CyBOK

Foundations and Resources for the Community

Professor Awais Rashid

contact@cybok.org
www.cybok.org

Codify ***foundational*** and generally recognised knowledge in cyber security following broad community engagement nationally and internationally

A ***guide*** to the body of knowledge

Focus is on ***established foundation*** of the subject (not on everything that has ever been written or on still-emerging, nascent, topics)

International effort

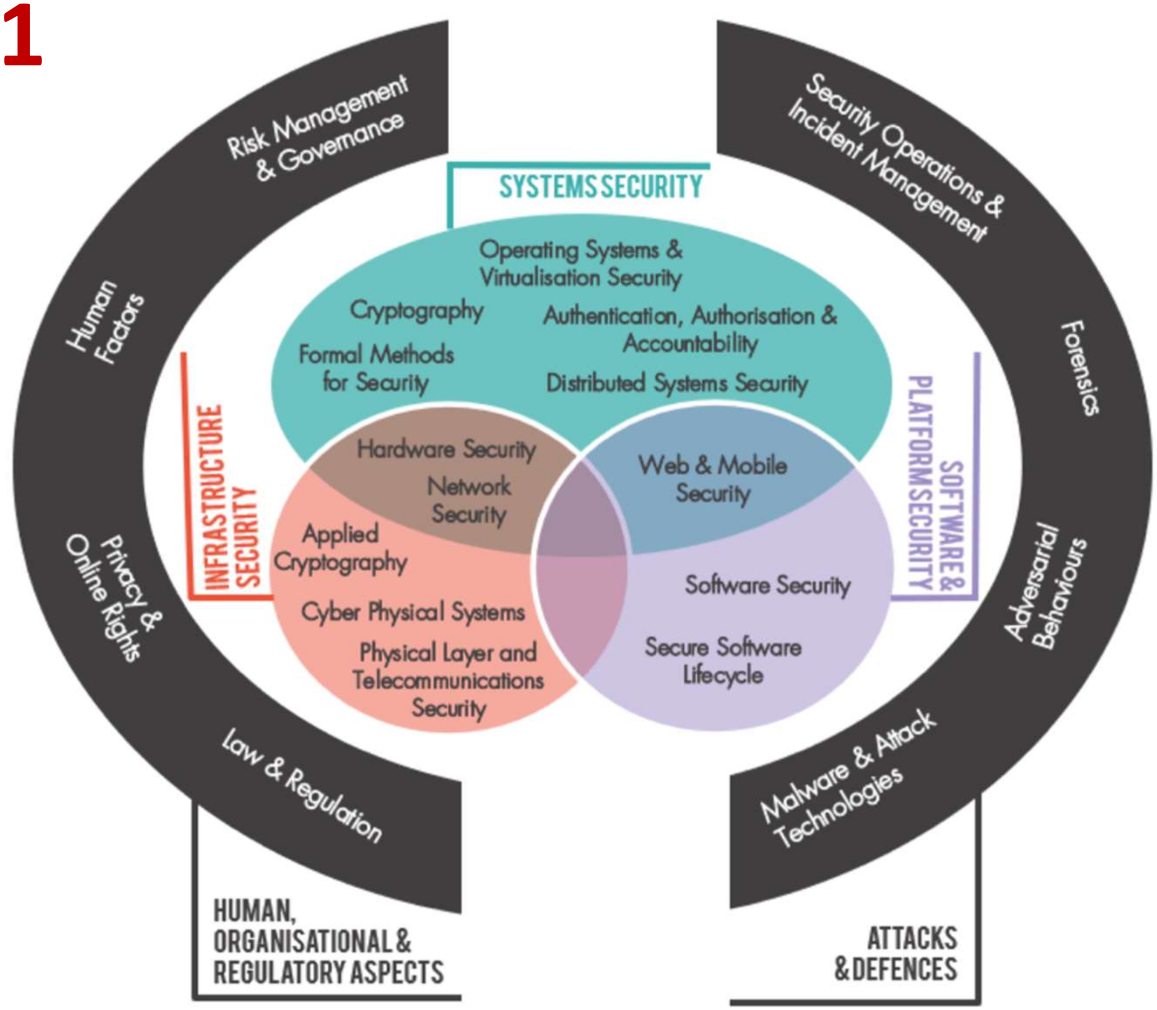
For the community by the community

Open and freely accessible

Transparency

>115	Experts: Authors, Reviewers, Advisors
>1000	Pages
>2200	Authoritative sources
>1600	Comments from wider community
>30	Invited talks, panels and keynotes

CyBOK 1.1


Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
Cryptography
Authentication, Authorisation & Accountability
Formal Methods for Security
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Applied Cryptography
Cyber Physical Systems
Physical Layer and Telecommunications Security
Web & Mobile Security
Software Security
Secure Software Lifecycle
SOFTWARE & PLATFORM SECURITY
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

Keeping the Foundations Strong

Open call for proposals to update current KAs or propose new ones: *CyBOK 1.0 -> CyBOK 1.1*

