Open source

Security Operations Center

Khashochir.B

#MNSEC_2024

ABOUT ME

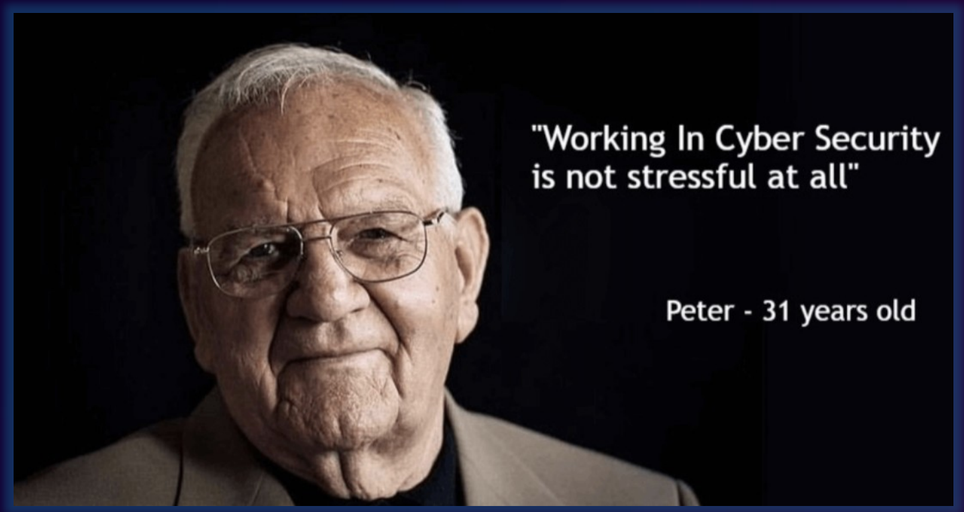
- Cyber security – 10+ years
- Computer system security engineer – CSMS, SICT
- Haruulzangi challenge creator - 5 years
- OSEP, OSWP

- National Data Center - Senior Cybersec analyst, now
- Golomt Bank - Cyber security analyst, ~5 years
- National Data Center - System analyst, ~3 years

TABLE OF CONTENT

SECURITY OPERATIONS CENTER (SOC)

What is Cyber Security Operations Center ?



A SOC is a centralised hub within an organisation dedicated to monitoring, detecting, analysing, and responding to cybersecurity threats and incidents.

SECURITY OPERATIONS CENTER

- Who needs Cyber Security Operations Center(CSOC) ?

- Software and system development company
- Government organization
- Financial company and banking
- Datacenter
- Cloud service provider
- Cyber security consulting and service provider
- Big technology service provider

- Any organization that prioritizes cybersecurity and wants to proactively manage risks can benefit from a SOC

Introduction

People

Technology

Process

OPEN SOURCE

SOC golden triangle

People

- SOC manager
- Cyber security analyst
- Threat hunter
- Security engineers

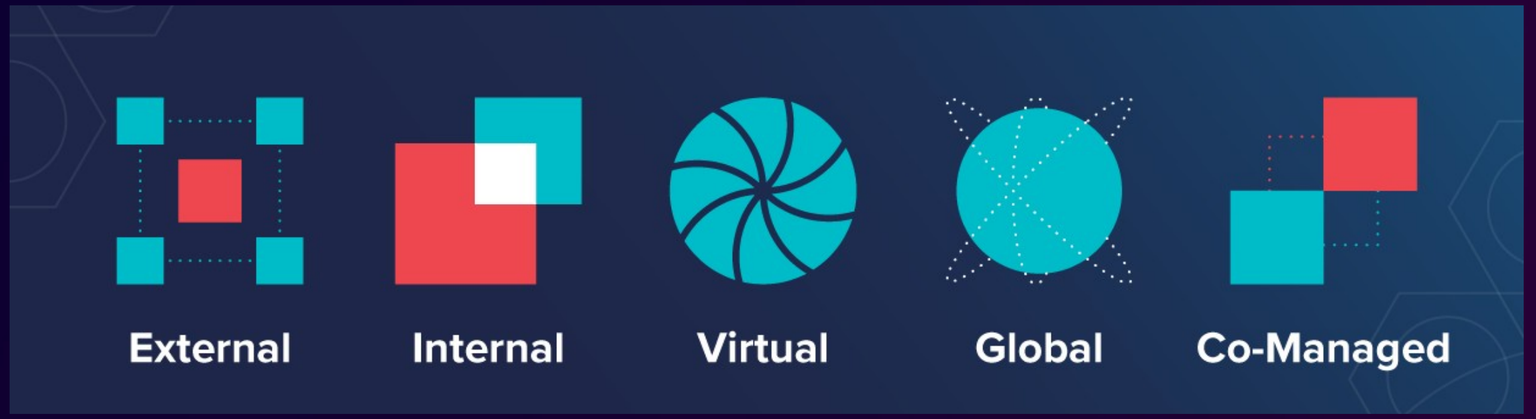
Technology

- SIEM
- IDS/IPS
- Vulnerability scan tools
- EDR/XDR
- Sandbox
- …

Process

- Monitoring
- Threat detection
- Threat hunting
- Incident response
- Red & Blue teaming
- Forensics analysis
- Reporting

