Proyek Mata Kuliah Pengamanan Sistem Komputer

Ari Sujarwo, S.Kom., MIT (Hons)

UNIVERSITAS
ISLAM
INDONESIA

NCBI Resources How To

PMC
US National Library of Medicine
National Institutes of Health

PMC
Advanced Journal list

Journal List > Sensors (Basel) > v.14(12); 2014 Dec > PMC4299037

MDPI OPEN ACCESS sensors
home this article this journal instructions for authors subscribe

Sensors (Basel). 2014 Dec; 14(12): 22754–22772.
Published online 2014 Dec 1. doi: 10.3390/s141222754

PMCID: PMC4299037

A Layered Trust Information Security Architecture

Robson de Oliveira Albuquerque,[1,2] Luis Javier García Villalba,[1,*] Ana Lucila Sandoval Orozco,[1] Fábio Buiati,[2] and Tai-Hoon Kim[3]

Author information ▶ Article notes ▶ Copyright and License information ▶

Sensors (Basel)

Abstract

Go to:

Information can be considered the most important asset of any modern organization. Securing this information involves preserving confidentially, integrity and availability, the well-known CIA triad. In addition, information security is a risk management job; the task is to manage the inherent risks of information disclosure. Current information security platforms do not deal with the different facets of information technology. This paper presents a layered trust information security architecture (TISA) and its creation was motivated by the need to consider information and security from different points of view in order to protect it. This paper also extends and discusses security information extensions as a way of helping the CIA triad. Furthermore, this paper suggests information representation and treatment elements, operations and support components that can be integrated to show the various risk sources when dealing with both information and security. An overview of how information is represented and treated nowadays

Write a paper about a specific topic

Then, make a PoC

About what?

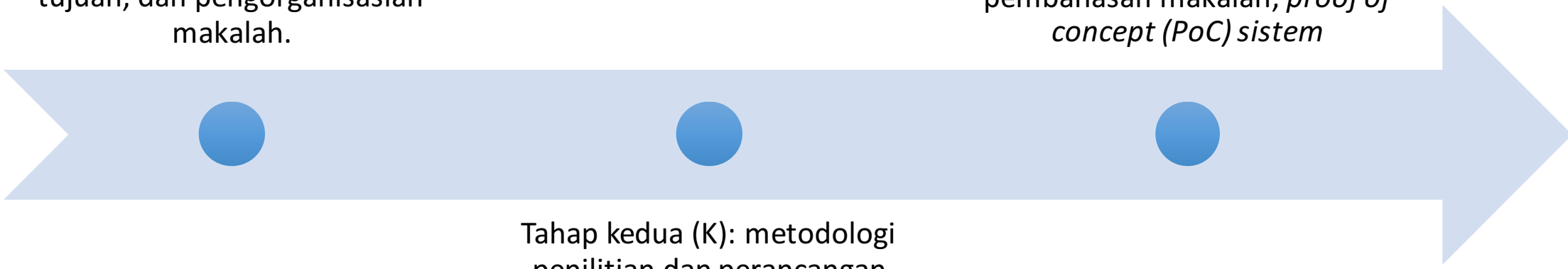
Pemerintahan Daerah	Pendidikan Tinggi	Rumah Sakit Umum	Perpustakaan dan Arsip Daerah
Balai Kebudayaan, Museum, dan Keraton Yogyakarta	Badan Mitigasi Bencana dan Pengawasan Gunung Api	Balai Konservasi Satwa	Sistem Transportasi Massal

What should we do?

Tahap pertama (P): Penentuan topik keamanan sistem, latar belakang, rumusan masalah, tujuan, dan pengorganisasian makalah.

