



iKNEX
Knowledge Sharing
for a Changing World

Into the Blue

Chonlatit Rujiphut | A

CISSP | CISM | CASP+ | CDPSE | CCSKv4 | PECB Certified ISO/IEC 27032 LCM | BTL1 | ECSA | CHFI | CEH | ECIH | CompTIA CySA+ | CompTIA Sec+ | CompTIA Network+ | CompTIA Project+ | CompTIA A+ | CompTIA CSIS | CompTIA CSAE | CompTIA CSAP | CompTIA CIOS | MCP | Microsoft Certified: Security, Compliance, and Identity Fundamentals | MTA: Security Fundamentals MTA: Networking Fundamentals | MTA: Windows Server Administration | MTA: Security Fundamentals | PaloAlto ACE | CSFPC™ | RWVCPCTM | SFPC™ | CQI IRCA certified ISO 27001:2013 Information Security Management Systems Lead Auditor | Data Protection Officer (DPO) by CEPAS, Bureau Veritas | CNSS Certified Network Security Specialist.



#SysAdminDay
Virtual Event
July 29, 2022

C:\Users\Sysad> Whoami



CHONLATIT RUJIPHUT

Executive - Cyber Security Management | Mitr Phol Sugar Corp., Ltd. | 2021 - Present

Manager - Computer Incident Response Team | B.Grimm Power PCL. | 2018-2021

Security Analyst and Administrator | e-Cop (Thailand) Co., Ltd. | 2016-2017

Network Engineer | Comp Trading Co., Ltd | 2015-2016

IT Administrator | Sky Commercial Co., Ltd. | 2014-2015

Computer Technology Teacher | Matthayom Wat That Thong School | 2013-2014

Mahanakorn University of Technology
Master of Science (MS), Information Systems Security (MiSS06)

Rajamangala University of Technology Thanyaburi
Bachelor of Education (BEd), Computer Education 5 Years

CISSP | CISM | CASP+ | CDPS | CCSKv4 | PECB Certified ISO/IEC 27032 LCM | BTL1 | ECSA | CHFI | CEH | ECIH | CompTIA CySA+ | CompTIA Sec+ | CompTIA Network+ | CompTIA Project+ | CompTIA A+ | CompTIA CSIS | CompTIA CSAE | CompTIA CSAP | CompTIA CIOS | MCP | Microsoft Certified: Security, Compliance, and Identity Fundamentals | MTA: Security Fundamentals MTA: Networking Fundamentals | MTA: Windows Server Administration | MTA: Security Fundamentals | PaloAlto ACE | CSFPC™ | RWVCPC™ | SFPC™ | CQI IRCA certified ISO 27001:2013 Information Security Management Systems Lead Auditor | Data Protection Officer (DPO) by CEPAS, Bureau Veritas | CNSS Certified Network Security Specialist.



2 Things to Talk About



**Understanding
Blue Team Roles**



**Sharing Experiences
BTL1 EXAM**



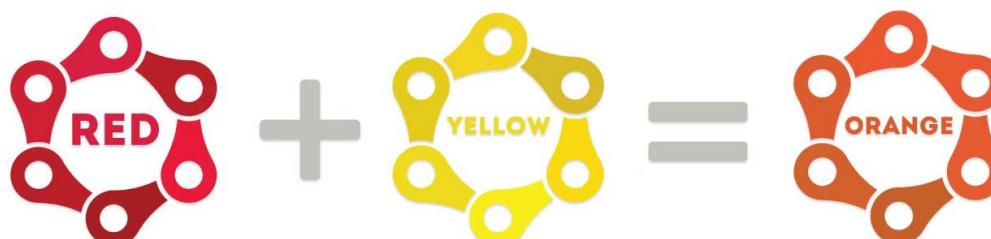
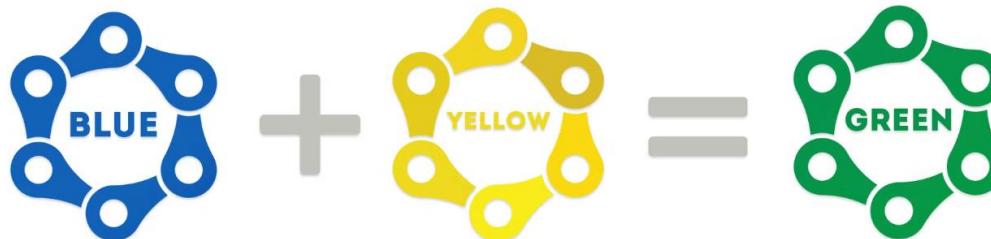
#SysAdminDay
Virtual Event
July 29, 2022

Understanding Blue Team Roles



#SysAdminDay
Virtual Event
July 29, 2022

InfoSec Color Wheel



InfoSec Color Wheel



RED TEAM

- ✓ Offensive Security
- ✓ Ethical Hacking
- ✓ Exploiting vulnerabilities
- ✓ Penetration Tests
- ✓ Black Box Testing
- ✓ Social Engineering
- ✓ Web App Scanning



PURPLE TEAM

- ✓ Facilitate improvements in detection and defence
- ✓ Sharpened the skills of Blue and Red team members
- ✓ Effective for spot-checking systems in larger organizations



BLUE TEAM

- ✓ Defensive Security
- ✓ Infrastructure protection
- ✓ Damage Control
- ✓ Incident Response(IR)
- ✓ Operational Security
- ✓ Threat Hunters
- ✓ Digital Forensics



#SysAdminDay
Virtual Event
July 29, 2022

InfoSec Color Wheel



YELLOW TEAM

- ✓ Software Builders
- ✓ Application Developers
- ✓ Software Engineers
- ✓ System Architects



GREEN TEAM

- ✓ Improved logging capability, working to standardise and prioritise important events
- ✓ Better data for digital forensics and incident response cases
- ✓ Safer Change Management including integrity monitoring
- ✓ Full coverage monitoring including improved Anti-Virus and End Point Protection on systems



BLUE TEAM

- ✓ Defensive Security
- ✓ Infrastructure protection
- ✓ Damage Control
- ✓ Incident Response(IR)
- ✓ Operational Security
- ✓ Threat Hunters
- ✓ Digital Forensics



InfoSec Color Wheel



YELLOW TEAM

- ✓ Software Builders
- ✓ Application Developers
- ✓ Software Engineers
- ✓ System Architects



ORANGE TEAM

- ✓ Inspire coders and architects to be more security conscious
- ✓ Benefit from current exposure to evolving security threats
- ✓ Offensive critical thinking included in builder's intrinsic thought pattern
- ✓ Decrease in overall security bug count over time