SOC models



Picture by: varonis

OPEN SOURCE IN CYBERSECURITY

Cybersecurity open source projects

Open source & Proprietary software table

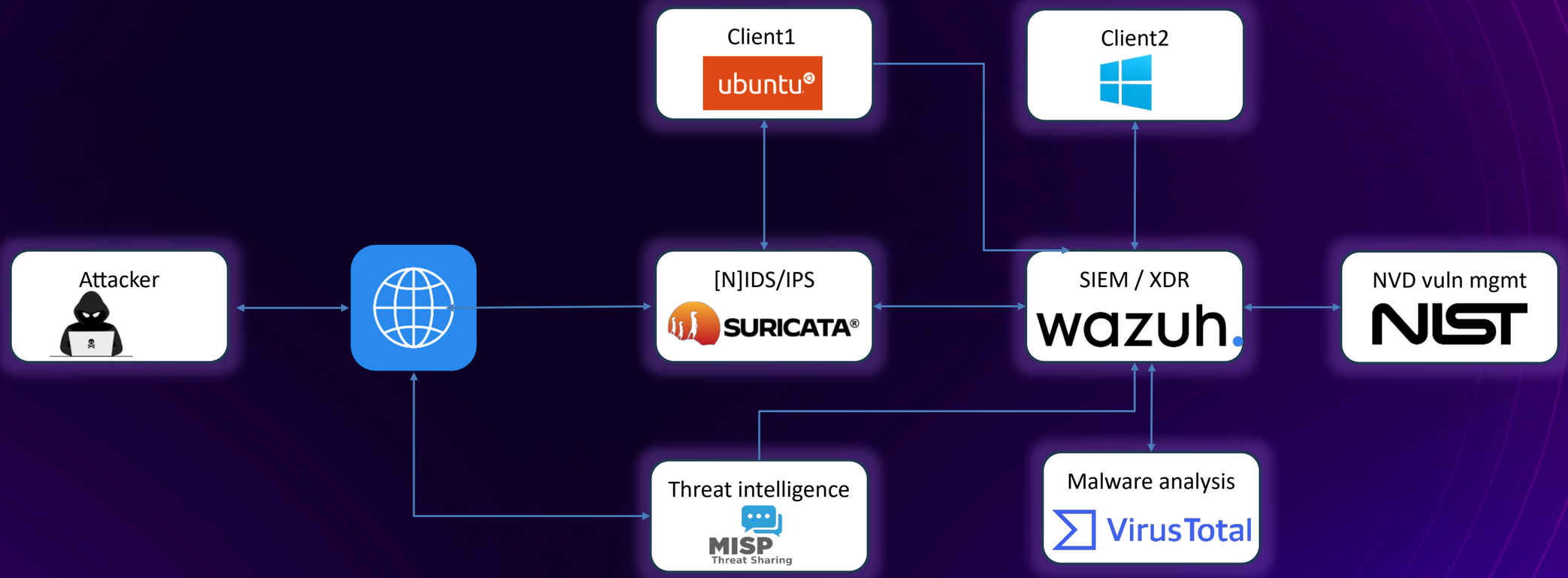
Security Feature	Open Source	Proprietary
Code Transparency	Publicly available for review and audit	Not publicly available, only accessible to developers
Patch Deployment	Faster deployment due to community involvement	Slower deployment, may prioritize patches based on company schedules
Resource Allocation	Community-driven, with many contributors	Limited resources, dependent on company investment
Vulnerability Management	Community involvement in identifying and addressing vulnerabilities	In-house security teams responsible for identifying and addressing vulnerabilities
Cost	Free or low-cost, with optional support and services	Can be expensive, with licensing fees and support costs
Customizability	Highly customizable, with access to source code	Limited customizability, with limited access to source code
Security Updates	Regular updates, with community involvement	Regular updates, but may be slower than open source

How to choose right open source project

- Users
- Community support
- Long term viability
- Usability and user experience
- Cost and licensing

OPEN SOURCE (SOC)

SOC lab architecture



Wazuh SIEM / XDR

Wazuh unifies historically separate functions into a single agent and platform architecture.
Protection is provided for public clouds, private clouds, and on-premise data centers.