Tahap kedua (K): metodologi penilitian dan perancangan sistem keamanan

Tahap ketiga (K): solusi dan pembahasan makalah; *proof of concept (PoC) sistem*

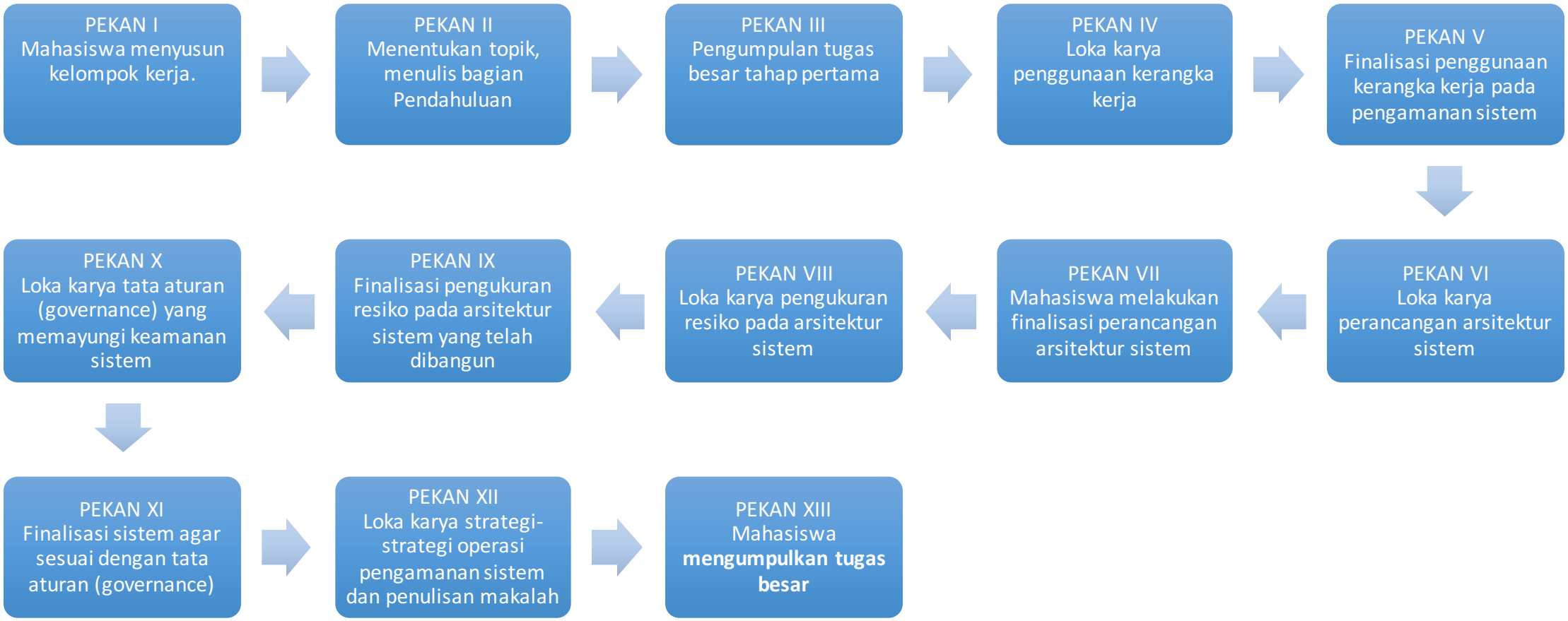


Our steps

LOKA KARYA - Mahasiswa akan bekerja dalam tim, menjalankan beberapa pekerjaan: menentukan topik tugas besar, melakukan penulisan, reviu, perbaikan makalah, dan pembuatan *proof of concept (PoC)* atas rancangan yang sudah dibuat.

KOLOKIUM - Mahasiswa mempresentasikan makalah yang ditulisnya pada sebuah forum yang dibangun dalam suasana ilmiah, yang insyaAllah dilaksanakan pada akhir semester.