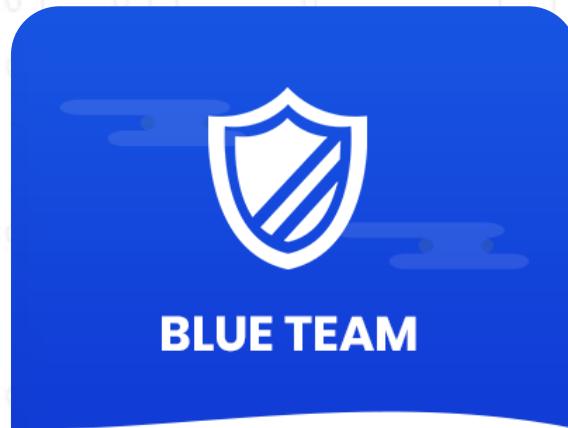


RED TEAM

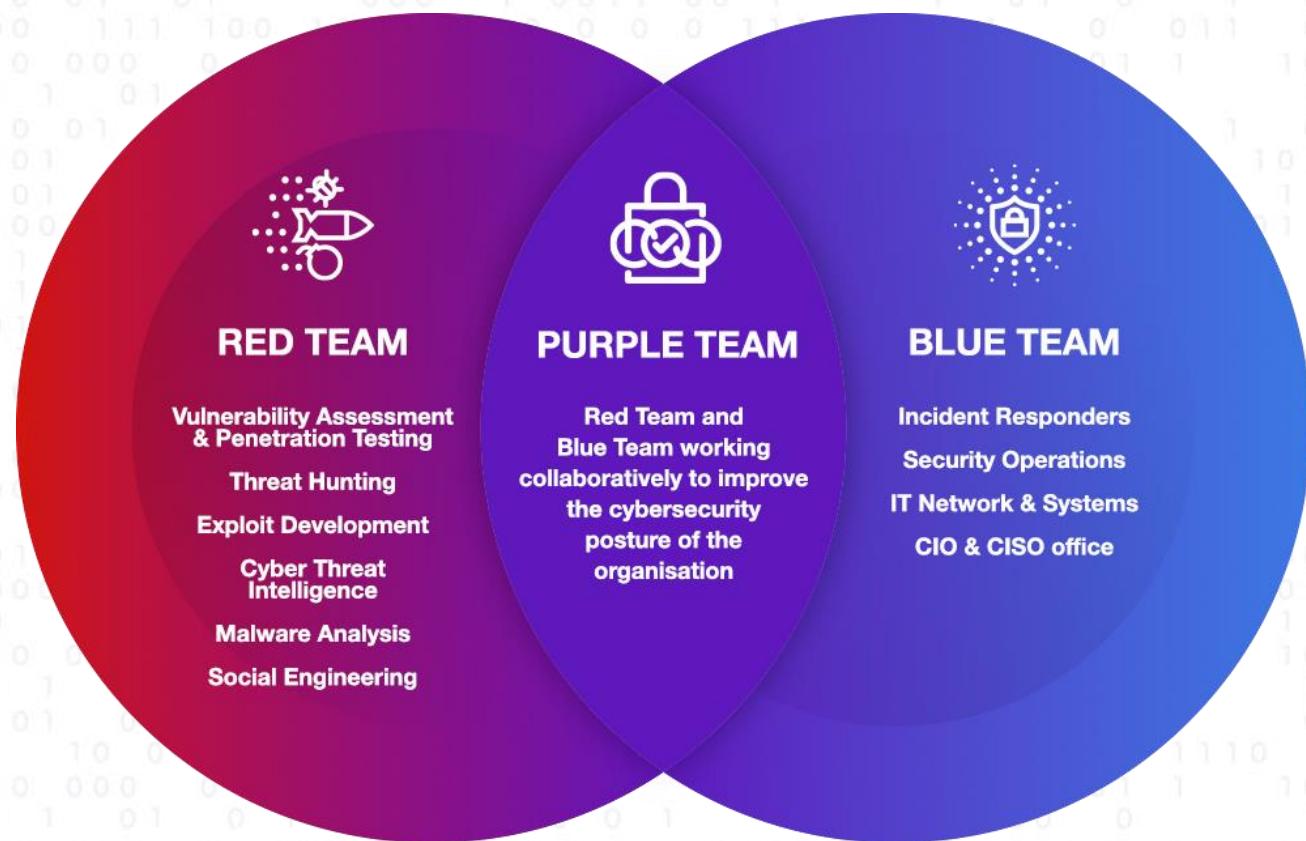
- ✓ Offensive Security
- ✓ Ethical Hacking
- ✓ Exploiting vulnerabilities
- ✓ Penetration Tests
- ✓ Black Box Testing
- ✓ Social Engineering
- ✓ Web App Scanning



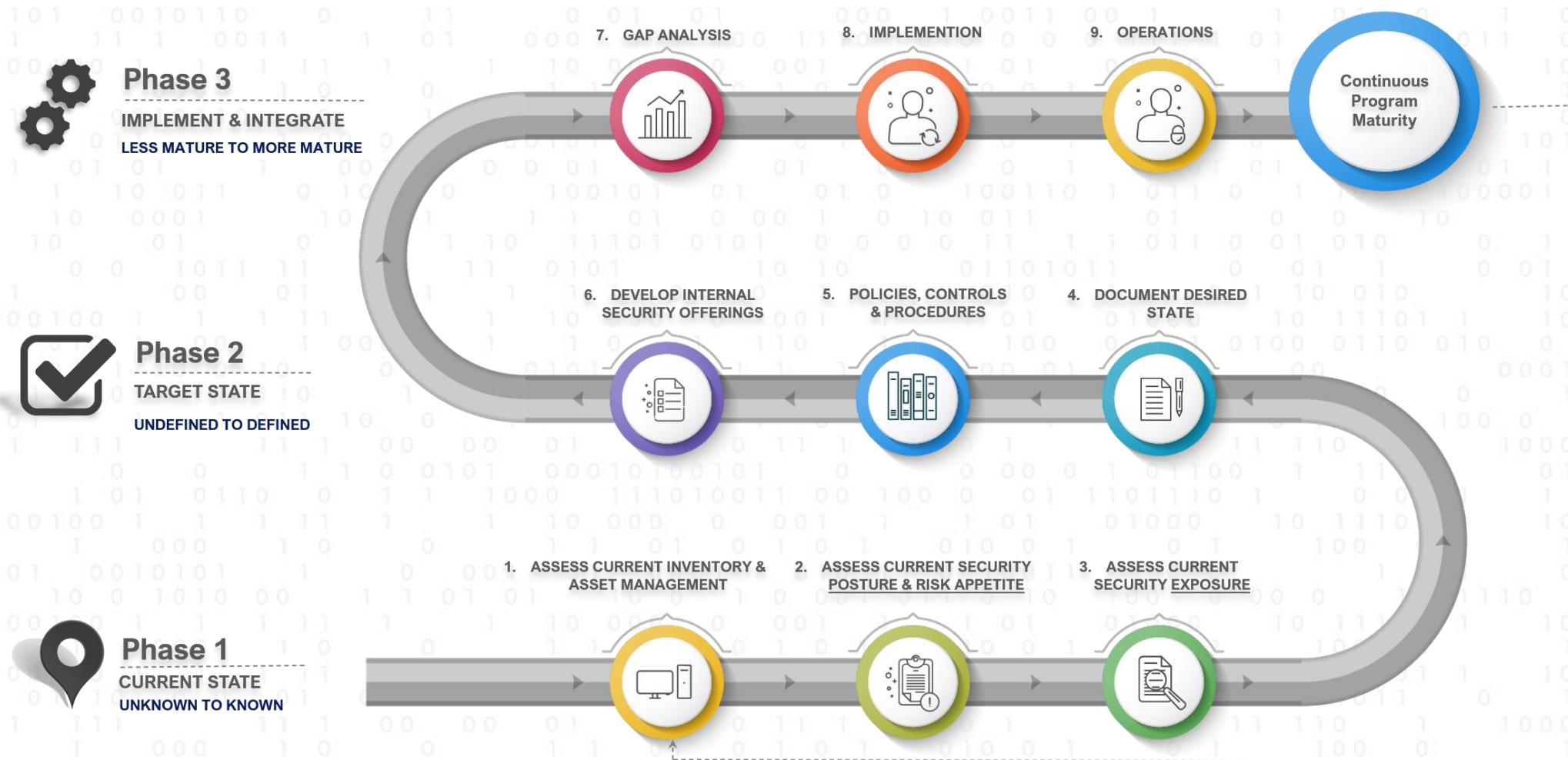
Blue Team Security



- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response (IR)
- Operational Security
- Threat Hunters
- Digital Forensics



