Ferramentas de Segurança que um Administrador de Redes deveria conhecer

IntraRede

PALESTRANTE

LAIOS BARBOSA

As opiniões expressas aqui são tão e somente as opiniões do palestrante e não expressam, direta ou indiretamente, as opiniões do seu empregador ou de outras pessoas ou grupos.

WHOAMI

- ✓ Engenheiro de Computação – Instituto Militar de Engenharia **(IME)**
- ✓ Pós-Graduação em Segurança da Informação
- ✓ Instrutor e Co-Fundador da **GoHacking**
- ✓ Foi instrutor do **SANS Institute**
- ✓ Diversos Cursos em Seg Info em Instituições Internacionais - **OffSec** e **SANS**
- ✓ Instrutor de Defesa Cibernética e Segurança Ofensiva nas Forças Armadas (desde 2011)
- ✓ Principais Certificações Internacionais em Seg Info: **CISSP**, **GSE #291, OSCP**, **OSWP**, **OSCE**, GSP, GX-CS, GX-IA, GX-IH, GSEC, GCED, GCIA, GCIH, GCWN, GCFA, GNFA, GWAPT, GPEN, GPYC, GMOB, GDAT, GAWN, GRID, GREM, GXPN (https://www.credly.com/users/laios-barbosa/badges)
- ✓ Mais de 15 anos de experiência em Administração de Redes/Sistemas e Segurança da Informação
- ✓ Participação ativa nos **Grandes Eventos** – Gerência e Proteção dos Sistemas de Comando e Controle do Ministério da Defesa: Rio +20, Copa das Confederações 2013, Jornada Mundial da Juventude, Copa do Mundo 2014, Jogos Olímpicos 2016
- ✓ Speaker: Brazil Cyber Defense 2018, SBRC, OWASP, BHACK, H2HC, Cyber Security Summit Brasil
- ✓ “Um pouco viciado em **CTF**… ☺”
- ✓ **NetWars** Champion (and Champion of Champions)
- ✓ Marido, Pai e Surfista

CERT
Incident Response Process Professional
Certificate Holder

WHOAMI

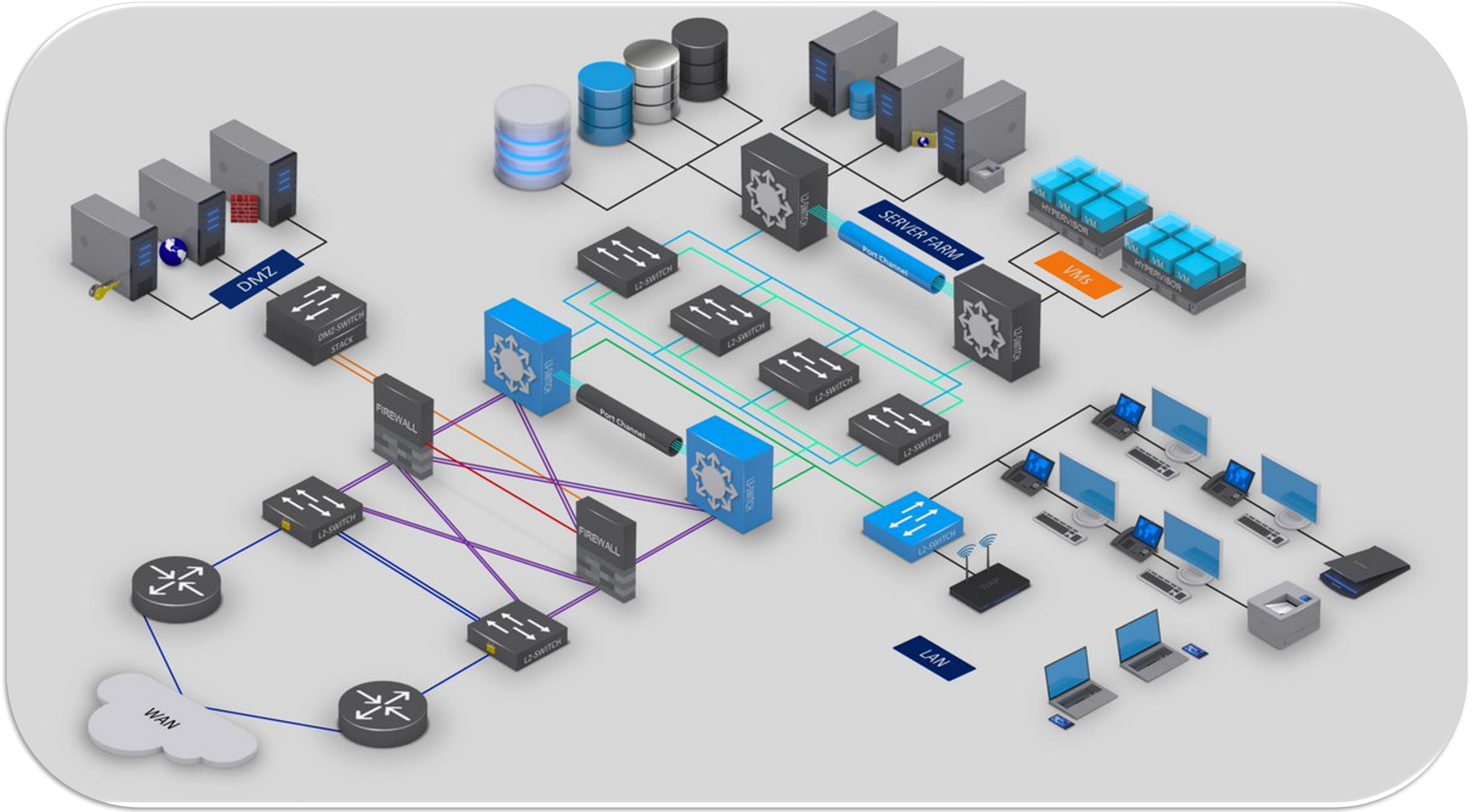
@laios_barbosa Laios Barbosa laiosbarbosa