Lini masa pengerjaan



Ruang Lingkup Pengamanan Sistem Komputer

Ari Sujarwo, S.Kom., MIT (Hons)

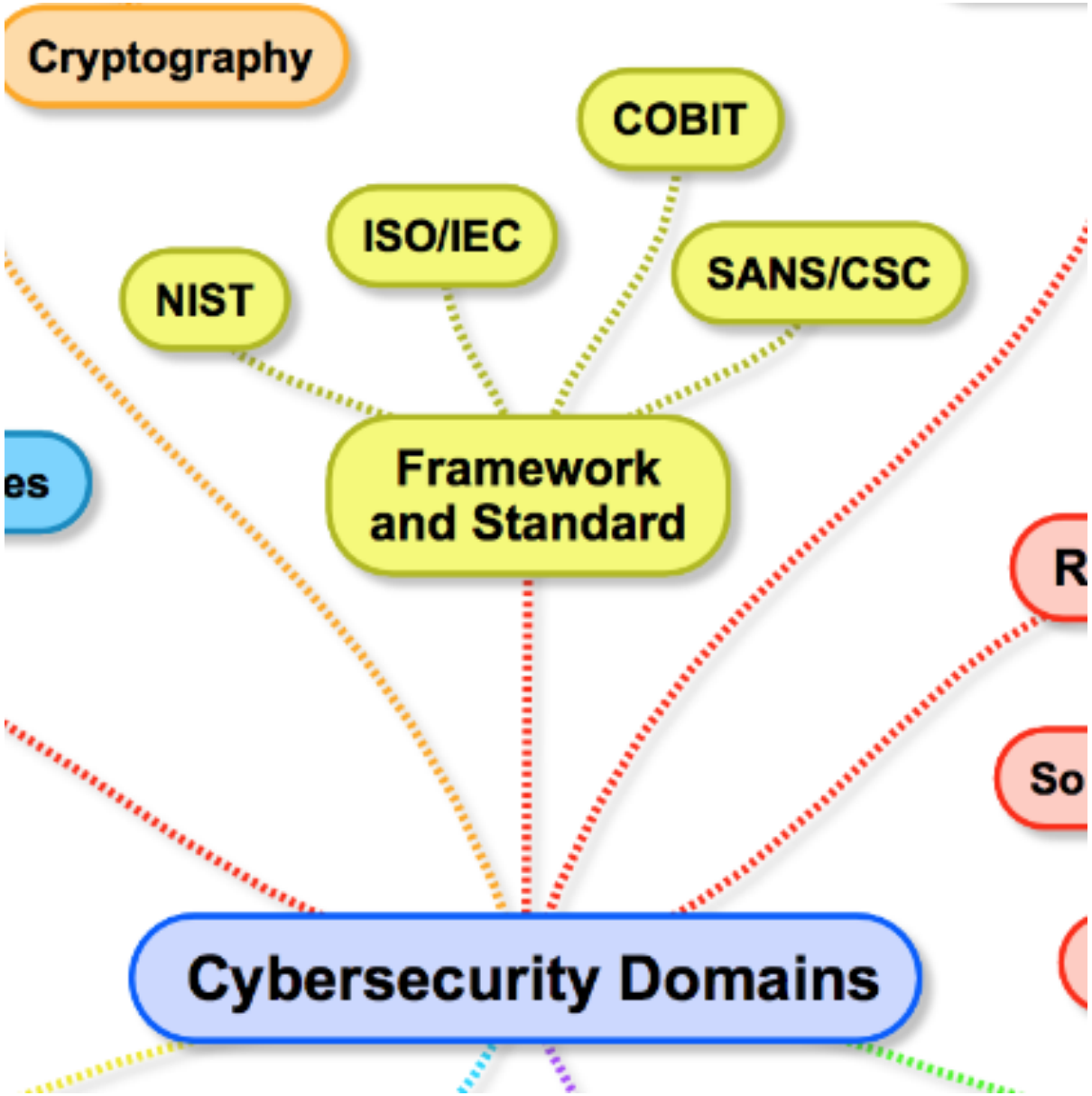