Blue Team Security

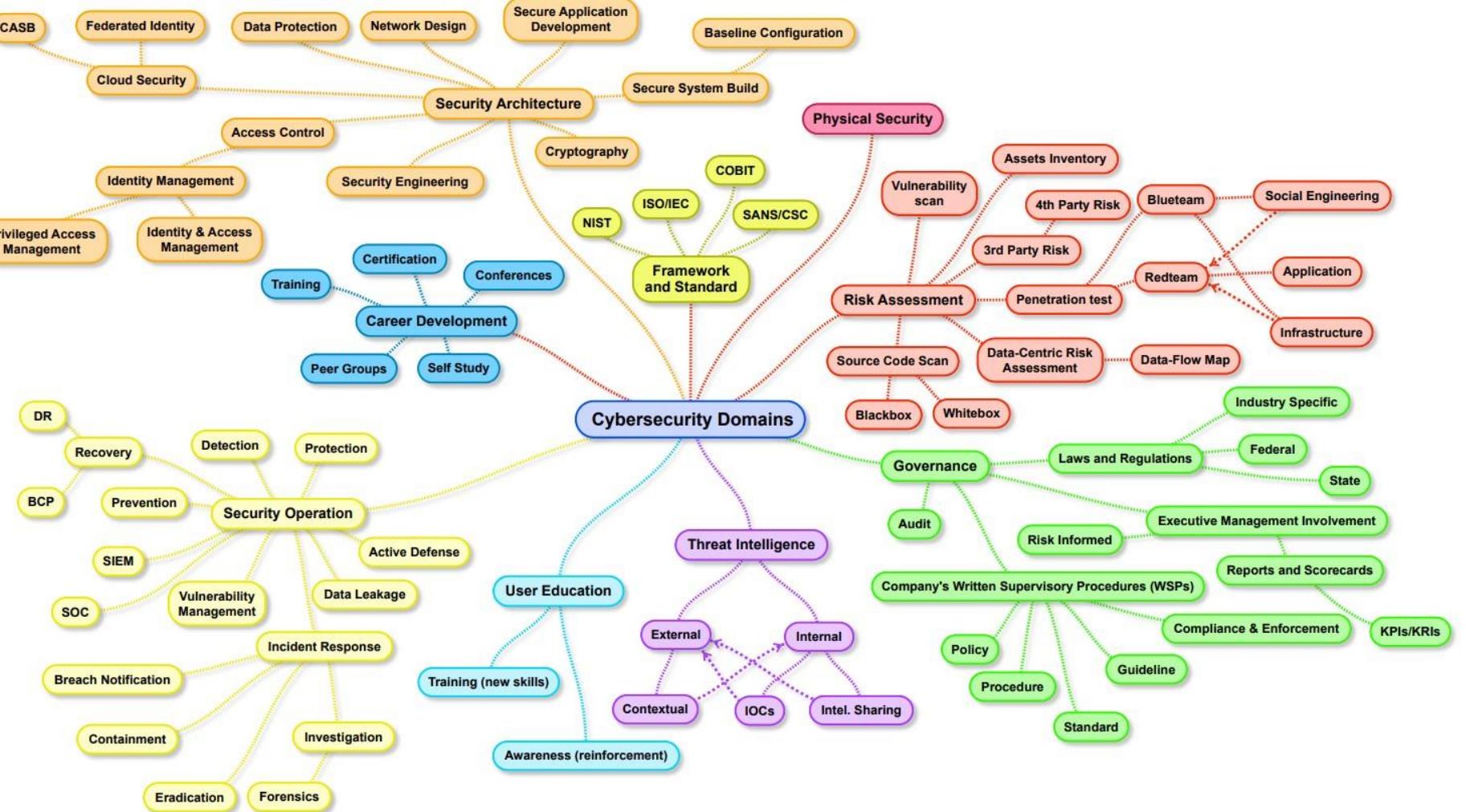


Blue Team Security

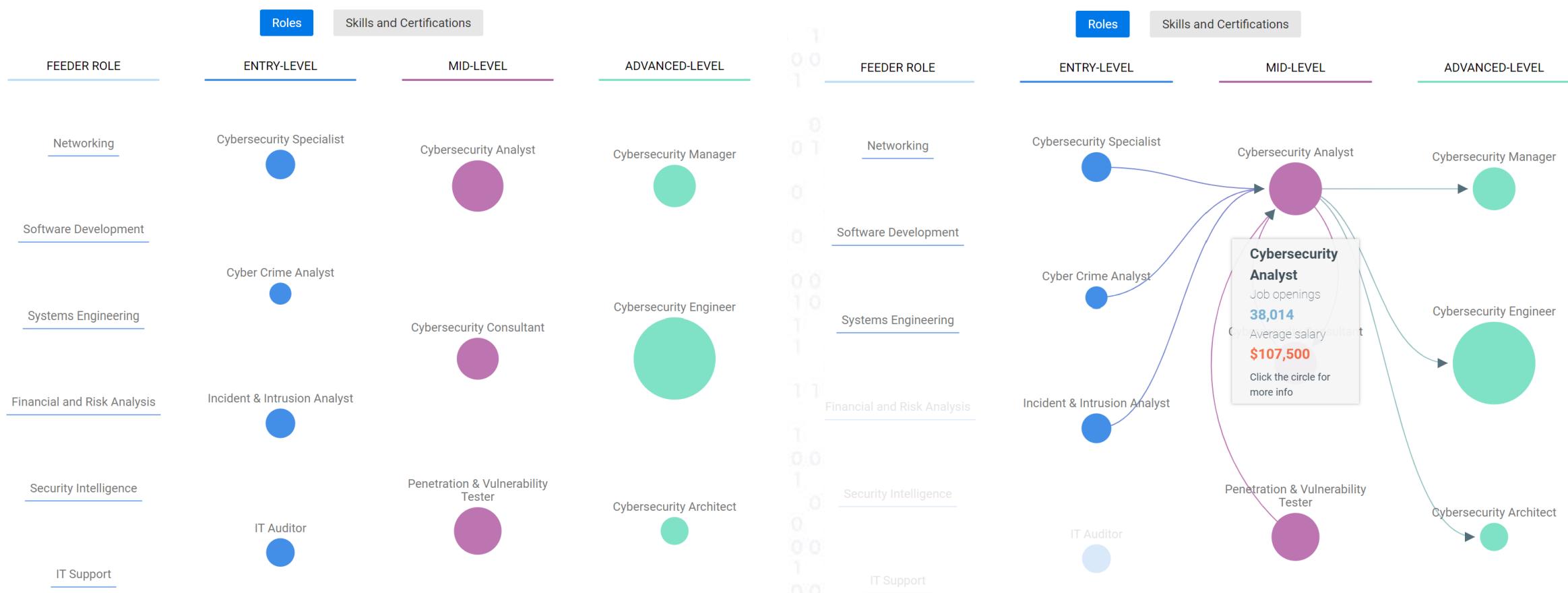
- Security Awareness training
- Domain Expirations
- Incident Response Process/Procedures
- Email Filters, Thresholds, and Spam Rules
- Logs and SIEM Config/Alerts
- Config & Patch Management
- Web Browser Config
- MS Office Security Settings
- Deny Log Relay Request
- White listing
- Authenticated Proxies
- Least Privilege
- Anti-virus
- FIM/WMI event triggers
- Firewall Rules
- Fix Up Protocols
- Secure Group Policy Settings
- Authenticated HTTP Proxies
- Application White Listing
- Canaries
- Segmentation
- Honeypots
- Admin Awareness Training
- Tarpits
- Manage Keys securely
- Host DLP
- Encryption
- Sensitive Data Stores
- Strong Account Policies
- Two-factor Authentication
- Mail client/server settings