Not just reactive but also proactive: *ongoing development of a process of expert review of subsets of KAs leading to regular refresh*

Pro-actively develop guides that capture practical pathways through CyBOK or emerging knowledge in the community

Supplementing the Foundations

Knowledge Guides: Emerging topics or those that are still developing broadly agreed foundations

- Security and Privacy of AI
- Security Economics

Topic Guides: Practical applications that cut across multiple CyBOK KAs

- AI for Security
- *Cloud Security*

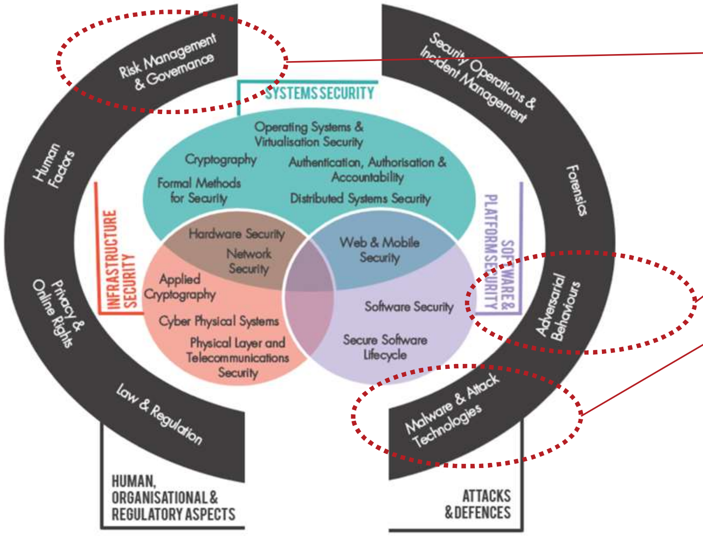
Working collaboratively with the Council

Sharing knowledge of CyBOK processes and governance structures

Supporting mappings as qualifications frameworks developed

Develop a strategy for sustainability of CyBOK for the medium to long term

How to build on the Foundation?


Risk Management & Governance
SYSTEMS SECURITY
Security Operations & Incident Management
Human Factors
Operating Systems & Virtualisation Security
Cryptography
Authentication, Authorisation & Accountability
Formal Methods for Security
Distributed Systems Security
Forensics
INFRASTRUCTURE SECURITY
SOFTWARE & PLATFORM SECURITY
Hardware Security
Network Security
Web & Mobile Security
Applied Cryptography
Software Security
Cyber Physical Systems
Privacy & Online Rights
Adversarial Behaviours
Physical Layer and Telecommunications Security
Secure Software Lifecycle
Law & Regulation
Malware & Attack Technologies
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
ATTACKS & DEFENCES

Risk Management & Governance

Adversarial Behaviours

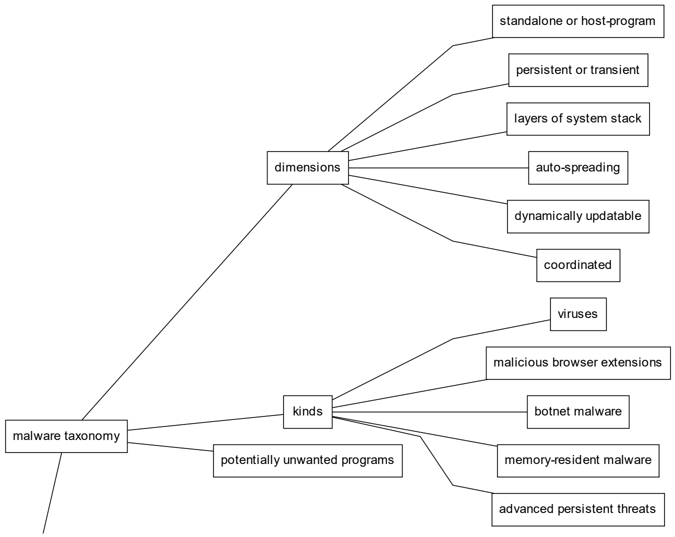
Malware and Attack Technologies

Mapping reference with > 13000 terms

An index for easy look up of terms

Designing a new training course

CyBOK



- malware taxonomy
  - dimensions
    - standalone or host-program
    - persistent or transient
    - layers of system stack
    - auto-spreading
    - dynamically updatable
    - coordinated
  - kinds
    - viruses
    - malicious browser extensions
    - botnet malware
    - memory-resident malware
    - advanced persistent threats
  - potentially unwanted programs

