Mirror, Mirror, On the Wall: What are we teaching them all?

Characterising the Focus of Cybersecurity Curricular Frameworks

Joseph Hallett

University of BRISTOL

There are lots of Cyber Security Curricular Frameworks

A couple of questions…

1. Are they all the same?
2. What are they all teaching?
3. Which one is best?

Are they the same?

Nope.

What are they
all teaching?

Risk management and Security ops mostly…

But it depends on the framework…

We’re going to describe them,
and present a method for describing others.

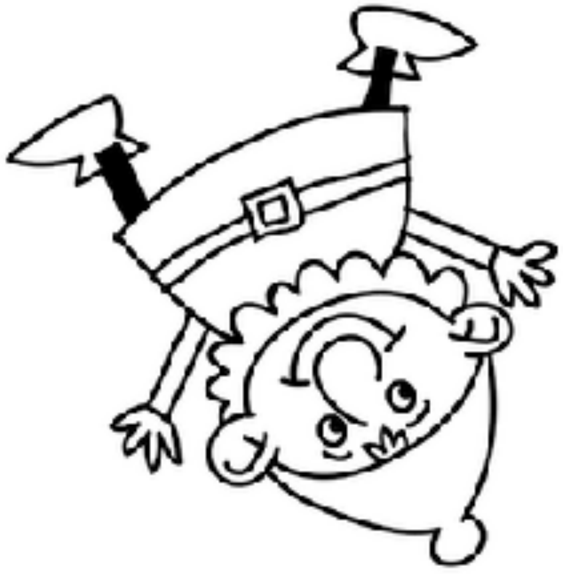
Which one is best?

Nope.

(depends)

They all serve different purposes and we’re not going to be making judgments here.

But we do want to clarify what their content is…



4 Curricular Frameworks

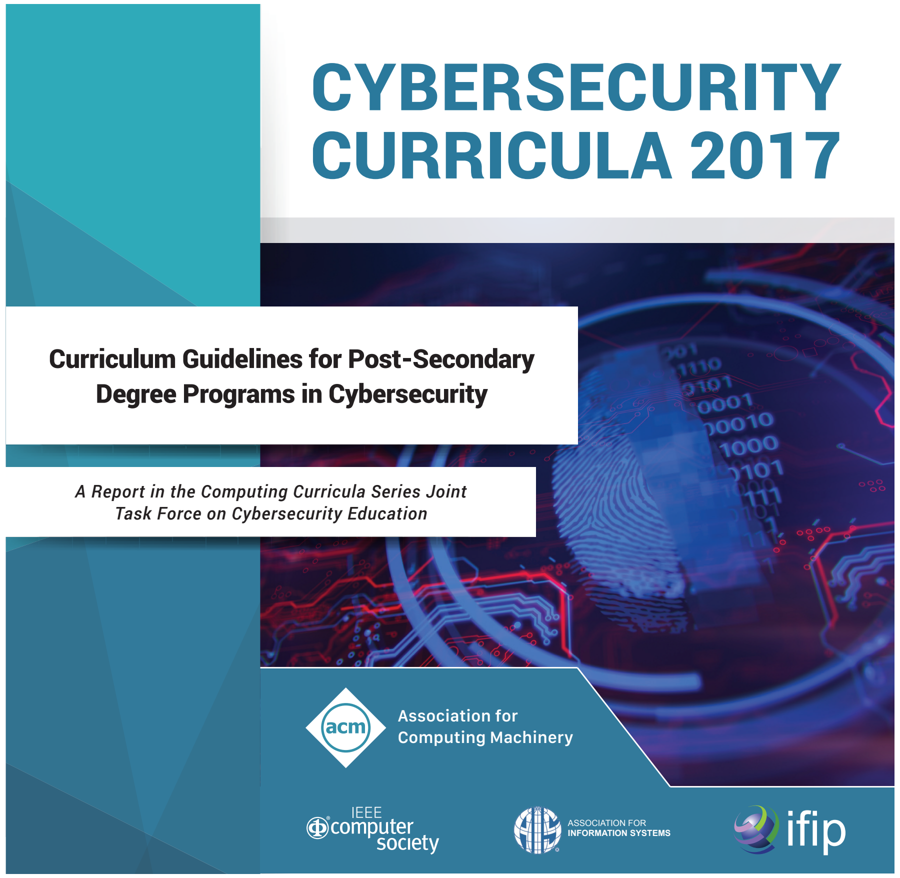
NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

iisp | Knowledge Framework.

National Cyber Security Centre

a part of GCHQ



CYBERSECURITY CURRICULA 2017

Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity

A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education

acm Association for Computing Machinery
IEEE computer society
AIS Association for Information Systems
ifip

IISP Knowledge Framework

UK-based non-profit Cybersecurity professional organisation

What knowledge is required to work in information security?

Aims *“to provide a foundation for curriculum development, course accreditation and for individual professional certification”*

iisp

NCSC Certified Masters Programmes in Cybersecurity

UK framework for cybersecurity degrees
Loosely based on IISP Knowledge Framework

Multiple pathways based around a common set of topics:

A: 4 year Computer science with cybersecurity
B: 4 year Cybersecurity
C: 4 year Digital forensics
CNIS: 4 year Computer networks and internet security

Masters: 1 year broad cybersecurity Masters programme

NICE Cybersecurity Workforce Framework

NIST Special Publication 800-181

Aims to describe all cybersecurity work and act as a reference guide for people implementing education programmes.

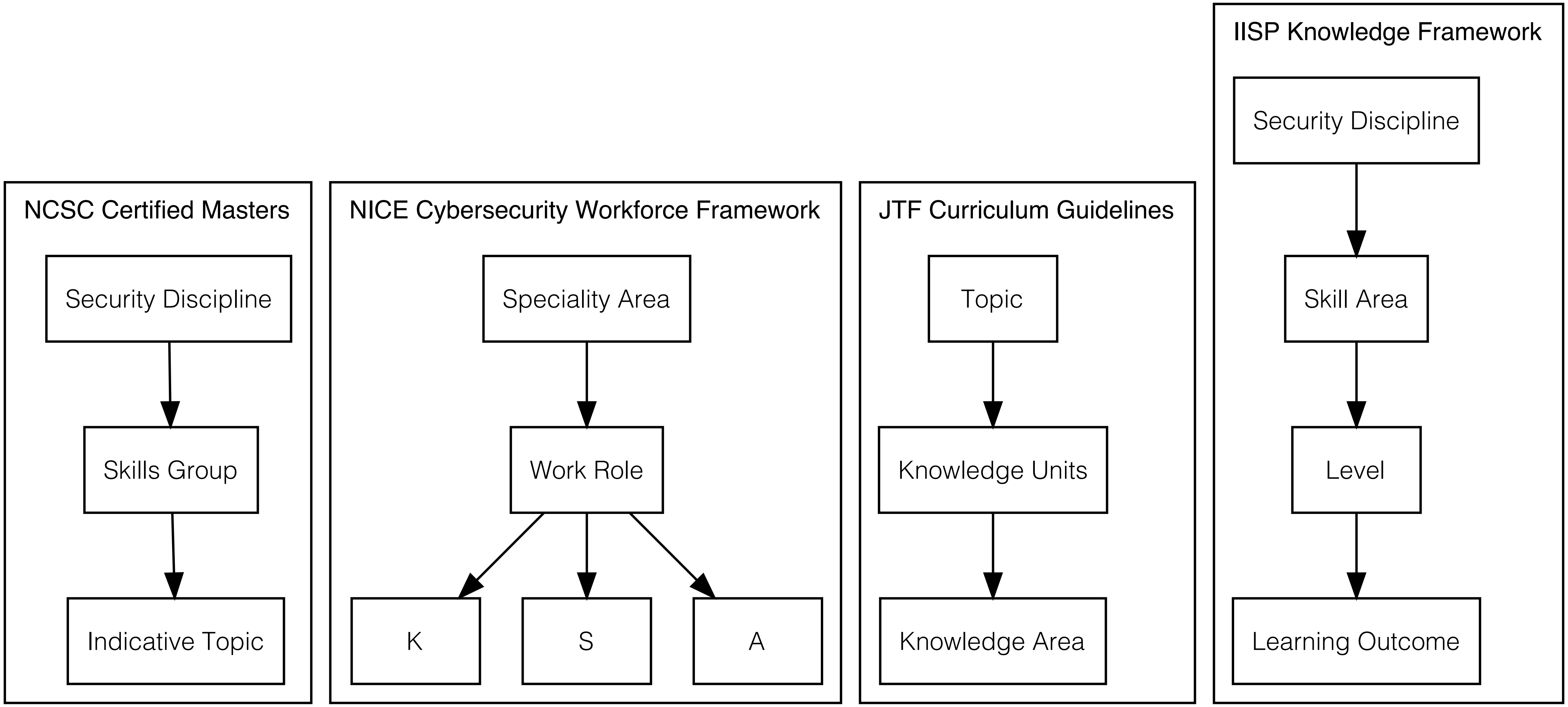
Big lists (~600) of Knowledge, Skills and Abilities