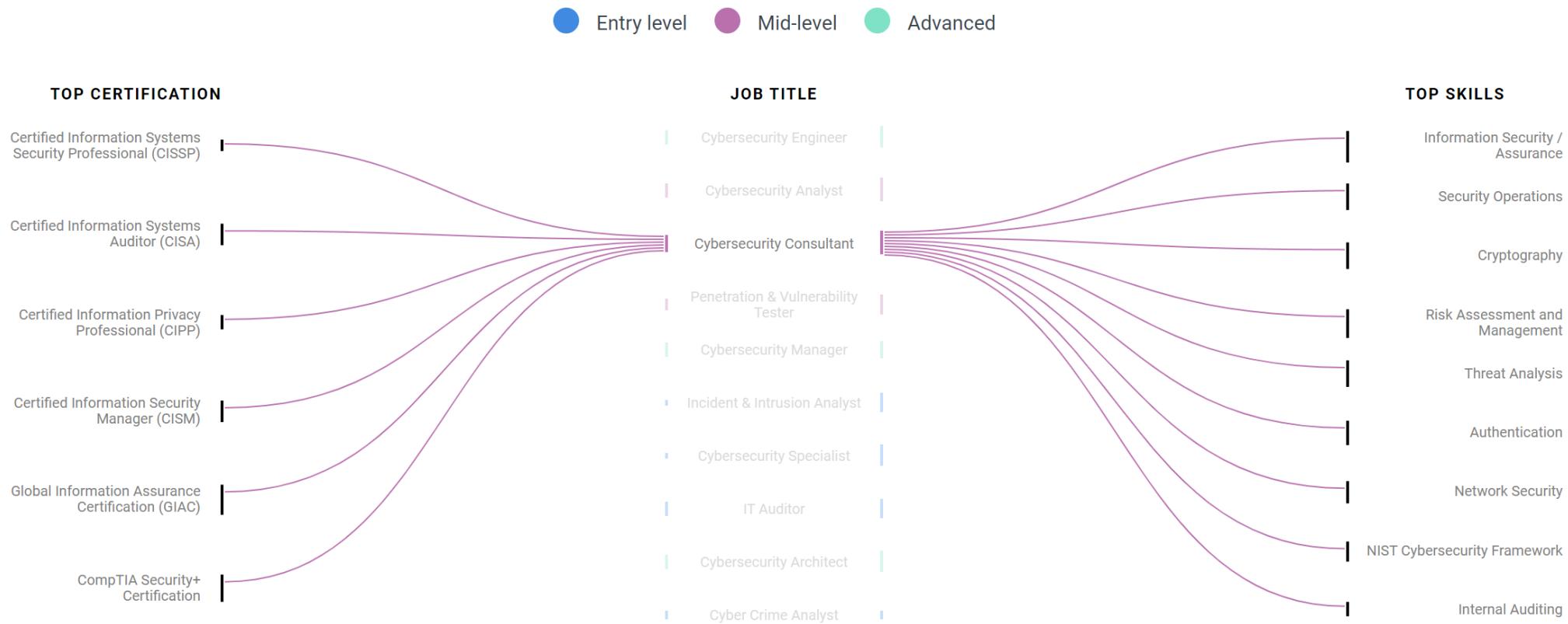
Blue Team Security



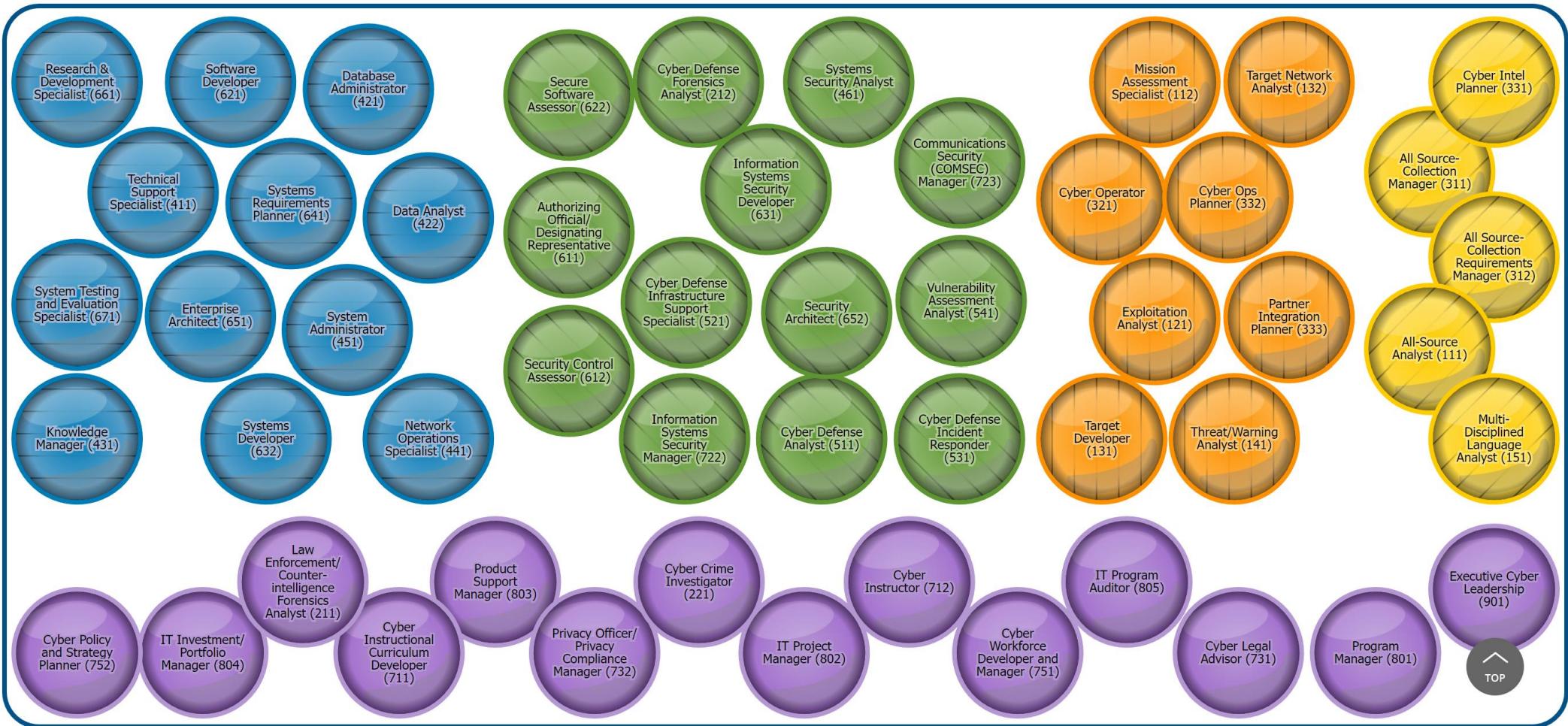
Cyber Security Role



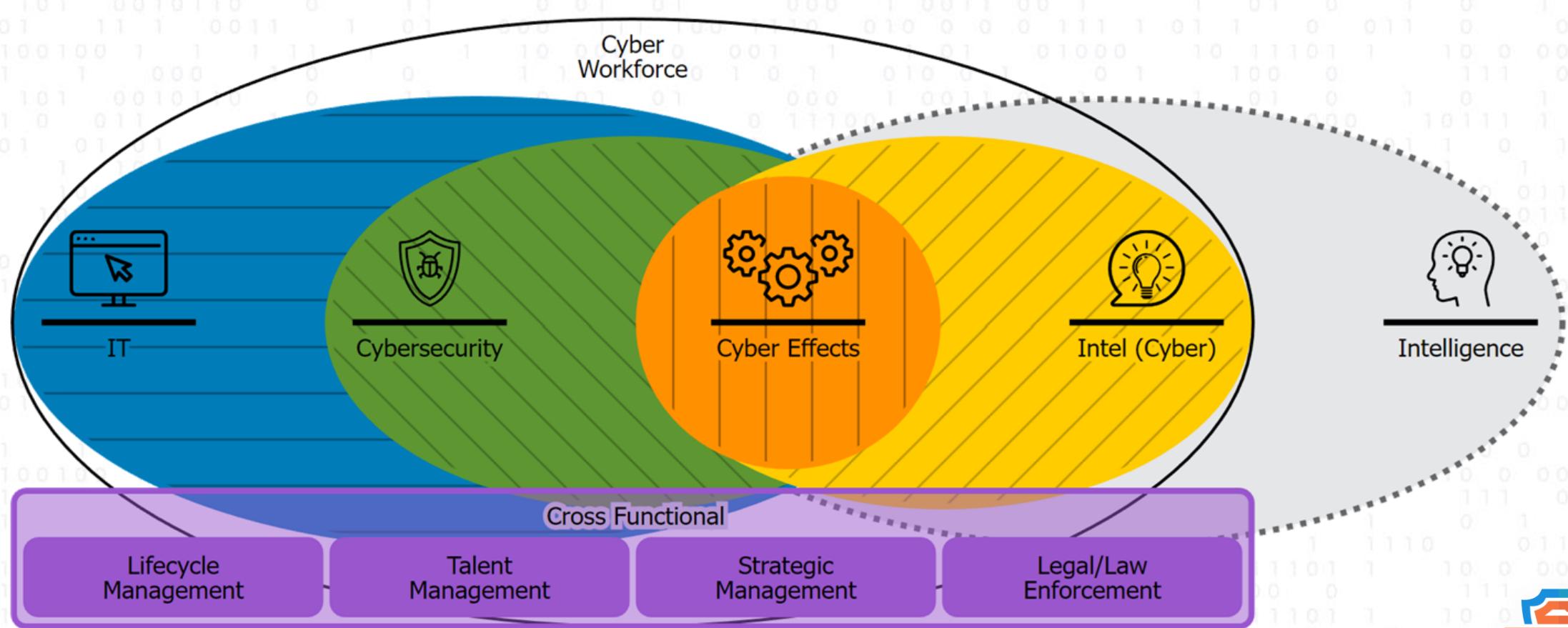
Cyber Security Role



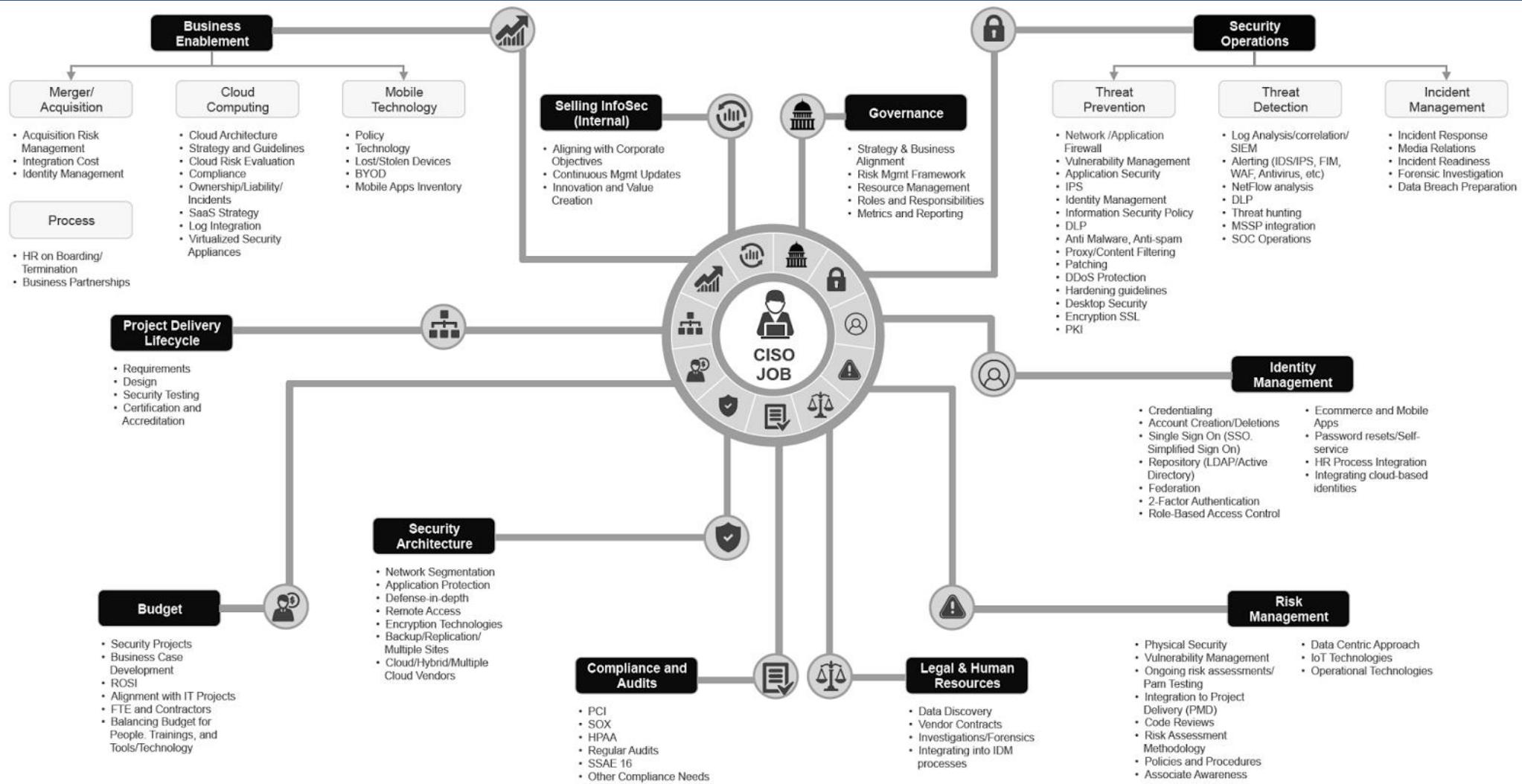
Cyber Security Role



Cyber Security Role



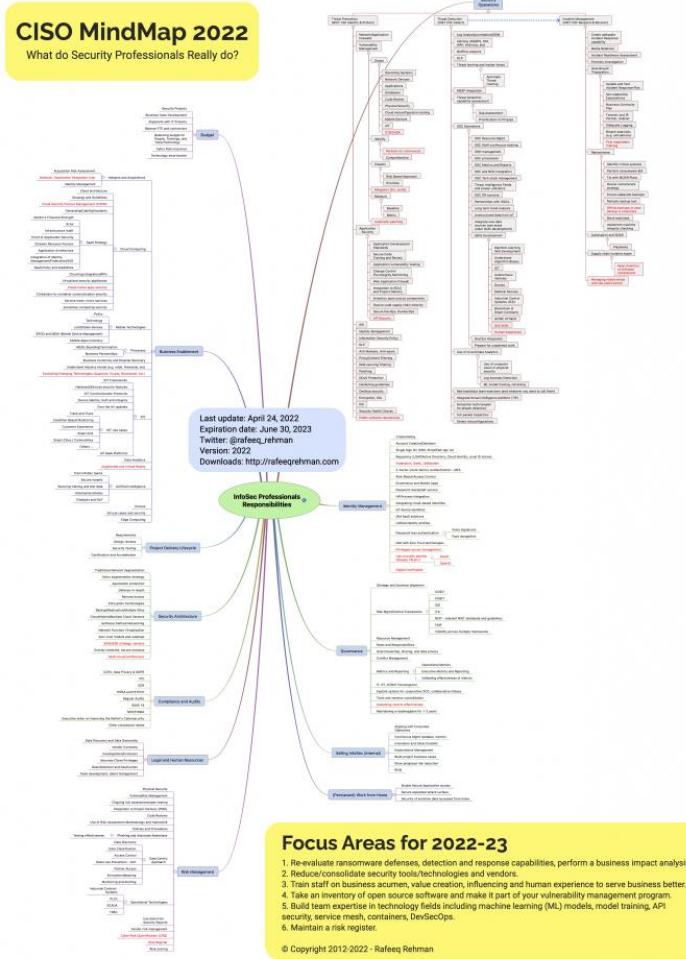
CISO Mind Map 2015



Source: Rafeeq Rehman: <http://rafeeqrehman.com/2015/05/17/the-latest-2015-ciso-mindmap-is-here/>



CISO Mind Map 2022



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



#SysAdminDay
Virtual Event
July 29, 2022

Cyber Security Role

- <https://www.cyberseek.org/pathway.html>
- <https://niccs.cisa.gov/workforce-development/cyber-career-pathways-tool>



Cyber Security Job Opportunities



IT security and Data Protection Manager

Boots Retail (Thailand) Ltd.

ดินแดง

- experiences in information security
- Knowledge and experience in multiple security
- Fluently in Thai and English

19 ชั่วโมงที่ผ่านมา



IT Cyber Security Analyst

Autoliv (Thailand) Ltd.

กรุงเทพมหานคร

- SIEM, IDS/IPS and other security data sources
- IT Security assurance
- FLUENT ENGLISH IS STRONGLY REQUIRED