PODCAST

Webinars

Slides

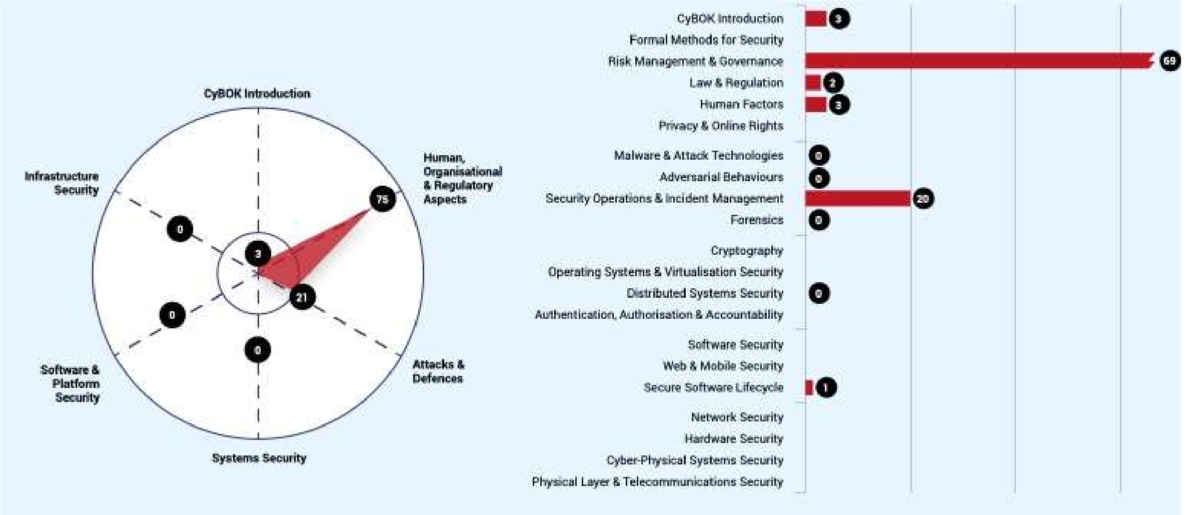
Lesson Plans, Labs and Exercises

Designing a new training course

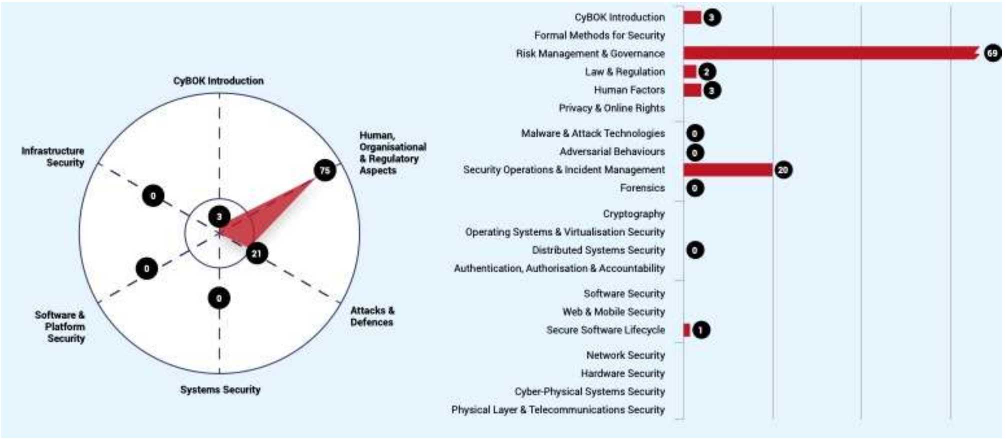
CyBOK

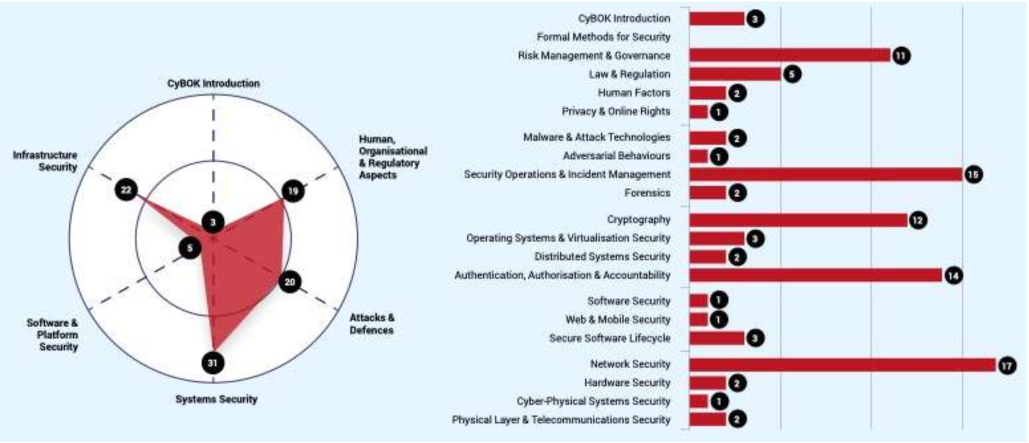
Mapping reference with > 13000 terms

Mapping Framework



Showing a course meets training needs

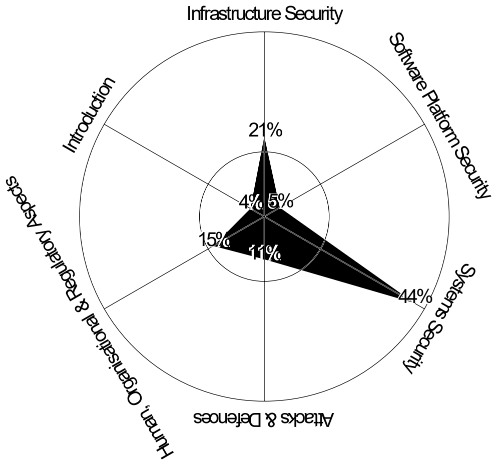


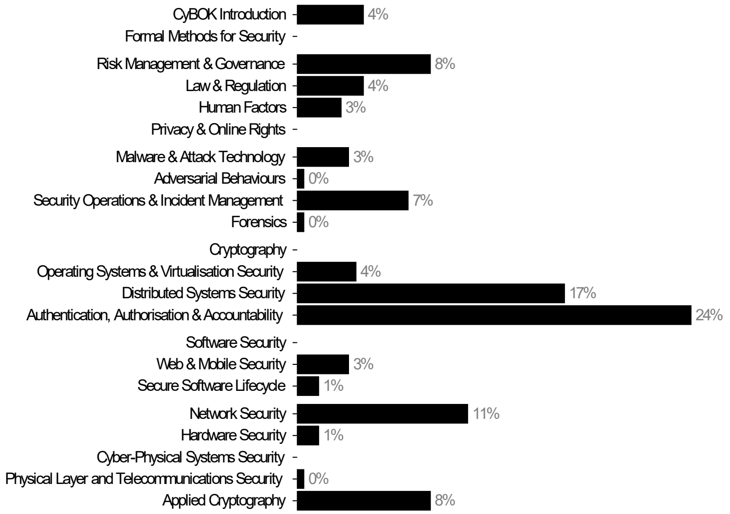


Learner, Recruiter, Certification Body

CyBOK

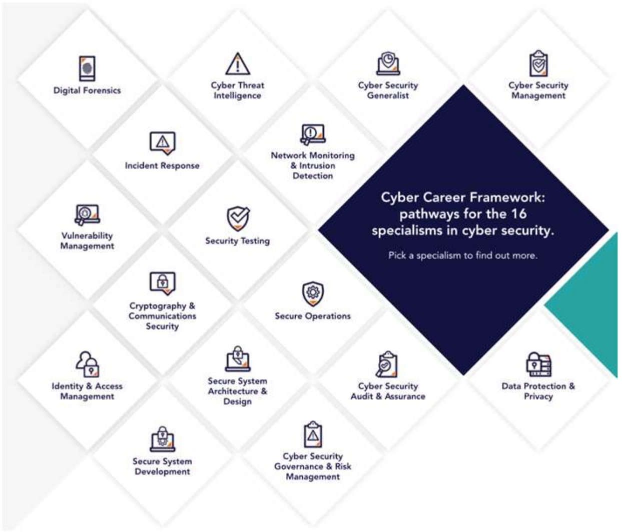
NCSC Cyber Advisor
(Cyber Essentials)





What knowledge to assess for particular roles?

CyBOK



Digital Forensics

Cyber Threat Intelligence

Cyber Security Generalist

Cyber Security Management

Incident Response

Network Monitoring & Intrusion Detection

Cyber Career Framework: pathways for the 16 specialisms in cyber security.

Pick a specialism to find out more.

Vulnerability Management

Security Testing

Cryptography & Communications Security

Secure Operations

Identity & Access Management

Secure System Architecture & Design

Cyber Security Audit & Assurance

Data Protection & Privacy

Secure System Development

Cyber Security Governance & Risk Management

CyBOK

UK CYBER SECURITY COUNCIL

What knowledge to assess for particular roles?

