# The Security Analyst Mind

RASHAD SULEYMANOV

# About me

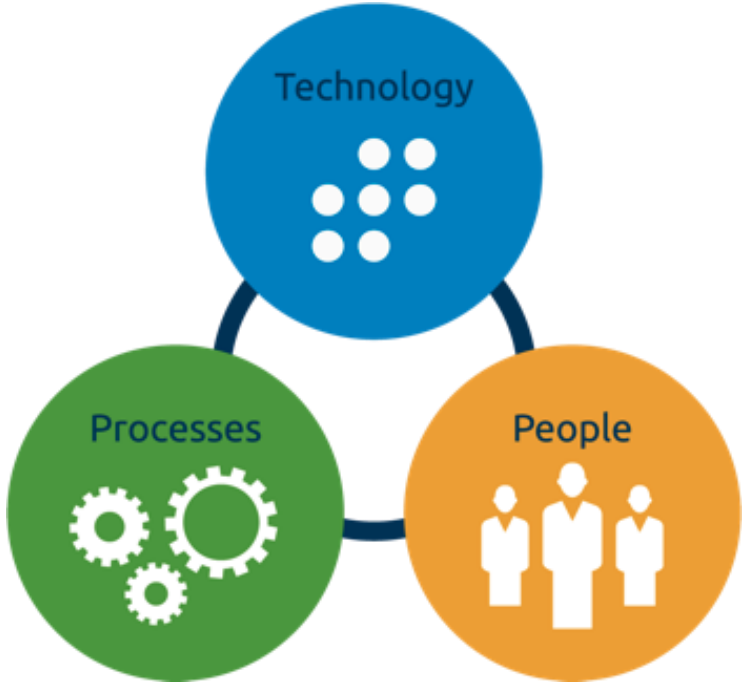
- BaSoTi Alumni (Riga - 2014)
- Cybersecurity Master Student (Tallinn University of Technology, Estonia)
- Threat Analyst (IBM X-Force Command Center, Wroclaw, Poland)

# Agenda

- What is SOC, who is SOC Security Analyst?
- Skills
  - Psychological (Investigation Process)
  - Theoretical (Understanding Technology)
  - Practical (Security Home Lab)
- Resources
  - People, Books, Certifications
- Questions?

# Security Operation Center (SOC)

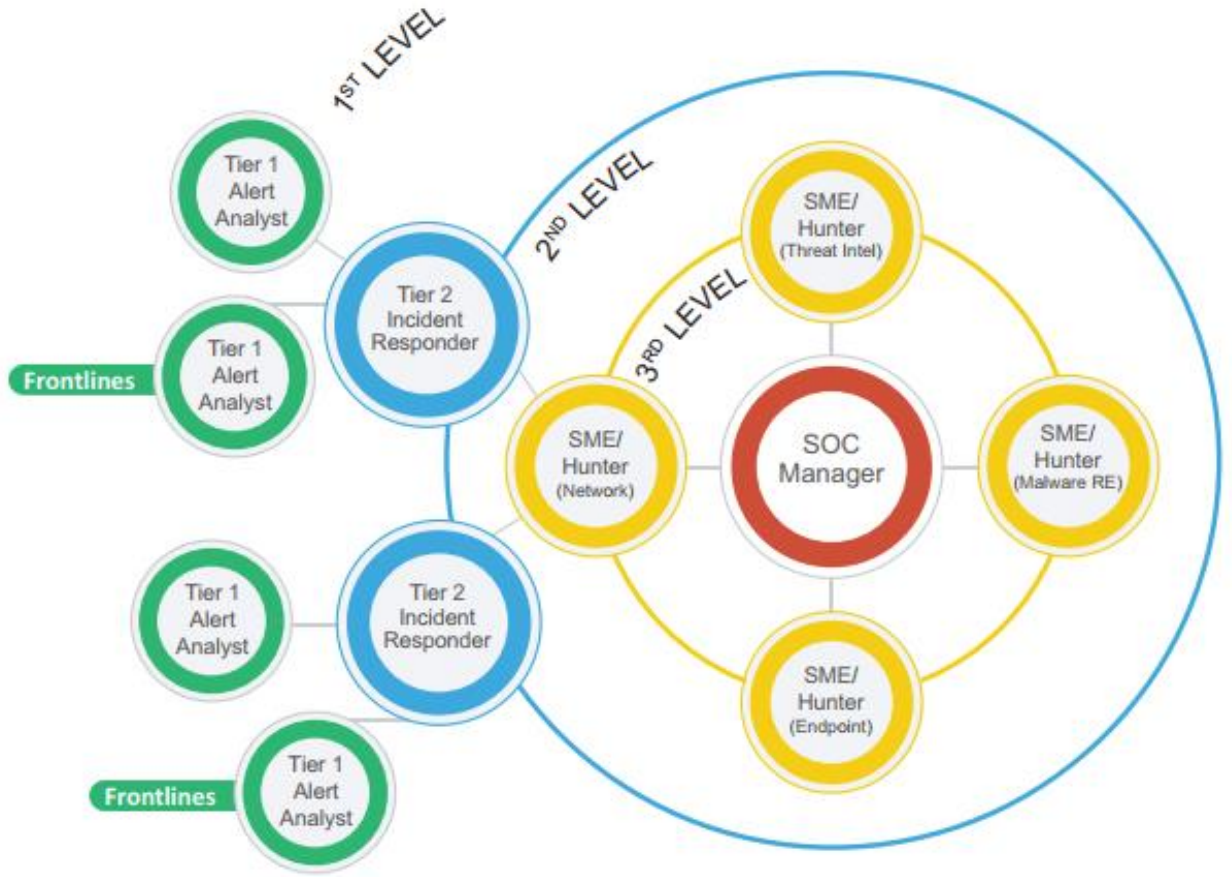
- The SOC is the facility where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops, other endpoints, and so on) are monitored, assessed, and defended. [1]
  - **threat-centric SOC**
  - **compliance-based SOC**
  - **operational-based SOC**