19 ชั่วโมงที่ผ่านมา



Information Security Compliance/Information Security Manager (ISO)

Advanced Personnel and Solutions Co., Ltd.

กรุงเทพมหานคร

- Information Security
- Compliance, ISO
- Security

6 วันที่ผ่านมา



Information Security Specialist – Blue Team

AXA Insurance Public Company Limited

สาทร

- 3-5 years experience in IT security
- Digital learning platform to grow your potential
- Flexi Time / Work from Home / Near MRT Lumpini

19 ชั่วโมงที่ผ่านมา



Senior IT Security

Honda Leasing (Thailand) Co., Ltd.

บางนา

- 3-5 years relevant experiences in IT Security
- Knowledge of various information security
- Good communication skills in English

2 วันที่ผ่านมา



Information Security Engineer (Corporate Security & Governance)

LINE Company (Thailand) Limited

ปทุมธานี

- Experience in a corporate security policy
- Understanding of Thailand PDPA
- Experience building ISMS or PIMS for enterprises

3 วันที่ผ่านมา



Cyber Security Job Opportunities



IT Security Governance and Architecture

TMBThanachart Bank or ttb / ทีเอ็มบีธนชาต หรือ ทีทีบี

กรุงเทพมหานคร

- Cyber Security Technology and solutions