CyBOK

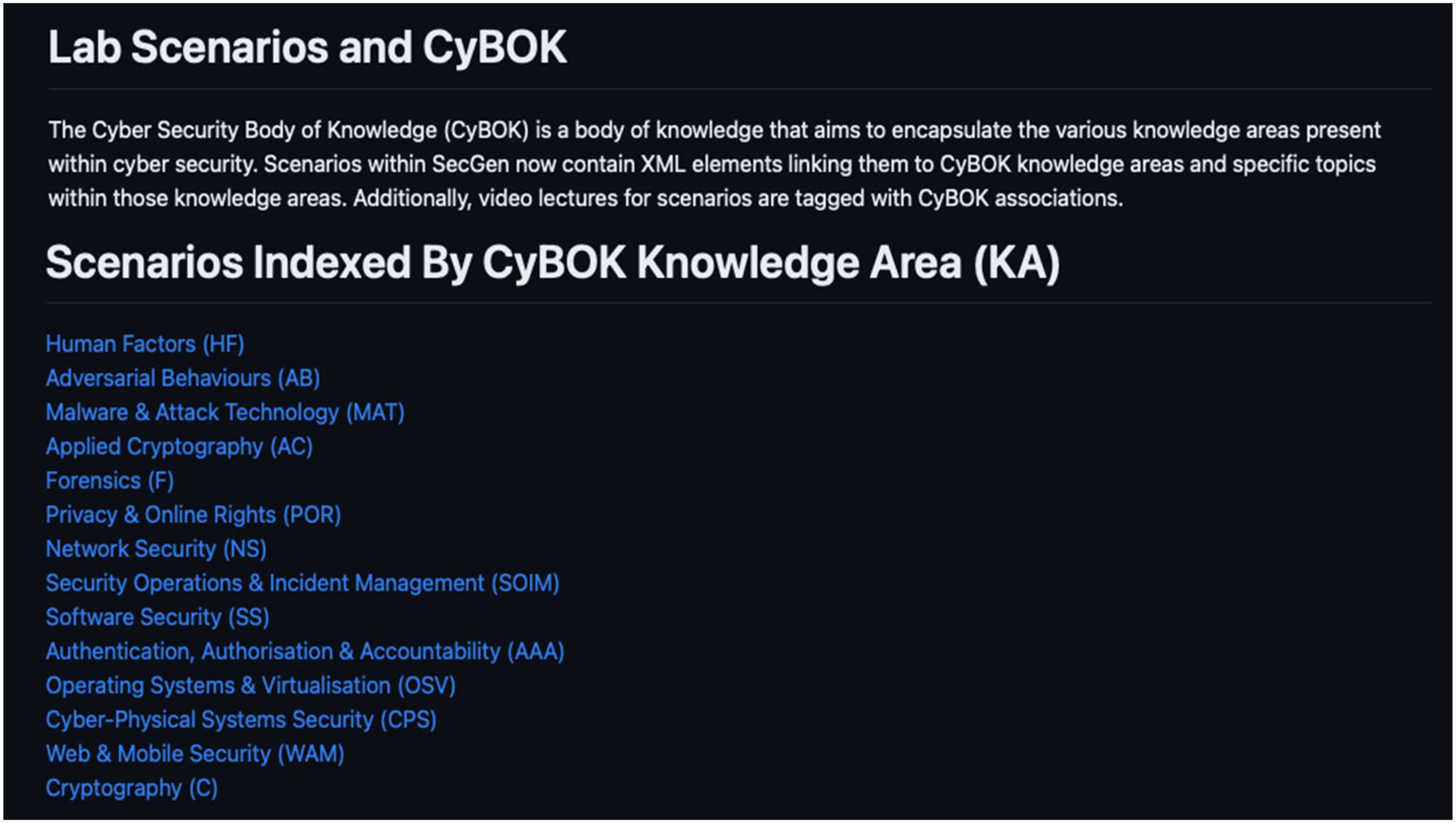
Practical exercises, labs and CTFs

Case studies

Learning skills to apply particular knowledge

CyBOK

Labs for multiple CyBOK KAs *(Cliffe Schreuders)*



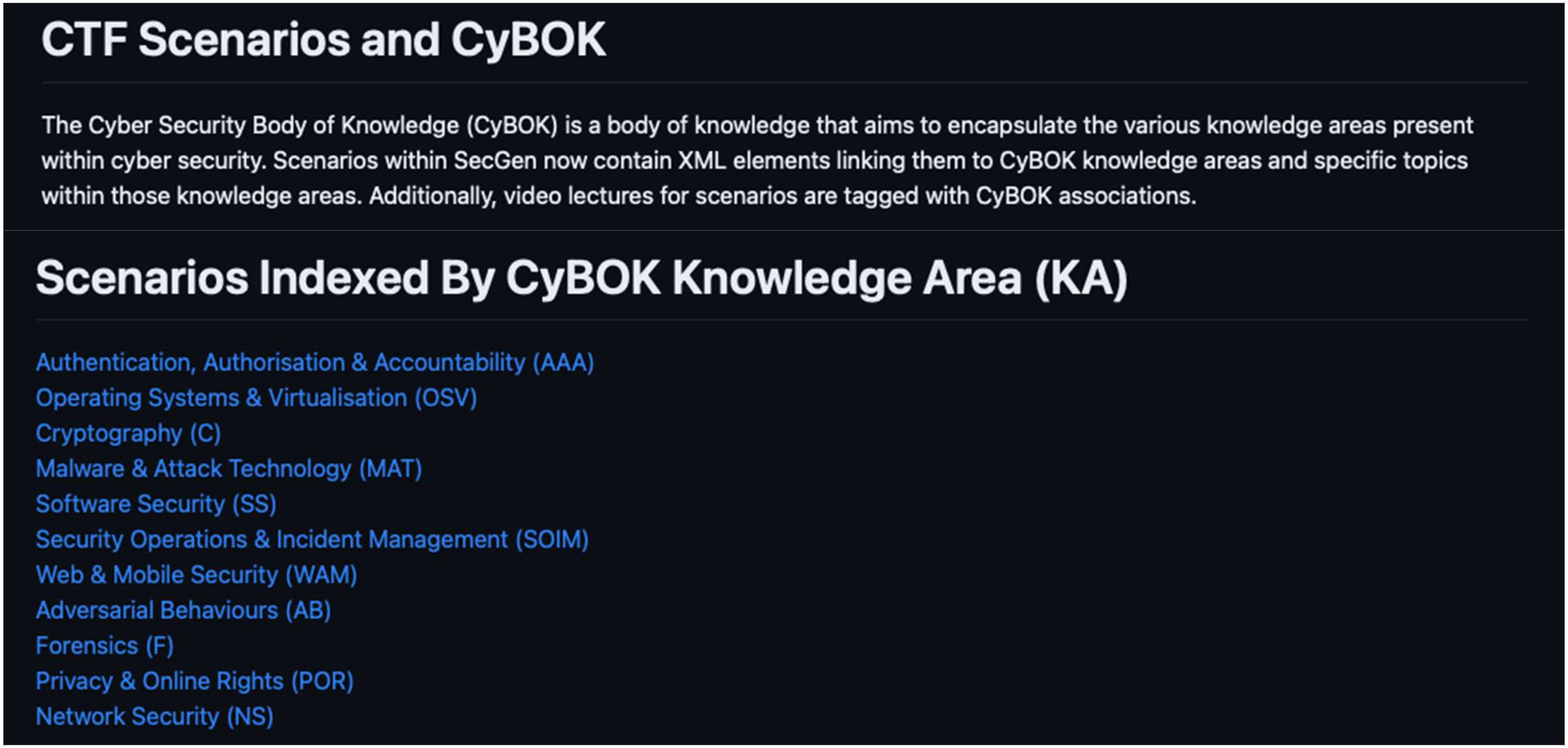
Lab Scenarios and CyBOK

The Cyber Security Body of Knowledge (CyBOK) is a body of knowledge that aims to encapsulate the various knowledge areas present within cyber security. Scenarios within SecGen now contain XML elements linking them to CyBOK knowledge areas and specific topics within those knowledge areas. Additionally, video lectures for scenarios are tagged with CyBOK associations.

Scenarios Indexed By CyBOK Knowledge Area (KA)

Human Factors (HF)
Adversarial Behaviours (AB)
Malware & Attack Technology (MAT)
Applied Cryptography (AC)
Forensics (F)
Privacy & Online Rights (POR)
Network Security (NS)
Security Operations & Incident Management (SOIM)
Software Security (SS)
Authentication, Authorisation & Accountability (AAA)
Operating Systems & Virtualisation (OSV)
Cyber-Physical Systems Security (CPS)
Web & Mobile Security (WAM)
Cryptography (C)

CTFs for multiple CyBOK KAs *(Cliffe Schreuders)*



CTF Scenarios and CyBOK