UNIVERSITAS
ISLAM
INDONESIA

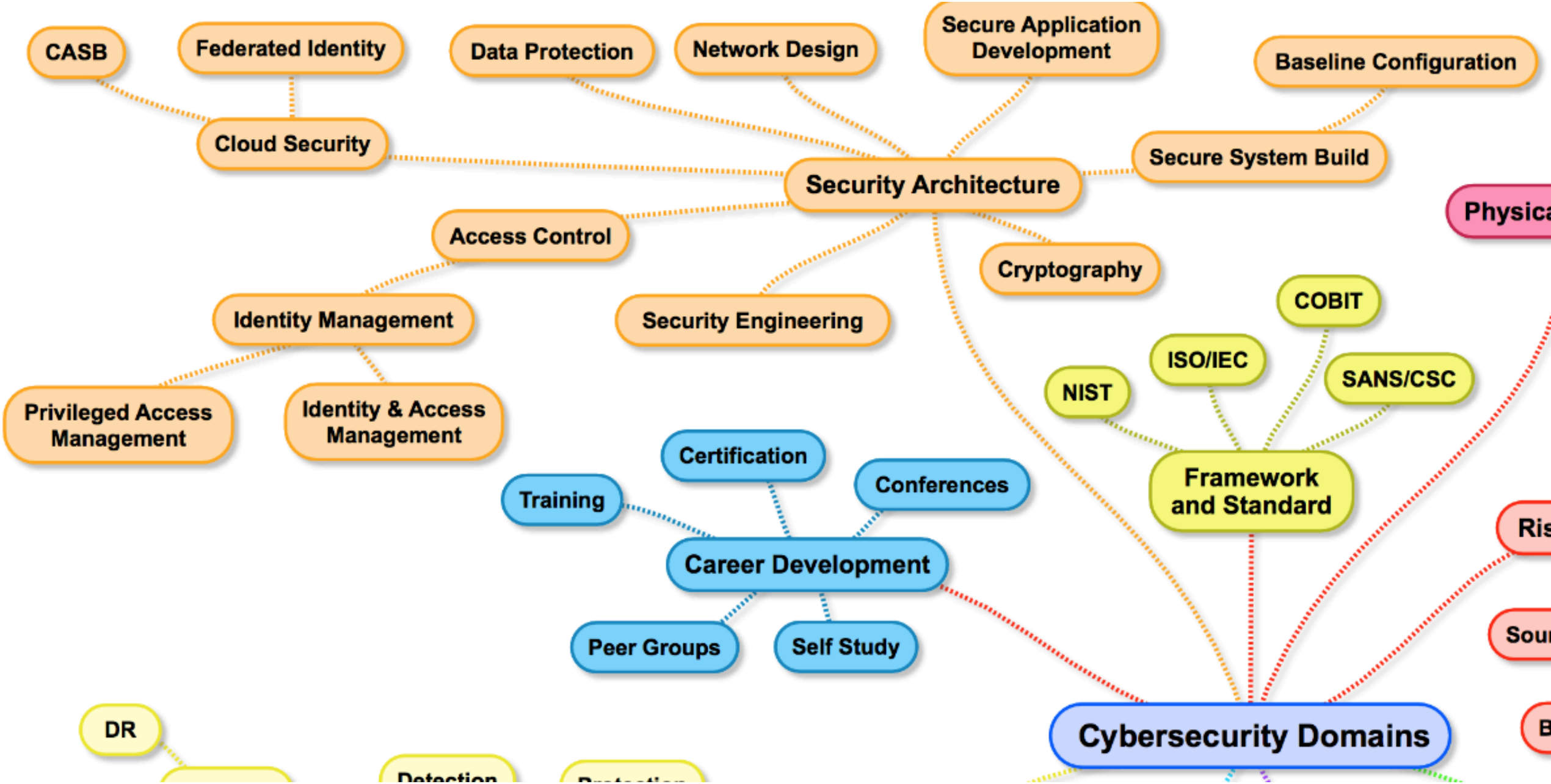
The World of Cybersecurity Map version 2.0

