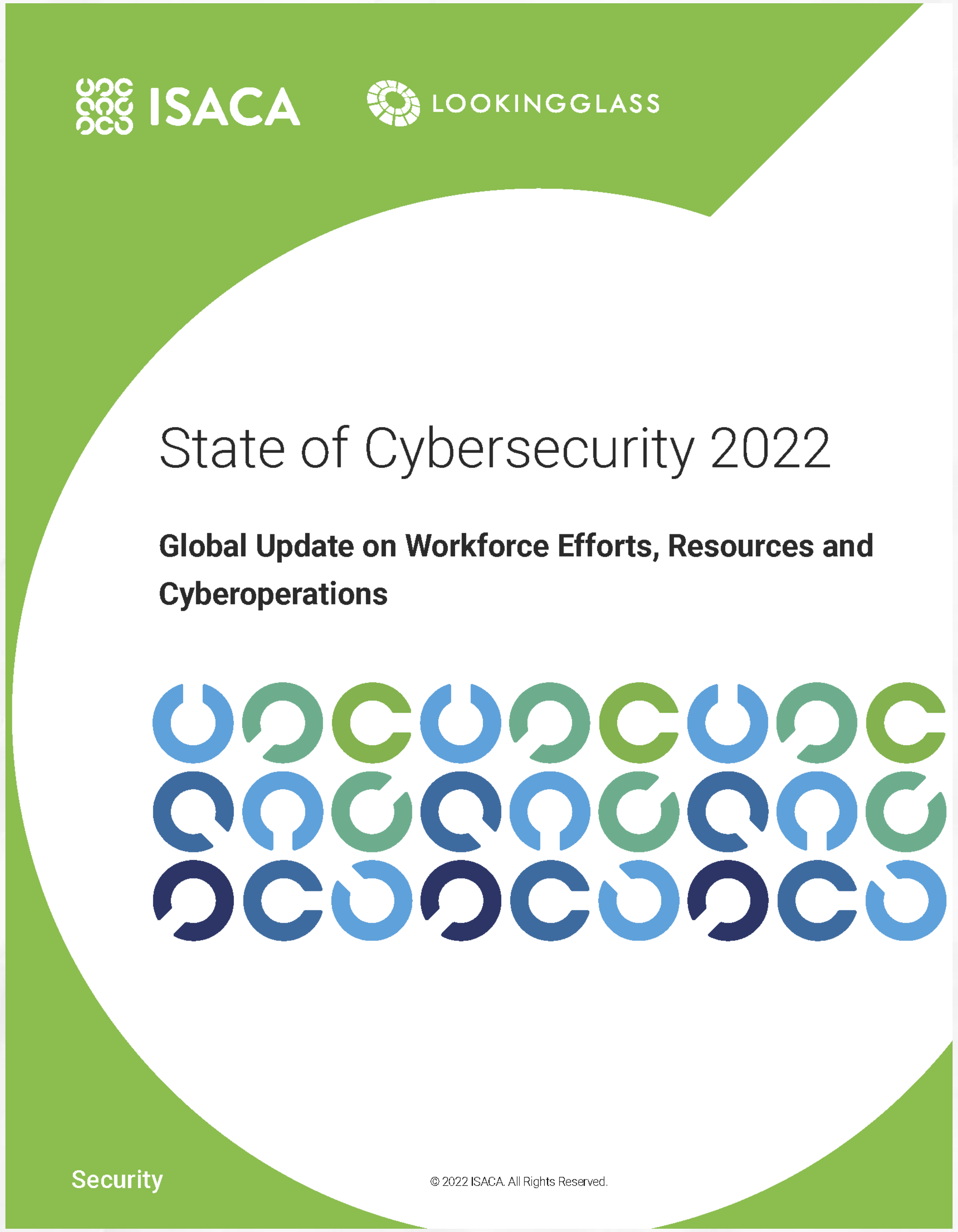
https://www.isaca.org/resources/infographics/state-of-cybersecurity-2022-infographic

Если опыт меньше 3 лет



https://www.isaca.org/resources/infographics/state-of-cybersecurity-2022-infographic

Рекомендации



ISACA LOOKINGGLASS

State of Cybersecurity 2022

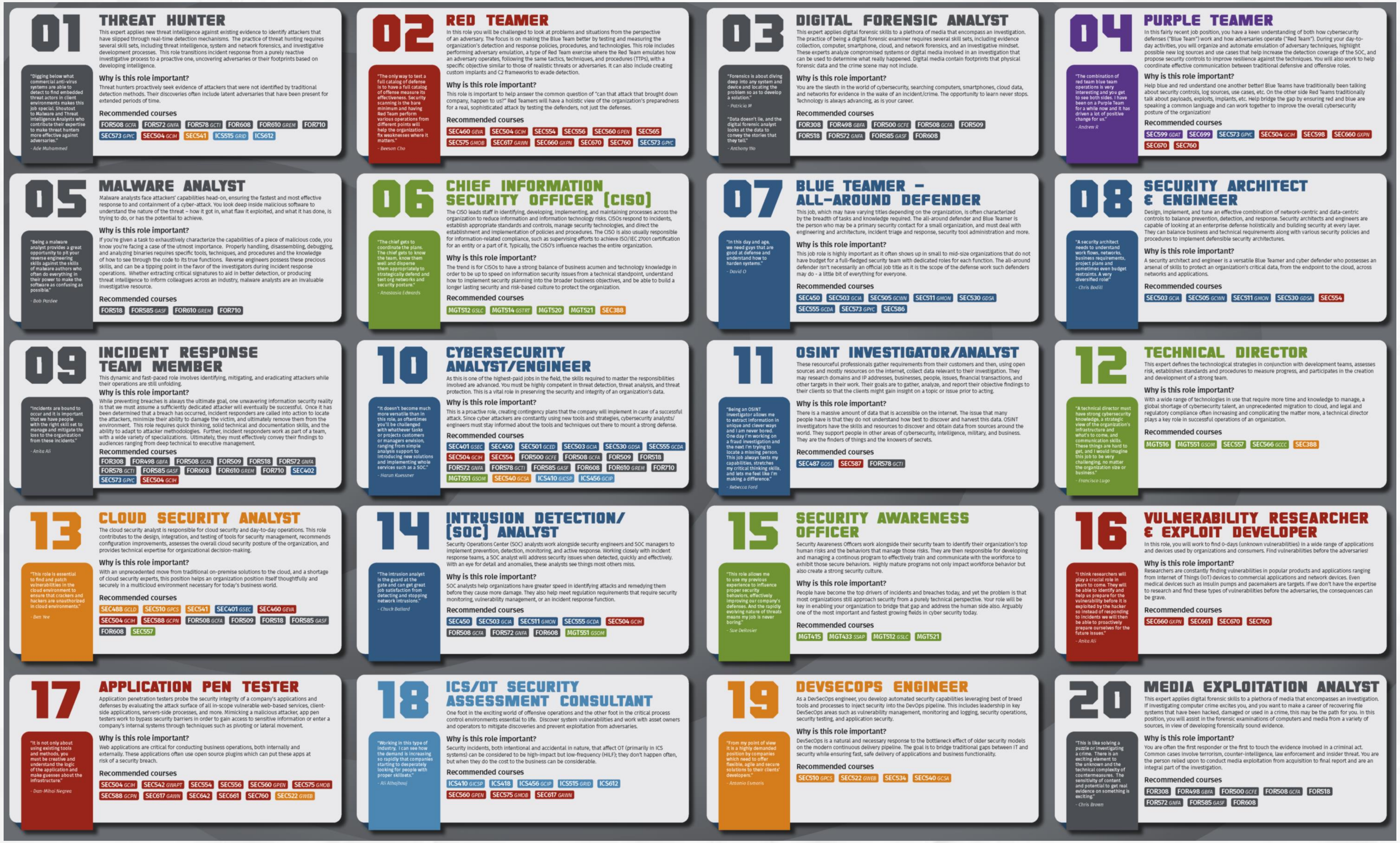
Global Update on Workforce Efforts, Resources and Cyberoperations

Security

© 2022 ISACA. All Rights Reserved.

https://www.isaca.org/resources/infographics/state-of-cybersecurity-2022-infographic

SANS «специализации»



01 THREAT HUNTER

This expert applies new threat intelligence against existing evidence to identify attackers that have slipped through real-time detection mechanisms. The practice of threat hunting requires several skill sets, including threat intelligence, system and network forensics, and investigative development processes. This role transitions incident response from a purely reactive investigative process to a proactive one, uncovering adversaries or their footprints based on developing intelligence.

> "Digging below what commercial anti-virus systems are able to detect to find embedded threat actors in client environments makes this job special. Shoutout to Malware and Threat Intelligence Analysts who contribute their expertise to make threat hunters more effective against adversaries."
>
> *- Ade Muhammed*

Why is this role important?

Threat hunters proactively seek evidence of attackers that were not identified by traditional detection methods. Their discoveries often include latent adversaries that have been present for extended periods of time.

Recommended courses

`FOR508 GCFA` `FOR572 GNFA` `FOR578 GCTI` `FOR608` `FOR610 GREM` `FOR710` `SEC573 GPYC` `SEC504 GCIH` `SEC541` `ICS515 GRID` `ICS612`

02 RED TEAMER

In this role you will be challenged to look at problems and situations from the perspective of an adversary. The focus is on making the Blue Team better by testing and measuring the organization's detection and response policies, procedures, and technologies. This role includes performing adversary emulation, a type of Red Team exercise where the Red Team emulates how an adversary operates, following the same tactics, techniques, and procedures (TTPs), with a specific objective similar to those of realistic threats or adversaries. It can also include creating custom implants and C2 frameworks to evade detection.

> "The only way to test a full catalog of defense is to have a full catalog of offense measure its effectiveness. Security scanning is the bare minimum and having Red Team perform various operations from different points will help the organization fix weaknesses where it matters."
>
> *- Beeson Cho*

Why is this role important?

This role is important to help answer the common question of "can that attack that brought down company, happen to us?" Red Teamers will have a holistic view of the organization's preparedness for a real, sophisticated attack by testing the defenders, not just the defenses.

Recommended courses

`SEC460 GEVA` `SEC504 GCIH` `SEC554` `SEC556` `SEC560 GPEN` `SEC565` `SEC575 GMOB` `SEC617 GAWN` `SEC660 GXPN` `SEC670` `SEC760` `SEC573 GPYC`

03 DIGITAL FORENSIC ANALYST

This expert applies digital forensic skills to a plethora of media that encompass an investigation. The practice of being a digital forensic examiner requires several skill sets, including evidence collection, computer, smartphone, cloud, and network forensics, and an investigative mindset. These experts analyze compromised systems or digital media involved in an investigation that can be used to determine what really happened. Digital media contain footprints that physical forensic data and the crime scene may not include.

> "Forensics is about diving deep into any system and device and locating the problem so as to develop a solution."
>
> *- Patricia M*
>
> "Data doesn't lie, and the digital forensic analyst looks at the data to convey the stories that they tell."
>
> *- Anthony Wo*

Why is this role important?

You are the sleuth in the world of cybersecurity, searching computers, smartphones, cloud data, and networks for evidence in the wake of an incident/crime. The opportunity to learn never stops. Technology is always advancing, as is your career.

Recommended courses

`FOR308` `FOR498 GBFA` `FOR500 GCFE` `FOR508 GCFA` `FOR509` `FOR518` `FOR572 GNFA` `FOR585 GASF` `FOR608`

04 PURPLE TEAMER

In this fairly recent job position, you have a keen understanding of both how cybersecurity defenses ("Blue Team") work and how adversaries operate ("Red Team"). During your day-to-day activities, you will organize and automate emulation of adversary techniques, highlight possible new log sources and use cases that help increase the detection coverage of the SOC, and propose security controls to improve resilience against the techniques. You will also work to help coordinate effective communication between traditional defensive and offensive roles.

> "The combination of red team blue team operations is very interesting and you get to see both sides. I have been on a Purple Team for a while now and it has driven a lot of positive change for us."
>
> *- Andrew R*

Why is this role important?

Help blue and red understand one another better! Blue Teams have traditionally been talking about security controls, log sources, use cases, etc. On the other side Red Teams traditionally talk about payloads, exploits, implants, etc. Help bridge the gap by ensuring red and blue are speaking a common language and can work together to improve the overall cybersecurity posture of the organization!

Recommended courses

`SEC599 GDAT` `SEC699` `SEC573 GPYC` `SEC504 GCIH` `SEC598` `SEC660 GXPN` `SEC670` `SEC760`

05 MALWARE ANALYST

Malware analysts face attackers' capabilities head-on, ensuring the fastest and most effective response to and containment of a cyber-attack. You look deep inside malicious software to understand the nature of the threat – how it got in, what flaw it exploited, and what it has done, is trying to do, or has the potential to achieve.

> "Being a malware analyst provides a great opportunity to pit your reverse engineering skills against the skills of malware authors who often do everything in their power to make the software as confusing as possible."
>
> *- Bob Pardee*

Why is this role important?

If you're given a task to exhaustively characterize the capabilities of a piece of malicious code, you know you're facing a case of the utmost importance. Properly handling, disassembling, debugging, and analyzing binaries requires specific tools, techniques, and procedures and the knowledge of how to see through the code to its true functions. Reverse engineers possess these precious skills, and can be a tipping point in the favor of the investigators during incident response operations. Whether extracting critical signatures to aid in better detection, or producing threat intelligence to inform colleagues across an industry, malware analysts are an invaluable investigative resource.

Recommended courses

`FOR518` `FOR585 GASF` `FOR610 GREM` `FOR710`

06 CHIEF INFORMATION SECURITY OFFICER [CISO]

The CISO leads staff in identifying, developing, implementing, and maintaining processes across the organization to reduce information and information technology risks. CISOs respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures. The CISO is also usually responsible for information-related compliance, such as supervising efforts to achieve ISO/IEC 27001 certification for an entity or a part of it. Typically, the CISO's influence reaches the entire organization.

> "The chief gets to coordinate the plans. The chief gets to know the team, know them well and disperse them appropriately to strategically defend and test org networks and security posture."
>
> *- Anastasia Edwards*

Why is this role important?

The trend is for CISOs to have a strong balance of business acumen and technology knowledge in order to be up to speed on information security issues from a technical standpoint, understand how to implement security planning into the broader business objectives, and be able to build a longer lasting security and risk-based culture to protect the organization.

Recommended courses

`MGT512 GSLC` `MGT514 GSTRT` `MGT520` `MGT521` `SEC388`

07 BLUE TEAMER – ALL-AROUND DEFENDER

This job, which may have varying titles depending on the organization, is often characterized by the breadth of tasks and knowledge required. The all-around defender and Blue Teamer is the person who may be a primary security contact for a small organization, and must deal with engineering and architecture, incident triage and response, security tool administration and more.