AGENDA

1. Rede Corporativa
2. Defesa em Profundidade
3. Proteção de Rede
4. Proteção de Sistemas
5. Proteção de Dispositivos Finais
6. Monitoramento de Segurança (SIEM)
7. SOC/CSIRT

Rede Corporativa

Rede Corporativa



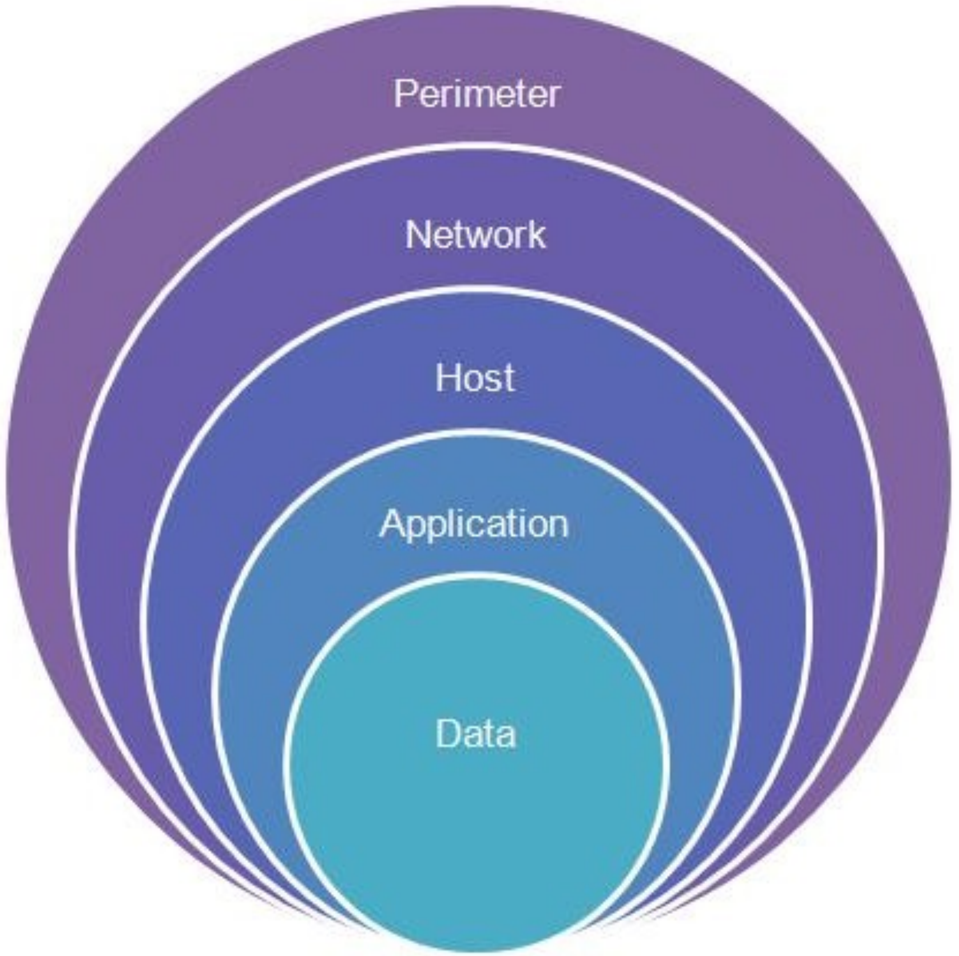
Segurança da Informação

Segurança Cibernética

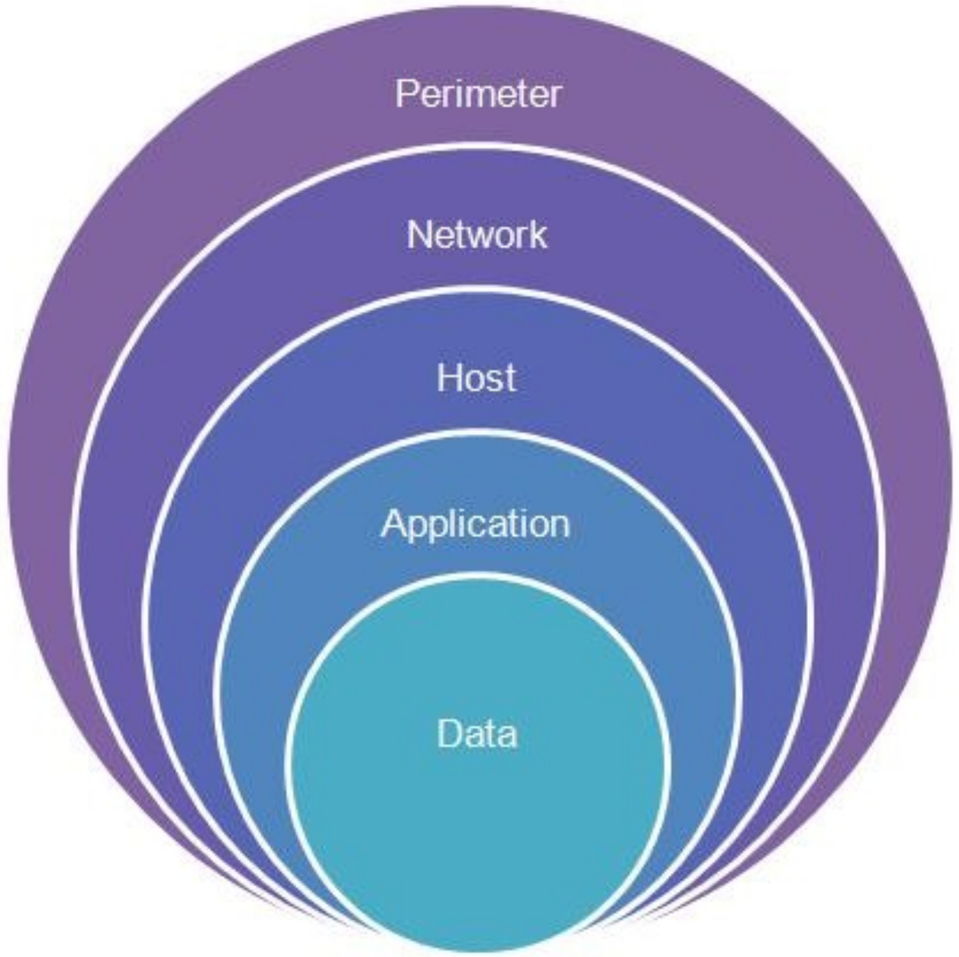
Defesa em Profundidade

Defesa em Profundidade

Defesa em Profundidade



Defesa em Profundidade



- Firewall de Rede (NGFW)
- IDS/IPS de Rede
- *Anti-DDoS* (volumetria)
- *Web Application Firewall* (WAF)
- *Anti-Spam*
- Antivírus/*Anti-Malware*
- *Data Loss Prevention* (DLP)
- *Endpoint Detection and Response* (EDR)
- *eXtended Detection and Response* (XDR)
- *Network Flow* (visibilidade de movimento lateral)
- *Security Information and Event Management* (SIEM)
- *Cyber Threat Intel* (CTI)/*Threat Intel Platform* (TIP)
- *Zero Trust*

Firewall

Next-Generation Firewall (NGFW)