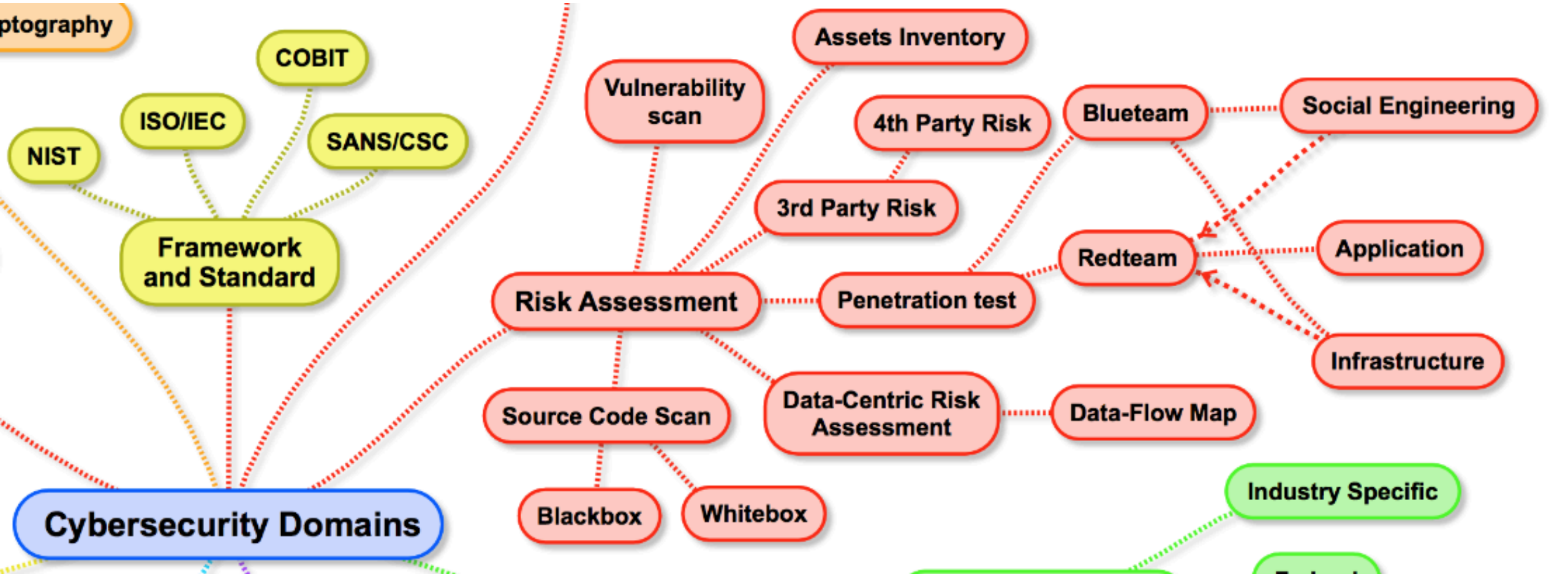
The map is about capturing key areas of cybersecurity practice in interconnected ways. The practice of cybersecurity is not just about "hacking." With the map, one should realize that hacking, perhaps a more appropriate definition of such activities should be "authorized penetration test" which is a sub-domain under "Risk Assessment," or under a another sub-domain called "Active Defense" under "Security Operation."

