

Security Domains- And Why We Need Them

Michal Davidson

Conf42
DevSecOps 2023

Michal Davidson

Software & Security Architect

NDS, HP, IBM, Cisco, Synamedia

Msc. CS in Cyber Security

Lecturer – Cyber Security

Jerusalem College of Technology, Azrieli College

Courses: Intro to Cyber Security, Agile SDLC

Software Architect @ Dell Technologies

Leading Public Cloud & Security for PowerFlex

Security Domains

A large, dense pile of books and papers, with a blue semi-transparent banner overlaid across the top containing the text 'Security Domains'. The books are of various colors and sizes, and the papers are scattered throughout the pile. The banner is a solid blue color with the text in white, sans-serif font.



Motivation



Diversity



Career & Community



Holistic Security



Compliance

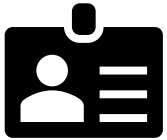


Compliance –3rd Party Standards

- FedRamp
- EO
- SOC 2/3
- ISO 27001
- DISA STIG
- HIPAA
- PCI-DSS
- EL 1-3
- GDPR

Protecting Network, Data & Resources

IAM



SSO &
MFA



Firewalls



Network
Security



Authenticating → Who?
Authorizing → What?
Why?

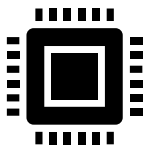


Monitoring- Detecting Cyber Threats & Breaches

- Anomaly Detection
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)

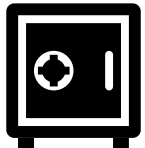
Expertise: Data Science, AI, M.L

Techniques for Secure Communication & Info Math & Algorithm Based



Embedded
Security

- Secure Boot
- TEE



Key
Protection, TPM

Cryptanalysis



Cryptography = Foundation of Cyber Security



Security Architecture



Using security elements to enforce security policies within and between domains



Security Review
\ Threat Modeling



Secure Protocols

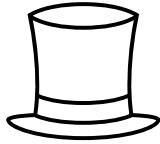
- SSL\TLS
- IPSec
- ...

Using Security Building Blocks

Identifying & exploiting weaknesses in a computer system/network



Pen-Testing



White-Hat
Hacking



Reverse Engineering

Time & Patience Required!

Hacking



FedRamp , EO, SOC 2/3, ISO 27001, DISA STIG,
HIPAA, PCI-DSS, EL 1-3, GDPR

Security Review, Threat Modeling
Secure Protocols



IAM
SSO
MFA

Embedded Security:
Secure Boot, TEE

Key Protection, TPM

White-Hat Hacking
Reverse Engineering
Pen Testing

Anomaly Detection, ML, IDS & IDP

Additional Resources

- [Cryptography \(Coursera\)](#)
- [Software Security \(Coursera\)](#)
- [Penetration Testing & Ethical Hacking\(Cybrary\)](#)

- [Taimur Ijlal- Cloud Security Guy \(Medium\)](#)
- [Prof. Bill Buchanan \(Medium\)](#)

 MichalSaraW@gmail.com

 [Linkedin.com/in/MichalWoolf](https://www.linkedin.com/in/MichalWoolf)

 medium.com/@MsArchitect

Thank You

CONF42

Michal Davidson

Dell Technologies



MichalSaraW@gmail.com



[Linkedin.com/in/MichalWoolf](https://www.linkedin.com/in/MichalWoolf)



medium.com/@MsArchitect