The Cyber Security Body of Knowledge (CyBOK) is a body of knowledge that aims to encapsulate the various knowledge areas present within cyber security. Scenarios within SecGen now contain XML elements linking them to CyBOK knowledge areas and specific topics within those knowledge areas. Additionally, video lectures for scenarios are tagged with CyBOK associations.

Scenarios Indexed By CyBOK Knowledge Area (KA)

Authentication, Authorisation & Accountability (AAA)
Operating Systems & Virtualisation (OSV)
Cryptography (C)
Malware & Attack Technology (MAT)
Software Security (SS)
Security Operations & Incident Management (SOIM)
Web & Mobile Security (WAM)
Adversarial Behaviours (AB)
Forensics (F)
Privacy & Online Rights (POR)
Network Security (NS)

Practical Exercises for Specific KAs

Memory Analysis Workshop *(Joakim Kävrestad)*	**Forensics** **Malware and Attack Technologies**
Practicals for Formal Methods *(Martin Lester)*	**Formal Methods for Security**
GSM Labs *(Denis Nicole)*	**Physical Layer and Telecommunications Security**
Wireless Remote Control Labs *(Denis Nicole)*	**Physical Layer and Telecommunications Security**
Mapping of Cyber Security Games *(Joseph Hallett)*	**Human Factors** **Risk Management and Governance**
Secure Coding Game-based Lab *(Manuel Maarek)*	**Software Security** **Secure Software Lifecycle**
Interactive Cyber-physical Systems Lab *(Phil Legg)*	**Cyber-Physical Systems Security**