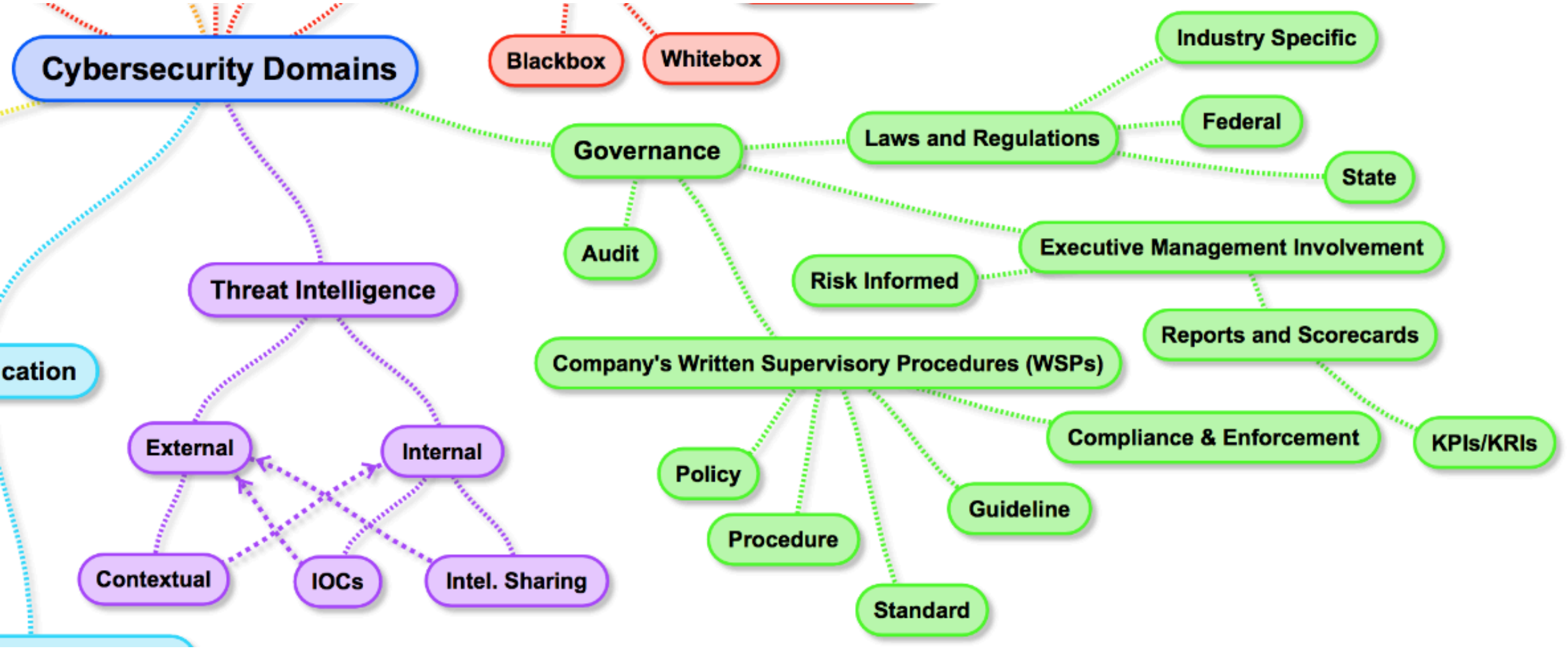
Henry Jiang - https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp/