> "In this day and age, we need guys that are good at defense and understand how to harden systems."
>
> *- David O*

Why is this role important?

This job role is highly important as it often shows up in small to mid-size organizations that do not have budget for a full-fledged security team with dedicated roles for each function. The all-around defender isn't necessarily an official job title as it is the scope of the defense work such defenders may do - a little bit of everything for everyone.

Recommended courses

`SEC450` `SEC503 GCIA` `SEC505 GCWN` `SEC511 GMON` `SEC530 GDSA` `SEC555 GCDA` `SEC573 GPYC` `SEC586`

08 SECURITY ARCHITECT & ENGINEER

Design, implement, and tune an effective combination of network-centric and data-centric controls to balance prevention, detection, and response. Security architects and engineers are capable of looking at an enterprise defense holistically and building security at every layer. They can balance business and technical requirements along with various security policies and procedures to implement defensible security architectures.

> "A security architect needs to understand work flows, networks, business requirements, project plans and sometimes even budget restraints. A very diversified role!"
>
> *- Chris Bodill*

Why is this role important?

A security architect and engineer is a versatile Blue Teamer and cyber defender who possesses an arsenal of skills to protect an organization's critical data, from the endpoint to the cloud, across networks and applications.

Recommended courses

`SEC503 GCIA` `SEC505 GCWN` `SEC511 GMON` `SEC530 GDSA` `SEC554`

09 INCIDENT RESPONSE TEAM MEMBER

This dynamic and fast-paced role involves identifying, mitigating, and eradicating attackers while their operations are still unfolding.

> "Incidents are bound to occur and it is important that we have people with the right skill set to manage and mitigate the loss to the organization from these incidents."
>
> *- Anita Ali*

Why is this role important?

While preventing breaches is always the ultimate goal, one unwavering information security reality is that we must assume a sufficiently dedicated attacker will eventually be successful. Once it has been determined that a breach has occurred, incident responders are called into action to locate the attackers, minimize their ability to damage the victim, and ultimately remove them from the environment. This role requires quick thinking, solid technical and documentation skills, and the ability to adapt to attacker methodologies. Further, incident responders work as part of a team, with a wide variety of specializations. Ultimately, they must effectively convey their findings to audiences ranging from deep technical to executive management.

Recommended courses

`FOR308` `FOR498 GBFA` `FOR508 GCFA` `FOR509` `FOR518` `FOR572 GNFA` `FOR578 GCTI` `FOR585 GASF` `FOR608` `FOR610 GREM` `FOR710` `SEC402` `SEC573 GPYC` `SEC504 GCIH`

10 CYBERSECURITY ANALYST/ENGINEER

As this is one of the highest-paid jobs in the field, the skills required to master the responsibilities involved are advanced. You must be highly competent in threat detection, threat analysis, and threat protection. This is a vital role in preserving the security and integrity of an organization's data.

> "It doesn't become much more versatile than in this role, as oftentimes you'll be challenged with whathever tasks or projects customers or managers envision, ranging from simple analysis support to introducing new solutions and implementing whole services such as a SOC."
>
> *- Harun Kuessner*

Why is this role important?

This is a proactive role, creating contingency plans that the company will implement in case of a successful attack. Since cyber attackers are constantly using new tools and strategies, cybersecurity analysts/engineers must stay informed about the tools and techniques out there to mount a strong defense.

Recommended courses

`SEC401 GSEC` `SEC450` `SEC501 GCED` `SEC503 GCIA` `SEC530 GDSA` `SEC555 GCDA` `SEC504 GCIH` `SEC554` `FOR500 GCFE` `FOR508 GCFA` `FOR509` `FOR518` `FOR572 GNFA` `FOR578 GCTI` `FOR585 GASF` `FOR608` `FOR610 GREM` `FOR710` `MGT551 GSOM` `SEC540 GCSA` `ICS410 GICSP` `ICS456 GCIP`

11 OSINT INVESTIGATOR/ANALYST

These resourceful professionals gather requirements from their customers and then, using open sources and mostly resources on the internet, collect data relevant to their investigation. They may research domains and IP addresses, businesses, people, issues, financial transactions, and other targets in their work. Their goals are to gather, analyze, and report their objective findings to their clients so that the clients might gain insight on a topic or issue prior to acting.

> "Being an OSINT investigator allows me to extract information in unique and clever ways and I am never bored. One day I'm working on a fraud investigation and the next I'm trying to locate a missing person. This job always tests my capabilities, stretches my critical thinking skills, and lets me feel like I'm making a difference."
>
> *- Rebecca Ford*

Why is this role important?

There is a massive amount of data that is accessible on the internet. The issue that many people have is that they do not understand how best to discover and harvest this data. OSINT investigators have the skills and resources to discover and obtain data from sources around the world. They support people in other areas of cybersecurity, intelligence, military, and business. They are the finders of things and the knowers of secrets.

Recommended courses

`SEC487 GOSI` `SEC587` `FOR578 GCTI`

12 TECHNICAL DIRECTOR

This expert defines the technological strategies in conjunction with development teams, assesses risk, establishes standards and procedures to measure progress, and participates in the creation and development of a strong team.

> "A technical director must have strong cybersecurity knowledge, a strategic view of the organization's infrastructure and what's to come, and communication skills. These things are hard to get, and I would imagine this job to be very challenging, no matter the organization size or business."
>
> *- Francisco Lugo*

Why is this role important?

With a wide range of technologies in use that require more time and knowledge to manage, a global shortage of cybersecurity talent, an unprecedented migration to cloud, and legal and regulatory compliance often increasing and complicating the matter more, a technical director plays a key role in successful operations of an organization.

Recommended courses

`MGT516` `MGT551 GSOM` `SEC557` `SEC566 GCCC` `SEC388`

13 CLOUD SECURITY ANALYST

The cloud security analyst is responsible for cloud security and day-to-day operations. This role contributes to the design, integration, and testing of tools for security management, recommends configuration improvements, assesses the overall cloud security posture of the organization, and provides technical expertise for organizational decision-making.

> "This role is essential to find and patch vulnerabilities in the cloud environment to ensure that crackers and hackers are unauthorized in cloud environments."
>
> *- Ben Yee*

Why is this role important?

With an unprecedented move from traditional on-premise solutions to the cloud, and a shortage of cloud security experts, this position helps an organization position itself thoughtfully and securely in a multicloud environment necessary for today's business world.

Recommended courses

`SEC488 GCLD` `SEC510 GPCS` `SEC541` `SEC401 GSEC` `SEC460 GEVA` `SEC504 GCIH` `SEC588 GCPN` `FOR508 GCFA` `FOR509` `FOR518` `FOR585 GASF` `FOR608` `SEC557`

14 INTRUSION DETECTION/ [SOC] ANALYST

Security Operations Center (SOC) analysts work alongside security engineers and SOC managers to implement prevention, detection, monitoring, and active response. Working closely with incident response teams, a SOC analyst will address security issues when detected, quickly and effectively. With an eye for detail and anomalies, these analysts see things most others miss.

> "The intrusion analyst is the guard at the gate and can get great job satisfaction from detecting and stopping network intrusions."
>
> *- Chuck Ballard*

Why is this role important?

SOC analysts help organizations have greater speed in identifying attacks and remedying them before they cause more damage. They also help meet regulation requirements that require security monitoring, vulnerability management, or an incident response function.

Recommended courses

`SEC450` `SEC503 GCIA` `SEC511 GMON` `SEC555 GCDA` `SEC504 GCIH` `FOR508 GCFA` `FOR572 GNFA` `FOR608` `MGT551 GSOM`

15 SECURITY AWARENESS OFFICER

Security Awareness Officers work alongside their security team to identify their organization's top human risks and the behaviors that manage those risks. They are then responsible for developing and managing a continous program to effectively train and communicate with the workforce to exhibit those secure behaviors. Highly mature programs not only impact workforce behavior but also create a strong security culture.

> "This role allows me to use my previous experience to influence proper security behaviors, effectively improving our company's defenses. And the rapidly evolving nature of threats means my job is never boring."
>
> *- Sue DeRosier*

Why is this role important?

People have become the top drivers of incidents and breaches today, and yet the problem is that most organizations still approach security from a purely technical perspective. Your role will be key in enabling your organization to bridge that gap and address the human side also. Arguably one of the most important and fastest growing fields in cyber security today.

Recommended courses

`MGT415` `MGT433 SSAP` `MGT512 GSLC` `MGT521`

16 VULNERABILITY RESEARCHER & EXPLOIT DEVELOPER

In this role, you will work to find 0-days (unknown vulnerabilities) in a wide range of applications and devices used by organizations and consumers. Find vulnerabilities before the adversaries!

> "I think researchers will play a crucial role in years to come. They will be able to identify and help us prepare for the vulnerability before it is exploited by the hacker so instead of responding to incidents we will then be able to proactively prepare ourselves for the future issues."
>
> *- Anita Ali*

Why is this role important?

Researchers are constantly finding vulnerabilities in popular products and applications ranging from Internet of Things (IoT) devices to commercial applications and network devices. Even medical devices such as insulin pumps and pacemakers are targets. If we don't have the expertise to research and find these types of vulnerabilities before the adversaries, the consequences can be grave.

Recommended courses

`SEC660 GXPN` `SEC661` `SEC670` `SEC760`

17 APPLICATION PEN TESTER

Application penetration testers probe the security integrity of a company's applications and defenses by evaluating the attack surface of all in-scope vulnerable web-based services, client-side applications, servers-side processes, and more. Mimicking a malicious attacker, app pen testers work to bypass security barriers in order to gain access to sensitive information or enter a company's internal systems through techniques such as pivoting or lateral movement.

> "It is not only about using existing tools and methods, you must be creative and understand the logic of the application and make guesses about the infrastructure."
>
> *- Dan-Mihai Negrea*

Why is this role important?

Web applications are critical for conducting business operations, both internally and externally. These applications often use open source plugins which can put these apps at risk of a security breach.

Recommended courses

`SEC504 GCIH` `SEC542 GWAPT` `SEC554` `SEC556` `SEC560 GPEN` `SEC575 GMOB` `SEC588 GCPN` `SEC617 GAWN` `SEC642` `SEC661` `SEC760` `SEC522 GWEB`

18 ICS/OT SECURITY ASSESSMENT CONSULTANT

One foot in the exciting world of offensive operations and the other foot in the critical process control environments essential to life. Discover system vulnerabilities and work with asset owners and operators to mitigate discoveries and prevent exploitation from adversaries.

> "Working in this type of industry, I can see how the demand is increasing so rapidly that companies starting to desperately looking for people with proper skillsets."
>
> *- Ali Alhajhouj*

Why is this role important?

Security incidents, both intentional and accidental in nature, that affect OT (primarily in ICS systems) can be considered to be high-impact but low-frequency (HILF); they don't happen often, but when they do the cost to the business can be considerable.

Recommended courses

`ICS410 GICSP` `ICS418` `ICS456 GCIP` `ICS515 GRID` `ICS612` `SEC560 GPEN` `SEC575 GMOB` `SEC617 GAWN`

19 DEVSECOPS ENGINEER

As a DevSecOps engineer, you develop automated security capabilities leveraging best of breed tools and processes to inject security into the DevOps pipeline. This includes leadership in key DevSecOps areas such as vulnerability management, monitoring and logging, security operations, security testing, and application security.

> "From my point of view it is a highly demanded position by companies which need to offer flexible, agile and secure solutions to their clients' developers."
>
> *- Antonio Esmoris*

Why is this role important?

DevSecOps is a natural and necessary response to the bottleneck effect of older security models on the modern continuous delivery pipeline. The goal is to bridge traditional gaps between IT and security while ensuring fast, safe delivery of applications and business functionality.

Recommended courses

`SEC510 GPCS` `SEC522 GWEB` `SEC534` `SEC540 GCSA`

20 MEDIA EXPLOITATION ANALYST

This expert applies digital forensic skills to a plethora of media that encompasses an investigation. If investigating computer crime excites you, and you want to make a career of recovering file systems that have been hacked, damaged or used in a crime, this may be the path for you. In this position, you will assist in the forensic examinations of computers and media from a variety of sources, in view of developing forensically sound evidence.

> "This is like solving a puzzle or investigating a crime. There is an exciting element to the unknown and the technical complexity of countermeasures. The sensitivity of content and potential to get real evidence on something is exciting."
>
> *- Chris Brown*

Why is this role important?

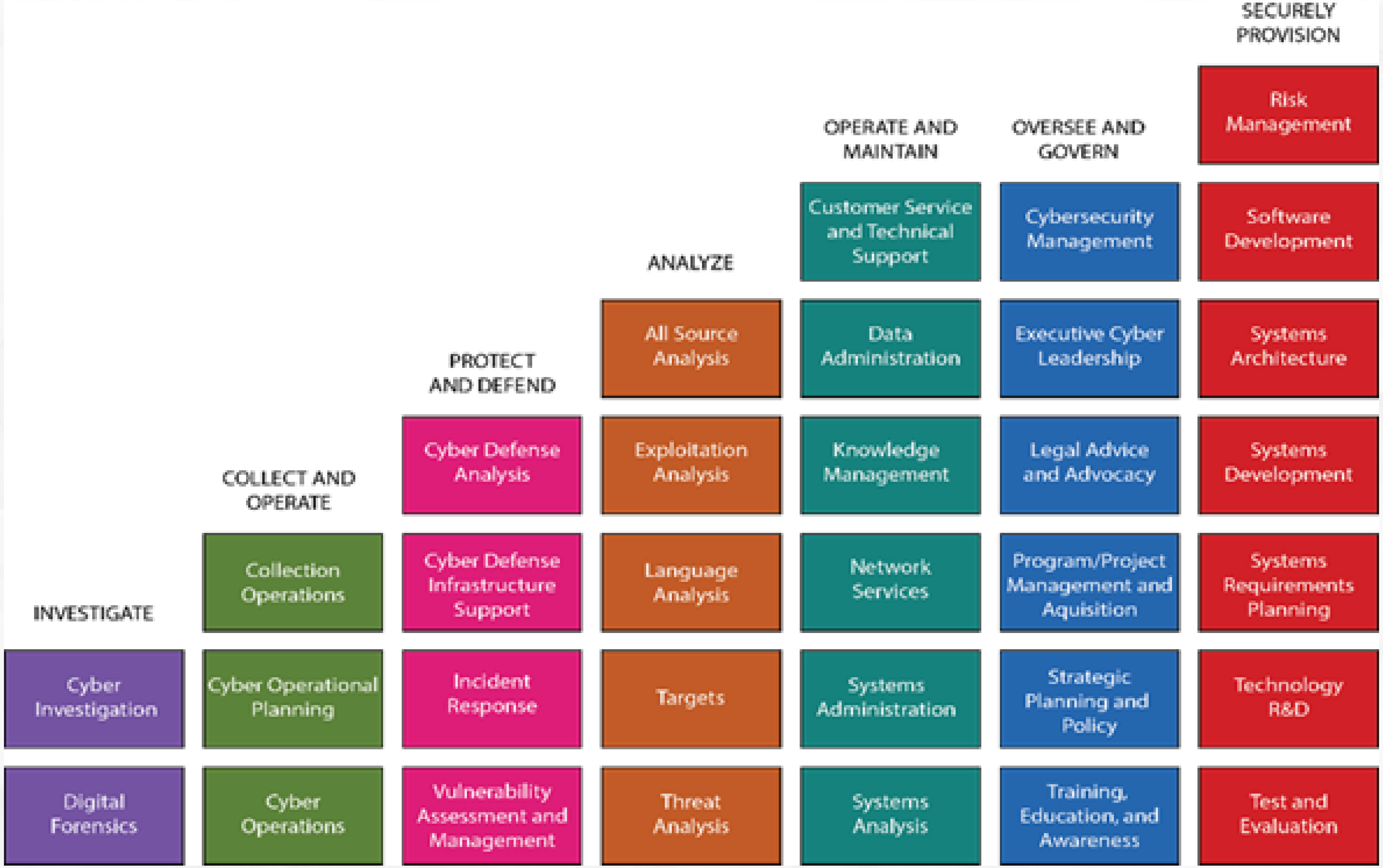
You are often the first responder or the first to touch the evidence involved in a criminal act. Common cases involve terrorism, counter-intelligence, law enforcement and insider threat. You are the person relied upon to conduct media exploitation from acquisition to final report and are an integral part of the investigation.