https://en.wikipedia.org/wiki/Information_security_operations_center [1]
https://logrhythm.com/solutions/security/soc-platform/ [pic]

# SOC Security Analyst

- Tier 1: Alert Analyst. Duties: Continuously monitors the alert queue
- Tier 2: Incident Responder. Duties: Performs deep-dive incident analysis by correlating data from various sources
- Tier 3 Subject Matter Expert/ Hunter. Duties: Possesses in-depth knowledge on network, endpoint, threat intelligence, forensics and malware reverse engineering, as well as the functioning of specific applications or underlying IT infrastructure [1]




https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf [1]
https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907 [pic]

# Skills (Psychological)

- Metacognition - Thinking about thinking - “Why did I do this?”
  - Metacognition is "cognition about cognition", "thinking about thinking", "knowing about knowing", becoming "aware of one's awareness" and higher-order thinking skills. The term comes from the root word meta, meaning "beyond". Metacognition can take many forms; it includes knowledge about when and how to use particular strategies for learning or for problem-solving. There are generally two components of metacognition: knowledge about cognition, and regulation of cognition.

https://en.wikipedia.org/wiki/Metacognition

# Skills (Psychological) cont.

## CHIRIS SANDERS (EXPERIMENT)

- Research Questions:
  - Are experts more metacognitively aware?
  - What separates novice and expert analysts?
- Sample:
  - Novice and expert analysts
- Methodology:
  - 30 case studies
  - Stimulated recall interviews
  - Focus on individual investigations of varying types
  - Perform key phrase analysis

https://www.slideshare.net/chrissanders88/presentations

# Skills (Psychological) cont.

## Key Phrase Mapping

- Dual Process Theory
  - Intuition: Implicit, unconscious, fast
  - Reflection: Explicit, controlled, slow

| Intuition |
| --- |
| Experimentation |
| Restructuring |
| Imagination |
| Incubation |

