Cybersecurity career – I did it my way

@DrAzureAD

About the speaker

Who?

- Dr. Nestori Syynimaa
- Senior Principal Security Researcher @ Secureworks CTU
- Creator of *AADInternals* toolkit
- MVP (Identity & Access, Mobile Device Management), MVR

Contact details

- nsyynimaa@secureworks.com
- Twitter: @DrAzureAD
- https://linkedin.com/in/nestori
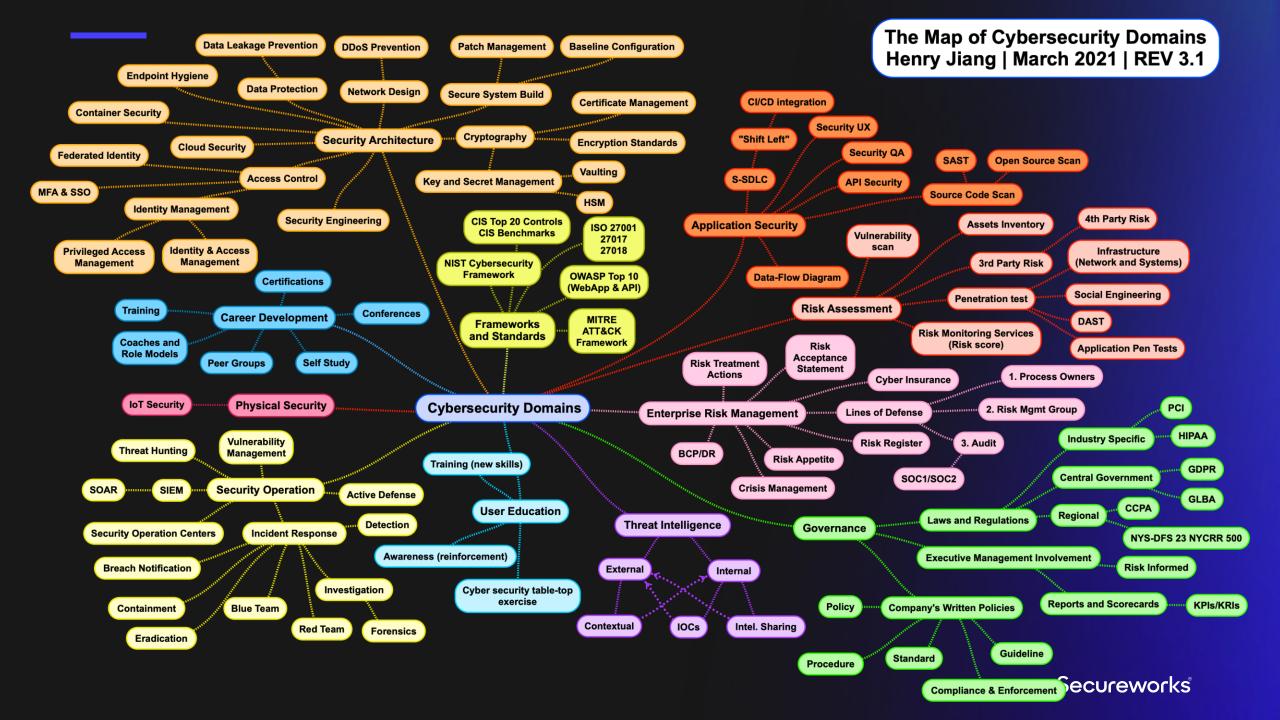- https://o365blog.com

Secureworks

Contents

- Cybersecurity domains

- How to get into cybersecurity

- My career path

Secureworks®

Secureworks®

Cybersecurity domains

The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1

Cybersecurity Domains (central node)

Security Architecture
- Data Leakage Prevention
- DDoS Prevention
- Patch Management
- Baseline Configuration
- Endpoint Hygiene
- Data Protection
- Network Design
- Secure System Build
- Container Security
- Certificate Management
- Cloud Security
- Cryptography
  - Encryption Standards
  - Key and Secret Management
    - Vaulting
    - HSM
- Federated Identity
- Access Control
- MFA & SSO
- Identity Management
- Security Engineering
- Privileged Access Management
- Identity & Access Management

Frameworks and Standards
- CIS Top 20 Controls / CIS Benchmarks
- ISO 27001 27017 27018
- NIST Cybersecurity Framework
- OWASP Top 10 (WebApp & API)
- MITRE ATT&CK Framework

Application Security
- CI/CD integration
- Security UX
- "Shift Left"
- Security QA
- SAST
- Open Source Scan
- S-SDLC
- API Security
- Source Code Scan
- Vulnerability scan
- Data-Flow Diagram

Risk Assessment
- Assets Inventory
- 4th Party Risk
- 3rd Party Risk
- Infrastructure (Network and Systems)
- Penetration test
- Social Engineering
- DAST
- Risk Monitoring Services (Risk score)
- Application Pen Tests

Enterprise Risk Management
- Risk Treatment Actions
- Risk Acceptance Statement
- Cyber Insurance
- 1. Process Owners
- Lines of Defense
- 2. Risk Mgmt Group
- BCP/DR
- Risk Register
- 3. Audit
- Risk Appetite
- SOC1/SOC2
- Crisis Management