Recommended courses

`FOR308` `FOR498 GBFA` `FOR500 GCFE` `FOR508 GCFA` `FOR518` `FOR572 GNFA` `FOR585 GASF` `FOR608`

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt6b6beaf55a366a55/Poster_Coolest-Careers_v0322.pdf

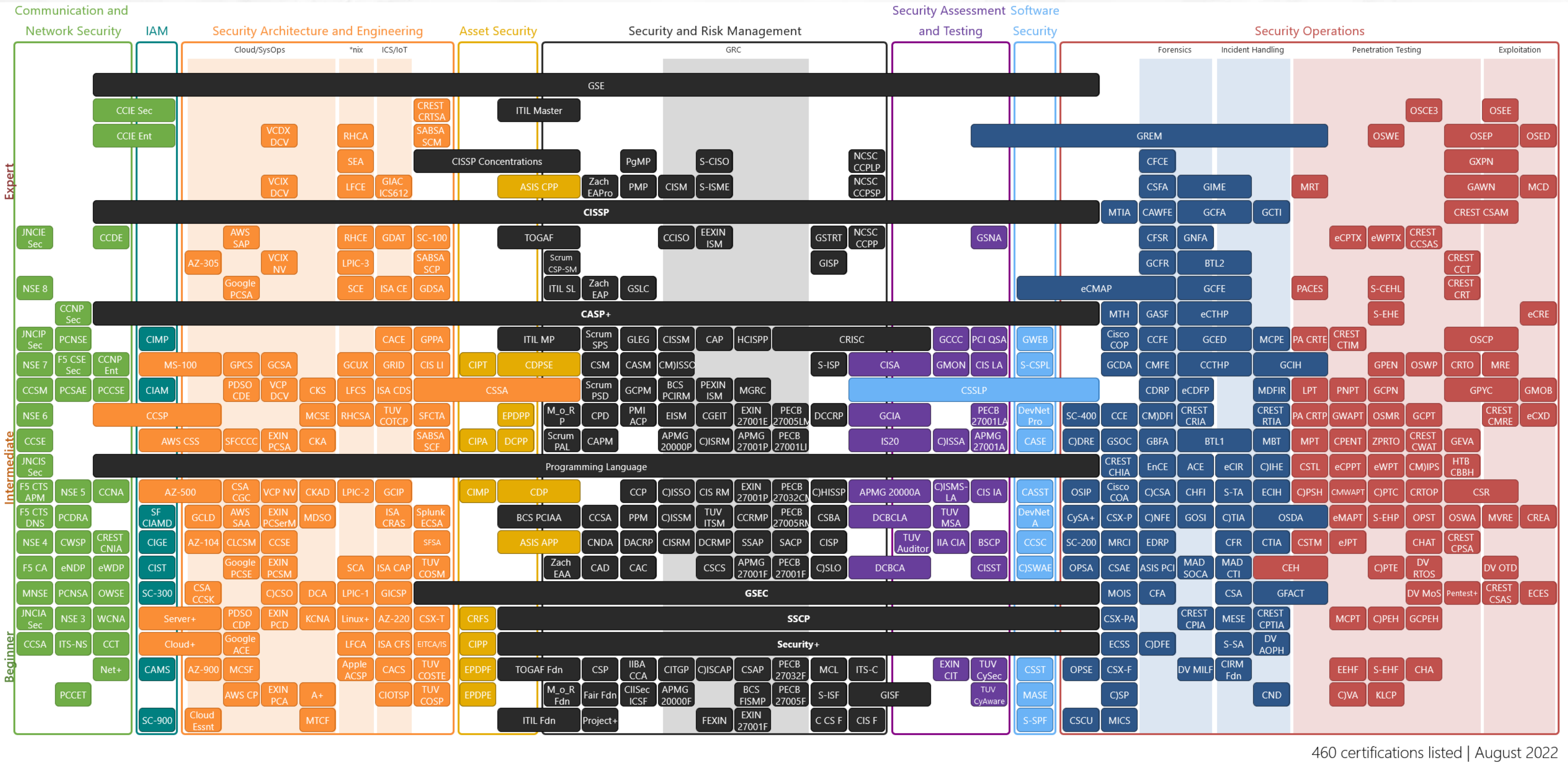
Зрелый NIST



INVESTIGATE	COLLECT AND OPERATE	PROTECT AND DEFEND	ANALYZE	OPERATE AND MAINTAIN	OVERSEE AND GOVERN	SECURELY PROVISION
						Risk Management
				Customer Service and Technical Support	Cybersecurity Management	Software Development
			All Source Analysis	Data Administration	Executive Cyber Leadership	Systems Architecture
		Cyber Defense Analysis	Exploitation Analysis	Knowledge Management	Legal Advice and Advocacy	Systems Development
	Collection Operations	Cyber Defense Infrastructure Support	Language Analysis	Network Services	Program/Project Management and Aquisition	Systems Requirements Planning
Cyber Investigation	Cyber Operational Planning	Incident Response	Targets	Systems Administration	Strategic Planning and Policy	Technology R&D
Digital Forensics	Cyber Operations	Vulnerability Assessment and Management	Threat Analysis	Systems Analysis	Training, Education, and Awareness	Test and Evaluation

https://niccs.cisa.gov/workforce-development/nice-framework

Сертификации



Communication and Network Security | IAM | Security Architecture and Engineering | Asset Security | Security and Risk Management | Security Assessment and Testing | Software Security | Security Operations

Cloud/SysOps | *nix | ICS/IoT | GRC | Forensics | Incident Handling | Penetration Testing | Exploitation

Expert

GSE

CCIE Sec, CREST CRTSA, ITIL Master, OSCE3, OSEE

CCIE Ent, VCDX DCV, RHCA, SABSA SCM, GREM, OSWE, OSEP, OSED

SEA, CISSP Concentrations, PgMP, S-CISO, NCSC CCPLP, CFCE, GXPN

VCIX DCV, LFCE, GIAC ICS612, ASIS CPP, Zach EAPro, PMP, CISM, S-ISME, NCSC CCPSP, CSFA, GIME, MRT, GAWN, MCD

CISSP, MTIA, CAWFE, GCFA, GCTI, CREST CSAM

JNCIE Sec, CCDE, AWS SAP, RHCE, GDAT, SC-100, TOGAF, CCISO, EEXIN ISM, GSTRT, NCSC CCP, GSNA, CFSR, GNFA, eCPTX, eWPTX, CREST CCSAS

AZ-305, VCIX NV, LPIC-3, SABSA SCP, Scrum CSP-SM, GISP, GCFR, BTL2, CREST CCT

NSE 8, Google PCSA, SCE, ISA CE, GDSA, ITIL SL, Zach EAP, GSLC, eCMAP, GCFE, PACES, S-CEHL, CREST CRT

Intermediate

CCNP Sec, CASP+, MTH, GASF, eCTHP, S-EHE, eCRE

JNCIP Sec, PCNSE, CIMP, CACE, GPPA, ITIL MP, Scrum SPS, GLEG, CISSM, CAP, HCISPP, CRISC, GCCC, PCI QSA, GWEB, Cisco COP, CCFE, GCED, MCPE, PA CRTE, CREST CTIM, OSCP

NSE 7, F5 CSE Sec, CCNP Ent, MS-100, GPCS, GCSA, GCUX, GRID, CIS LI, CIPT, CDPSE, CSM, CASM, C)ISSO, S-ISP, CISA, GMON, CIS LA, S-CSPL, GCDA, CMFE, CCTHP, GCIH, GPEN, OSWP, CRTO, MRE

CCSM, PCSAE, PCCSE, CIAM, PDSO CDE, VCP DCV, CKS, LFCS, ISA CDS, CSSA, Scrum PSD, GCPM, BCS PCIRM, PEXIN ISM, MGRC, CSSLP, CDRP, eCDFP, MDFIR, LPT, PNPT, GCPN, GPYC, GMOB

NSE 6, CCSP, MCSE, RHCSA, TUV COTCP, SFCTA, EPDPP, M_o_R P, CPD, PMI ACP, EISM, CGEIT, EXIN 27001E, PECB 27005LM, DCCRP, GCIA, PECB 27001LA, DevNet Pro, SC-400, CCE, CM)DFI, CREST CRIA, CREST RTIA, PA CRTP, GWAPT, OSMR, GCPT, CREST CMRE, eCXD

CCSE, AWS CSS, SFCCCC, EXIN PCSA, CKA, SABSA SCF, CIPA, DCPP, Scrum PAL, CAPM, APMG 20000P, C)ISRM, APMG 27001P, PECB 27001LI, IS20, C)ISSA, APMG 27001A, CASE, C)DRE, GSOC, GBFA, BTL1, MBT, MPT, CPENT, ZPRTO, CREST CWAT, GEVA

JNCIS Sec, Programming Language, CREST CHIA, EnCE, ACE, eCIR, C)IHE, CSTL, eCPPT, eWPT, CM)IPS, HTB CBBH

F5 CTS APM, NSE 5, CCNA, AZ-500, CSA CGC, VCP NV, CKAD, LPIC-2, GCIP, CIMP, CDP, CCP, C)ISSO, CIS RM, EXIN 27001P, PECB 27032CM, C)HISSP, APMG 20000A, C)ISMS-LA, CIS IA, CASST, OSIP, Cisco COA, C)CSA, CHFI, S-TA, ECIH, C)PSH, CMWAPT, C)PTC, CRTOP, CSR

F5 CTS DNS, PCDRA, SF CIAMD, GCLD, AWS SAA, EXIN PCSerM, MDSO, ISA CRAS, Splunk ECSA, BCS PCIAA, CCSA, PPM, C)ISSM, TUV ITSM, CCRMP, PECB 27005RM, CSBA, DCBCLA, TUV MSA, DevNet A, CySA+, CSX-P, C)NFE, GOSI, C)TIA, OSDA, eMAPT, S-EHP, OPST, OSWA, MVRE, CREA

NSE 4, CWSP, CREST CNIA, CIGE, AZ-104, CLCSM, CCSE, SFSA, ASIS APP, CNDA, DACRP, CISRM, DCRMP, SSAP, SACP, CISP, TUV Auditor, IIA CIA, BSCP, CCSC, SC-200, MRCI, EDRP, CFR, CTIA, CSTM, eJPT, CHAT, CREST CPSA

F5 CA, eNDP, eWDP, CIST, Google PCSE, EXIN PCSM, SCA, ISA CAP, TUV COSM, Zach EAA, CAD, CAC, CSCS, APMG 27001F, PECB 27001F, C)SLO, DCBCA, CISST, C)SWAE, OPSA, CSAE, ASIS PCI, MAD SOCA, MAD CTI, CEH, C)PTE, DV RTOS, DV OTD

Beginner

MNSE, PCNSA, OWSE, SC-300, CSA CCSK, C)CSO, DCA, LPIC-1, GICSP, GSEC, MOIS, CFA, CSA, GFACT, DV MoS, Pentest+, CREST CSAS, ECES

JNCIA Sec, NSE 3, WCNA, Server+, PDSO CDP, EXIN PCD, KCNA, Linux+, AZ-220, CSX-T, CRFS, SSCP, CSX-PA, CREST CPIA, MESE, CREST CPTIA, MCPT, C)PEH, GCPEH

CCSA, ITS-NS, CCT, Cloud+, Google ACE, LFCA, ISA CFS, EITCA/IS, CIPP, Security+, ECSS, C)DFE, S-SA, DV AOPH

Net+, CAMS, AZ-900, MCSF, Apple ACSP, CACS, TUV COSTE, EPDPF, TOGAF Fdn, CSP, IIBA CCA, CITGP, C)ISCAP, CSAP, PECB 27032F, MCL, ITS-C, EXIN CIT, TUV CySec, CSST, OPSE, CSX-F, DV MILF, CIRM Fdn, EEHF, S-EHF, CHA