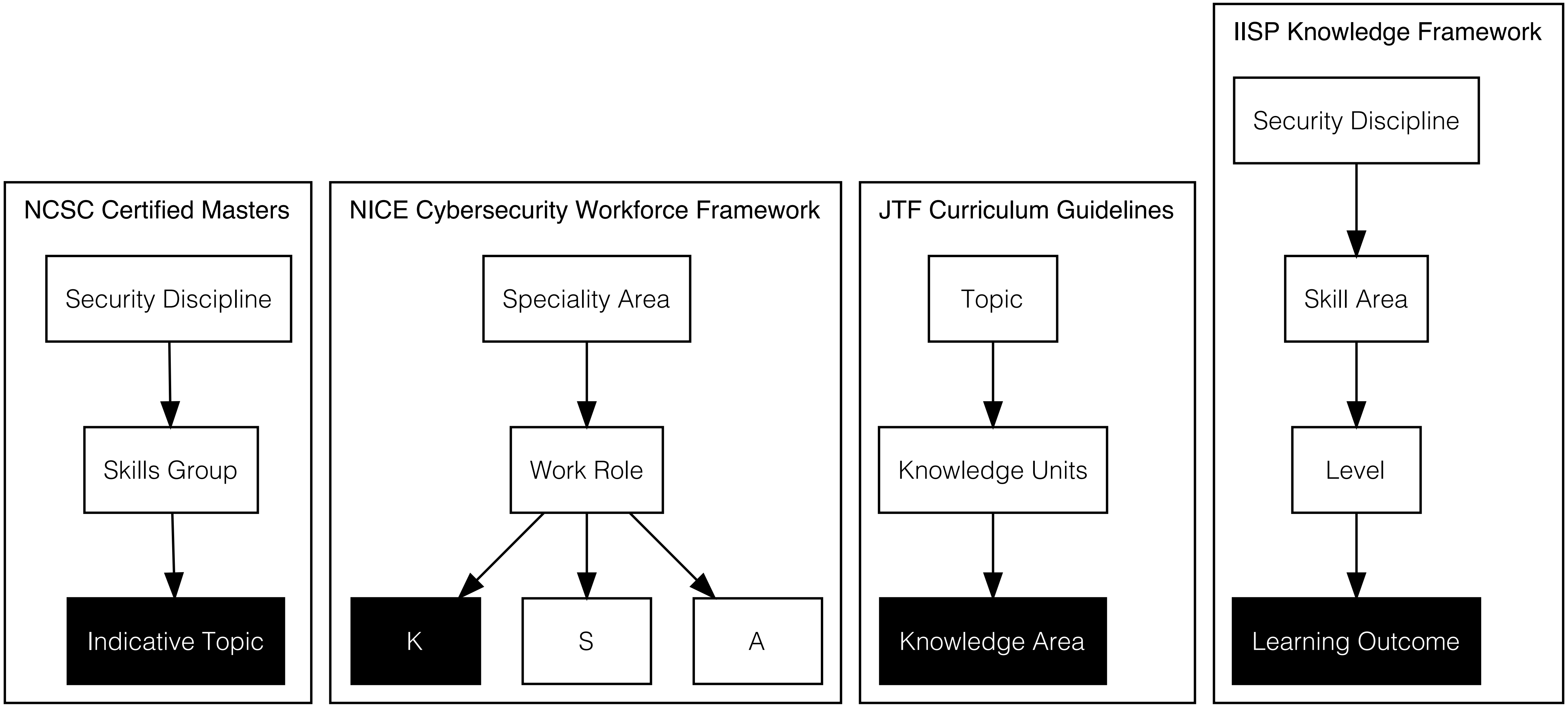
Each tied and cross-referenced to jobs and roles within cybersecurity

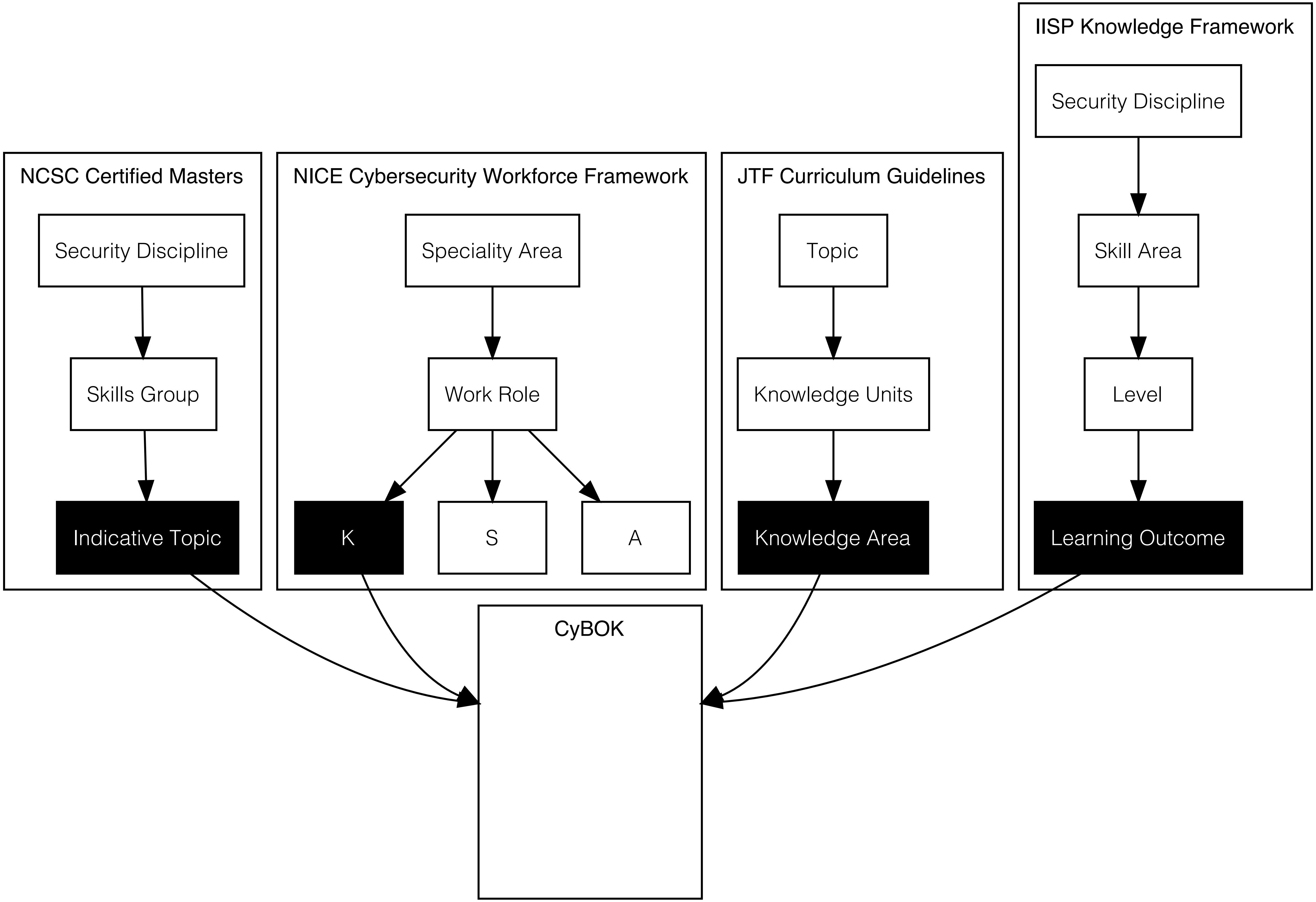
Joint Task Force Cybersecurity Curricula

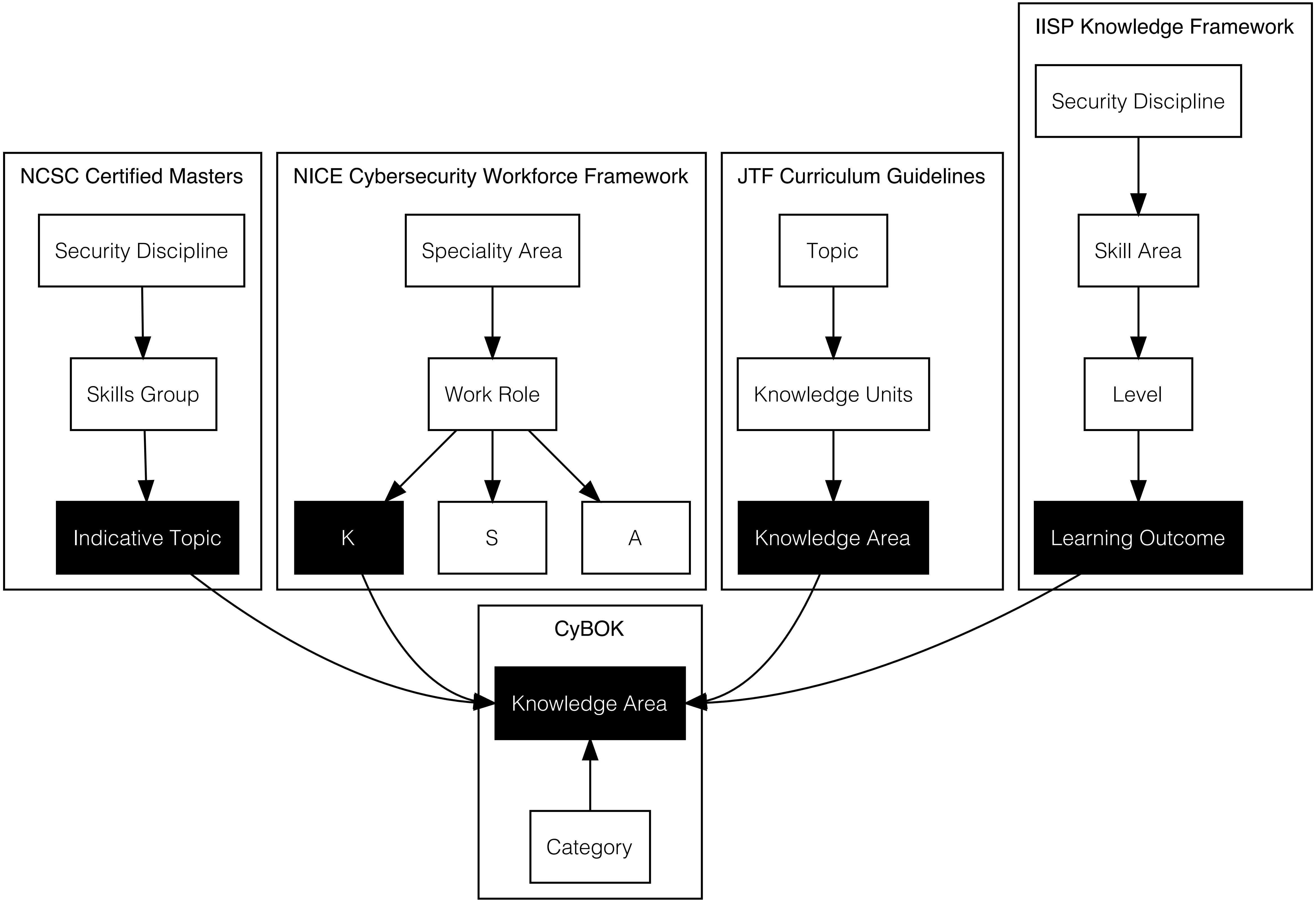
Collaboration between **ACM, IEEE-CS, AIS SIGSEC** and **IFIP WG 11.8**