Governance
- Laws and Regulations
  - Industry Specific
    - PCI
    - HIPAA
    - GDPR
    - GLBA
  - Central Government
  - Regional
    - CCPA
  - NYS-DFS 23 NYCRR 500
- Executive Management Involvement
  - Risk Informed
- Reports and Scorecards
  - KPIs/KRIs
- Policy
- Company's Written Policies
  - Procedure
  - Standard
  - Guideline
  - Compliance & Enforcement

Career Development
- Certifications
- Training
- Conferences
- Coaches and Role Models
- Peer Groups
- Self Study

IoT Security

Physical Security

Security Operation
- Threat Hunting
- Vulnerability Management
- SOAR
- SIEM
- Active Defense
- Security Operation Centers
- Incident Response
  - Detection
  - Breach Notification
  - Investigation
  - Containment
  - Blue Team
  - Red Team
  - Forensics
  - Eradication

User Education
- Training (new skills)
- Awareness (reinforcement)
- Cyber security table-top exercise

Threat Intelligence
- External
- Internal
- Contextual
- IOCs
- Intel. Sharing

Secureworks

Secureworks®

How to get into cybersecurity

How to get into cybersecurity

- Formal education

- Work experience

- Certifications

- Contributing to community

Secureworks®

Secureworks®

My career path

My career path

- 2000   First job on IT industry (software developer/architect)

- 2004   Chief Technology Officer (CTO)

- 2007   Chief Information Officer (CIO), Anvia konserni

- 2013   IT Trainer

- 2017   University Lecturer, University of Jyväskylä

- 2018   CIO, Tampereen kehyskunnat

- 2021   Senior Principal Security Researcher, Secureworks

Formal education

- 2003   Datanomi, Tietojärjestelmät

- 2007   BBa, SME Bus. Adm, Marketing (Seinäjoki UaS)

- 2009   MSc, Econ. & Bus. Adm, Computer Science (UWasa)

- 2015   PhD, Informatics (Henley Business School / UoReading)

- 2017   Professional Teacher Qualification (HAMK)

- 2020   Specialisation Education in Cyber Security (TAMK)

- *2023   Master of Engineering, Cyber Security (JAMK)*

- *2023   D.Sc. In Economics, University of Jyväskylä*

Certifications

Cybersecurity certifications companies are hiring for

Certification	LinkedIn	Indeed	Simply Hired	Total
CISSP	52,000	23,711	11,547	87,258
CISA	22,063	12,544	7,127	41,734
CISM	14,795	7,021	3,463	25,279
Security+	7,366	10,161	3,235	20,762
CEH	21,125	3,961	1,918	27,004
GSEC	4,189	4,054	2,545	10,788
SSCP	4,177	3,569	2,231	9,977
CASP	3,096	1,391	925	5,412
GCIH	4,111	2,985	1,764	8,860
OSCP	4,162	3,054	1,232	8,448

Secureworks®

Contributing to community

- Why?

  - To get attention & to gain expert status

- How?

  - Blog, tweet, Youtube

  - Create tools

  - Speak in user groups, conferences

Secureworks®

GoldenSAML history

Nov 16: First blog on abusing identity federation[1]

Nov 21: "GoldenSAML" coined by CyberArk[2]

Oct 25: First AADInternals release[3]

Mar 21: ADFSDump and ADFSSpoof released[4]

Aug 16: AADInternals w/ certificate export

Apr 27: Remote AD FS config dump[5,6]

Nov 8: WhiskeySAML and Friends[7]

SOLORIGATE

2017   2018   2019   2020   2021

1. https://o365blog.com/post/federation-vulnerability/
2. https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps
3. https://o365blog.com/post/aadinternals/
4. https://troopers.de/troopers19/agenda/fpxwmn/
5. https://o365blog.com/post/adfs/
6. https://www.mandiant.com/resources/abusing-replication-stealing-adfs-secrets-over-the-network
7. https://www.blackhat.com/eu-21/arsenal/schedule/#whiskeysaml-and-friends-25024

Secureworks®

AADInternals

- Admin & hacking toolkit for Azure AD & Microsoft 365

- Open source:

  - https://github.com/gerenios/aadinternals

  - https://o365blog.com/aadinternals/

- MITRE ATT&CK

  - https://attack.mitre.org/software/S0677/

Groups That Use This Software

ID	Name	References
G0016	APT29	[5]

Secureworks®

2022 conference talks

- Mar: Teams Nation 2022 (virtual)

- Apr: ICEIS2022 (virtual)

- May: M365 Security & Compliance User Group UK (virtual)

- Jun: TROOPERS (GER), CERT-EE (EST)

- Aug: Black Hat (USA), DEF CON, Tech Mentor

- Sep: Identity Summit (GER), ROMHACK (ITA)

- Nov: Tech Mentor (USA)

Secureworks®

Is it worth it?

- Executives (CISO etc.) $200 000

- Mid-level IT professionals $120 000

- Consultants, admins $ 80 000

Secureworks

Secureworks®

Thank you!