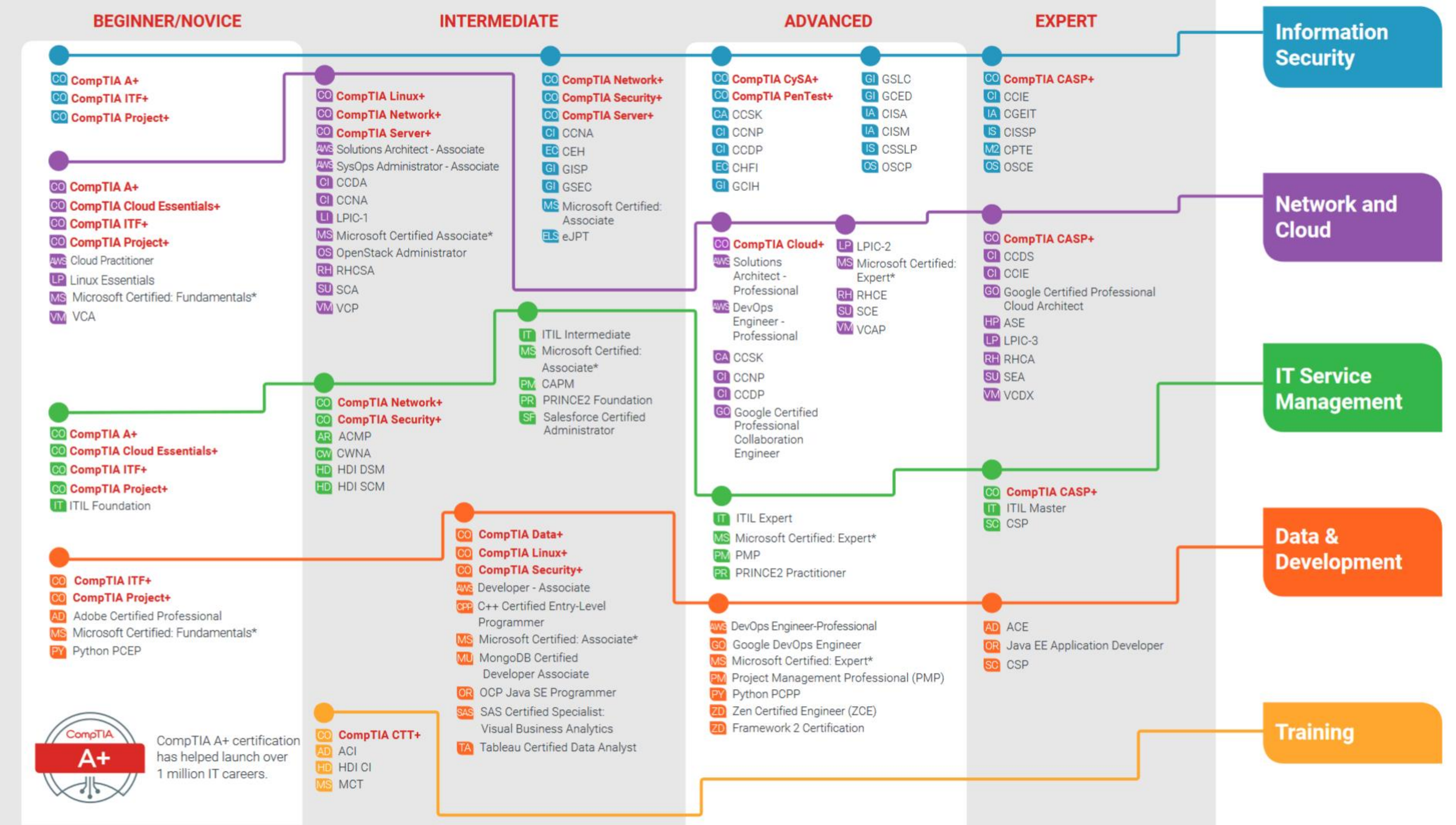
PCCET, AWS CP, EXIN PCA, A+, CIOTSP, TUV COSP, EPDPE, M_o_R Fdn, Fair Fdn, CIISec ICSF, APMG 20000F, BCS FISMP, PECB 27005F, S-ISF, GISF, TUV CyAware, MASE, C)SP, CND, C)VA, KLCP

SC-900, Cloud Essnt, MTCF, ITIL Fdn, Project+, FEXIN, EXIN 27001F, C CS F, CIS F, S-SPF, CSCU, MICS

460 certifications listed | August 2022

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

Еще один вариант



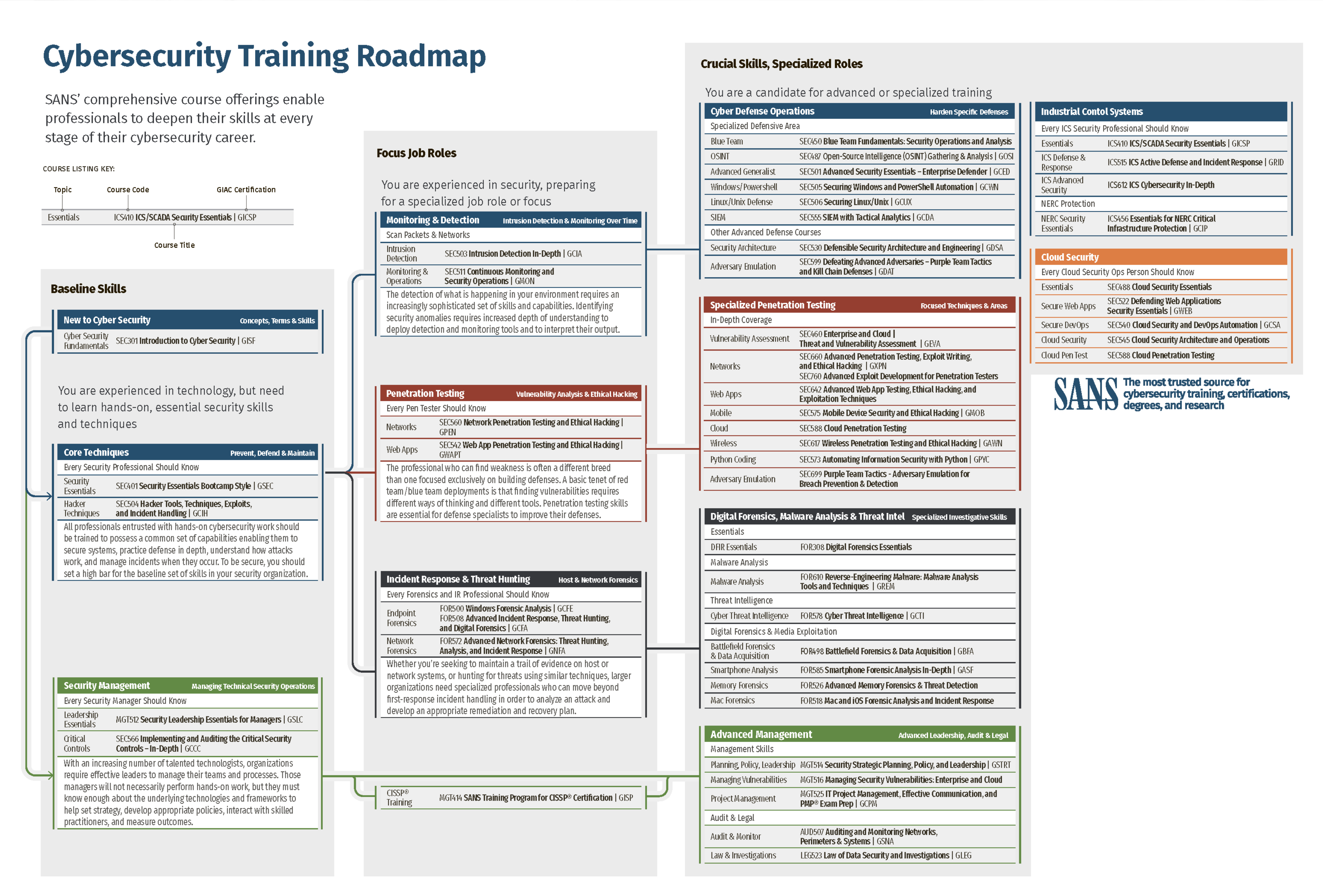
BEGINNER/NOVICE	INTERMEDIATE	ADVANCED	EXPERT	
CO CompTIA A+ CO CompTIA ITF+ CO CompTIA Project+	CO CompTIA Network+ CO CompTIA Security+ CO CompTIA Server+ CI CCNA EC CEH GI GISP GI GSEC MS Microsoft Certified: Associate ELS eJPT	CO CompTIA CySA+ CO CompTIA PenTest+ CA CCSK CI CCNP CI CCDP EC CHFI GI GCIH GI GSLC GI GCED IA CISA IA CISM IS CSSLP OS OSCP	CO CompTIA CASP+ CI CCIE IA CGEIT IS CISSP M2 CPTE OS OSCE	Information Security
CO CompTIA A+ CO CompTIA Cloud Essentials+ CO CompTIA ITF+ CO CompTIA Project+ AWS Cloud Practitioner LP Linux Essentials MS Microsoft Certified: Fundamentals* VM VCA	CO CompTIA Linux+ CO CompTIA Network+ CO CompTIA Server+ AWS Solutions Architect - Associate AWS SysOps Administrator - Associate CI CCDA CI CCNA LI LPIC-1 MS Microsoft Certified Associate* OS OpenStack Administrator RH RHCSA SU SCA VM VCP	CO CompTIA Cloud+ AWS Solutions Architect - Professional AWS DevOps Engineer - Professional CA CCSK CI CCNP CI CCDP GO Google Certified Professional Collaboration Engineer LP LPIC-2 MS Microsoft Certified: Expert* RH RHCE SU SCE VM VCAP	CO CompTIA CASP+ CI CCDS CI CCIE GO Google Certified Professional Cloud Architect HP ASE LP LPIC-3 RH RHCA SU SEA VM VCDX	Network and Cloud
CO CompTIA A+ CO CompTIA Cloud Essentials+ CO CompTIA ITF+ CO CompTIA Project+ IT ITIL Foundation	CO CompTIA Network+ CO CompTIA Security+ AR ACMP CW CWNA HD HDI DSM HD HDI SCM IT ITIL Intermediate MS Microsoft Certified: Associate* PM CAPM PR PRINCE2 Foundation SF Salesforce Certified Administrator	IT ITIL Expert MS Microsoft Certified: Expert* PM PMP PR PRINCE2 Practitioner	CO CompTIA CASP+ IT ITIL Master SC CSP	IT Service Management
CO CompTIA ITF+ CO CompTIA Project+ AD Adobe Certified Professional MS Microsoft Certified: Fundamentals* PY Python PCEP	CO CompTIA Data+ CO CompTIA Linux+ CO CompTIA Security+ AWS Developer - Associate CPP C++ Certified Entry-Level Programmer MS Microsoft Certified: Associate* MU MongoDB Certified Developer Associate OR OCP Java SE Programmer SAS SAS Certified Specialist: Visual Business Analytics TA Tableau Certified Data Analyst	AWS DevOps Engineer-Professional GO Google DevOps Engineer MS Microsoft Certified: Expert* PM Project Management Professional (PMP) PY Python PCPP ZD Zen Certified Engineer (ZCE) ZD Framework 2 Certification	AD ACE OR Java EE Application Developer SC CSP	Data & Development
	CO CompTIA CTT+ AD ACI HD HDI CI MS MCT			Training

CompTIA A+

CompTIA A+ certification has helped launch over 1 million IT careers.

https://partners.comptia.org/docs/default-source/resources/08314-it-certification-roadmap-nov2020-update-8-5x11-online

Еще один вариант



Cybersecurity Training Roadmap

SANS’ comprehensive course offerings enable professionals to deepen their skills at every stage of their cybersecurity career.

COURSE LISTING KEY:

Topic — Course Code — GIAC Certification

Essentials ICS410 **ICS/SCADA Security Essentials** | GICSP

Course Title

Baseline Skills

New to Cyber Security	Concepts, Terms & Skills
Cyber Security Fundamentals	SEC301 **Introduction to Cyber Security** | GISF

You are experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Techniques	Prevent, Defend & Maintain
Every Security Professional Should Know	
Security Essentials	SEC401 **Security Essentials Bootcamp Style** | GSEC
Hacker Techniques	SEC504 **Hacker Tools, Techniques, Exploits, and Incident Handling** | GCIH

All professionals entrusted with hands-on cybersecurity work should be trained to possess a common set of capabilities enabling them to secure systems, practice defense in depth, understand how attacks work, and manage incidents when they occur. To be secure, you should set a high bar for the baseline set of skills in your security organization.

Security Management	Managing Technical Security Operations
Every Security Manager Should Know	
Leadership Essentials	MGT512 **Security Leadership Essentials for Managers** | GSLC
Critical Controls	SEC566 **Implementing and Auditing the Critical Security Controls – In-Depth** | GCCC

With an increasing number of talented technologists, organizations require effective leaders to manage their teams and processes. Those managers will not necessarily perform hands-on work, but they must know enough about the underlying technologies and frameworks to help set strategy, develop appropriate policies, interact with skilled practitioners, and measure outcomes.

Focus Job Roles

You are experienced in security, preparing for a specialized job role or focus

Monitoring & Detection	Intrusion Detection & Monitoring Over Time
Scan Packets & Networks	
Intrusion Detection	SEC503 **Intrusion Detection In-Depth** | GCIA
Monitoring & Operations	SEC511 **Continuous Monitoring and Security Operations** | GMON

The detection of what is happening in your environment requires an increasingly sophisticated set of skills and capabilities. Identifying security anomalies requires increased depth of understanding to deploy detection and monitoring tools and to interpret their output.

Penetration Testing	Vulnerability Analysis & Ethical Hacking
Every Pen Tester Should Know	
Networks	SEC560 **Network Penetration Testing and Ethical Hacking** | GPEN
Web Apps	SEC542 **Web App Penetration Testing and Ethical Hacking** | GWAPT

The professional who can find weakness is often a different breed than one focused exclusively on building defenses. A basic tenet of red team/blue team deployments is that finding vulnerabilities requires different ways of thinking and different tools. Penetration testing skills are essential for defense specialists to improve their defenses.