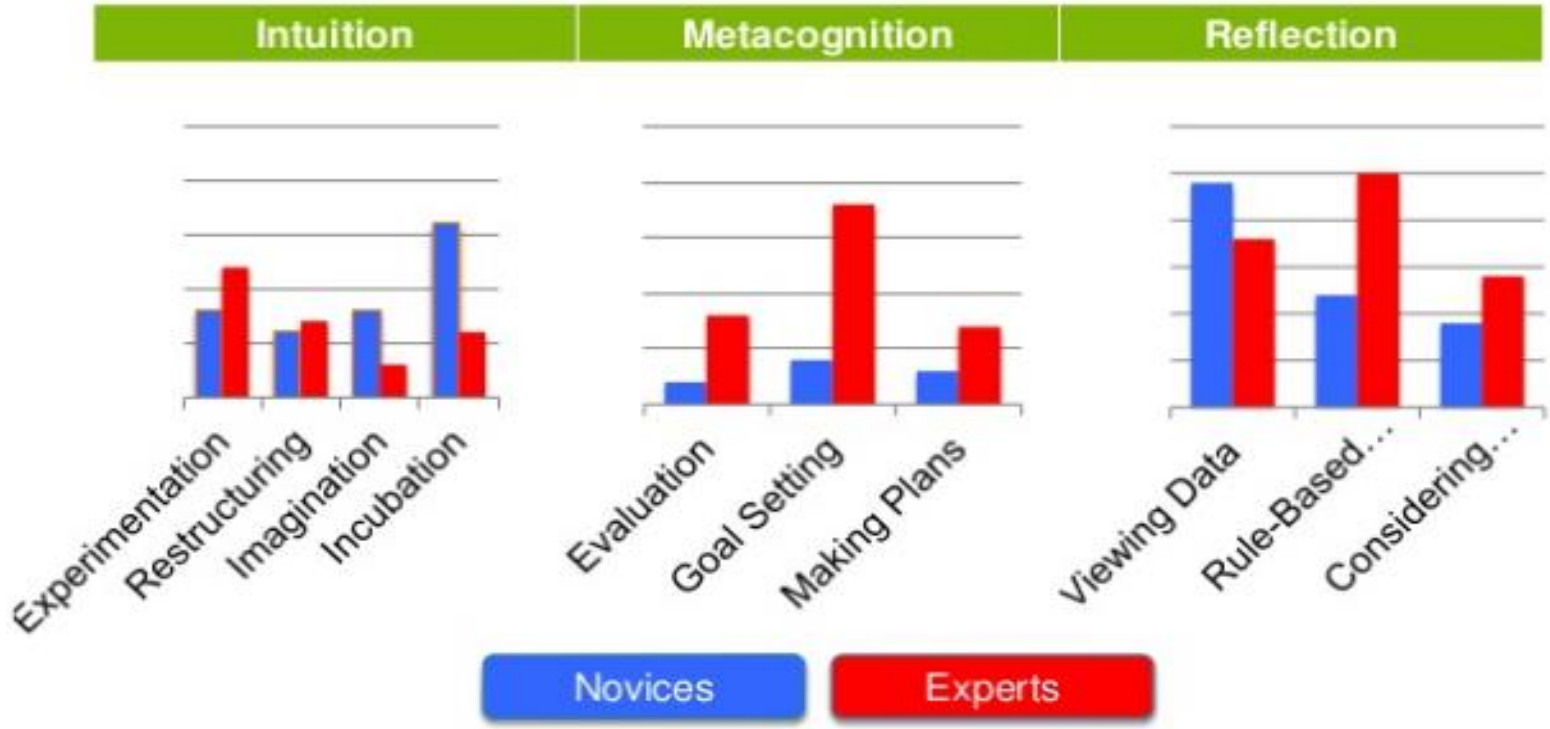
| Metacognition |
| --- |
| Evaluation |
| Goal Setting |
| Making Plans |

| Reflection |
| --- |
| Analytically Viewing Data |
| Rule-Based Reasoning |
| Considering Alternatives |

https://www.slideshare.net/chrissanders88/presentations

# Skills (Psychological) cont.

Results




https://www.slideshare.net/chrissanders88/presentations

# Skills (Psychological) cont.

## Findings

- Experienced analysts rely on rule-based reasoning to a much larger extent.
- Experienced analysts are more metacognitively aware than novice analysts.

# Skills (Theoretical)

## Understanding Cisco Cybersecurity Fundamentals

- Network Concepts
- Security Concepts
- Cryptography
- Host-Based Analysis
- Security Monitoring
- Attack Methods

## Implementing Cisco Cybersecurity Operations

- Endpoint Threat Analysis and Computer Forensics
- Network Intrusion Analysis
- Incident Response
- Data and Event Analysis
- Incident Handling

https://learningnetwork.cisco.com/community/certifications/ccna-cyber-ops/secfnd/exam-topics

