



Six essential ingredients of a modern **Security Operations Center (SOC)**

Presented by

Rafeeq Rehman

October 28, 2023

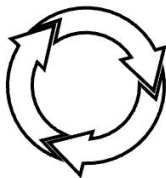
Six Essential Ingredients

1



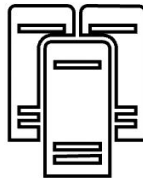
People
(SOC Staff)

2



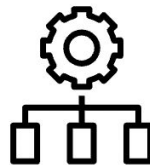
SOC
Processes

3



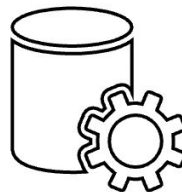
Technology
Stack

4



SOC
Governance

5



Data
Sources

6



Threat
Intelligence

CONTINUOUS IMPROVEMENT ACTIVITIES

1. People

Hiring and retention - the highest issue

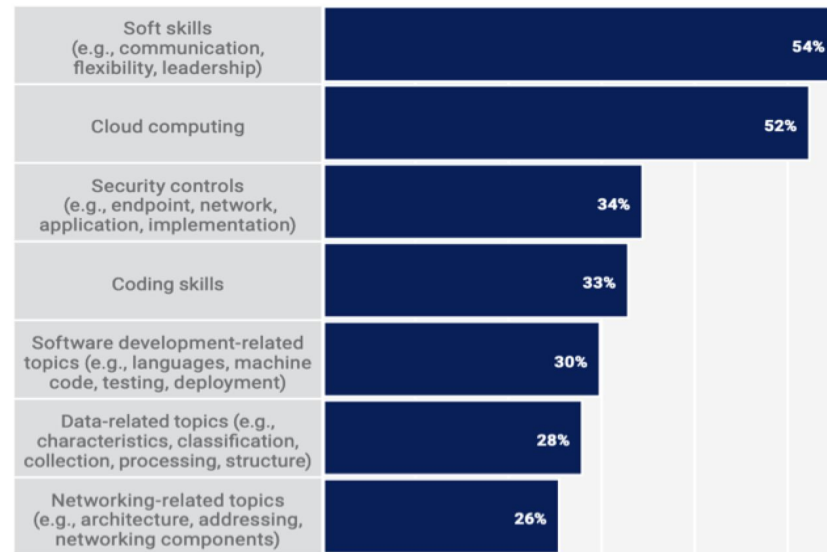
Skill gaps - train, borrow, buy?

The **2022 ISACA Report on State of Cybersecurity** professionals. The biggest skill gap identified in the included “**communications, flexibility, leadership**”

Lack of **business acumen, poor communication**, | other factors causing **brand damage of otherwise**

FIGURE 14—QUANTIFIED SKILL GAPS

What are the biggest skill gaps you see in today's cybersecurity professionals?

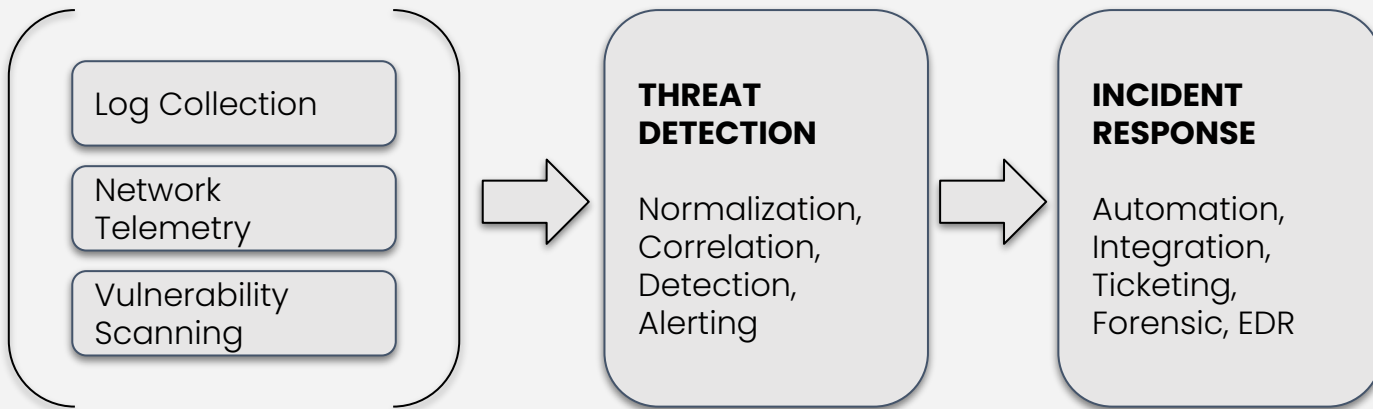


2. Processes

Maturity of processes is a key factor for SOC success.