Incident Response & Threat Hunting	Host & Network Forensics
Every Forensics and IR Professional Should Know	
Endpoint Forensics	FOR500 **Windows Forensic Analysis** | GCFE FOR508 **Advanced Incident Response, Threat Hunting, and Digital Forensics** | GCFA
Network Forensics	FOR572 **Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response** | GNFA

Whether you’re seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

CISSP® Training	MGT414 **SANS Training Program for CISSP® Certification** | GISP

Crucial Skills, Specialized Roles

You are a candidate for advanced or specialized training

Cyber Defense Operations	Harden Specific Defenses
Specialized Defensive Area	
Blue Team	SEC450 **Blue Team Fundamentals: Security Operations and Analysis**
OSINT	SEC487 Open-Source Intelligence (OSINT) Gathering & Analysis | GOSI
Advanced Generalist	SEC501 **Advanced Security Essentials – Enterprise Defender** | GCED
Windows/Powershell	SEC505 **Securing Windows and PowerShell Automation** | GCWN
Linux/Unix Defense	SEC506 **Securing Linux/Unix** | GCUX
SIEM	SEC555 **SIEM with Tactical Analytics** | GCDA
Other Advanced Defense Courses	
Security Architecture	SEC530 **Defensible Security Architecture and Engineering** | GDSA
Adversary Emulation	SEC599 **Defeating Advanced Adversaries – Purple Team Tactics and Kill Chain Defenses** | GDAT

Specialized Penetration Testing	Focused Techniques & Areas
In-Depth Coverage	
Vulnerability Assessment	SEC460 **Enterprise and Cloud | Threat and Vulnerability Assessment** | GEVA
Networks	SEC660 **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** | GXPN SEC760 **Advanced Exploit Development for Penetration Testers**
Web Apps	SEC642 **Advanced Web App Testing, Ethical Hacking, and Exploitation Techniques**
Mobile	SEC575 **Mobile Device Security and Ethical Hacking** | GMOB
Cloud	SEC588 **Cloud Penetration Testing**
Wireless	SEC617 **Wireless Penetration Testing and Ethical Hacking** | GAWN
Python Coding	SEC573 **Automating Information Security with Python** | GPYC
Adversary Emulation	SEC699 **Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection**

Digital Forensics, Malware Analysis & Threat Intel	Specialized Investigative Skills
Essentials	
DFIR Essentials	FOR308 **Digital Forensics Essentials**
Malware Analysis	
Malware Analysis	FOR610 **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** | GREM
Threat Intelligence	
Cyber Threat Intelligence	FOR578 **Cyber Threat Intelligence** | GCTI
Digital Forensics & Media Exploitation	
Battlefield Forensics & Data Acquisition	FOR498 **Battlefield Forensics & Data Acquisition** | GBFA
Smartphone Analysis	FOR585 **Smartphone Forensic Analysis In-Depth** | GASF
Memory Forensics	FOR526 **Advanced Memory Forensics & Threat Detection**
Mac Forensics	FOR518 **Mac and iOS Forensic Analysis and Incident Response**

Advanced Management	Advanced Leadership, Audit & Legal
Management Skills	
Planning, Policy, Leadership	MGT514 **Security Strategic Planning, Policy, and Leadership** | GSTRT
Managing Vulnerabilities	MGT516 **Managing Security Vulnerabilities: Enterprise and Cloud**
Project Management	MGT525 **IT Project Management, Effective Communication, and PMP® Exam Prep** | GCPM
Audit & Legal	
Audit & Monitor	AUD507 **Auditing and Monitoring Networks, Perimeters & Systems** | GSNA
Law & Investigations	LEG523 **Law of Data Security and Investigations** | GLEG

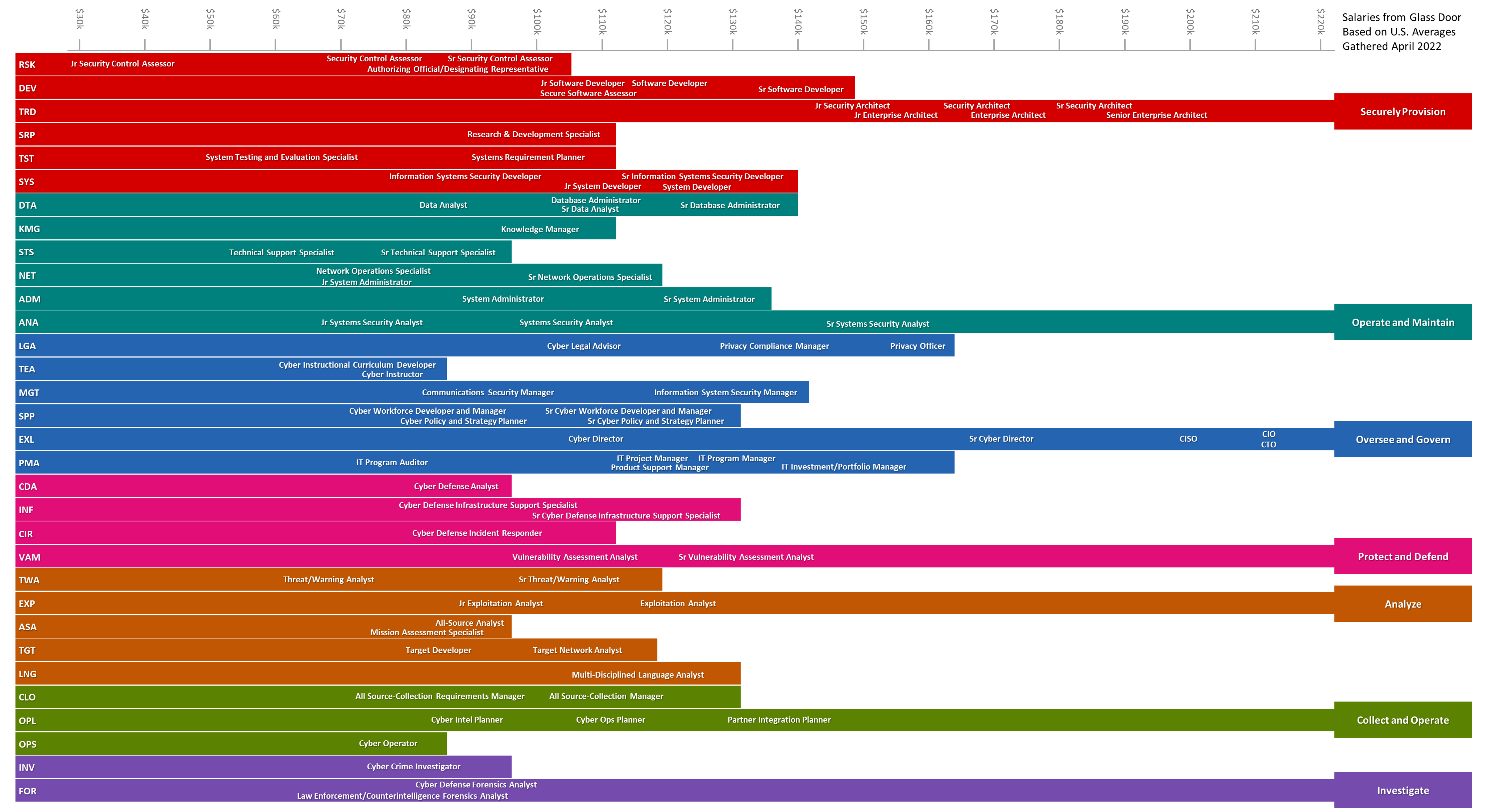
Industrial Contol Systems	
Every ICS Security Professional Should Know	
Essentials	ICS410 **ICS/SCADA Security Essentials** | GICSP
ICS Defense & Response	ICS515 **ICS Active Defense and Incident Response** | GRID
ICS Advanced Security	ICS612 **ICS Cybersecurity In-Depth**
NERC Protection	
NERC Security Essentials	ICS456 **Essentials for NERC Critical Infrastructure Protection** | GCIP

Cloud Security	
Every Cloud Security Ops Person Should Know	
Essentials	SEC488 **Cloud Security Essentials**
Secure Web Apps	SEC522 **Defending Web Applications Security Essentials** | GWEB
Secure DevOps	SEC540 **Cloud Security and DevOps Automation** | GCSA
Cloud Security	SEC545 **Cloud Security Architecture and Operations**
Cloud Pen Test	SEC588 **Cloud Penetration Testing**

SANS The most trusted source for cybersecurity training, certifications, degrees, and research

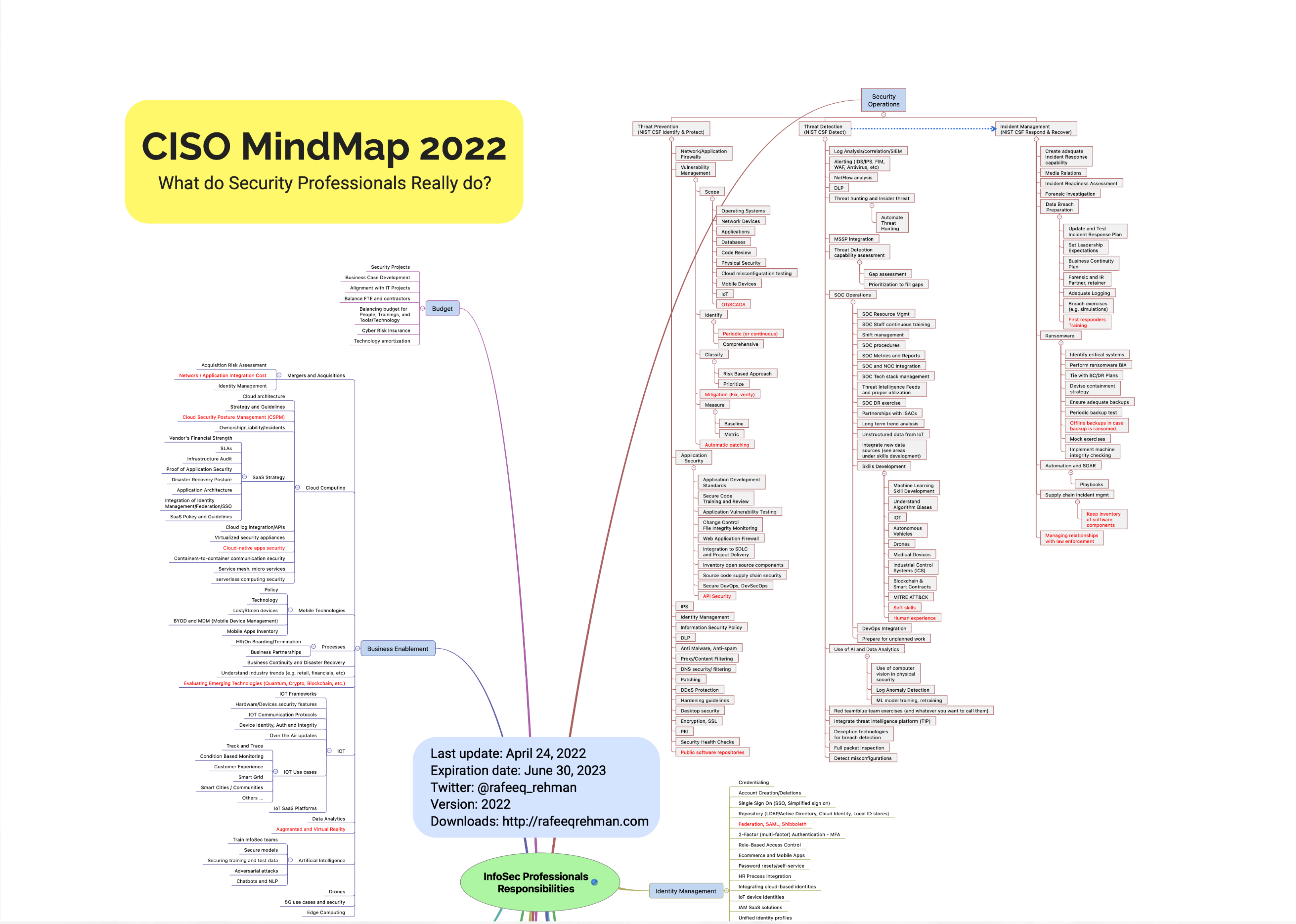
https://www.sans.org/media/SANS_Roadmap.pdf

Как много, но...



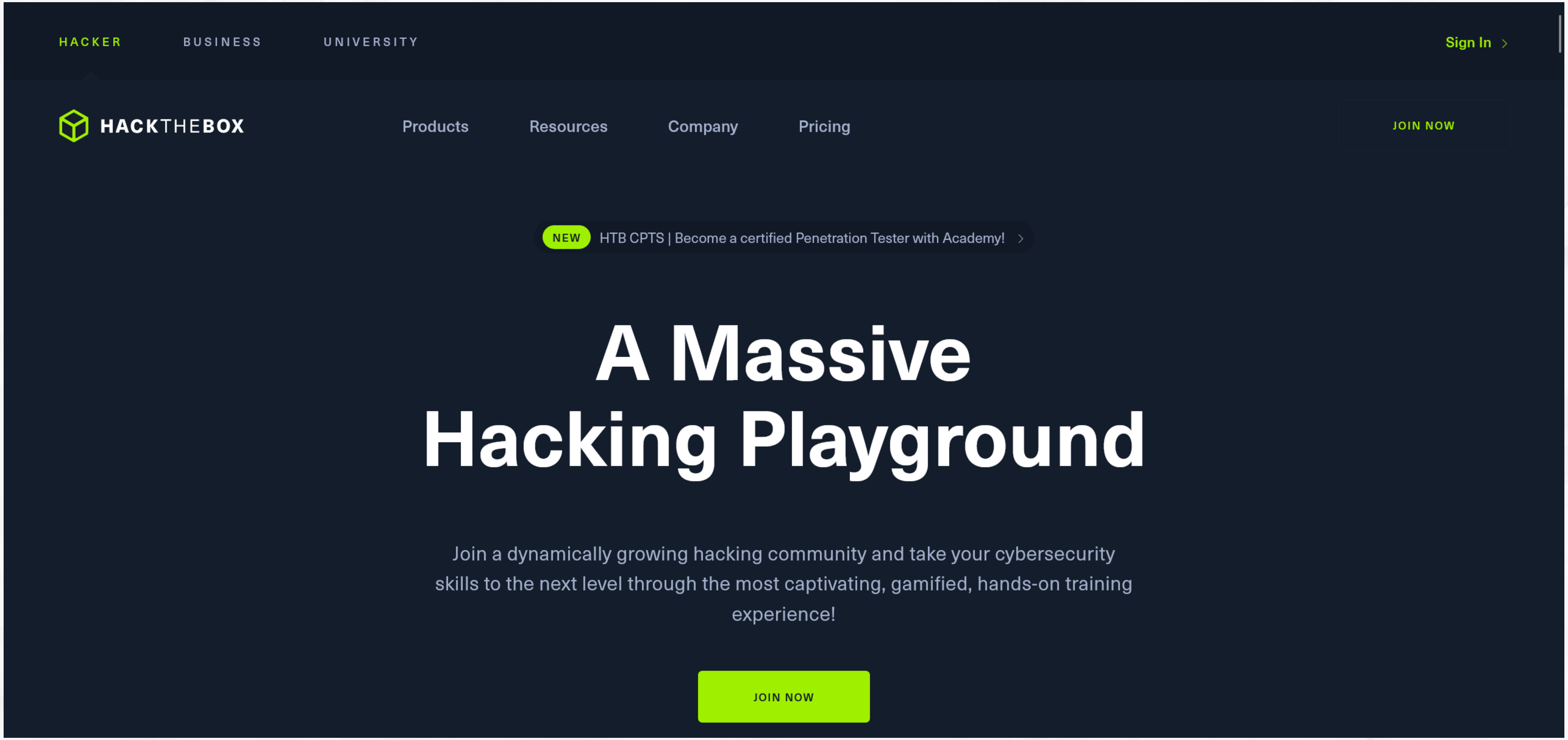
https://pauljerimy.com/it-career-roadmap/