- IT Security Governance
- OT, ISO27001, PCI DSS

5 วันที่ผ่านมา



Cyber Security (Penetration Professional)

Bangkok Bank Public Company Limited

ยานนาวา

- Penetration testing, security hardening
- Conduct the risk-based analysis
- Consolidate and Tracking the vulnerabilities.



2 วันที่ผ่านมา



IT Security Architect

Krungthai Bank PCL

รัตนนา

- security advisory
- IT risks and compliance
- secure development practices

3 วันที่ผ่านมา



Senior IT Auditor/เจ้าหน้าที่อิจูสติวิสต์ตรวจสอบระบบ

สารสนเทศ

Betagro Public Company Limited

หลักสี่

- ประสบการณ์ 3 ปี ด้าน IT Audit, IT Security
- มีความรู้เกี่ยวกับ COBIT, ITIL, ITGC, COSO
- มี Certificate CISA,CISM,CISSP,CIA จะพิจารณาพิเศษ

5 วันที่ผ่านมา



IT Security Specialist

Greenline Synergy Co., Ltd.

สวนหลวง

- IT knowledge is all around you in everyday
- Culture of Sharing and innovation
- Develop technical solutions and new security tools



3 วันที่ผ่านมา



Manager, SOC & Cyber Security

dtac

ปทุมธานี

- Experience as SOC, Cyber Security Incident Manager
- Strong Vendor Management Skill
- Flexible working hours & Work from home