- **Além da análise tradicional de camada 4 (IP/Porta)**
- *Intrusion Detection/Prevention System* (IDS/IPS)
- *Virtual Private Network* (VPN, *Site-to-Site*, *Client-to-Site*)
- Controle de Aplicação (Camada 7, C2)
- URL *Filtering*
- Controle de Acesso do Usuário
- SSL/TLS *Inspection*
- Anti-Malware
- Anti-Spam
- Anti-DDoS

Next-Generation Firewall (NGFW)

CISCO

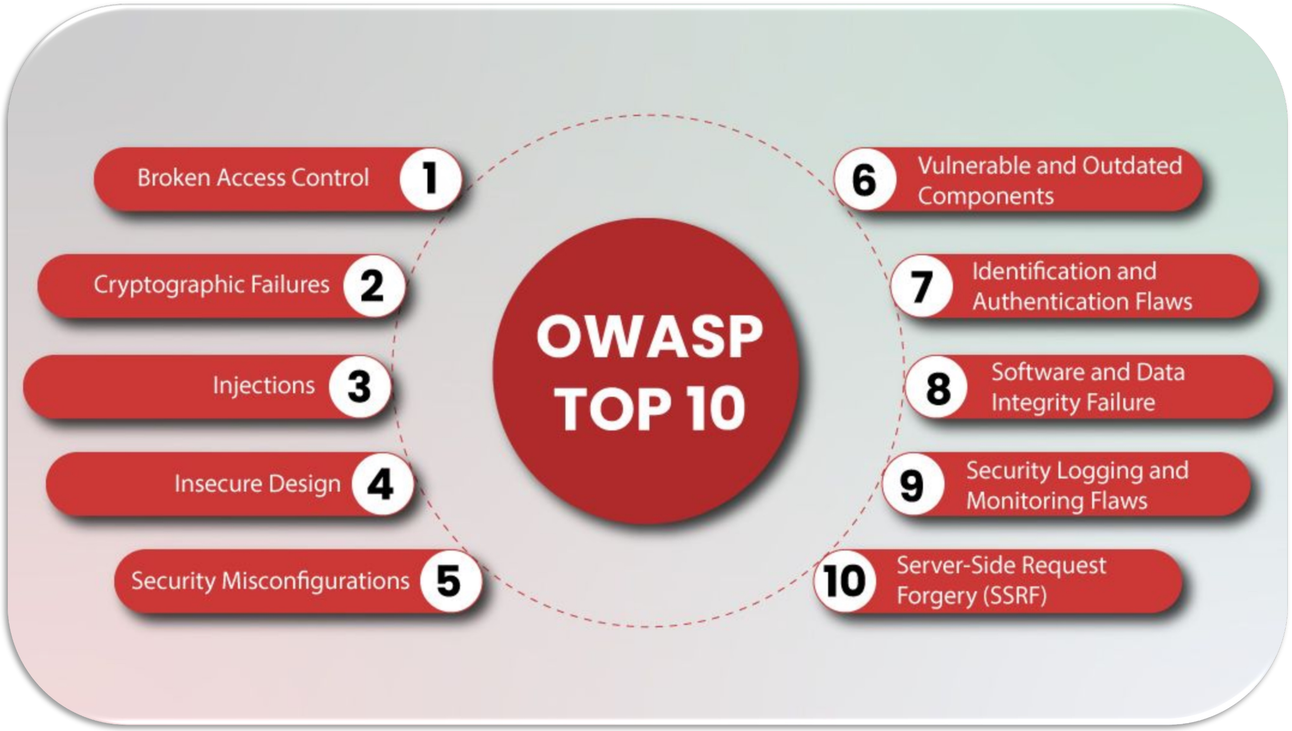
paloalto NETWORKS

CHECK POINT™

FORTINET®

Blockbit

Web Application Firewall (WAF)