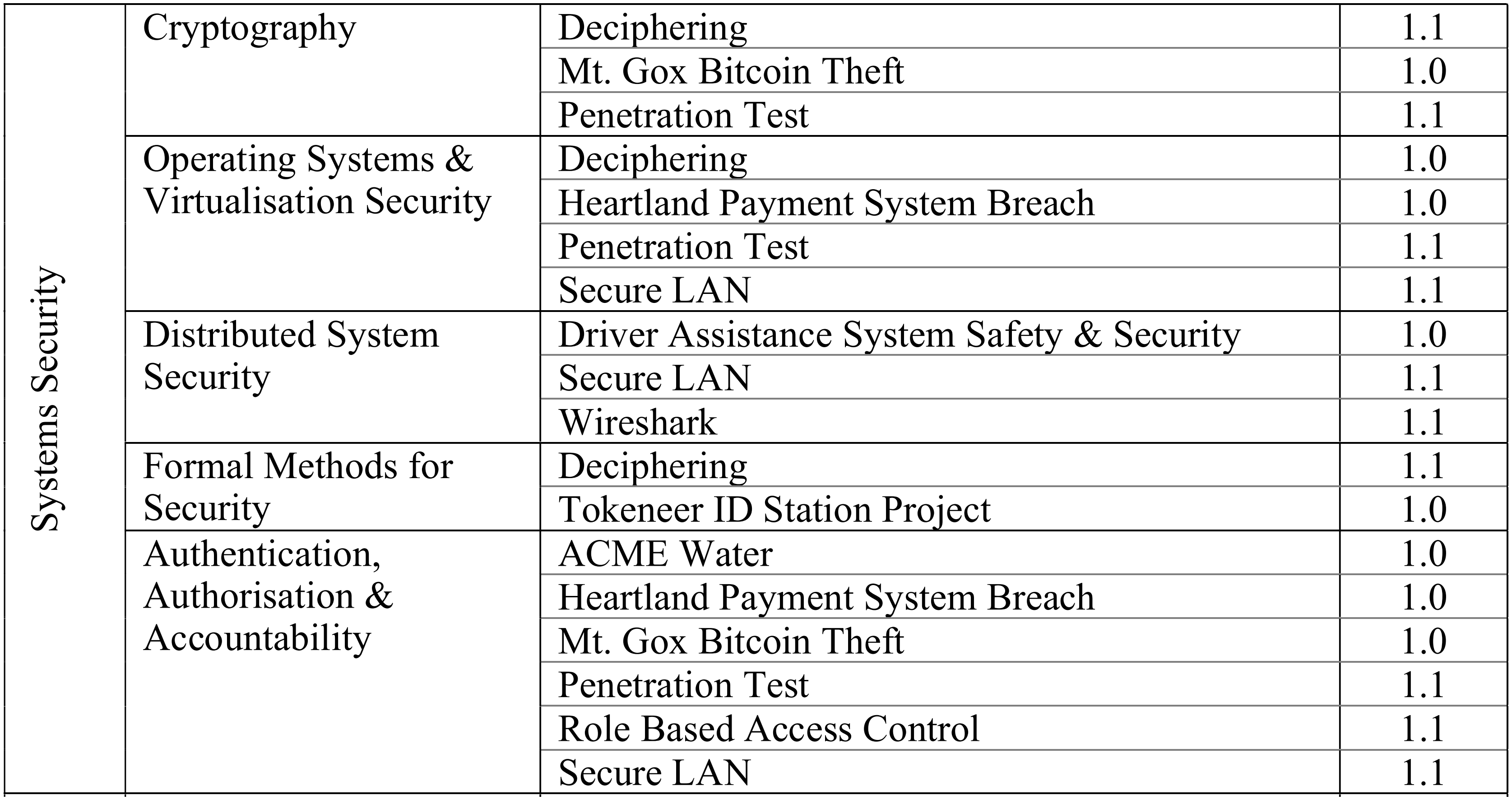
Case Studies for multiple CyBOK KAs *(Nancy Mead)*

Cat.	Knowledge Area	Case Study Mapping	CyBOK version
Human, Organizational and Regulatory Aspects	Risk Management & Governance	ACME Water	1.0
		Archetypal Users – Personae non Gratae	1.0
		FAA ERAM Outage	1.0
		GPS Spoofing of UAV	1.0
		National Cybersecurity Governance	1.1
		National Grid SAP Adoption	1.0
		Organization Risk Management: The Widget Company	1.0
		Penetration Test	1.1
		Ransomware	1.1
		Secure LAN	1.1
	Law & Regulation	National Cybersecurity Governance	1.0
		Ransomware	1.1
	Human Factors	ACME Water	1.0
		FAA ERAM Outage	1.0
	Privacy & Online Rights	ACME Water	1.0
		Driver Assistance System Safety & Security	1.0
		Penetration Test	1.1
		Role Based Access Control	1.1

Case Studies for multiple CyBOK KAs *(Nancy Mead)*

Attacks and Defences	Malware & Attack Technologies	Deciphering	1.0
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
		Ransomware	1.1
		Using Malware Analysis to Improve Security Reqs	1.1
		Wireshark	1.1
	Adversarial Behaviours	Heartland Payment System Breach	1.0
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
		Ransomware	1.1
	Security Operations & Incident Management	Heartland Payment System Breach	1.0
		Mt. Gox Bitcoin Theft	1.0
		National Cybersecurity Governance	1.1
		Penetration Test	1.1
		Ransomware	1.1
	Forensics	Mt. Gox Bitcoin Theft	1.0
		Wireshark	1.1

Case Studies for multiple CyBOK KAs *(Nancy Mead)*



Systems Security	Cryptography	Deciphering	1.1
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
	Operating Systems & Virtualisation Security	Deciphering	1.0
		Heartland Payment System Breach	1.0
		Penetration Test	1.1
		Secure LAN	1.1
	Distributed System Security	Driver Assistance System Safety & Security	1.0
		Secure LAN	1.1
		Wireshark	1.1
	Formal Methods for Security	Deciphering	1.1
		Tokeneer ID Station Project	1.0
	Authentication, Authorisation & Accountability	ACME Water	1.0
		Heartland Payment System Breach	1.0
		Mt. Gox Bitcoin Theft	1.0
		Penetration Test	1.1
		Role Based Access Control	1.1
		Secure LAN	1.1