1. **IT Processes** (patching, upgrades, change management, problem management etc.)
2. **SOC Policies and Standards** (log collection standards)
3. Threat detection process
4. Incident Response process
5. Threat hunting process
6. Use case development process
7. Shift management process

3. Technology Stack

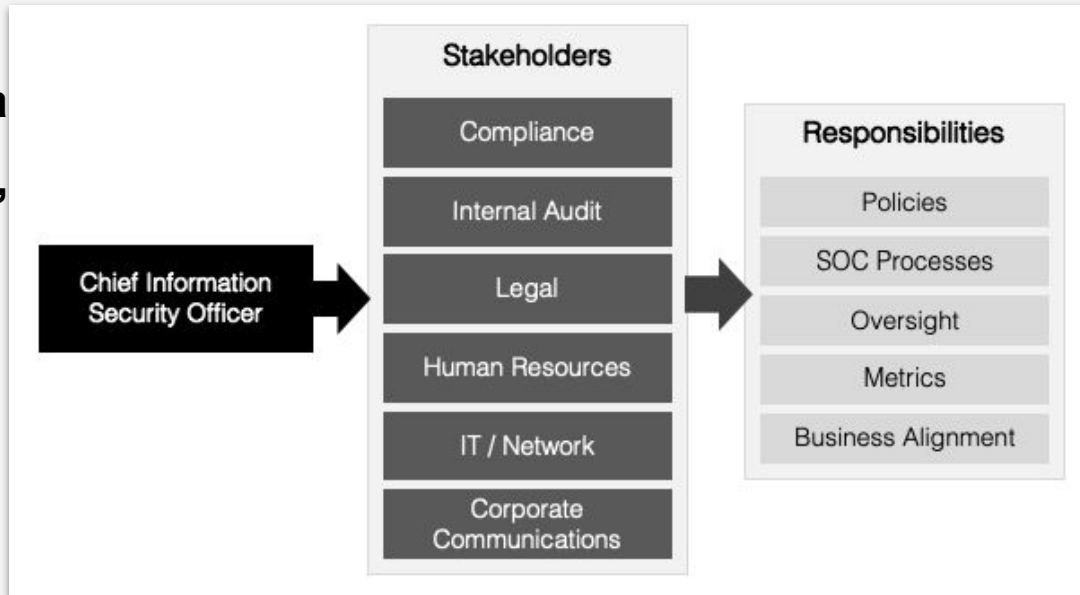


ENABLING TECHNOLOGIES

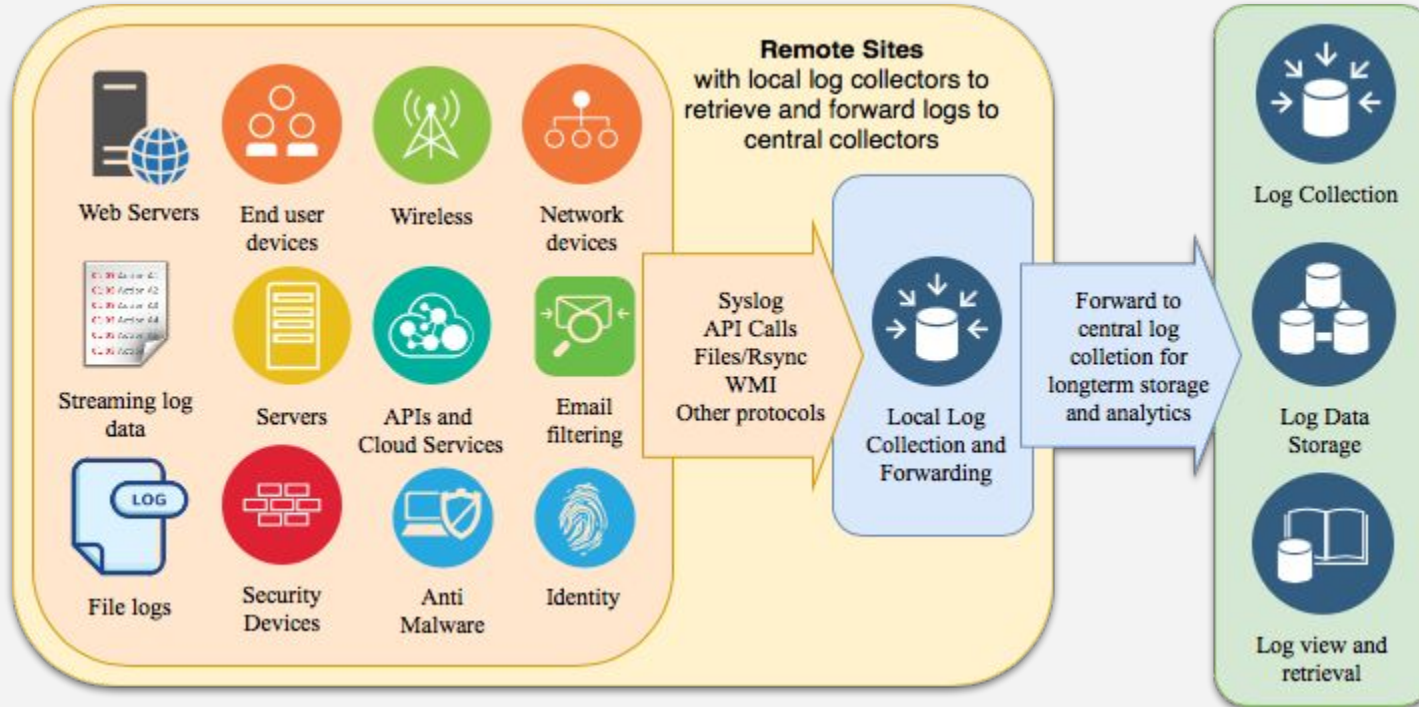
Servers, OS, Storage, Backup, Encryption, Routers, Switches, knowledge management

4. SOC Governance

- Governance **board**
- SOC **organizational chart**
- **Business case, finance,**
- **Marketing**
- **Collaboration**



5. Data Sources



5. Data Source – Log Prioritization

Log Source	Usefulness for threat detection?	Required for compliance?	Related to business critical application?	Valuable for forensic investigation?	Total score
DMZ Firewall	X	X	X	X	4
URL Filtering Proxy	X	X		X	3
Ecommerce Apache Server	X	X	X	X	4
Development Web Server WAF				X	1

6. Threat Intelligence

- STIX and TAXII
- Open and commercial threat intelligence
- TI automation with TIP
- Exploited Vulnerabilities databases and integration into incident prioritization
- Exploit Prediction Scoring System (EPSS)