4 วันที่ผ่านมา

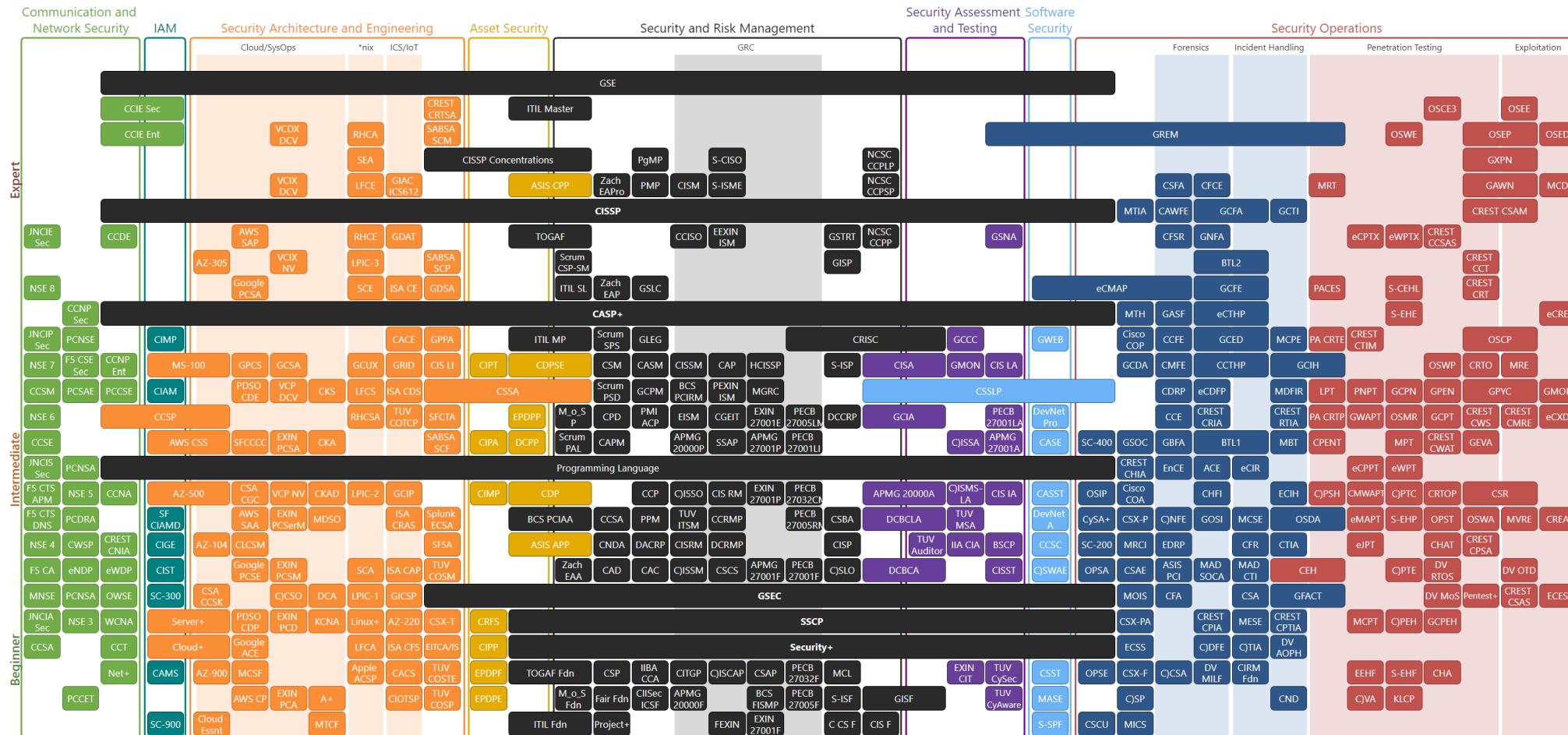


#SysAdminDay

Virtual Event

July 29, 2022

Cyber Security Certification Roadmap



<https://pauljeremy.com/security-certification-roadmap/>



Cyber Security Role

- Certified Information Systems Security Professional [CISSP] | Thailand [284](#) | Member counts are updated bi-annually
- Certified Information Security Manager [CISM]
- Certified in Risk and Information Systems Control [CRISC]
- Certified Information Systems Auditor [CISA]
- CompTIA Security+
- CompTIA Cybersecurity Analyst [CySA+]
- CompTIA Advanced Security Practitioner [CASP+]
- Certified Ethical Hacker [CEH]
- **Blue Team Level 1 [BTL1]**



Sharing Experiences BTL1 EXAM



#SysAdminDay
Virtual Event
July 29, 2022

Blue Team Level 1 [BTL1]

Blue Team Level 1 [BTL1]

- Domain 1 - Security Fundamentals
- Domain 2 - Phishing Analysis
- Domain 3 - Threat Intelligence
- Domain 4 - Digital Forensics
- Domain 5 - SIEM
- Domain 6 - Incident Response



Blue Team Level 1 [BTL1]

Blue Team Level 1 [BTL1]

- Domain 1 - Security Fundamentals
 - Introduction to Security Fundamentals
 - Soft Skills
 - Security Controls
 - Networking 101
 - Management Principles
- Domain 2 - Phishing Analysis
 - Introduction to Emails and Phishing
 - Types of Phishing Emails
 - Tactics and Techniques Used
 - Analyzing URLs, Attachments, and Artifacts
 - Taking Defensive Measures
 - Report Writing
 - Lessons Learned
 - Phishing Response Challenge



Blue Team Level 1 [BTL1]

Blue Team Level 1 [BTL1]

- Domain 3 - Threat Intelligence
 - Introduction to Threat Intelligence
 - Threat Actors and APTs
 - Operational Threat Intelligence
 - Tactical Threat Intelligence
 - Strategic Threat Intelligence
 - Malware and Global Campaigns
- Domain 4 - Digital Forensics
 - Introduction to Digital Forensics
 - Forensics Fundamentals
 - Digital Evidence Collection
 - Windows Investigations
 - Linux Investigations
 - Volatility
 - Autopsy



Blue Team Level 1 [BTL1]

Blue Team Level 1 [BTL1]

- Domain 5 - SIEM
 - Introduction to SIEM
 - Logging
 - Aggregation
 - Correlation
 - Using Splunk SIEM
- Domain 6 - Incident Response
 - Introduction to Incident Response
 - Preparation Phase
 - Detection and Analysis Phase
 - Containment, Eradication, and Recovery Phase
 - Lessons Learned
 - MITRE ATT&CK



Blue Team Level 1 [BTL1]

300+

LESSONS, VIDEOS, ACTIVITIES
AND QUIZZES

18

BROWSER LABS WITH 100
HOURS OF ACCESS

4 Months

ACCESS TO THE TRAINING
MATERIAL

£399

TRAINING AND EXAM PRICE

Individuals:
Register Now →

Team Leaders:
Request A Quote →

Download
Informational PDF 

Free BTL1 Demo
Access →

<https://securityblue.team/why-btl1/>



#SysAdminDay
Virtual Event
July 29, 2022

Blue Team Level 1 [BTL1]

C

Contact <Contact@securityblue.team>
to me ▾

Fri, Oct 15, 2021, 3:03 PM



Dear Chonlatit,

We are pleased to announce that you have successfully passed the Blue Team Level 1 certification exam with a **score of 100/100%!** If this is your first attempt, then you are eligible for our **GOLD challenge coin!** Please confirm your full name as shown below and state your current postal address (house name/number, street name, city name, postcode, country) so we can issue your Acclaim digital badge and post your physical rewards including certificate and challenge coin.

- You all of the key events in this exam and demonstrated your competency with SIEM, forensics, phishing, and incident response knowledge and practical ability.
- Your Incident Questions section was completed with a huge amount of detail, investigating all leads.
- Your Post Incident Recommendations section was very well done - good work!



Exam Feedback (DO NOT SHARE ANY EXAM DETAILS WITH ANYONE. DO NOT BREACH THE EXAM NDA):

Blue Team Level 1 [BTL1]

The image displays a collage of screenshots from the Blue Team Academy platform, illustrating the curriculum and tools used for training blue team members.

- Top Left:** A screenshot of the main academy dashboard for a user named "JO". It shows sections for "Introduction", "Security Fundamentals", "Phishing Analysis", "Threat Intelligence", "Incident Response", and "BTL1 Exam Preparation".
- Top Middle:** A screenshot of the "Your Hours" section, showing 115.6 Hours Left and a progress bar indicating tasks completed.
- Top Right:** A screenshot of the "Physical Security" module, which includes sections on "Introduction to Security Fundamentals", "Soft Skills", and "Physical Security".
- Bottom Left:** A screenshot of a threat intelligence exercise titled "APT41". It details the mission to collect information on the threat group APT41 and lists tactics such as T1112 - Modify Registry, T1192 - Spear Phishing Link, T1123 - Audio Capture, T1053 - Scheduled Task, and T1055 - Process Injection.
- Bottom Middle:** A screenshot of a terminal window running Volatility Framework 2.6.1 on an Ubuntu 10.0.7-148 system. The command `vol.py -f /home/ubuntu/Desktop/Volatility Exercise/memdump1.mem` is being run, and the output shows memory dump files (memdump, memdump1) and a file manager listing them.
- Bottom Right:** A screenshot of the "Questions" section of the Volatility exercise, containing three memory identification questions and a generic process list question.