Хард скилы


CISO MindMap 2022
What do Security Professionals Really do?
Budget
Security Projects
Business Case Development
Alignment with IT Projects
Balance FTE and contractors
Balancing budget for People, Trainings, and Tools/Technology
Cyber Risk Insurance
Technology amortization
Business Enablement
Mergers and Acquisitions
Acquisition Risk Assessment
Network / Application Integration Cost
Identity Management
Cloud Computing
Cloud architecture
Strategy and Guidelines
Cloud Security Posture Management (CSPM)
Ownership/Liability/Incidents
SaaS Strategy
Vendor's Financial Strength
SLAs
Infrastructure Audit
Proof of Application Security
Disaster Recovery Posture
Application Architecture
Integration of Identity Management/Federation/SSO
SaaS Policy and Guidelines
Cloud log integration/APIs
Virtualized security appliances
Cloud-native apps security
Containers-to-container communication security
Service mesh, micro services
serverless computing security
Mobile Technologies
Policy
Technology
Lost/Stolen devices
BYOD and MDM (Mobile Device Management)
Mobile Apps Inventory
Processes
HR/On Boarding/Termination
Business Partnerships
Business Continuity and Disaster Recovery
Understand industry trends (e.g. retail, financials, etc)
Evaluating Emerging Technologies (Quantum, Crypto, Blockchain, etc.)
IOT
IOT Frameworks
Hardware/Devices security features
IOT Communication Protocols
Device Identity, Auth and Integrity
Over the Air updates
IOT Use cases
Track and Trace
Condition Based Monitoring
Customer Experience
Smart Grid
Smart Cities / Communities
Others ...
IoT SaaS Platforms
Data Analytics
Augmented and Virtual Reality
Artificial Intelligence
Train InfoSec teams
Secure models
Securing training and test data
Adversarial attacks
Chatbots and NLP
Drones
5G use cases and security
Edge Computing
Last update: April 24, 2022
Expiration date: June 30, 2023
Twitter: @rafeeq_rehman
Version: 2022
Downloads: http://rafeeqrehman.com
InfoSec Professionals Responsibilities
Identity Management
Credentialing
Account Creation/Deletions
Single Sign On (SSO, Simplified sign on)
Repository (LDAP/Active Directory, Cloud Identity, Local ID stores)
Federation, SAML, Shibboleth
2-Factor (multi-factor) Authentication - MFA
Role-Based Access Control
Ecommerce and Mobile Apps
Password resets/self-service
HR Process Integration
Integrating cloud-based identities
IoT device identities
IAM SaaS solutions
Unified identity profiles
Security Operations
Threat Prevention (NIST CSF Identify & Protect)
Network/Application Firewalls
Vulnerability Management
Scope
Operating Systems
Network Devices
Applications
Databases
Code Review
Physical Security
Cloud misconfiguration testing
Mobile Devices
IoT
OT/SCADA
Identify
Periodic (or continuous)
Comprehensive
Classify
Risk Based Approach
Prioritize
Mitigation (Fix, verify)
Measure
Baseline
Metric
Automatic patching
Application Security
Application Development Standards
Secure Code Training and Review
Application Vulnerability Testing
Change Control File Integrity Monitoring
Web Application Firewall
Integration to SDLC and Project Delivery
Inventory open source components
Source code supply chain security
Secure DevOps, DevSecOps
API Security
IPS
Identity Management
Information Security Policy
DLP
Anti Malware, Anti-spam
Proxy/Content Filtering
DNS security/ filtering
Patching
DDoS Protection
Hardening guidelines
Desktop security
Encryption, SSL
PKI
Security Health Checks
Public software repositories
Threat Detection (NIST CSF Detect)
Log Analysis/correlation/SIEM
Alerting (IDS/IPS, FIM, WAF, Antivirus, etc)
NetFlow analysis
DLP
Threat hunting and Insider threat
Automate Threat Hunting
MSSP integration
Threat Detection capability assessment
Gap assessment
Prioritization to fill gaps
SOC Operations
SOC Resource Mgmt
SOC Staff continuous training
Shift management
SOC procedures
SOC Metrics and Reports
SOC and NOC Integration
SOC Tech stack management
Threat Intelligence Feeds and proper utilization
SOC DR exercise
Partnerships with ISACs
Long term trend analysis
Unstructured data from IoT
Integrate new data sources (see areas under skills development)
Skills Development
Machine Learning Skill Development
Understand Algorithm Biases
IOT
Autonomous Vehicles
Drones
Medical Devices
Industrial Control Systems (ICS)
Blockchain & Smart Contracts
MITRE ATT&CK
Soft skills
Human experience
DevOps Integration
Prepare for unplanned work
Use of AI and Data Analytics
Use of computer vision in physical security
Log Anomaly Detection
ML model training, retraining
Red team/blue team exercises (and whatever you want to call them)
Integrate threat intelligence platform (TIP)
Deception technologies for breach detection
Full packet inspection
Detect misconfigurations
Incident Management (NIST CSF Respond & Recover)
Create adequate Incident Response capability
Media Relations
Incident Readiness Assessment
Forensic Investigation
Data Breach Preparation
Update and Test Incident Response Plan
Set Leadership Expectations
Business Continuity Plan
Forensic and IR Partner, retainer
Adequate Logging
Breach exercises (e.g. simulations)
First responders Training
Ransomware
Identify critical systems
Perform ransomware BIA
Tie with BC/DR Plans
Devise containment strategy
Ensure adequate backups
Periodic backup test
Offline backups in case backup is ransomed.
Mock exercises
Implement machine integrity checking
Automation and SOAR
Playbooks
Supply chain incident mgmt
Keep inventory of software components
Managing relationships with law enforcement

https://rafeeqrehman.com/wp-content/uploads/2022/04/CISO_Mindmap_2022_no_headings.png

Hackthebox



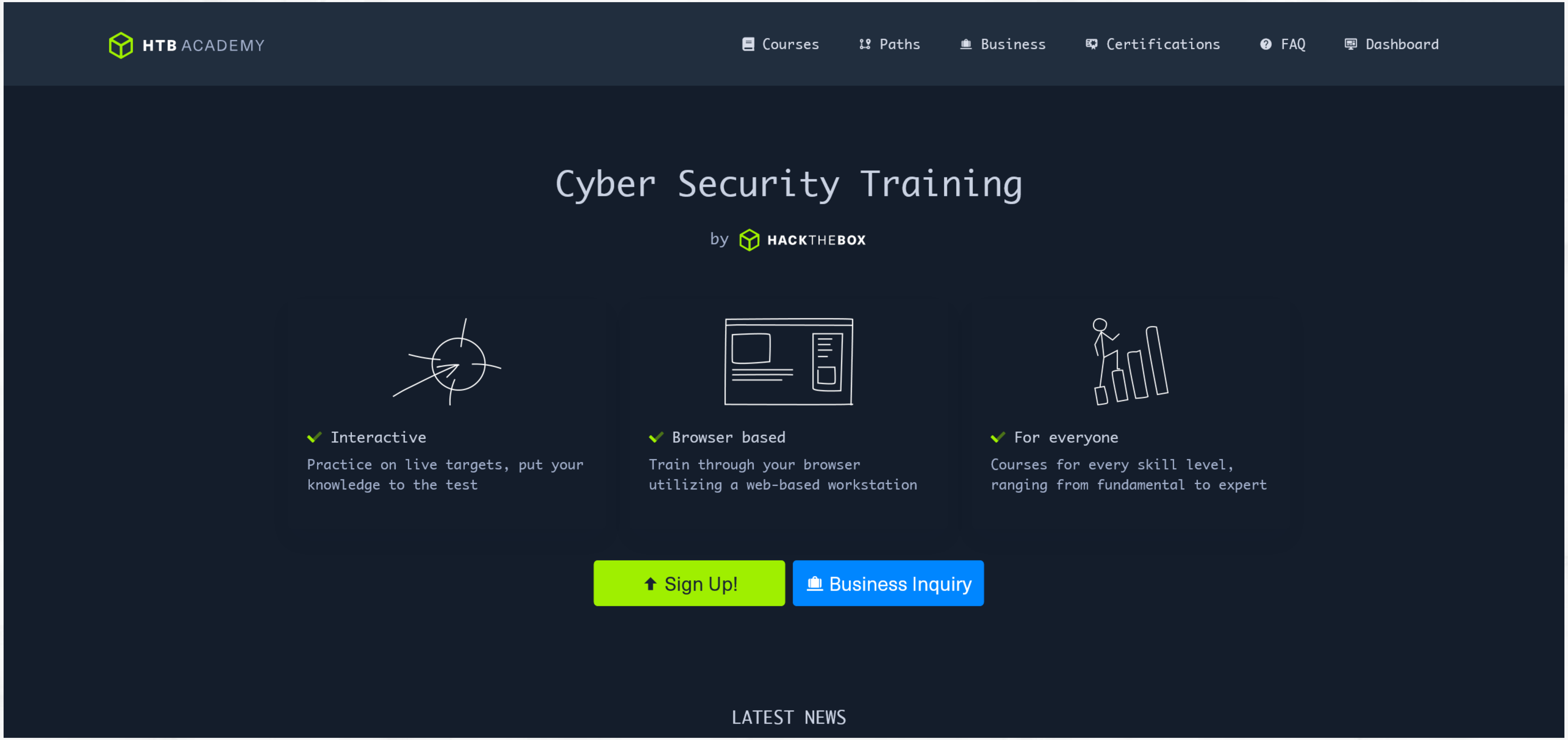
NEW HTB CPTS | Become a certified Penetration Tester with Academy! ›

A Massive Hacking Playground

Join a dynamically growing hacking community and take your cybersecurity skills to the next level through the most captivating, gamified, hands-on training experience!

https://www.hackthebox.com/

Academy Hackthebox



Cyber Security Training

by HACKTHEBOX

✓ Interactive

Practice on live targets, put your knowledge to the test

✓ Browser based

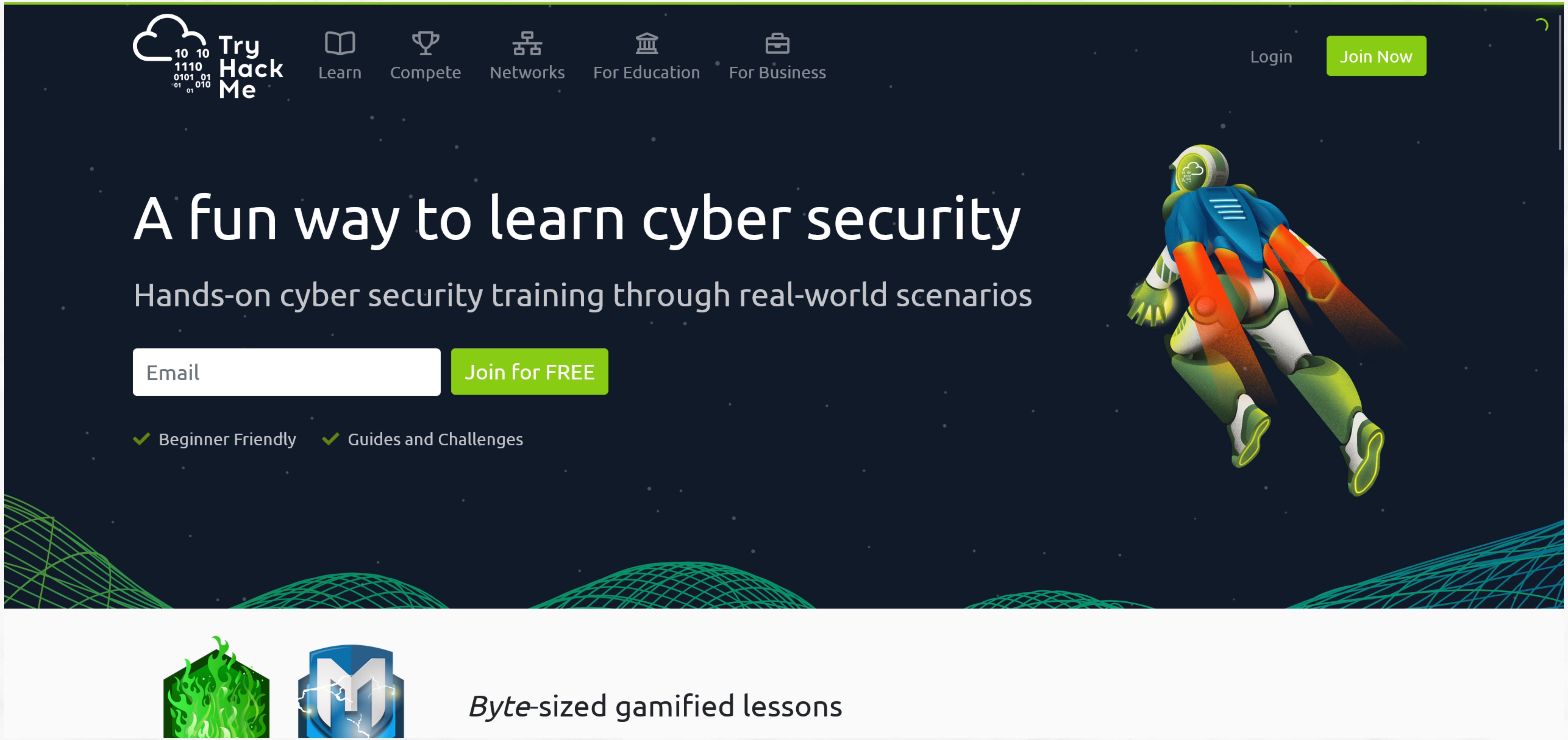
Train through your browser utilizing a web-based workstation