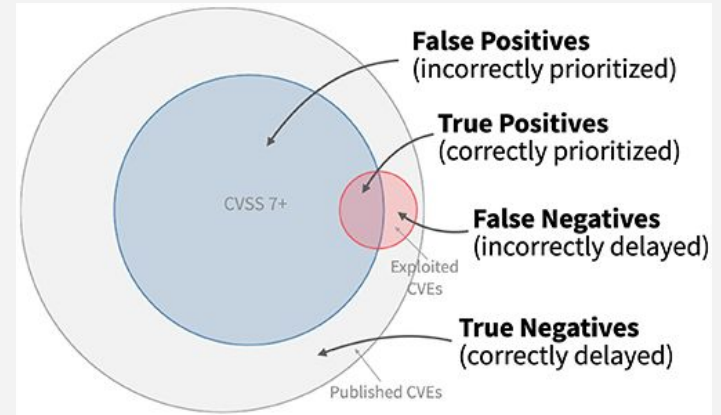
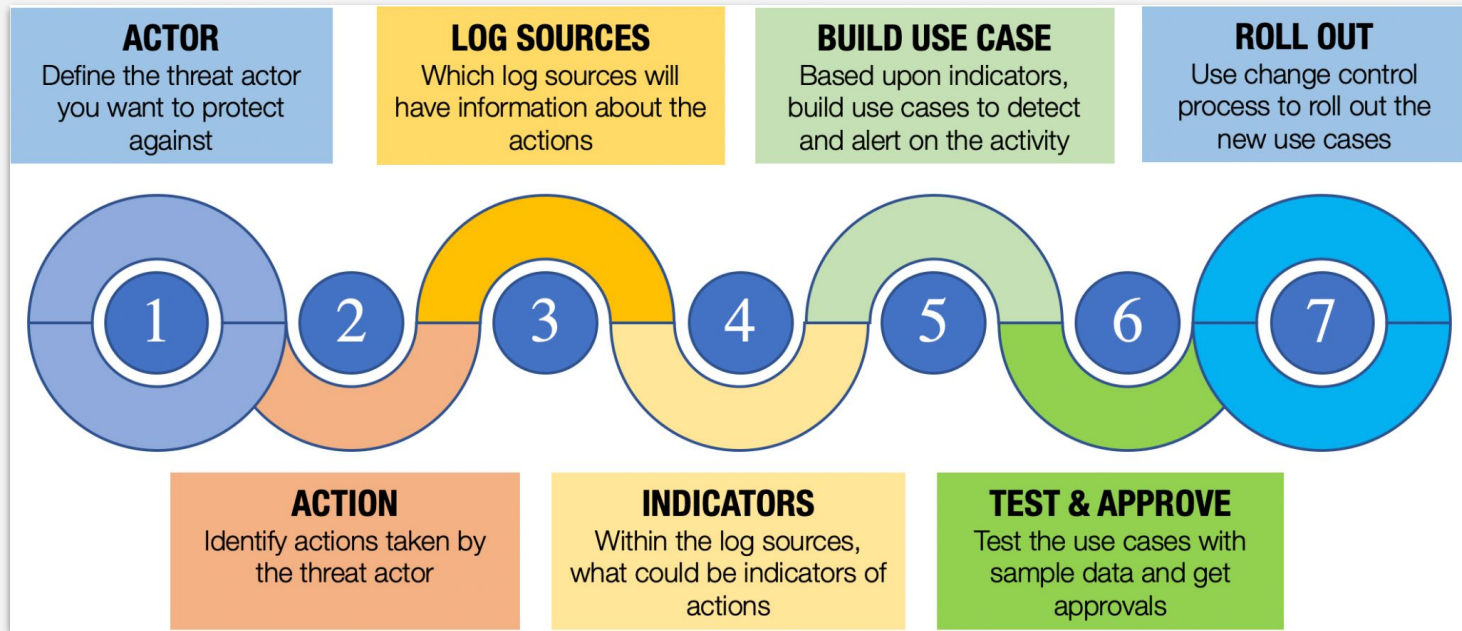