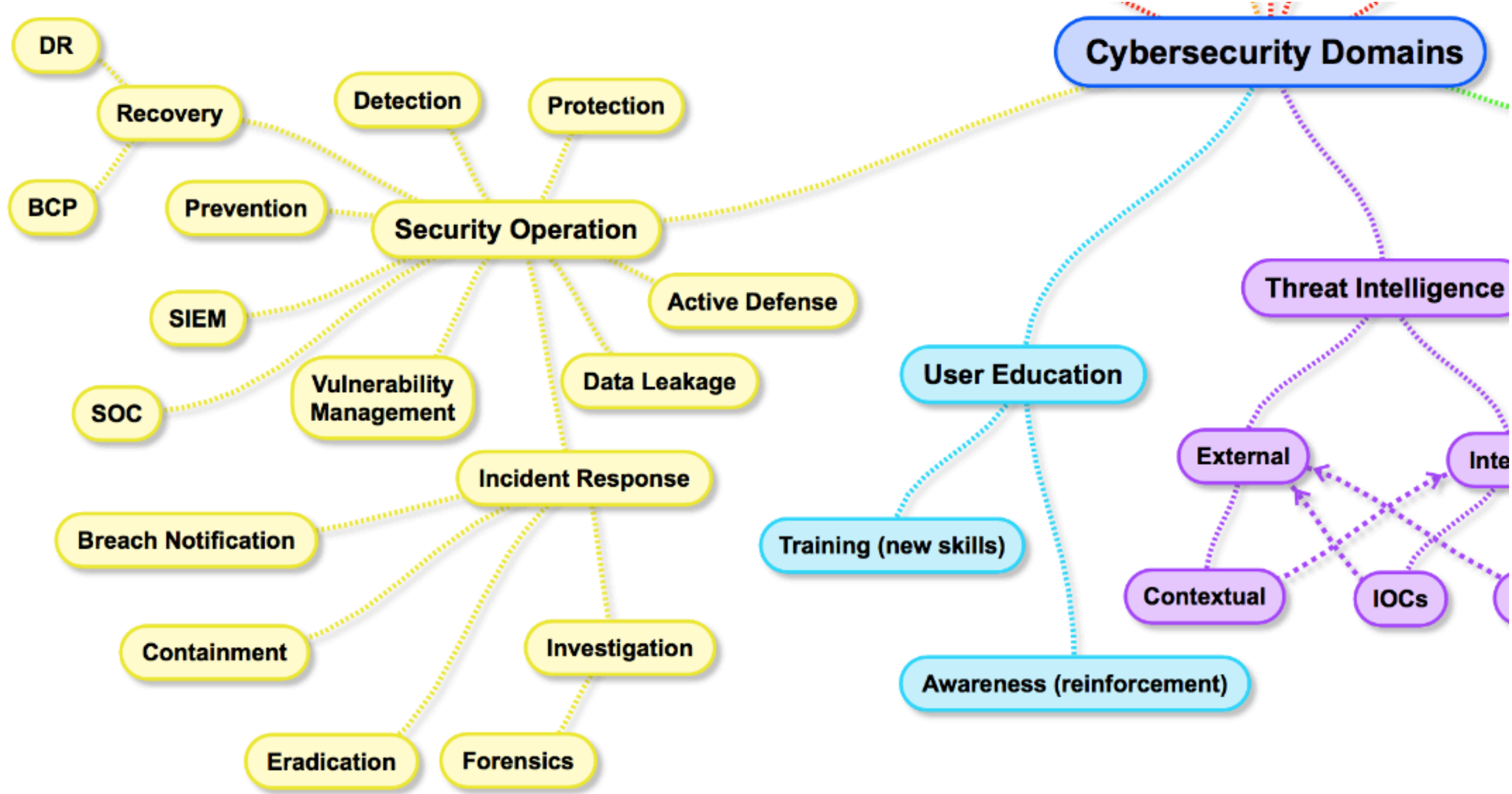
Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Identity Management
Privileged Access Management
Identity & Access Management
Security Engineering
Cryptography
Framework and Standard
COBIT
ISO/IEC
NIST
SANS/CSC
Career Development
Certification
Training
Conferences
Peer Groups
Self Study
Physical Security
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Penetration test
Blueteam
Social Engineering
Redteam
Application
Infrastructure
Source Code Scan
Blackbox
Whitebox
Data-Centric Risk Assessment
Data-Flow Map
Governance
Laws and Regulations
Industry Specific
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Procedure
Guideline
Standard
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Eradication
Investigation
Forensics