✓ For everyone

Courses for every skill level, ranging from fundamental to expert

https://academy.hackthebox.com/

Tryhackme



A fun way to learn cyber security

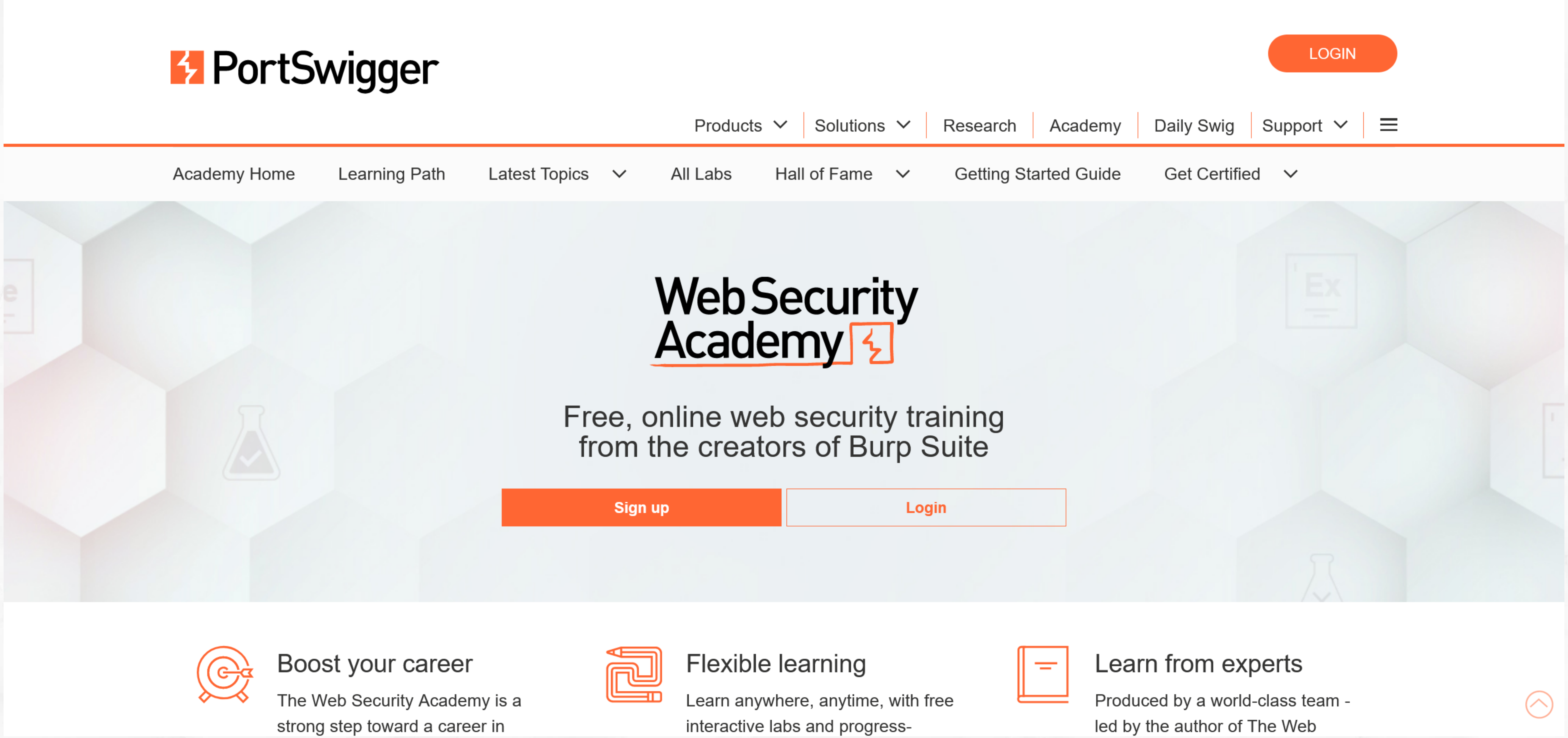
Hands-on cyber security training through real-world scenarios

✓ Beginner Friendly ✓ Guides and Challenges

Byte-sized gamified lessons

https://tryhackme.com/

PortSwigger



PortSwigger

LOGIN

Products ⌄ | Solutions ⌄ | Research | Academy | Daily Swig | Support ⌄ | ☰

Academy Home | Learning Path | Latest Topics ⌄ | All Labs | Hall of Fame ⌄ | Getting Started Guide | Get Certified ⌄

Web Security Academy

Free, online web security training from the creators of Burp Suite

Sign up | Login

Boost your career

The Web Security Academy is a strong step toward a career in

Flexible learning

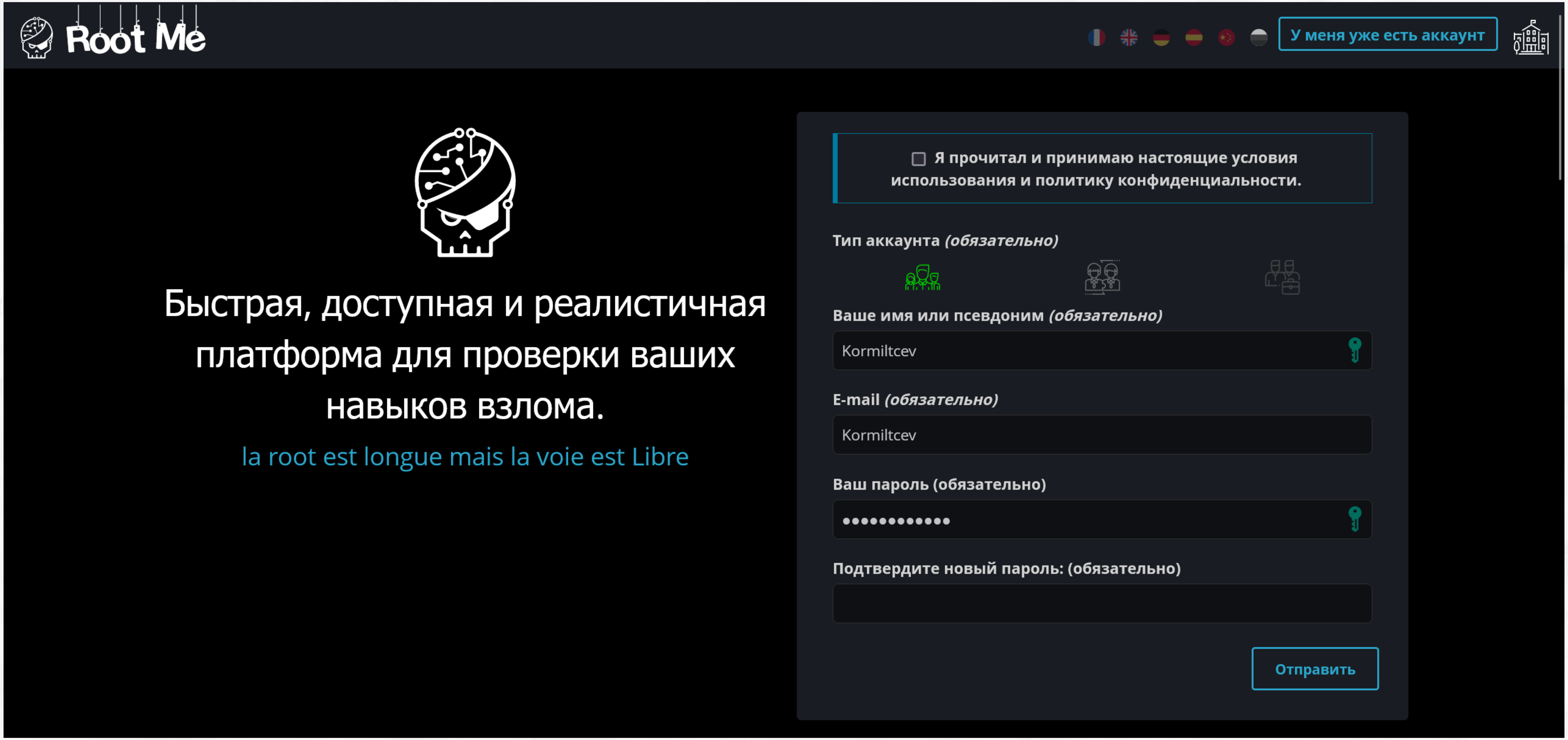
Learn anywhere, anytime, with free interactive labs and progress-

Learn from experts

Produced by a world-class team - led by the author of The Web

https://portswigger.net/web-security

Root me



Быстрая, доступная и реалистичная платформа для проверки ваших навыков взлома.

la root est longue mais la voie est Libre

□ Я прочитал и принимаю настоящие условия использования и политику конфиденциальности.

Тип аккаунта *(обязательно)*

Ваше имя или псевдоним *(обязательно)*

Kormiltcev

E-mail *(обязательно)*

Kormiltcev

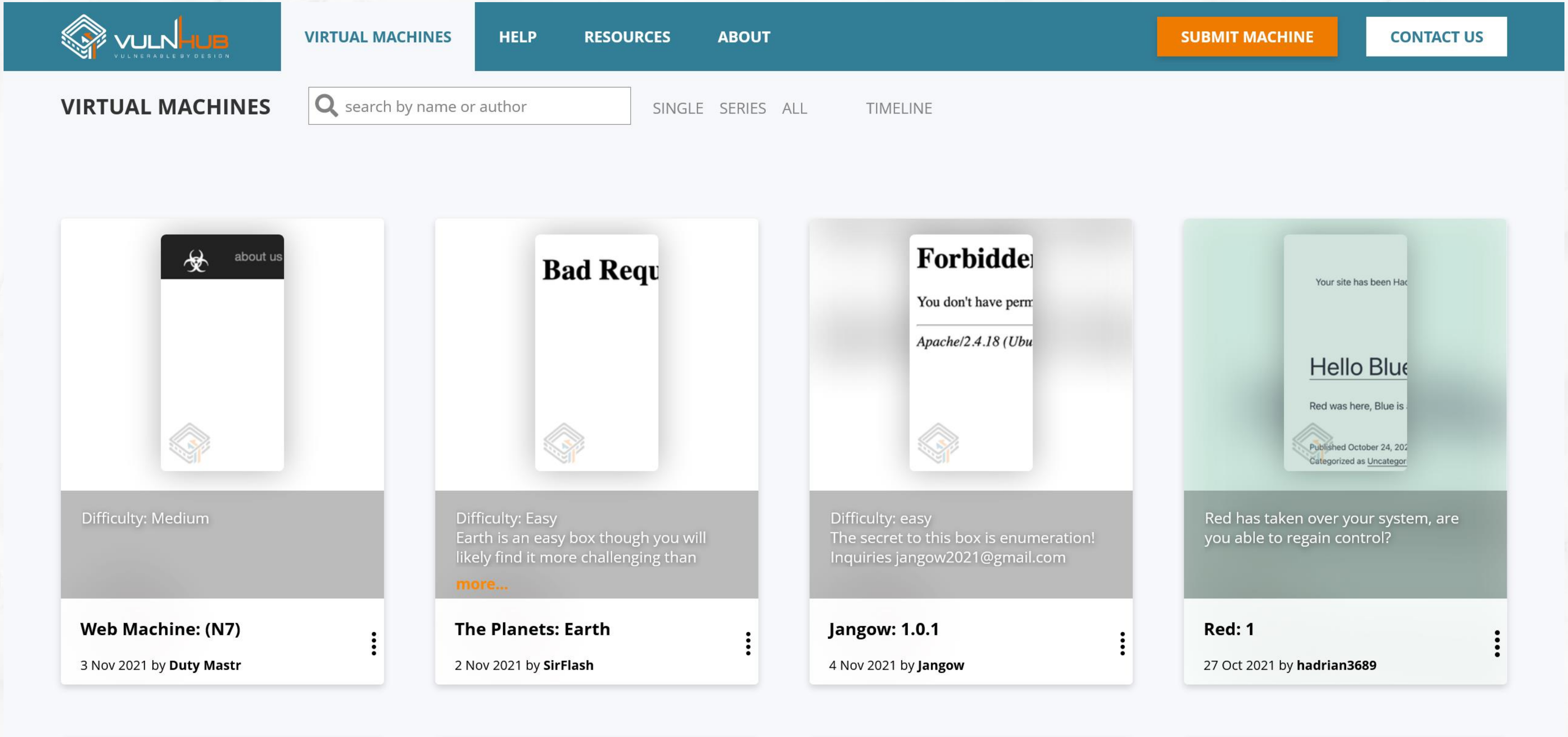
Ваш пароль (обязательно)

●●●●●●●●●●●●

Подтвердите новый пароль: (обязательно)

https://www.root-me.org/?lang=ru

VulnHub



Difficulty: Medium

Web Machine: (N7)

3 Nov 2021 by **Duty Mastr**

Difficulty: Easy
Earth is an easy box though you will likely find it more challenging than
more...

The Planets: Earth

2 Nov 2021 by **SirFlash**

Difficulty: easy
The secret to this box is enumeration!
Inquiries jangow2021@gmail.com

Jangow: 1.0.1

4 Nov 2021 by **Jangow**

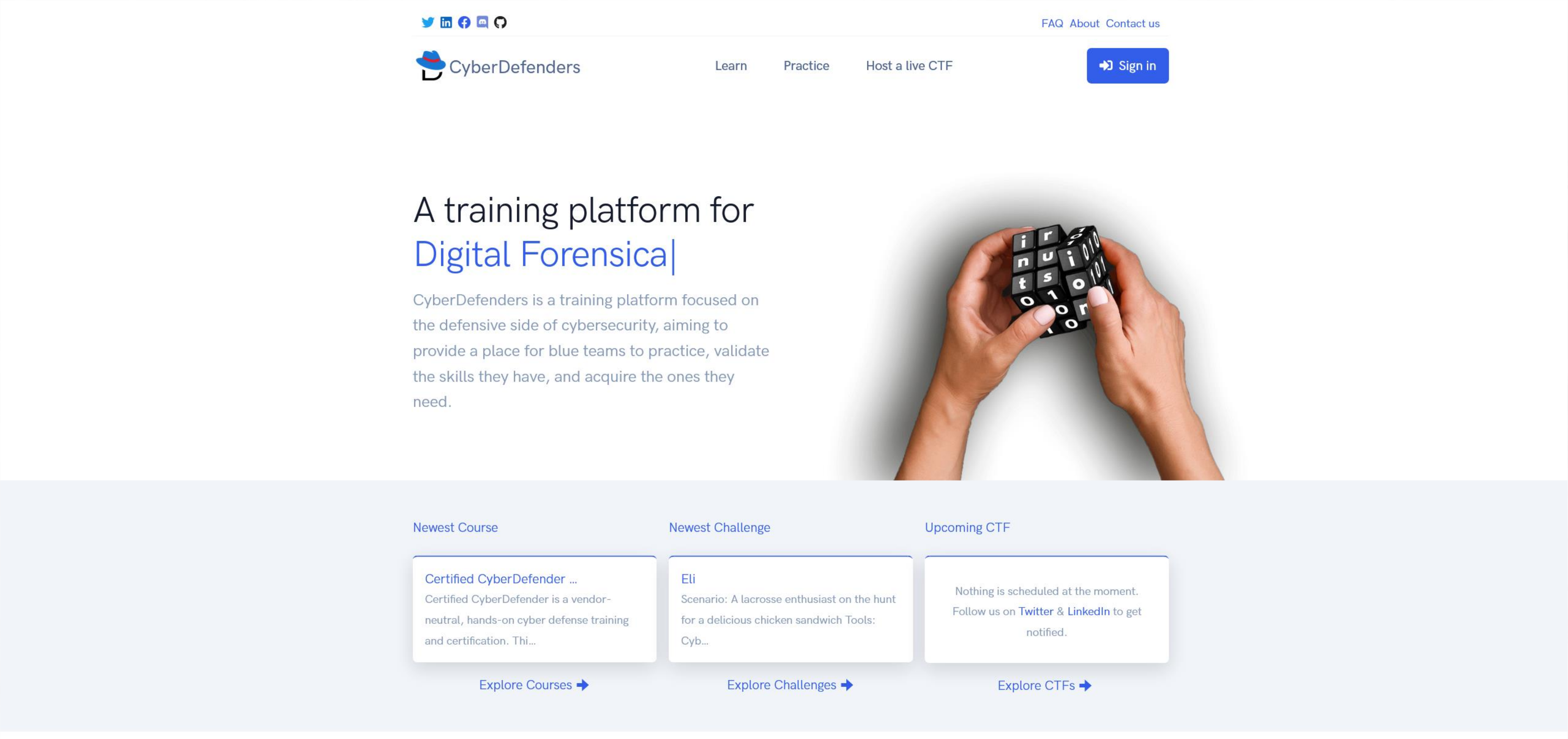
Red has taken over your system, are you able to regain control?