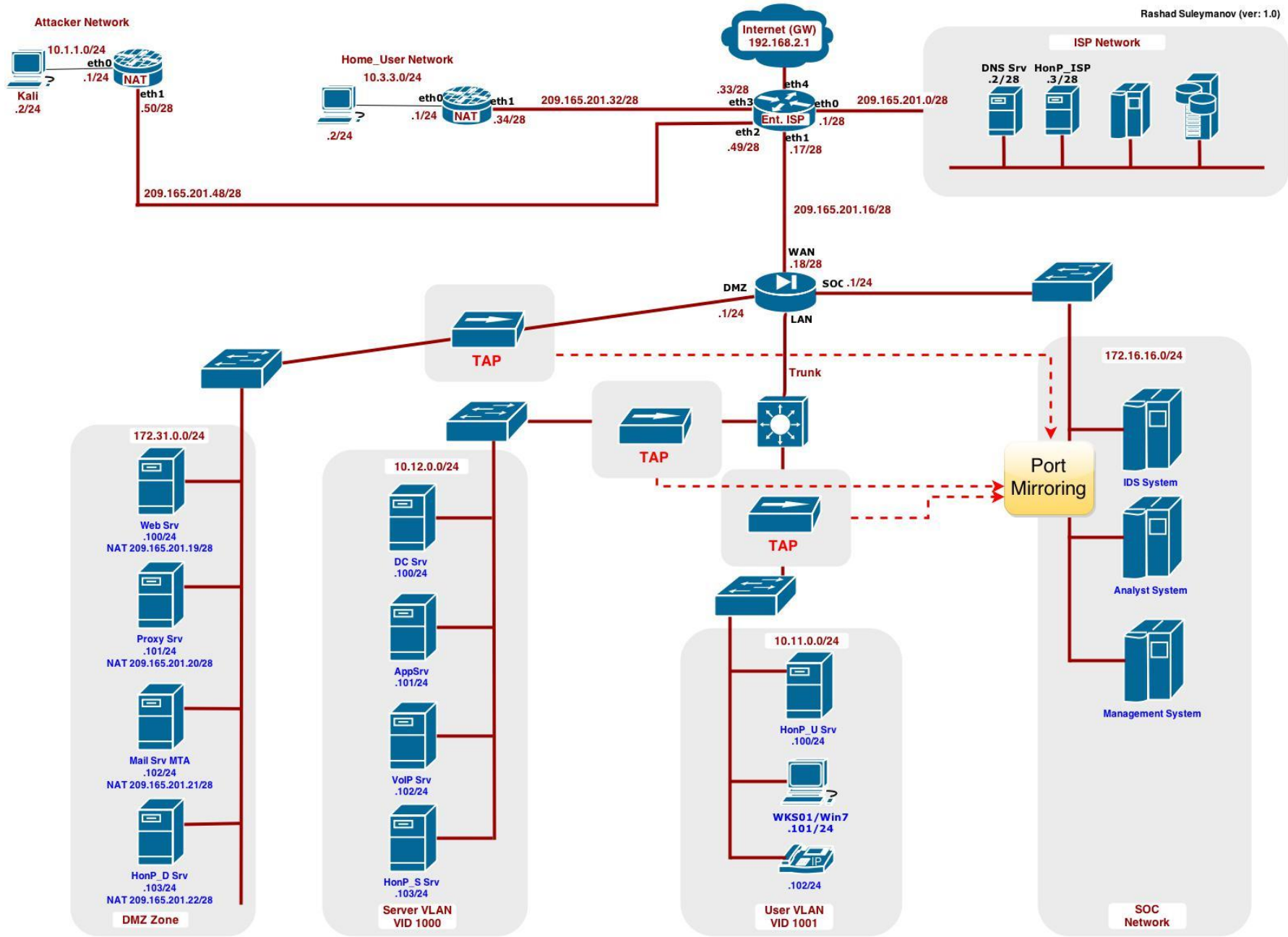
https://learningnetwork.cisco.com/community/certifications/ccna-cyber-ops/secops/exam-topics

# Skills (Practical)

- Why Build a LAB?
  - A laboratory is as vital to computer-security specialist as it is to a chemist or biologist. It is the studio in which you can control a large number of variables that come to bear upon the outcome of your experiments.
- Consider some of the other items that might motivate your to construct such a lab:
  - Certification
  - Job advancement
  - Knowledge
  - Experimentation
  - Evaluation of new tools

# Skills (Prac

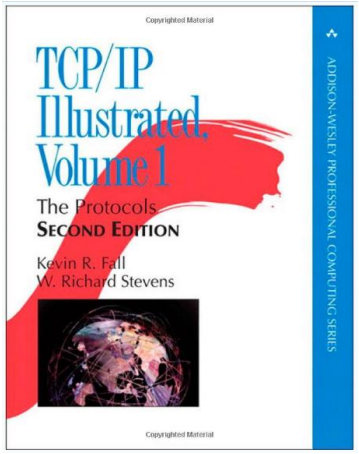
- Build Your Own Cyb
  - Motherboard: S
    1600 LGA 1150
  - CPU: Intel Xeon
    1150
  - RAM: Kingston
    of 4 (4 x 8 GB) D
  - PC3 12800 ECC
    Workstation Me
  - HDD: 3TB NAS H
  - OnTheHub par
    (http://ontheh
  - AVATAR Projec
    (https://www.c