Aims to *“leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level”*


NCSC Certified Masters
Security Discipline
Skills Group
Indicative Topic
NICE Cybersecurity Workforce Framework
Speciality Area
Work Role
K
S
A
JTF Curriculum Guidelines
Topic
Knowledge Units
Knowledge Area
IISP Knowledge Framework
Security Discipline
Skill Area
Level
Learning Outcome


NCSC Certified Masters
Security Discipline
Skills Group
Indicative Topic
NICE Cybersecurity Workforce Framework
Speciality Area
Work Role
K
S
A
JTF Curriculum Guidelines
Topic
Knowledge Units
Knowledge Area
IISP Knowledge Framework
Security Discipline
Skill Area
Level
Learning Outcome


IISP Knowledge Framework
Security Discipline
Skill Area
Level
Learning Outcome
NCSC Certified Masters
Security Discipline
Skills Group
Indicative Topic
NICE Cybersecurity Workforce Framework
Speciality Area
Work Role
K
S
A
JTF Curriculum Guidelines
Topic
Knowledge Units
Knowledge Area
CyBOK


IISP Knowledge Framework
Security Discipline
Skill Area
Level
Learning Outcome
NCSC Certified Masters
Security Discipline
Skills Group
Indicative Topic
NICE Cybersecurity Workforce Framework
Speciality Area
Work Role
K
S
A
JTF Curriculum Guidelines
Topic
Knowledge Units
Knowledge Area
CyBOK
Knowledge Area
Category

CyBOK

Cybersecurity

Body

of

Knowledge

Equations
2z = -64
√(4.
T = 2
Schrödinger's Bat
Just Physics
MONEYBALL
BILL JAMES
HISTORICAL
BASEBALL ABSTRACT
F=MA
e^iπ+1=0
STATS

Adversarial Behaviours

Malware and Attack Technologies

Security Operations and Incident Management

Forensics

Human Factors

Law and Regulation

Privacy and Online Rights

Risk Management and Governance

Network Security

Hardware Security

Cyber-Physical Systems Security

Physical Layer Security

Operating Systems and Virtualisation Security

Cryptography

Distributed Systems Security

Authentication, Authorisation and Accountability

Software Security

Web and Mobile Security

Secure Software Lifecycle

Attacks and Defences

Adversarial Behaviours

Malware and Attack Technologies

Security Operations and Incident Management

Forensics

Human Factors

Law and Regulation

Privacy and Online Rights

Risk Management and Governance

Network Security

Hardware Security

Cyber-Physical Systems Security

Physical Layer Security

Operating Systems and Virtualisation Security

Cryptography

Distributed Systems Security

Authentication, Authorisation and Accountability

Software Security

Web and Mobile Security

Secure Software Lifecycle

Human Organisational and Regulatory Aspects

Adversarial Behaviours

Malware and Attack Technologies

Security Operations and Incident Management

Forensics

Human Factors

Law and Regulation

Privacy and Online Rights

Risk Management and Governance

Network Security

Hardware Security

Cyber-Physical Systems Security

Physical Layer Security

Operating Systems and Virtualisation Security

Cryptography

Distributed Systems Security

Authentication, Authorisation and Accountability

Software Security

Web and Mobile Security

Secure Software Lifecycle

Adversarial Behaviours

Malware and Attack Technologies

Security Operations and Incident Management

Forensics

Human Factors

Law and Regulation

Privacy and Online Rights

Risk Management and Governance

Network Security

Infrastructure Security

Hardware Security

Cyber-Physical Systems Security

Physical Layer Security

Operating Systems and Virtualisation Security

Cryptography

Distributed Systems Security

Authentication, Authorisation and Accountability

Software Security

Web and Mobile Security

Secure Software Lifecycle

Systems Security

Adversarial Behaviours

Malware and Attack Technologies

Security Operations and Incident Management

Forensics

Human Factors

Law and Regulation

Privacy and Online Rights

Risk Management and Governance

Network Security

Hardware Security

Cyber-Physical Systems Security

Physical Layer Security

Operating Systems and Virtualisation Security

Cryptography

Distributed Systems Security

Authentication, Authorisation and Accountability

Software Security

Web and Mobile Security

Secure Software Lifecycle

Adversarial Behaviours

Malware and Attack Technologies

Security Operations and Incident Management

Forensics

Human Factors

Law and Regulation

Privacy and Online Rights

Risk Management and Governance

Network Security

Hardware Security

Cyber-Physical Systems Security

Physical Layer Security

Operating Systems and Virtualisation Security

Cryptography

Distributed Systems Security

Authentication, Authorisation and Accountability

Software Security

Web and Mobile Security

Secure Software Lifecycle

Software Platform Security

Adversarial Behaviours

Malware and Attack Technologies

Security Operations and Incident Management

Forensics

Human Factors

Law and Regulation

Privacy and Online Rights

Risk Management and Governance

Network Security

Hardware Security

Cyber-Physical Systems Security

Physical Layer Security

Operating Systems and Virtualisation Security

Cryptography

Distributed Systems Security

Authentication, Authorisation and Accountability

Software Security

Web and Mobile Security

Secure Software Lifecycle

Adversarial Behaviours

Malware and Attack Technologies

Security Operations and Incident Management

Forensics

Human Factors

Law and Regulation

Privacy and Online Rights

Risk Management and Governance

Network Security

Hardware Security

Cyber-Physical Systems Security

Physical Layer Security

Operating Systems and Virtualisation Security

Cryptography

Distributed Systems Security

Authentication, Authorisation and Accountability

Software Security

Web and Mobile Security

Secure Software Lifecycle

Adversarial Behaviours

Malware and Attack Technologies

Security Operations and Incident Management

Forensics

Human Factors

Law and Regulation

Privacy and Online Rights

Risk Management and Governance

Network Security

Hardware Security

Cyber-Physical Systems Security

Physical Layer Security

Operating Systems and Virtualisation Security

Cryptography

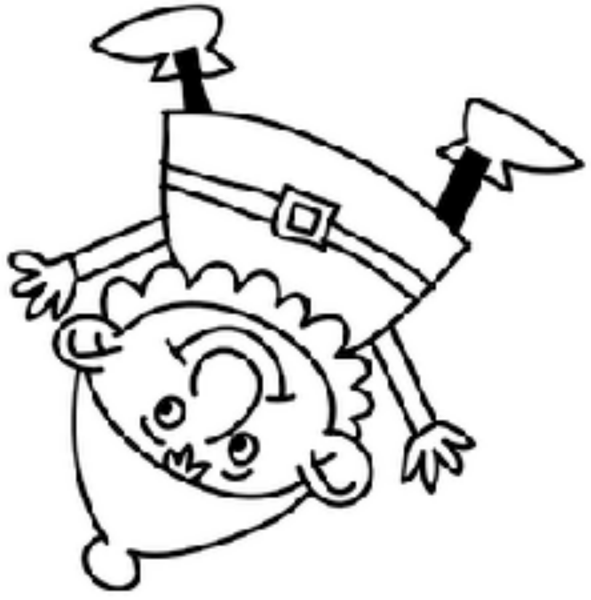
Distributed Systems Security

Authentication, Authorisation and Accountability

Software Security

Web and Mobile Security

Secure Software Lifecycle



Map the topics from the curricular frameworks onto CyBOK Knowledge Areas

Map the topics from the curricular frameworks onto CyBOK ~~Knowledge Areas~~ Scope Document

“They shall be able to list the major applicable legislation and regulations affecting an example organization and describe their overall purpose.”

—a learning outcome for the IISP Knowledge Framework Skill Area A6.1

> “They shall be able to list the major applicable legislation and regulations affecting an example organization and describe their overall purpose.”
>
> —a learning outcome for the IISP Knowledge Framework Skill Area A6.1

> “International and national statutory and regulatory requirements, compliance obligations including data protection...”
>
> —CyBOK Scope document for the Law and Regulation Knowledge Area

“They shall be able to list the major applicable legislation and regulations affecting an example organization and describe their overall purpose.”

—a learning outcome for the IISP Knowledge Framework Skill Area A6.1

Law and Regulation

“They shall be able to list the major applicable legislation and regulations affecting an example organization and describe their overall purpose.”

—a learning outcome for the IISP Knowledge Framework Skill Area A6.1

Curricular Framework	Mapped / Total	Mapped Percentage
IISP	215/252	85%
JTF	286/287	100%
NICE	206/630	33%
NCSC	114/118	97%

Curricular Framework	Mapped / Total	Mapped Percentage
IISP	215/252	85%
JTF	286/287	100%
NICE	206/630	33%
NCSC	114/118	97%

“Knowledge of computer algorithms.”

—NICE K0015

“Knowledge of computer algorithms.”