Image reference: <https://www.first.org/epss/model>

Continuous Improvement

Developing and fine tuning use cases

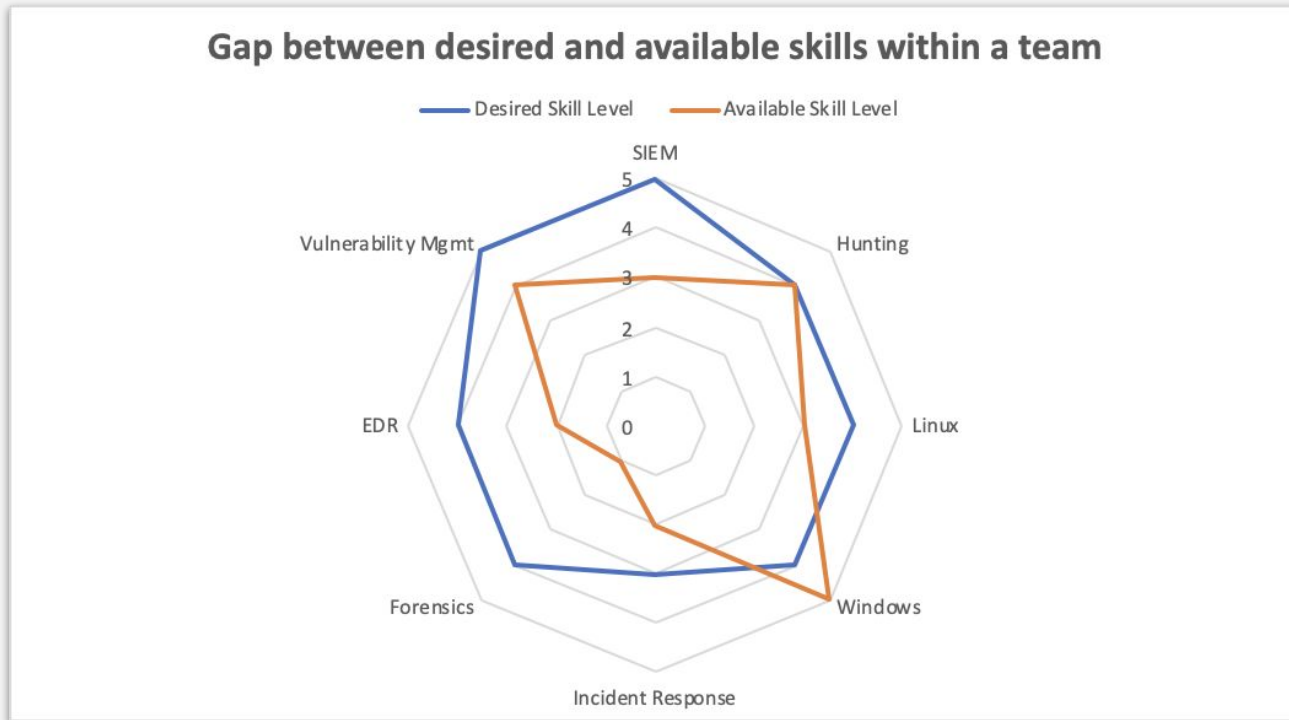


Digging Deeper **Managing SOC Skills**

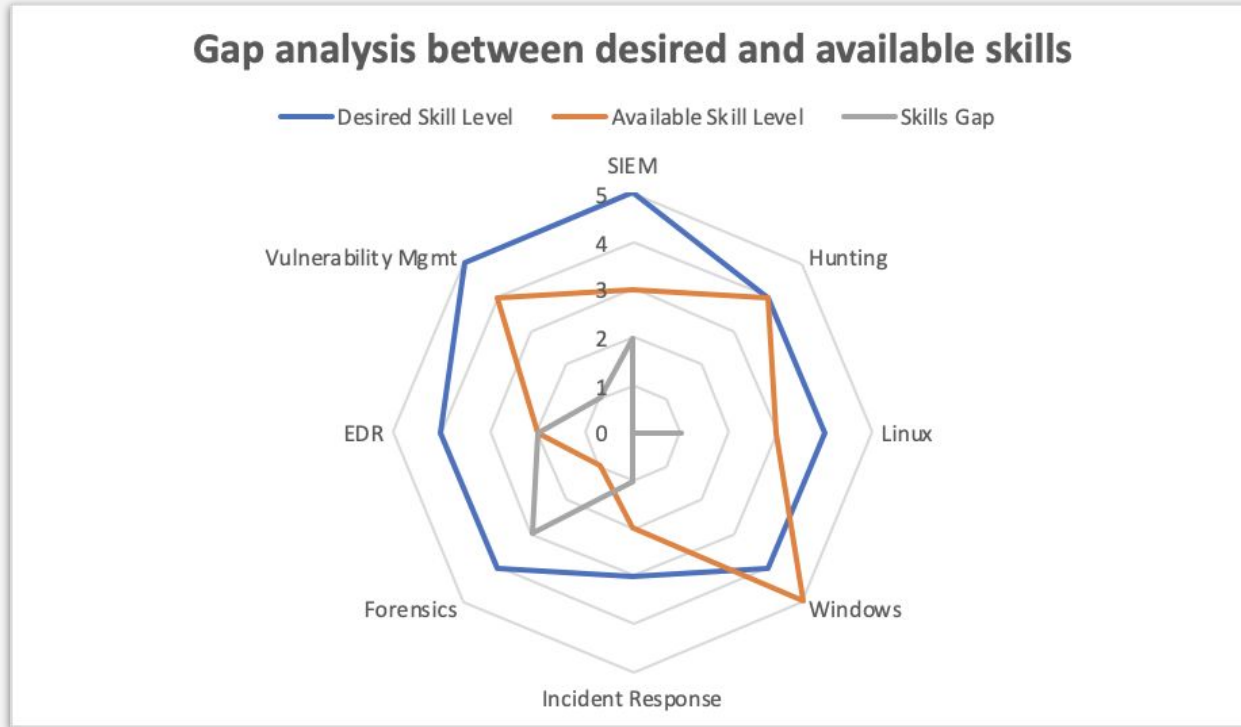
Skill Gaps - Scale of 1-5

	SIEM	Hunting	Linux	Windows	Incident Response	Forensics	EDR	Vulnerability Mgmt
Desired Skill Level	5	4	4	4	3	4	4	5
Available Skill Level	3	4	3	5	2	1	2	4
Skills Gap	2	0	1	0	1	3	2	1