Blue Team Level 1 [BTL1]



Blue Team Level 1 [BTL1]



SECURITY BLUE TEAM



Blue Team Level 1
JUNIOR SECURITY OPERATIONS



Security operations training course and certification exam that teaches students real-world, applicable skills and knowledge across 5 domains:

- Phishing Analysis
- Threat Intelligence
- Digital Forensics
- Security Information & Event Management
- Incident Response

Includes 4 months of on-demand access, 120 lab hours, and 2 certification exam attempts.
Discounts start at 5 students.



300+
Lessons, videos, activities and quizzes



16
Browser-based labs



24 Hour
Realistic incident response exam lab

1

Common Use Case

The vast majority of our clients use BTL1 as a standard for all of their analysts, baselining their skills and demonstrating professional development.

2

Common Use Case

Our clients use BTL1 as part of their internal promotion pipeline, identifying when analysts have the skills to move to a more senior position.



Blue Team Level 1 [BTL1]

C

SBT Support <contact@securityblue.team>

to me ▾

Tue, Jun 7, 6:07 AM



Hi there, your package has been dispatched! You'll be able to track it using the following URL and code shortly! <https://www.royalmail.com/track-your-item> ---
[REDACTED]

Kind regards,

Student Support Team

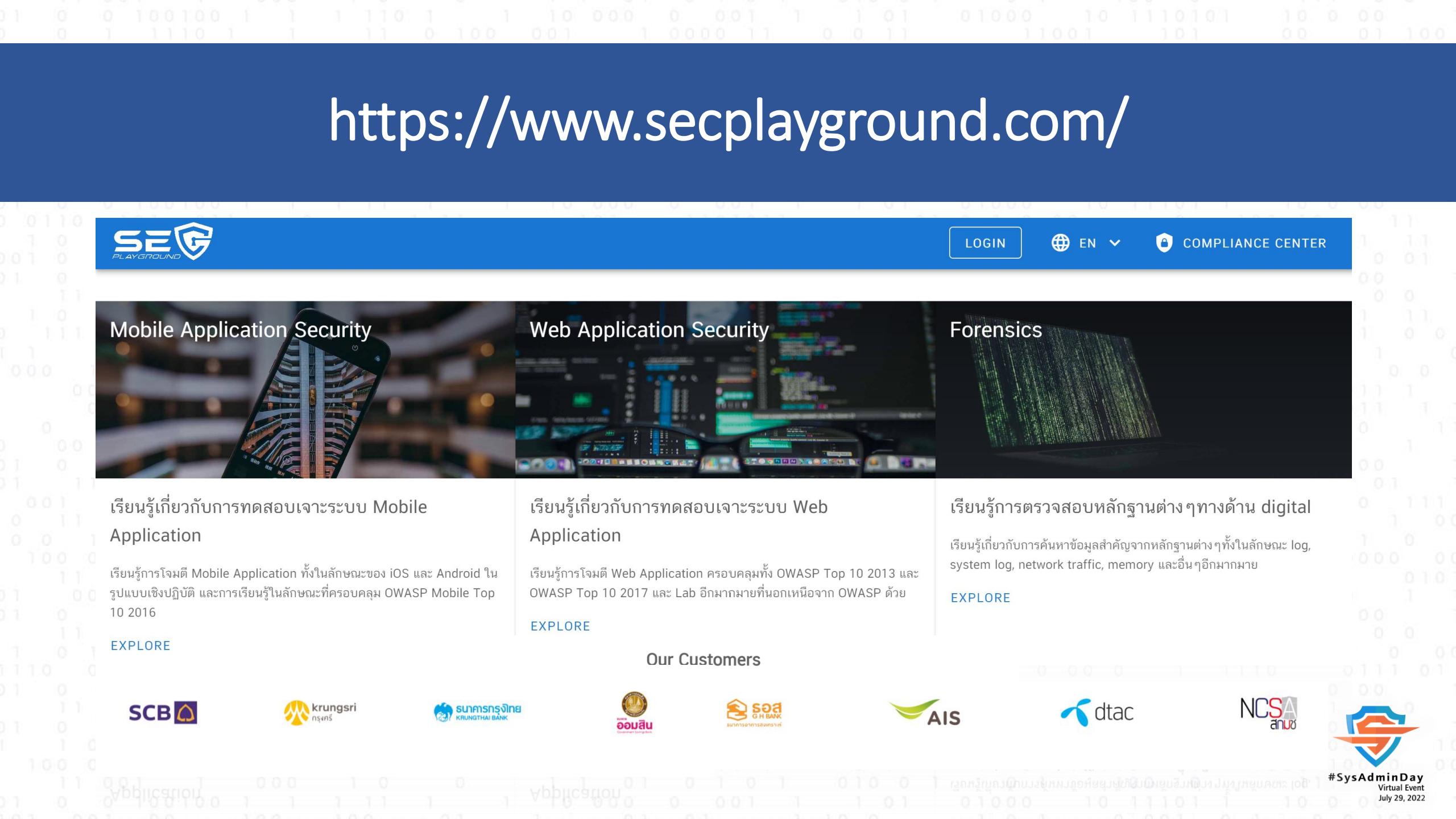
Security Blue Team

Office Hours: 9AM - 5PM (GMT)



#SysAdminDay
Virtual Event
July 29, 2022

<https://www.secplayground.com/>



The screenshot shows the homepage of the SEC PLAYGROUND website. The header features the logo "SEC PLAYGROUND" with a shield icon, a "LOGIN" button, and language selection "EN". A "COMPLIANCE CENTER" link is also present. Below the header are three main sections: "Mobile Application Security" (image of a smartphone), "Web Application Security" (image of a computer monitor displaying multiple windows and logs), and "Forensics" (image of a laptop screen showing green binary or hex code). Each section has a brief description and an "EXPLORE" button.

Mobile Application Security



เรียนรู้เกี่ยวกับการทดสอบเจาะระบบ Mobile Application

เรียนรู้การโจมตี Mobile Application ทั้งในลักษณะของ iOS และ Android ในรูปแบบเชิงปฏิบัติ และการเรียนรู้ในลักษณะที่ครอบคลุม OWASP Mobile Top 10 2016

[EXPLORE](#)

Web Application Security



เรียนรู้เกี่ยวกับการทดสอบเจาะระบบ Web Application

เรียนรู้การโจมตี Web Application ครอบคลุมทั้ง OWASP Top 10 2013 และ OWASP Top 10 2017 และ Lab อีกมากmany ที่นอกเหนือจาก OWASP ด้วย

[EXPLORE](#)

Forensics



เรียนรู้การตรวจสอบหลักฐานต่างๆทางด้าน digital

เรียนรู้เกี่ยวกับการค้นหาข้อมูลสำคัญจากหลักฐานต่างๆทั้งในลักษณะ log, system log, network traffic, memory และอื่นๆอีกมากมาย

[EXPLORE](#)



Question & Answer



#SysAdminDay
Virtual Event
July 29, 2022



iKNEX

*Knowledge Sharing
for a Changing World*



Thank you



System Administrator Appreciation Day 2022
(Friday) July 29, 2022



#SysAdminDay
Virtual Event
July 29, 2022