—NICE K0015

Too General For CyBOK

:-(

Curricular Framework	Mapped / Total	Mapped Percentage
IISP	215/252	85%
JTF	286/287	100%
NICE	206/630	33%
NCSC	114/118	97%

Not Cybersecurity

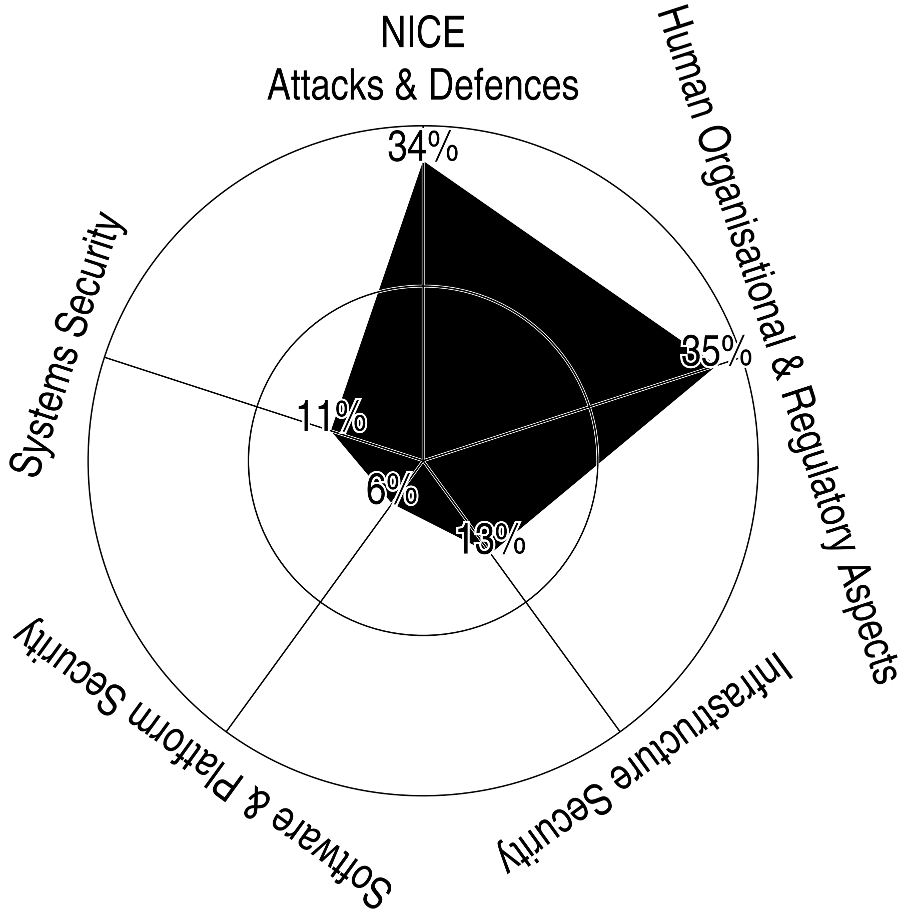
:-(

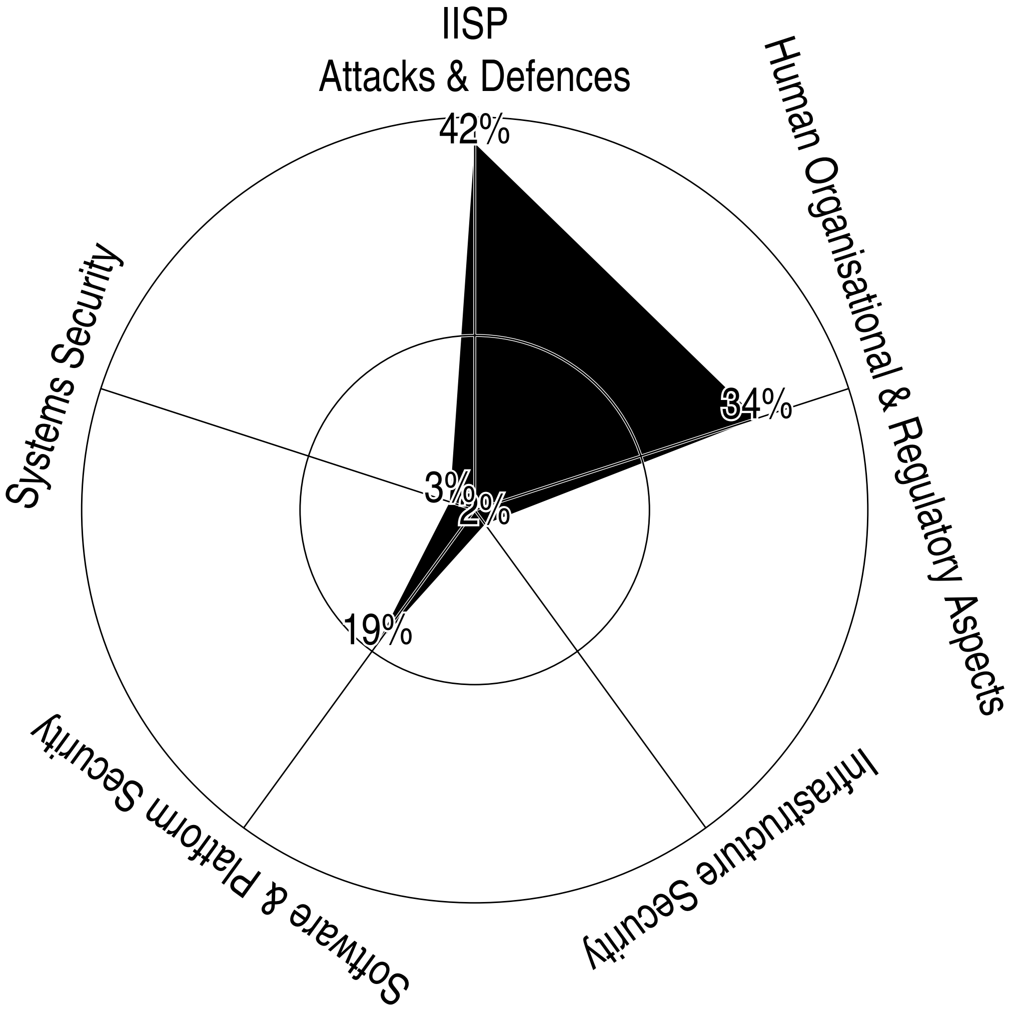
Research skills

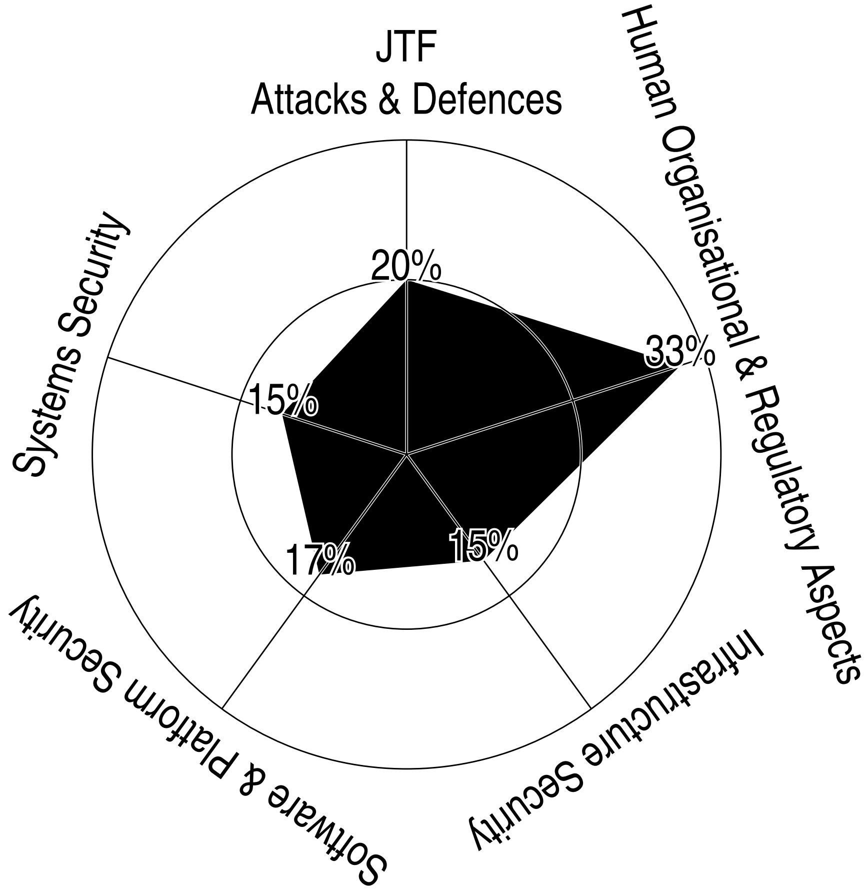
Physical security

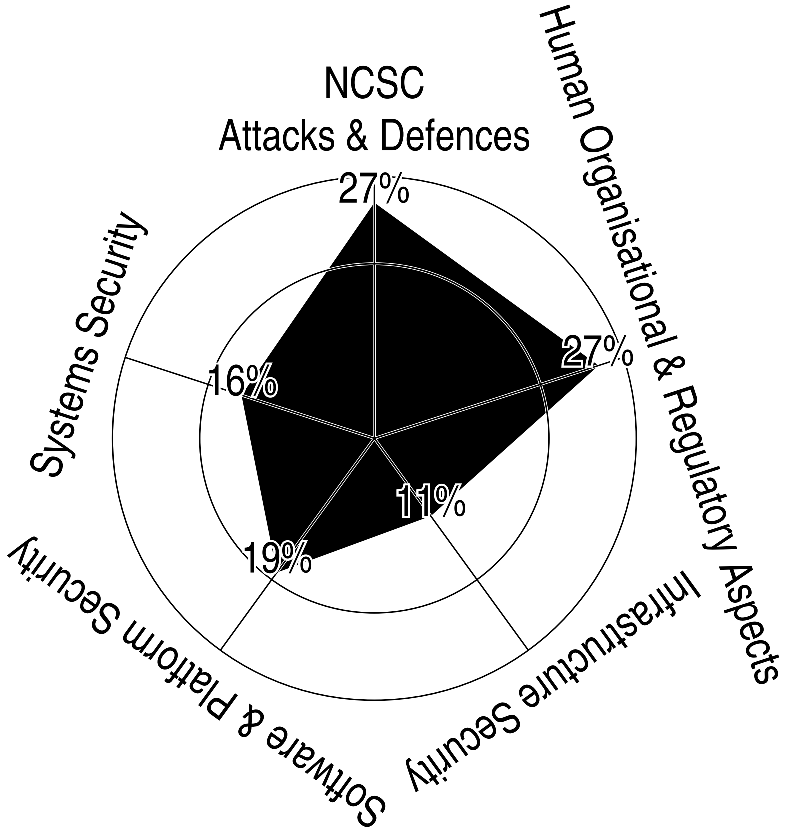
Intra-personal skills

General Computer Science

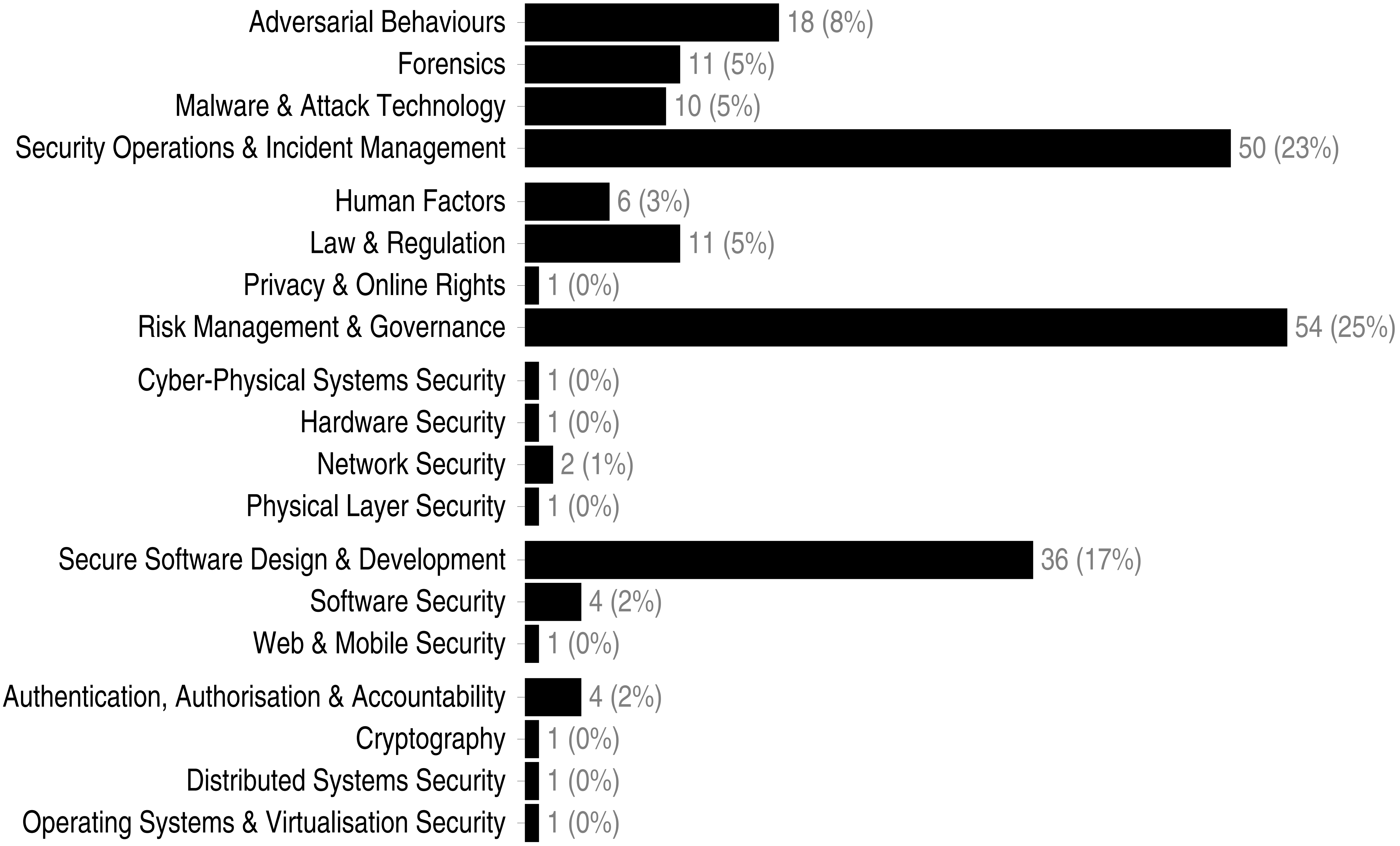

NICE
Attacks & Defences
34%
Human Organisational & Regulatory Aspects
35%
Infrastructure Security