https://owasp.org/Top10/pt_BR/

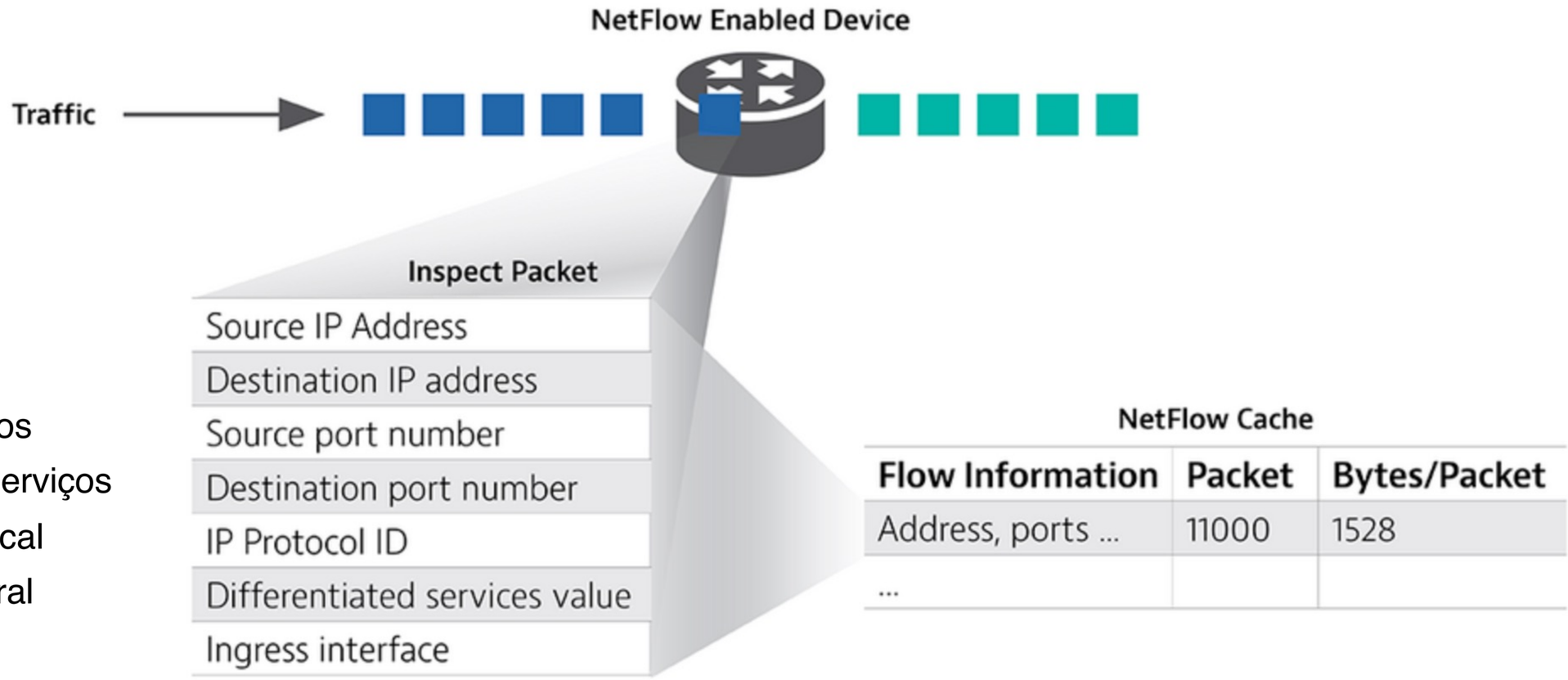
Web Application Firewall (WAF)

Figure 1: Magic Quadrant for Web Application and API Protection

Source: Gartner (August 2022)