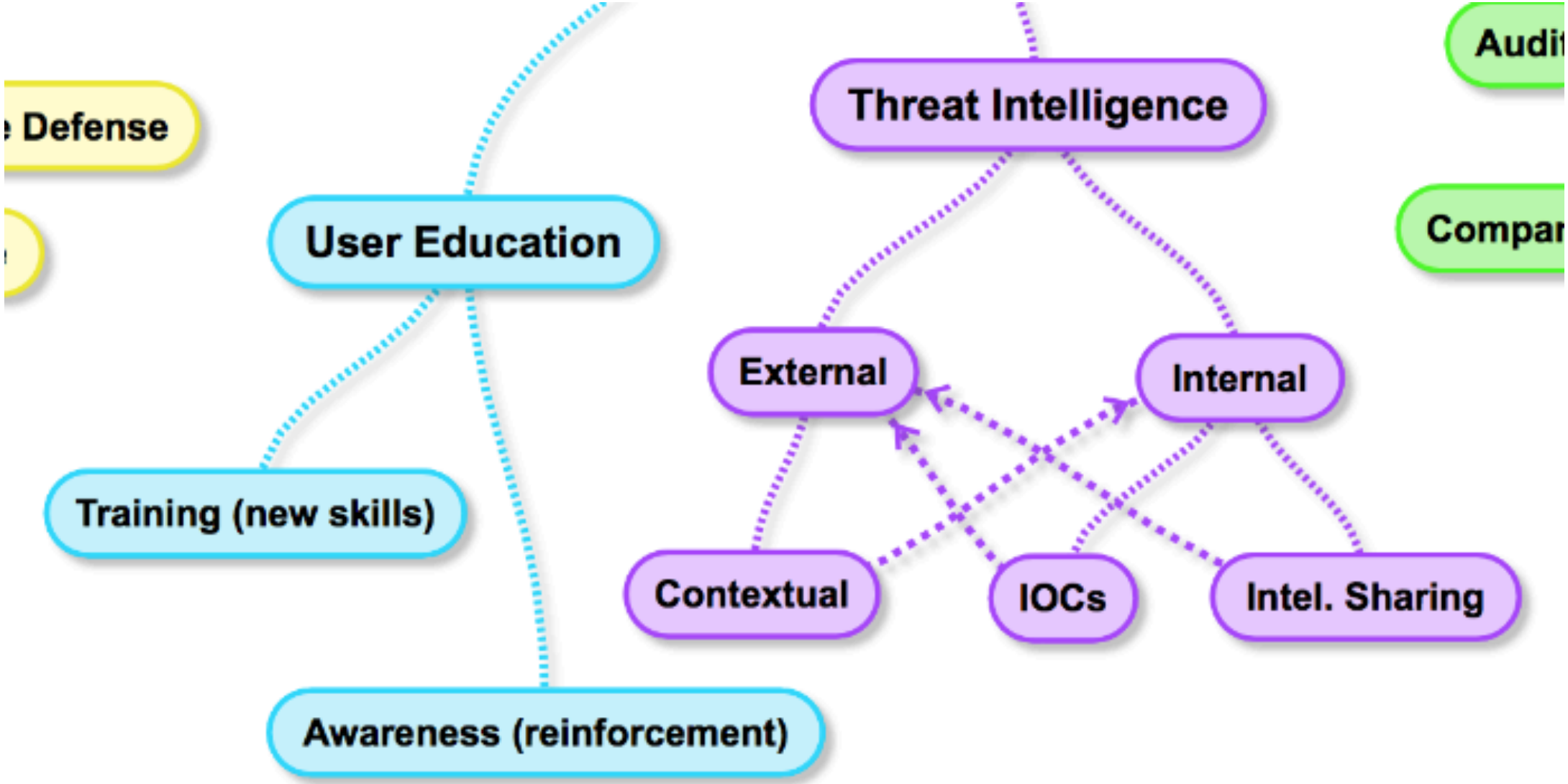

Cryptography
COBIT
ISO/IEC
SANS/CSC
NIST
es
Framework and Standard
R
So
Cybersecurity Domains


CASB
Federated Identity
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Cloud Security
Secure System Build
Security Architecture
Physica
Access Control
Cryptography
COBIT
Identity Management
Security Engineering
ISO/IEC
NIST
SANS/CSC
Privileged Access Management
Identity & Access Management
Certification
Conferences
Training
Framework and Standard
Career Development
Ris
Peer Groups
Self Study
Sou
DR
Cybersecurity Domains
B


ptography
COBIT
ISO/IEC
SANS/CSC
NIST
Framework and Standard
Cybersecurity Domains
Assets Inventory
Vulnerability scan
4th Party Risk
3rd Party Risk
Risk Assessment
Source Code Scan
Blackbox
Whitebox
Blueteam
Social Engineering
Redteam
Application
Penetration test
Infrastructure
Data-Centric Risk Assessment
Data-Flow Map
Industry Specific


Cybersecurity Domains
Blackbox
Whitebox
Governance
Industry Specific
Laws and Regulations
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
KPIs/KRIs
Compliance & Enforcement
Policy
Guideline
Procedure
Standard
Threat Intelligence
cation
External
Internal
Contextual
IOCs
Intel. Sharing


Cybersecurity Domains
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Eradication
Investigation
Forensics
User Education
Training (new skills)
Awareness (reinforcement)
Threat Intelligence
External
Contextual
IOCs


e Defense
User Education
Training (new skills)
Awareness (reinforcement)
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
Audit
Compar

Certification
Training
Conferences
Career Development
Peer Groups
Self Study
Physical Security