13%
Software & Platform Security
6%
Systems Security
11%


IISP
Attacks & Defences
42%
Human Organisational & Regulatory Aspects
34%
Infrastructure Security
2%
Software & Platform Security
19%
Systems Security
3%

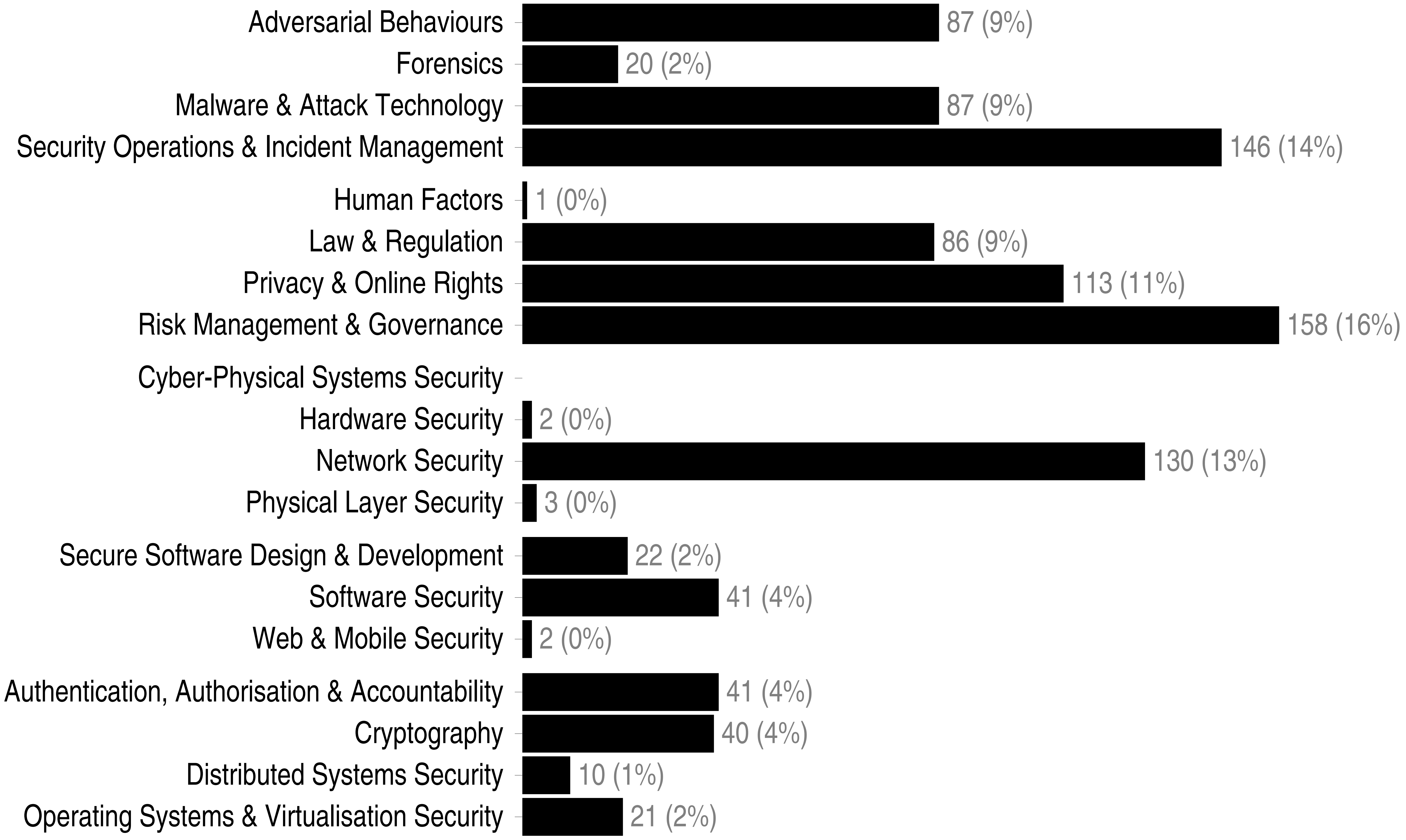

JTF
Attacks & Defences
20%
Human Organisational & Regulatory Aspects
33%
Infrastructure Security
15%
Software & Platform Security
17%
Systems Security
15%


NCSC
Attacks & Defences
27%
Human Organisational & Regulatory Aspects
27%
Infrastructure Security
11%
Software & Platform Security
19%
Systems Security
16%