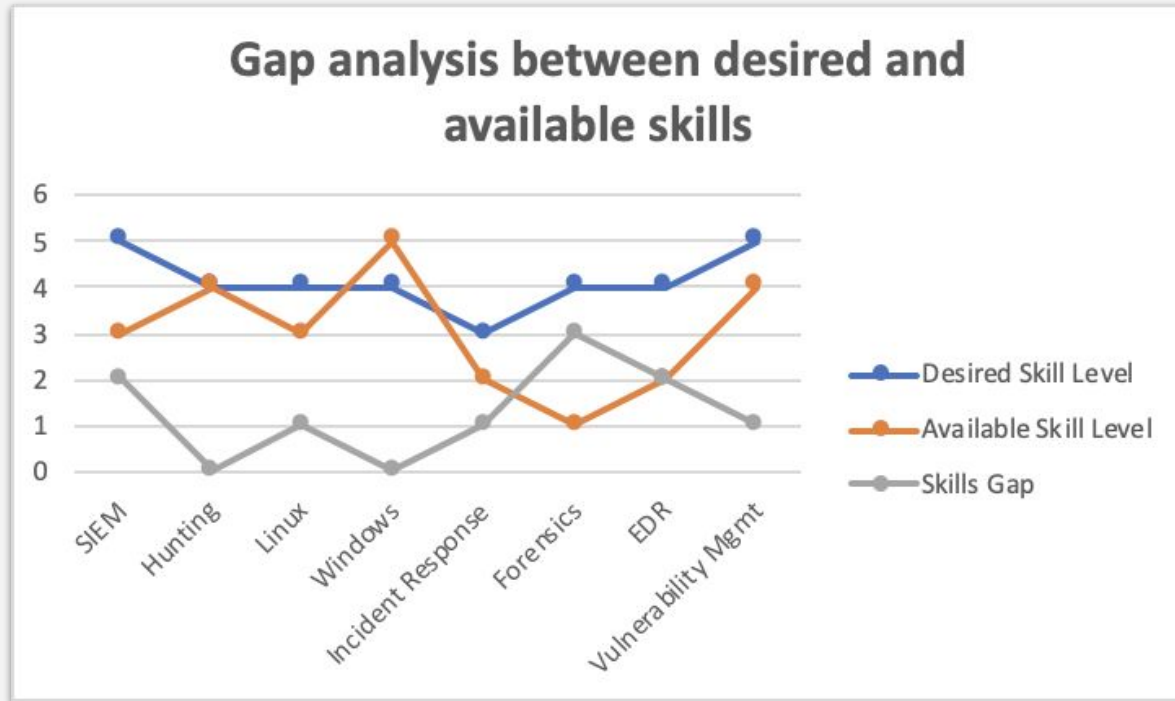
Skill Gaps - Desired and Available Skills