Endpoint security

- Configuration assestment
- Malware detection
- FIM

Threat intelligence

- Threat hunting
- Log data analysis
- Vulnerability

Security operations

- Incident response
- Regulatory compliance
- IT hygiene

Cloud security

- Container security
- Posture management
- Workload protection

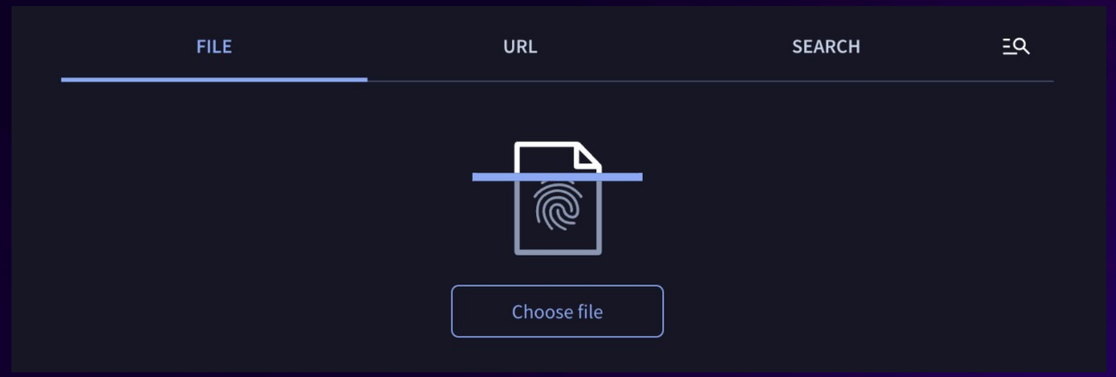
Suricata (N)IDS

Suricata is a high performance, open source network analysis and threat detection software used by most private and public organizations, and embedded by major vendors to protect their assets.

- **IDS alerts**
- **Protocol Transactions**
- **Network flows**
- **PCAP recording**
- **Extracted files**

Virustotal multiscan

VirusTotal is a popular online service that allows users to analyze files and URLs for potential viruses, malware, and other security threats.



MISP threat sharing

MISP is an open source software solution for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis

SOC lab

Conclusion

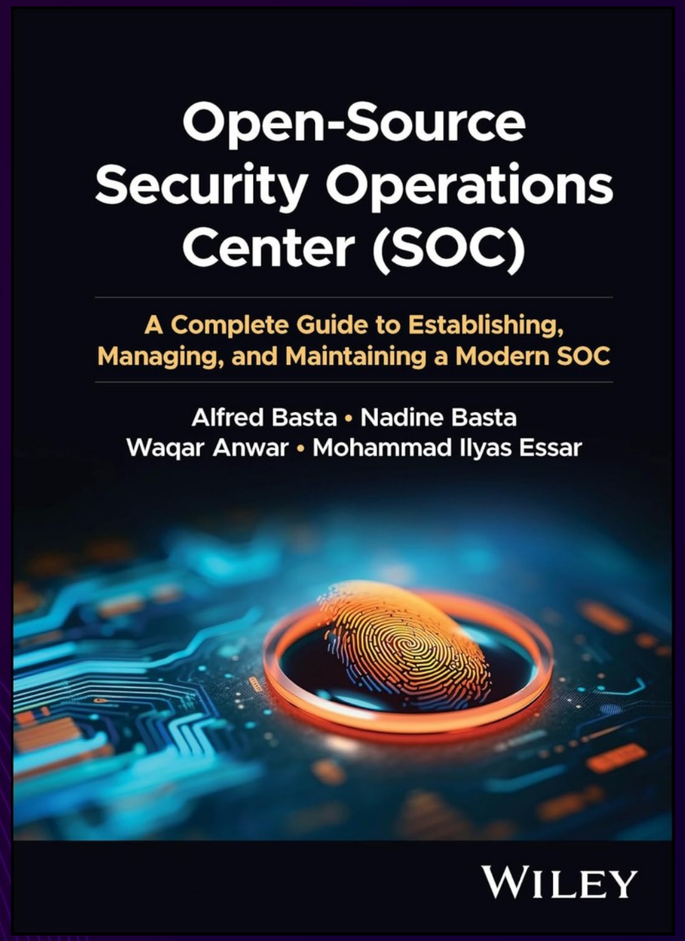
- Money alone can't solve all cybersecurity issues.
- Open source projects play a significant role in enhancing cybersecurity.

Reference

- Security Monitoring with Wazuh , Author: Rajneesh Gupta 2024
- Cyber Threat Hunting – Meap edition, Author: Nadhem Alfarden 2023

- https://www.ibm.com/topics/security-operations-center
- https://daily.dev/blog/open-source-vs-proprietary-software-security-comparison
- https://ventureinsecurity.net/p/open-source-in-cybersecurity-a-deep
- http://www.freepik.com/
- https://medium.com/@AdonayT/1-misp-overview-a0b79d683234
- https://documentation.wazuh.com/

FYI



Launch date: November 20, 2024

#MNSEC_2024

THANK YOU