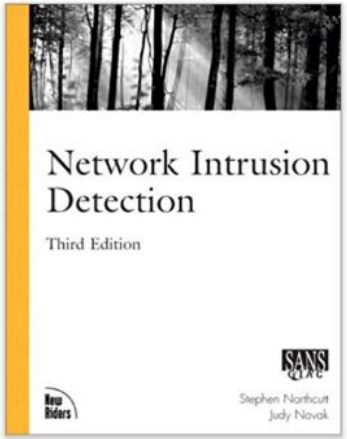

Rashad Suleymanov (ver: 1.0)
Attacker Network
10.1.1.0/24
eth0
.1/24
NAT
eth1
.50/28
Kali
.2/24
Home_User Network
10.3.3.0/24
eth0
.1/24
NAT
eth1
.34/28
.2/24
209.165.201.32/28
Internet (GW)
192.168.2.1
.33/28
eth4
eth3
Ent. ISP
eth0
.1/28
eth2
.49/28
eth1
.17/28
209.165.201.0/28
ISP Network
DNS Srv
.2/28
HonP_ISP
.3/28
209.165.201.48/28
209.165.201.16/28
WAN
.18/28
DMZ
.1/24
SOC .1/24
LAN
TAP
Trunk
TAP
TAP
Port
Mirroring
172.16.16.0/24
IDS System
Analyst System
Management System
SOC
Network
172.31.0.0/24
Web Srv
.100/24
NAT 209.165.201.19/28
Proxy Srv
.101/24
NAT 209.165.201.20/28
Mail Srv MTA
.102/24
NAT 209.165.201.21/28
HonP_D Srv
.103/24
NAT 209.165.201.22/28
DMZ Zone
10.12.0.0/24
DC Srv
.100/24
AppSrv
.101/24
VoIP Srv
.102/24
HonP_S Srv
.103/24
Server VLAN
VID 1000
10.11.0.0/24
HonP_U Srv
.100/24
WKS01/Win7
.101/24
.102/24
User VLAN
VID 1001

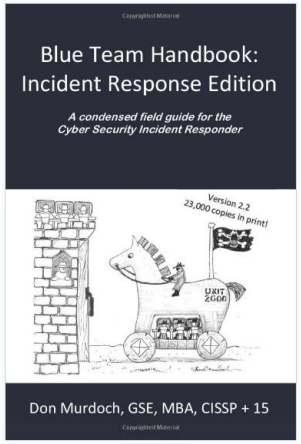
# Resources (People)

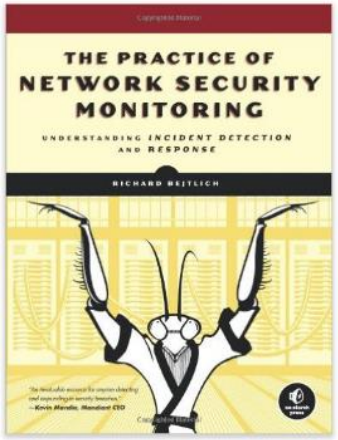
- NSM, Investigation Theory – Chris Sanders (http://chrissanders.org/)
- SIEM, Log Management – Anton Chuvakin (http://www.chuvakin.org/)
- Security Data Visualization - Raffael Marty (http://raffy.ch/)
- Threat Hunting - David J. Bianco (http://www.threathunting.net/)
- SANS Instructors

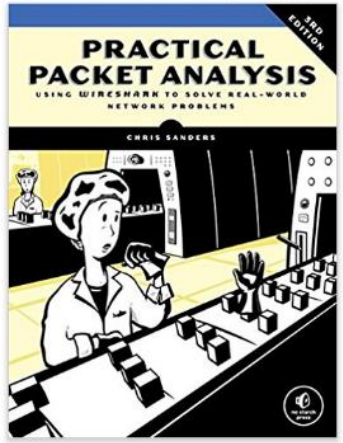
# Resources (Books)

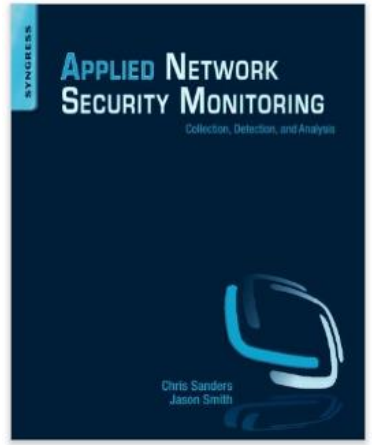


# Resources (Certifications)

- Cisco
  - ICND1 (Exam Number: 101-105)
  - Understanding Cisco Cybersecurity Fundamentals (Exam Number: 210-250 SECFND)
  - Implementing Cisco Cybersecurity Operations (Exam Number: 210-255 SECOPS)
- CEH (Certified Ethical Hacker)
- SANS - Cyber Threat Intelligence (FOR578)

Thank You!