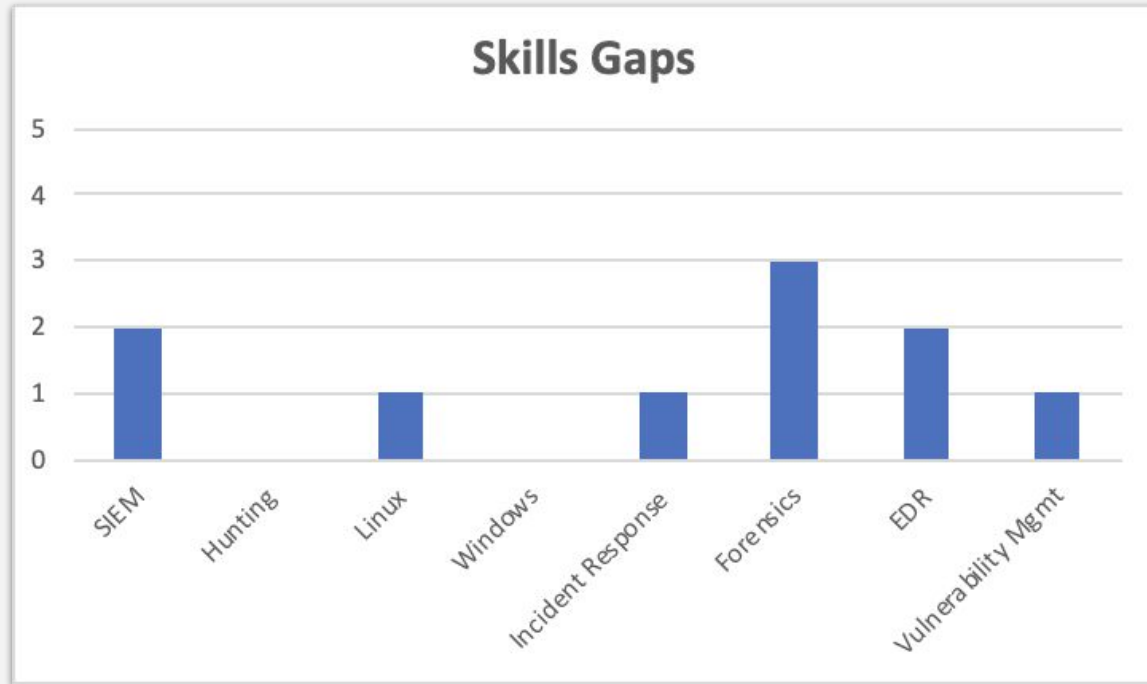
Skill Gaps - Analysis



Skill Gaps - Analysis



Skill Gaps - Analysis



Skill Gaps - Actions

	SIEM	Hunting	Linux	Windows	Incident Response	Forensics	EDR	Vulnerability Mgmt
Desired Skill Level	5	4	4	4	3	4	4	5
Available Skill Level	3	4	3	5	2	1	2	4
Skills Gap	2	0	1	0	1	3	2	1
Action Required	Hire	No Action	Upskill	No Action	Upskill	Hire	Hire	Upskill

Essential Skills for SOC Staff

1. **Foundational information security principles** (e.g. CIA triad, least privileges, need to know, defense in depth, etc.)
2. **Operating Systems and Cloud** - Linux/Unix and Windows
3. **Networking and application protocols**
 - Very good knowledge of TCP/IP, DNS, HTTP, SMTP, SSH etc. Hands on practice for routers and switches, packet capture, nmap, curl, etc.
4. **Programming** (at least basic level)
 - Shell scripting, Python, C would be great to know, understand how web applications are built, HTML, JavaScript, SQL/Databases
5. **Encryption technologies** - PKI concepts, TLS
6. **Research** – Including LLM tools



Thank You!

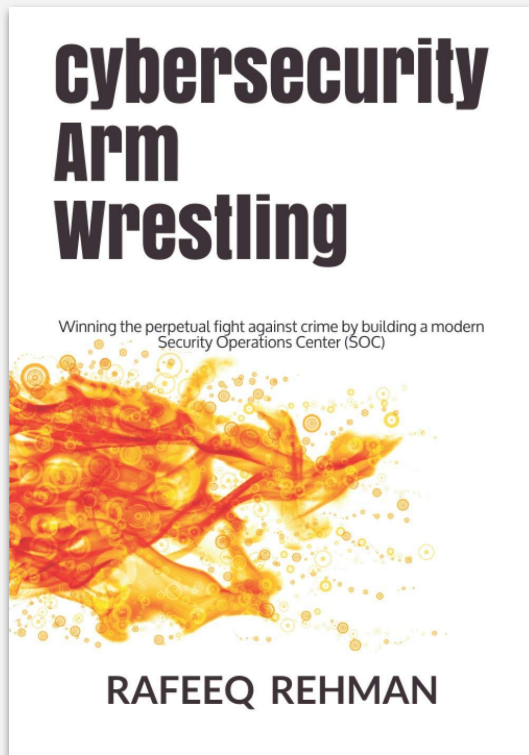
- **Follow me on Twitter (or DM): @rafeeq_rehman**
- **Subscribe to my personal blog:** <https://rafeeqrehman.com>
- **Follow me on LinkedIn:** <https://www.linkedin.com/in/rafeeq/>

Further Study and Reference

Cybersecurity Arm Wrestling:

Winning the perpetual fight against crime by building a modern Security Operations Center

<https://www.amazon.com/Cybersecurity-Arm-Wrestling-perpetual-Operations/dp/B091LWPGCV/>



What is Cybersecurity Learning Saturday?

- This is a learning network supported by volunteers
- Instructor-led and live online training sessions are held on Saturdays
- Diverse topics
- Have something to offer? You can volunteer to be a trainer
- **Join Cybersecurity Learning Saturday LinkedIn Group** -
<https://www.linkedin.com/groups/8988689/>
- **Follow LinkedIn Page**
<https://www.linkedin.com/company/cybersecurity-learning-saturday>