Red: 1

27 Oct 2021 by **hadrian3689**

https://www.vulnhub.com/

CyberDefenders



FAQ About Contact us

CyberDefenders

Learn Practice Host a live CTF Sign in

A training platform for

Digital Forensica|

CyberDefenders is a training platform focused on the defensive side of cybersecurity, aiming to provide a place for blue teams to practice, validate the skills they have, and acquire the ones they need.

Newest Course

Certified CyberDefender ...

Certified CyberDefender is a vendor-neutral, hands-on cyber defense training and certification. Thi...

Explore Courses

Newest Challenge

Eli

Scenario: A lacrosse enthusiast on the hunt for a delicious chicken sandwich Tools: Cyb...

Explore Challenges

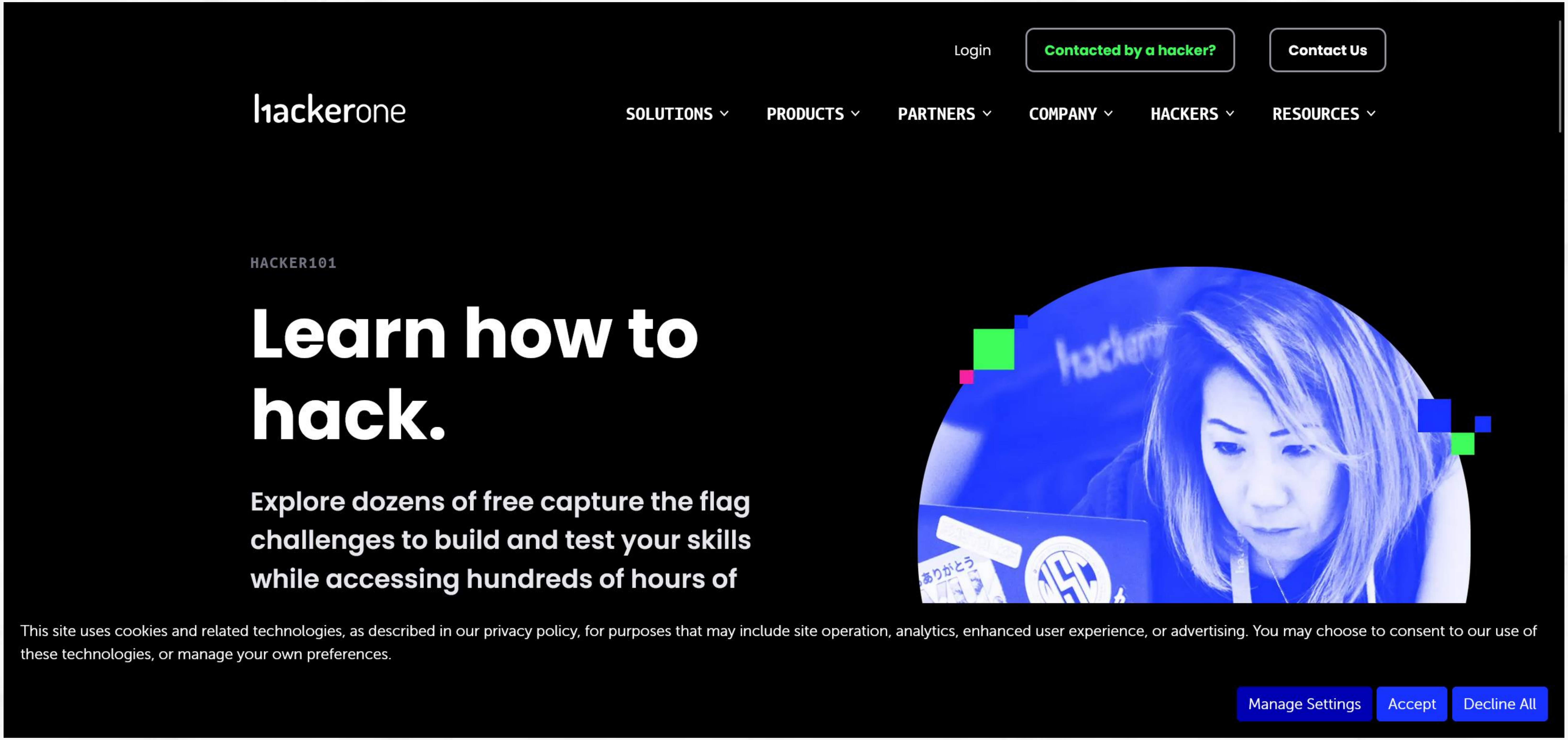
Upcoming CTF

Nothing is scheduled at the moment. Follow us on Twitter & LinkedIn to get notified.

Explore CTFs

https://cyberdefenders.org/

Hackerone



HACKER101

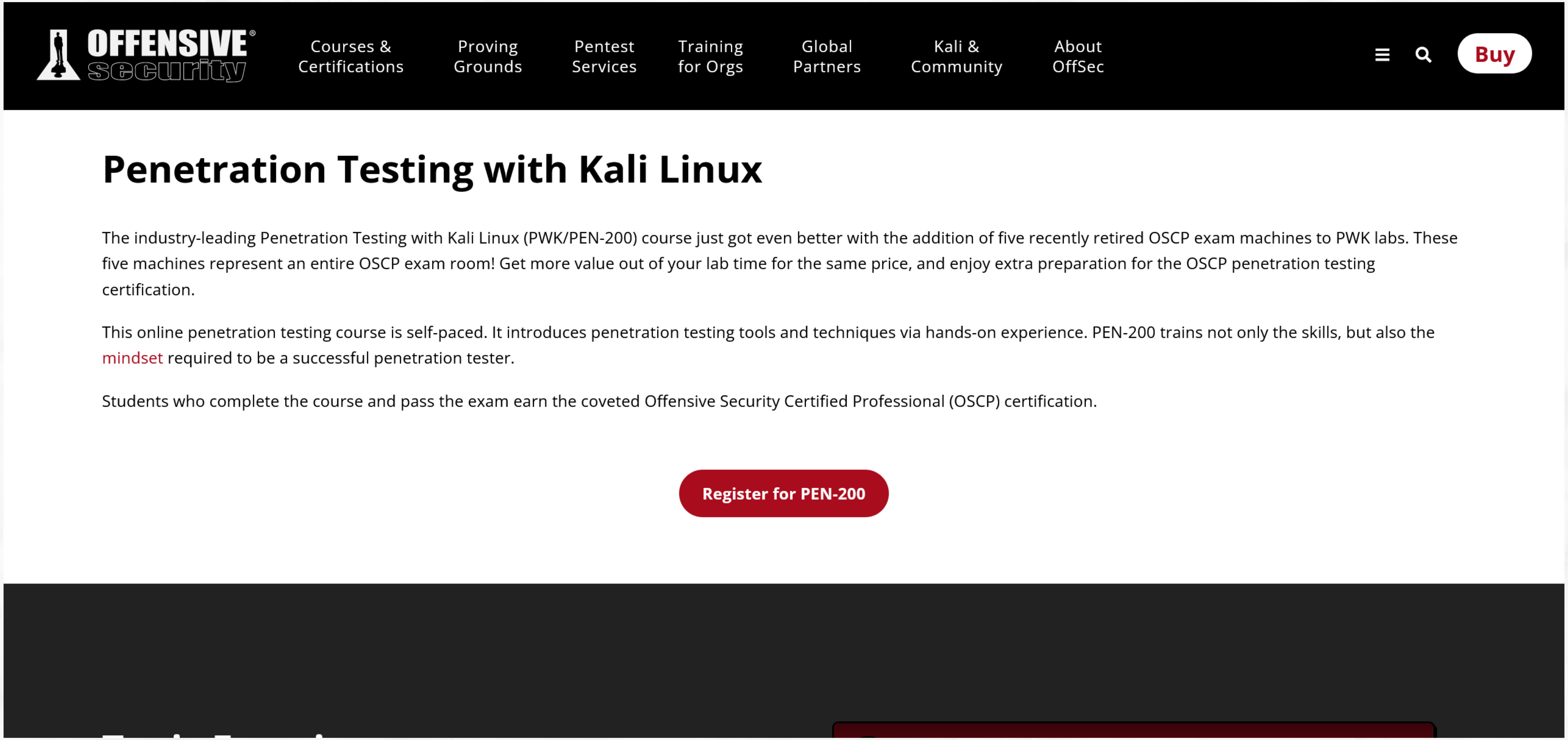
Learn how to hack.

Explore dozens of free capture the flag challenges to build and test your skills while accessing hundreds of hours of

This site uses cookies and related technologies, as described in our privacy policy, for purposes that may include site operation, analytics, enhanced user experience, or advertising. You may choose to consent to our use of these technologies, or manage your own preferences.

https://www.hackerone.com/hackers/hacker101

PEN-200



Penetration Testing with Kali Linux

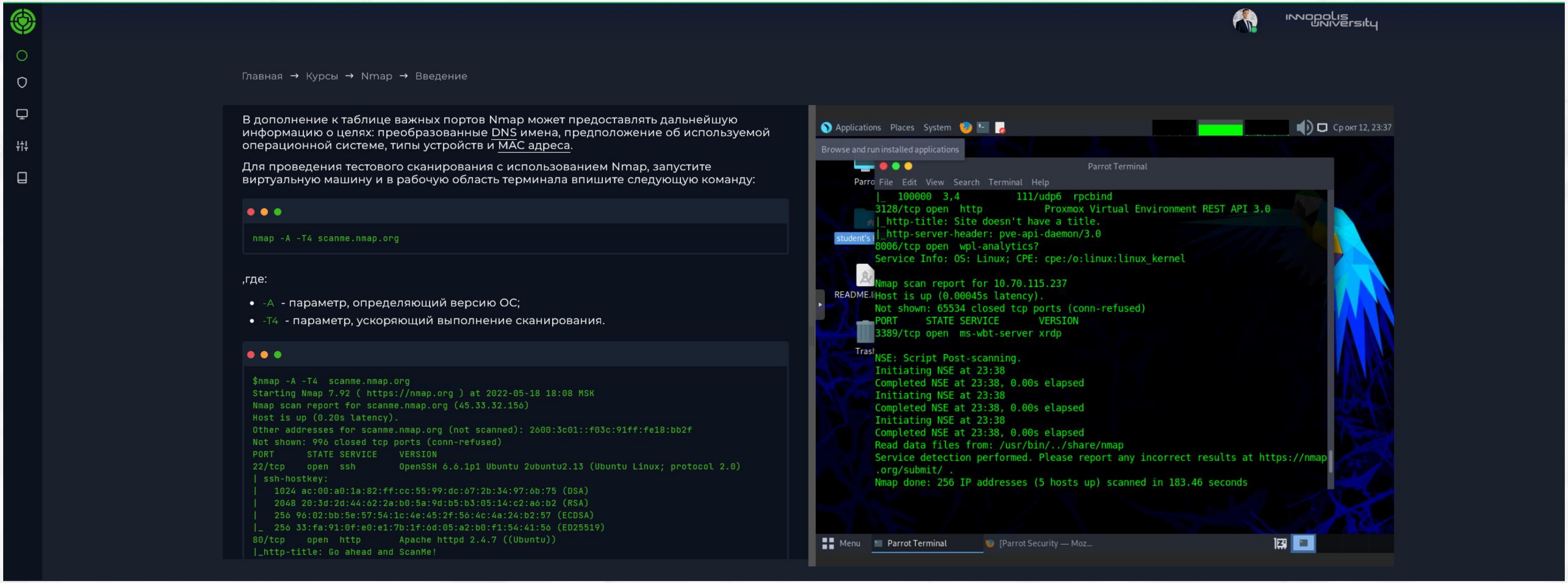
The industry-leading Penetration Testing with Kali Linux (PWK/PEN-200) course just got even better with the addition of five recently retired OSCP exam machines to PWK labs. These five machines represent an entire OSCP exam room! Get more value out of your lab time for the same price, and enjoy extra preparation for the OSCP penetration testing certification.

This online penetration testing course is self-paced. It introduces penetration testing tools and techniques via hands-on experience. PEN-200 trains not only the skills, but also the mindset required to be a successful penetration tester.

Students who complete the course and pass the exam earn the coveted Offensive Security Certified Professional (OSCP) certification.

https://www.offensive-security.com/pwk-oscp/#about-pwk

ИнноКиберполигон



Главная → Курсы → Nmap → Введение

В дополнение к таблице важных портов Nmap может предоставлять дальнейшую информацию о целях: преобразованные DNS имена, предположение об используемой операционной системе, типы устройств и MAC адреса.

Для проведения тестового сканирования с использованием Nmap, запустите виртуальную машину и в рабочую область терминала впишите следующую команду:

```
nmap -A -T4 scanme.nmap.org
```

,где:

- -A - параметр, определяющий версию ОС;
- -T4 - параметр, ускоряющий выполнение сканирования.

```
$nmap -A -T4  scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-18 18:08 MSK
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
```

```
|_  100000  3,4         111/udp6  rpcbind
3128/tcp open  http          Proxmox Virtual Environment REST API 3.0
|_http-title: Site doesn't have a title.
|_http-server-header: pve-api-daemon/3.0
8006/tcp open  wpl-analytics?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.70.115.237
Host is up (0.00045s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server xrdp

NSE: Script Post-scanning.
Initiating NSE at 23:38
Completed NSE at 23:38, 0.00s elapsed
Initiating NSE at 23:38
Completed NSE at 23:38, 0.00s elapsed
Initiating NSE at 23:38
Completed NSE at 23:38, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 183.46 seconds
```

Готов ответить на ваши вопросы

E-mail: n.kormiltcev@innopolis.ru
Phone: +79963351810