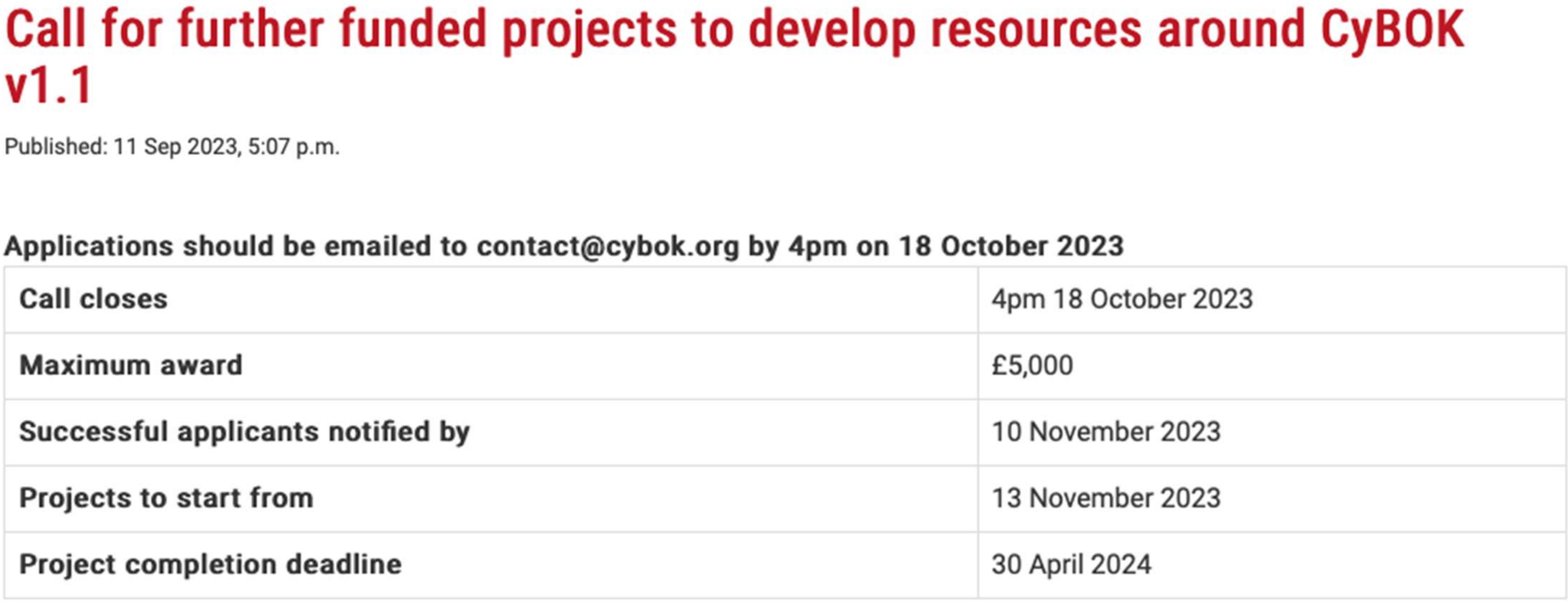
Case Studies for multiple CyBOK KAs *(Nancy Mead)*

Software Platform Security	Software Security	Driver Assistance System Safety & Security	1.0
		FAA ERAM Outage	1.0
		Penetration Test	1.1
	Web & Mobile Security	Driver Assistance System Safety & Security	1.0
		Role Based Access Control	1.1
		Secure LAN	1.1
	Secure Software Lifecycle	ACME Water	1.0
		Aircraft Service Application	1.0
		Drone Swarm	1.0
		National Grid SAP Adoption	1.0
		Secure Acquisition	1.0
		SQUARE	1.0
		Tokeneer ID Station Project	1.0
		Using Malware Analysis to Improve Security Reqs	1.1

Case Studies for multiple CyBOK KAs *(Nancy Mead)*

Infrastructure Security	Applied Cryptography	Deciphering	1.1
		Penetration Test	1.1
	Network Security	Role Based Access Control	1.1
		Secure LAN	1.1
		Wireshark	1.1
	Hardware Security	Driver Assistance System Safety & Security	1.0
	Cyber-Physical Sys Security	Driver Assistance System Safety & Security	1.0
	Physical Layer & Telecommunications	Penetration Test	1.1
		Secure LAN	1.1
		Wireshark	1.1

Join us to build more resources



Call for further funded projects to develop resources around CyBOK v1.1

Published: 11 Sep 2023, 5:07 p.m.

Applications should be emailed to contact@cybok.org by 4pm on 18 October 2023

Call closes	4pm 18 October 2023
Maximum award	£5,000
Successful applicants notified by	10 November 2023
Projects to start from	13 November 2023
Project completion deadline	30 April 2024

CyBOK

For the Community
By the Community