IISP

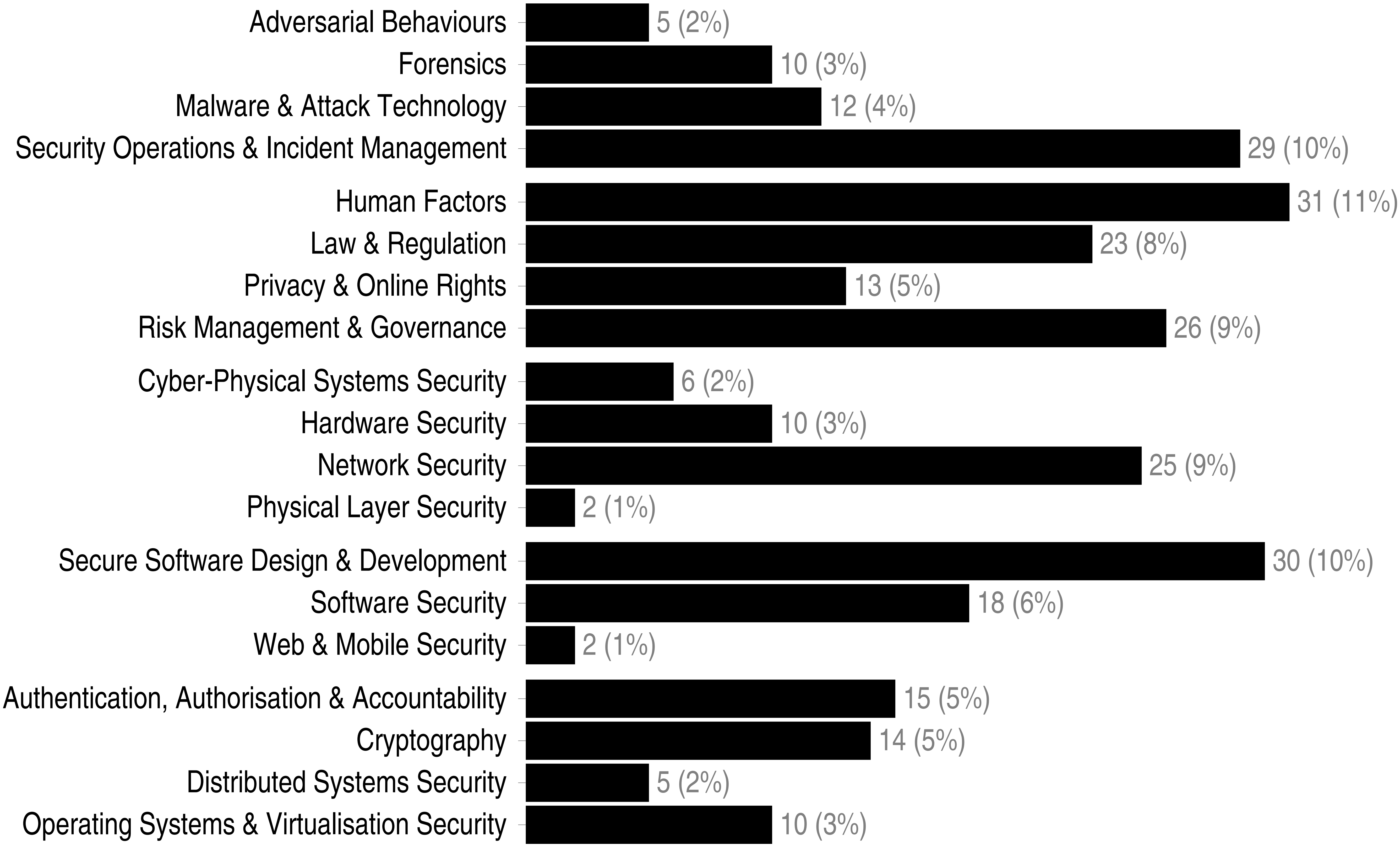

Adversarial Behaviours
18 (8%)
Forensics
11 (5%)
Malware & Attack Technology
10 (5%)
Security Operations & Incident Management
50 (23%)
Human Factors
6 (3%)
Law & Regulation
11 (5%)
Privacy & Online Rights
1 (0%)
Risk Management & Governance
54 (25%)
Cyber-Physical Systems Security
1 (0%)
Hardware Security
1 (0%)
Network Security
2 (1%)
Physical Layer Security
1 (0%)
Secure Software Design & Development
36 (17%)
Software Security
4 (2%)
Web & Mobile Security
1 (0%)
Authentication, Authorisation & Accountability
4 (2%)
Cryptography
1 (0%)
Distributed Systems Security
1 (0%)
Operating Systems & Virtualisation Security
1 (0%)

NICE

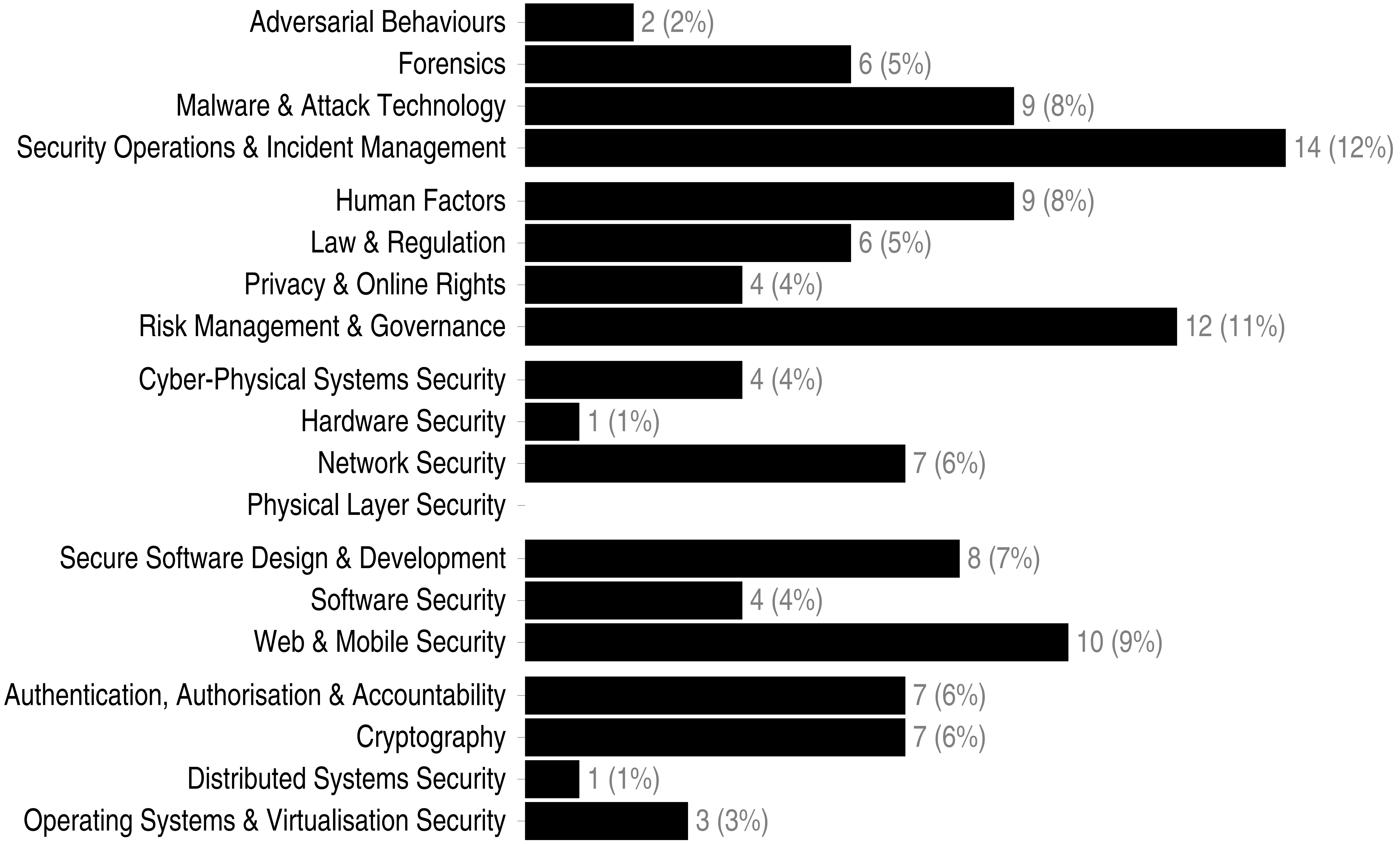


Adversarial Behaviours
87 (9%)
Forensics
20 (2%)
Malware & Attack Technology
87 (9%)
Security Operations & Incident Management
146 (14%)
Human Factors
1 (0%)
Law & Regulation
86 (9%)
Privacy & Online Rights
113 (11%)
Risk Management & Governance
158 (16%)
Cyber-Physical Systems Security
Hardware Security
2 (0%)
Network Security
130 (13%)
Physical Layer Security
3 (0%)
Secure Software Design & Development
22 (2%)
Software Security
41 (4%)
Web & Mobile Security
2 (0%)
Authentication, Authorisation & Accountability
41 (4%)
Cryptography
40 (4%)
Distributed Systems Security
10 (1%)
Operating Systems & Virtualisation Security
21 (2%)

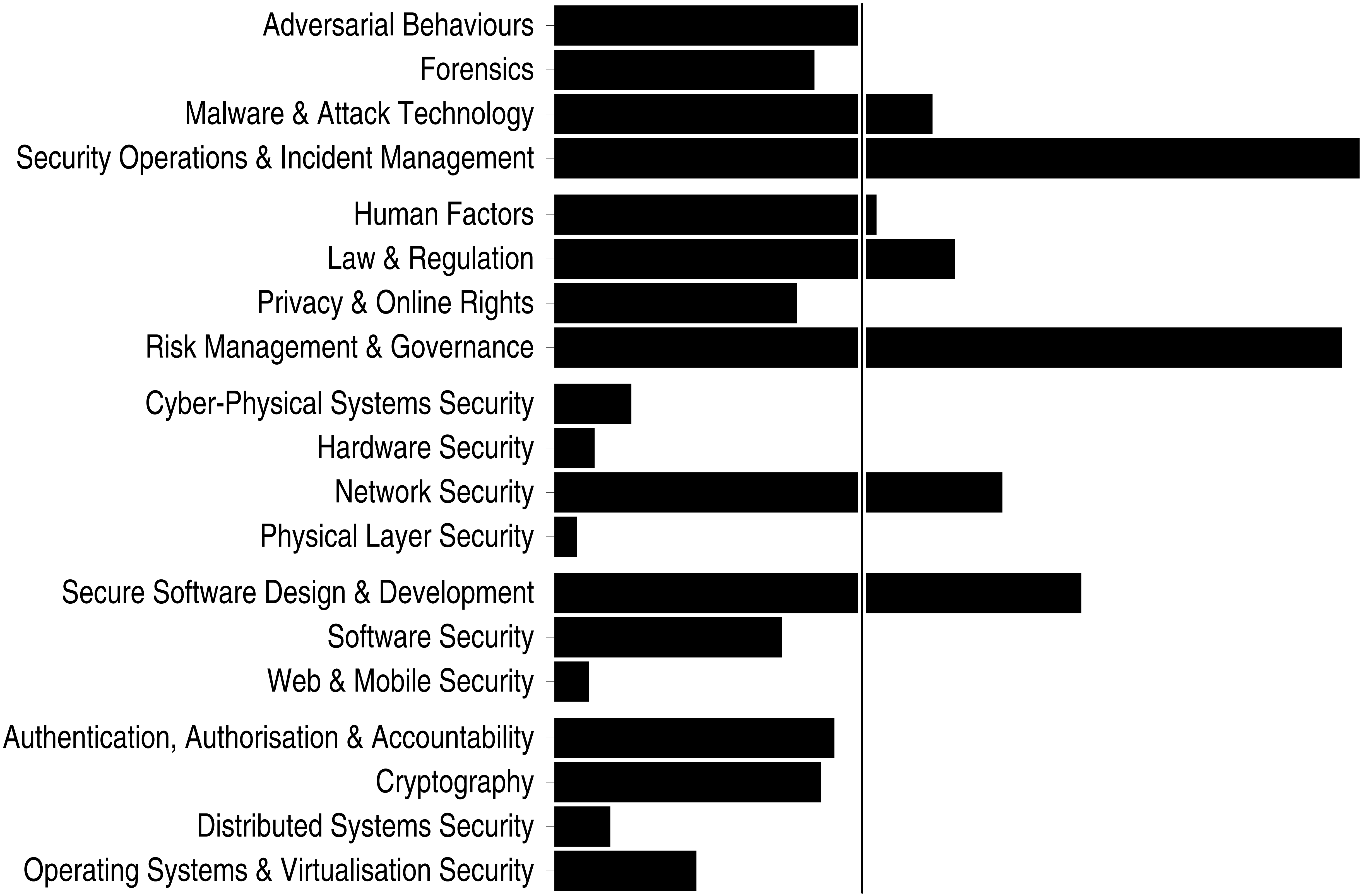
JTF


Adversarial Behaviours
5 (2%)
Forensics
10 (3%)
Malware & Attack Technology
12 (4%)
Security Operations & Incident Management
29 (10%)
Human Factors
31 (11%)
Law & Regulation
23 (8%)
Privacy & Online Rights
13 (5%)
Risk Management & Governance
26 (9%)
Cyber-Physical Systems Security
6 (2%)
Hardware Security
10 (3%)
Network Security
25 (9%)
Physical Layer Security
2 (1%)
Secure Software Design & Development
30 (10%)
Software Security
18 (6%)
Web & Mobile Security
2 (1%)
Authentication, Authorisation & Accountability
15 (5%)
Cryptography
14 (5%)
Distributed Systems Security
5 (2%)
Operating Systems & Virtualisation Security
10 (3%)

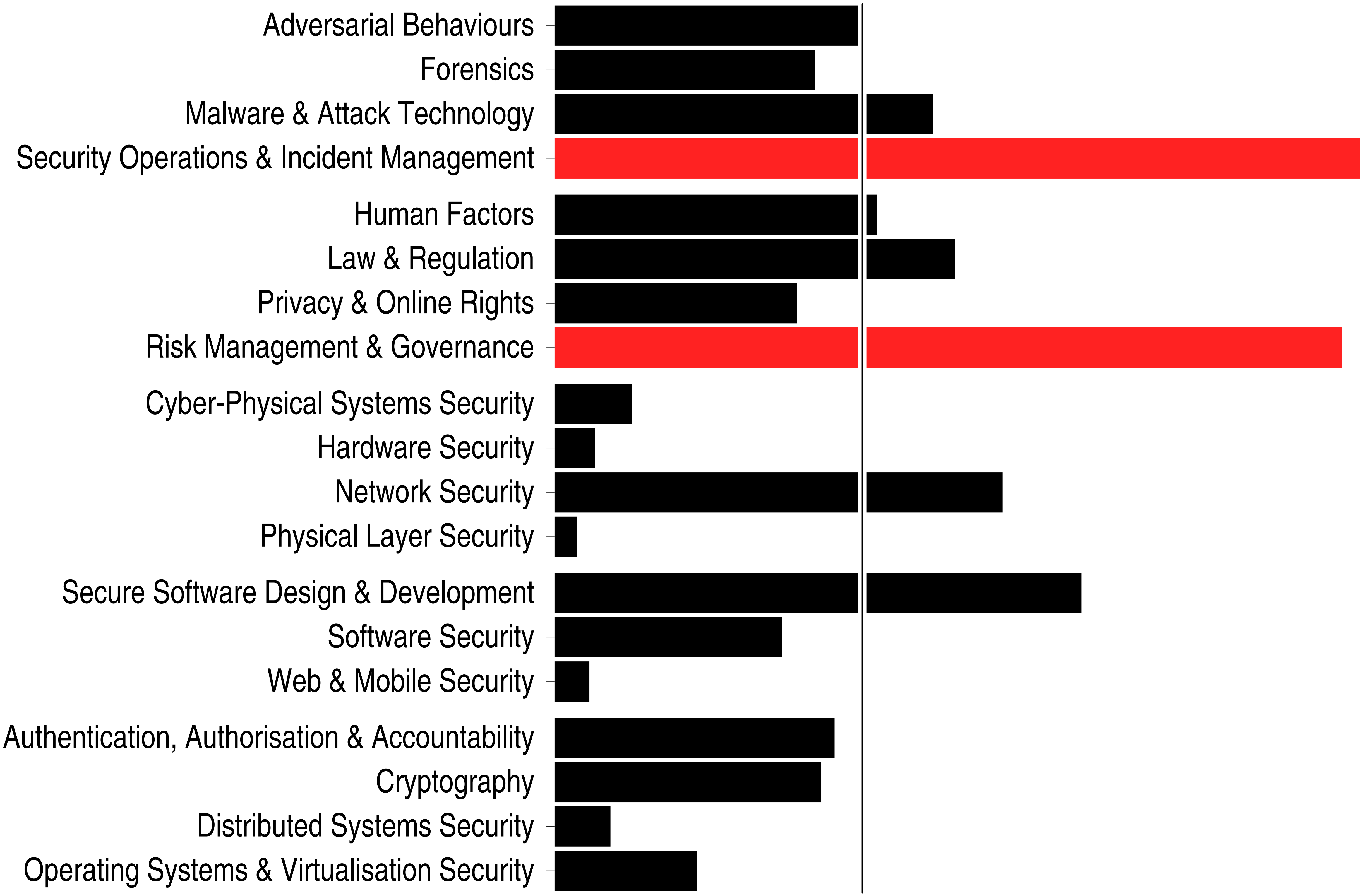
NCSC


Adversarial Behaviours
2 (2%)
Forensics
6 (5%)
Malware & Attack Technology
9 (8%)
Security Operations & Incident Management
14 (12%)
Human Factors
9 (8%)
Law & Regulation
6 (5%)
Privacy & Online Rights
4 (4%)
Risk Management & Governance
12 (11%)
Cyber-Physical Systems Security
4 (4%)
Hardware Security
1 (1%)
Network Security
7 (6%)
Physical Layer Security
Secure Software Design & Development
8 (7%)
Software Security
4 (4%)
Web & Mobile Security
10 (9%)
Authentication, Authorisation & Accountability
7 (6%)
Cryptography
7 (6%)
Distributed Systems Security
1 (1%)
Operating Systems & Virtualisation Security
3 (3%)

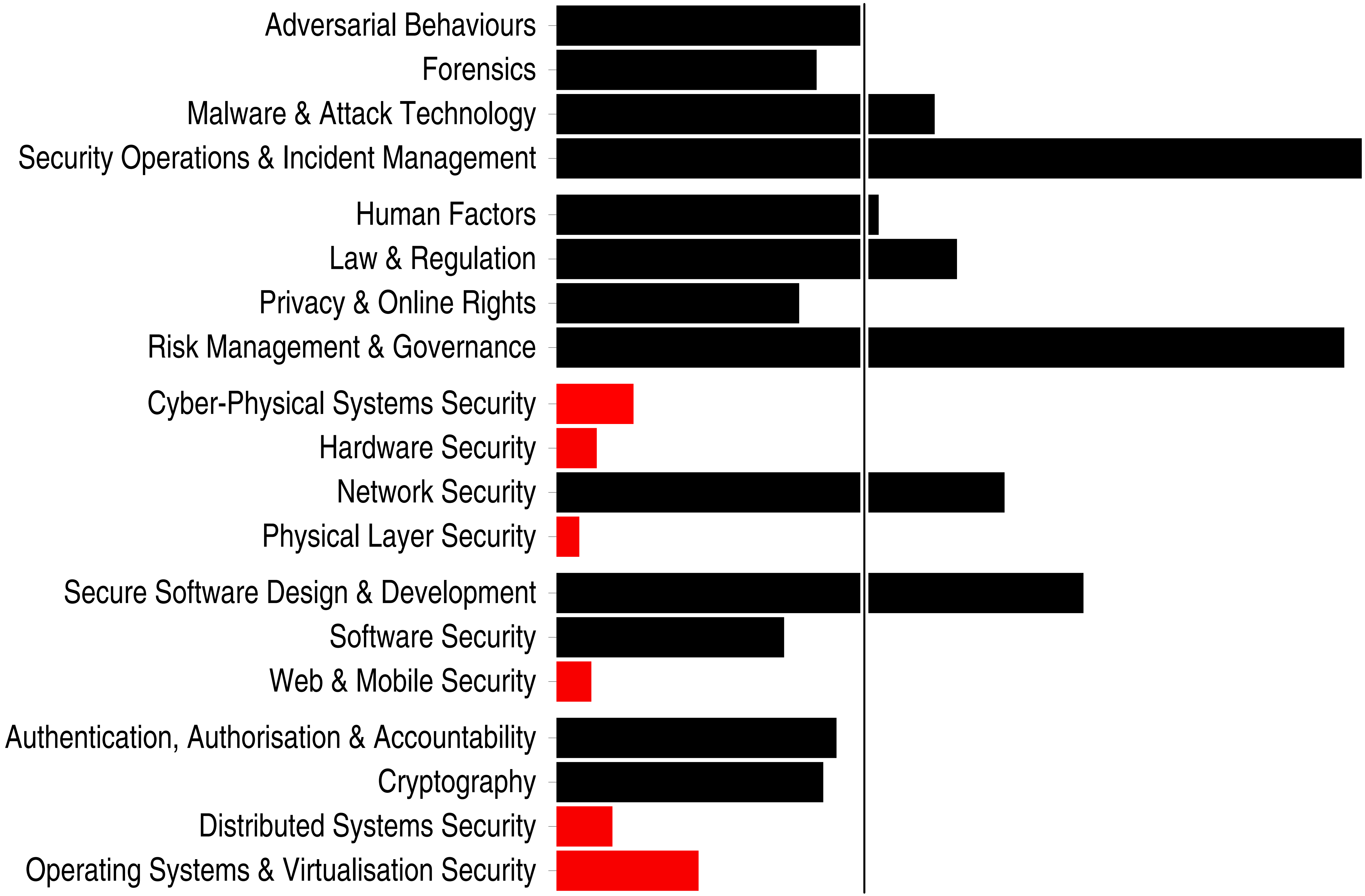
Median


Adversarial Behaviours
Forensics
Malware & Attack Technology
Security Operations & Incident Management
Human Factors
Law & Regulation
Privacy & Online Rights
Risk Management & Governance
Cyber-Physical Systems Security
Hardware Security
Network Security
Physical Layer Security
Secure Software Design & Development
Software Security
Web & Mobile Security
Authentication, Authorisation & Accountability
Cryptography
Distributed Systems Security
Operating Systems & Virtualisation Security

Median


Adversarial Behaviours
Forensics
Malware & Attack Technology
Security Operations & Incident Management
Human Factors
Law & Regulation
Privacy & Online Rights
Risk Management & Governance
Cyber-Physical Systems Security
Hardware Security
Network Security
Physical Layer Security
Secure Software Design & Development
Software Security
Web & Mobile Security
Authentication, Authorisation & Accountability
Cryptography
Distributed Systems Security
Operating Systems & Virtualisation Security

Median


Adversarial Behaviours
Forensics
Malware & Attack Technology
Security Operations & Incident Management
Human Factors
Law & Regulation
Privacy & Online Rights
Risk Management & Governance
Cyber-Physical Systems Security
Hardware Security
Network Security
Physical Layer Security
Secure Software Design & Development
Software Security
Web & Mobile Security
Authentication, Authorisation & Accountability
Cryptography
Distributed Systems Security
Operating Systems & Virtualisation Security

This doesn’t account for *time spent* on any topic…

This doesn’t look at how knowledge in these topics is *evaluated*…

1. Are they all the same?
2. What are they all teaching?
3. Which one is best?

Are they the same?

Nope.

What are they
all teaching?

Risk management and Security ops mostly…

But it depends on the framework…

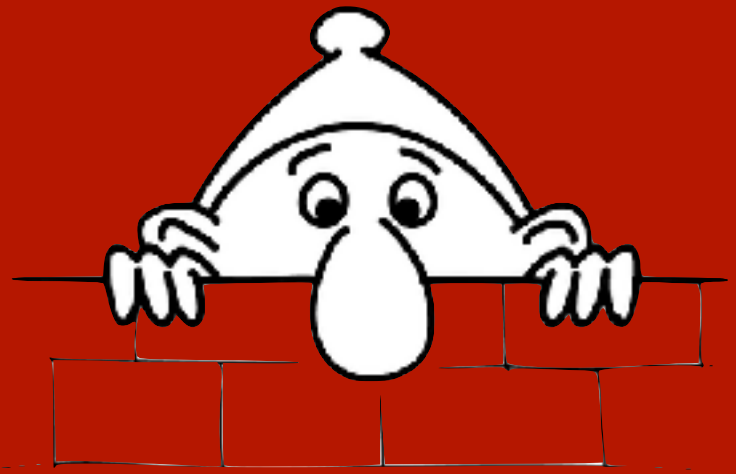
Using CyBOK we can characterise what is in them

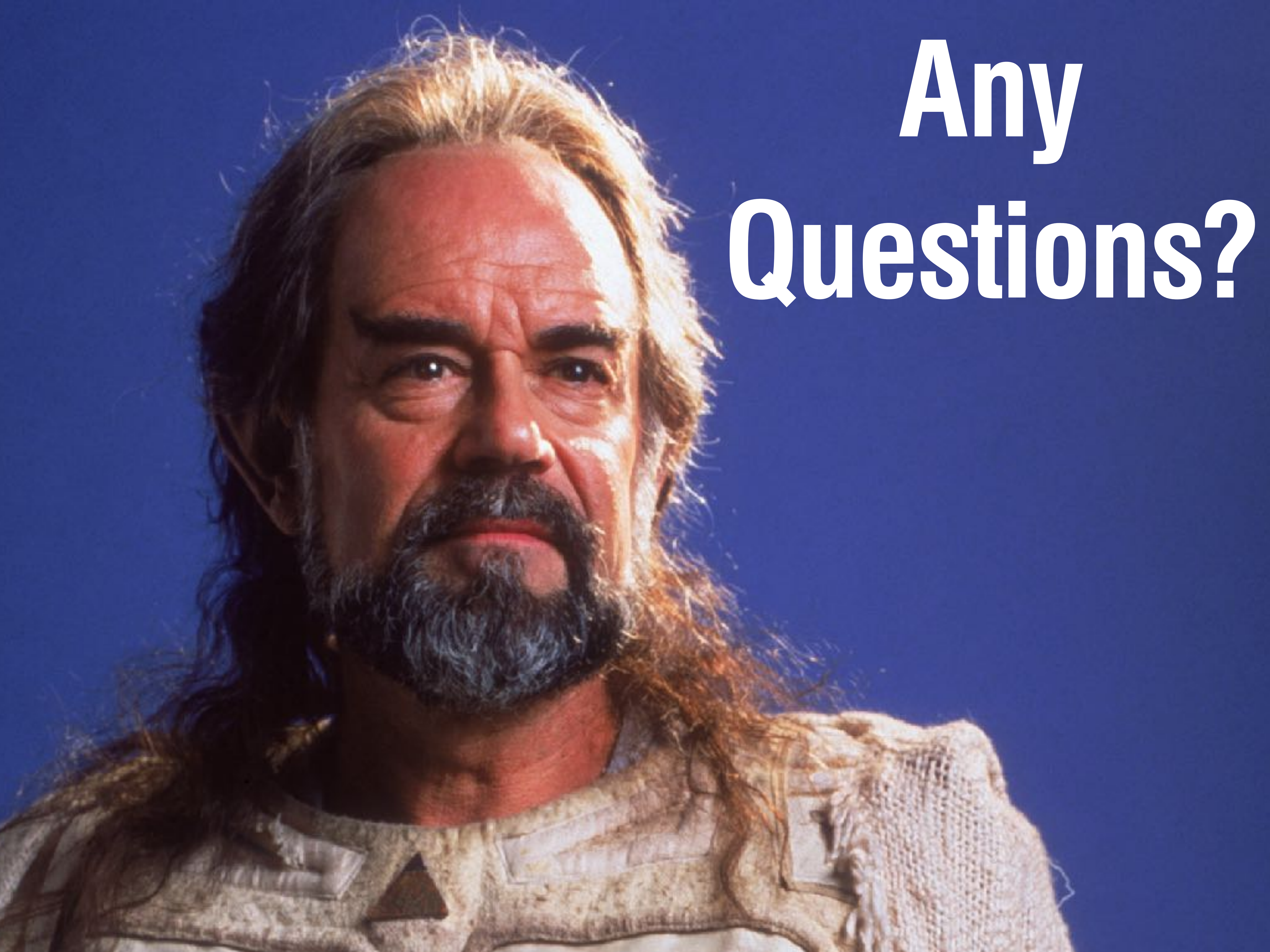
Which one is best?

It depends what you want out of it…

But using CyBOK we can see what the emphasis is

● ● ●





Any Questions?