Network Flow

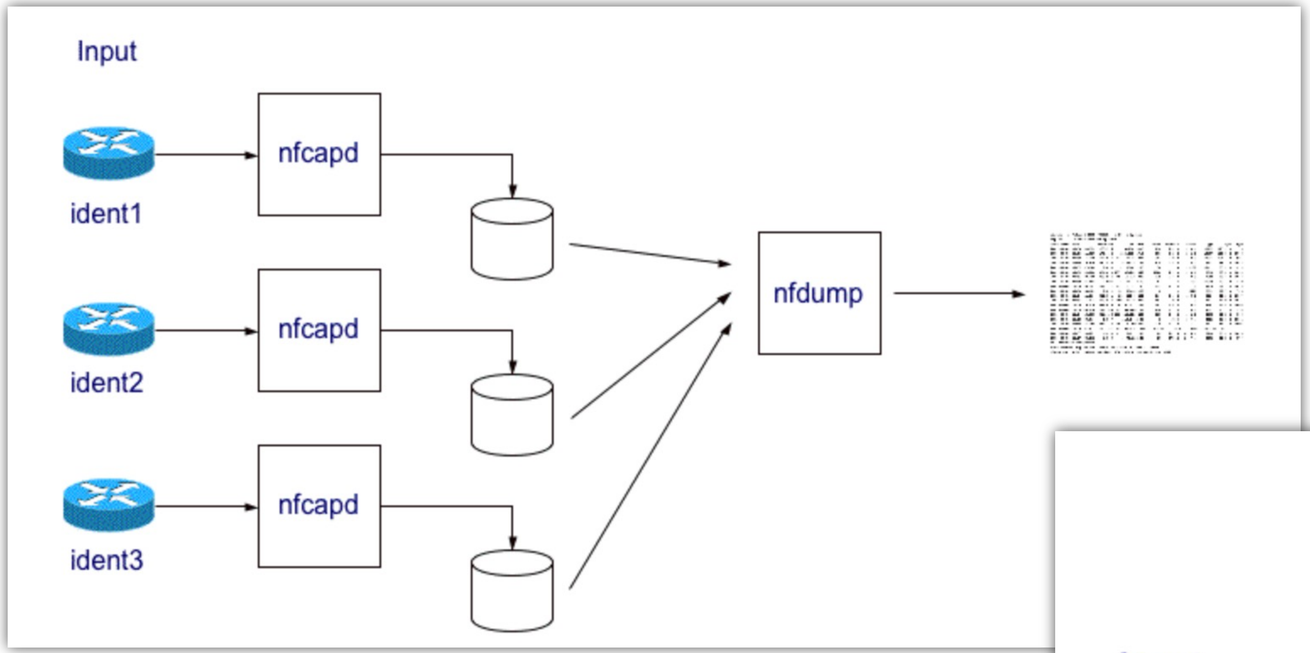
Network Flow

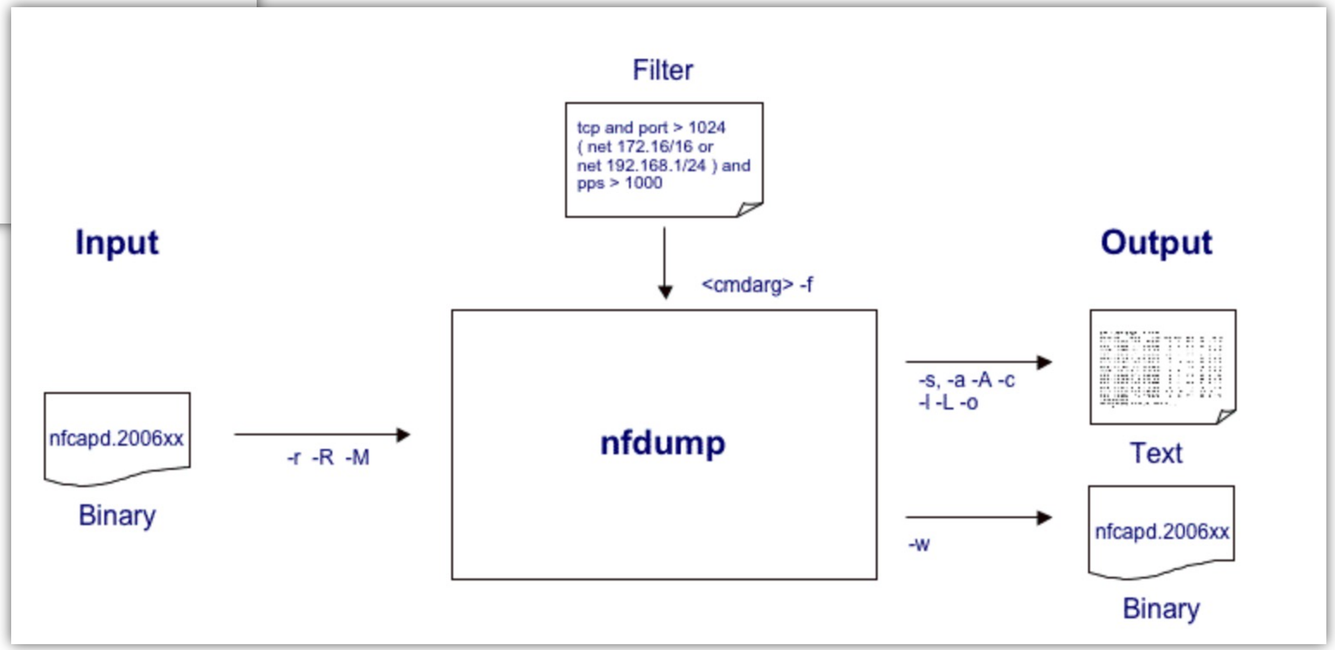


- Top *Talkers*
- Top Protocolos
- Top Portas/Serviços
- Tráfego Vertical
- Tráfego Lateral

https://www.viavisolutions.com/sites/default/files/styles/1000_wide/public/netflow-enabled-devices.png

NFDUMP





https://nfdump.sourceforge.net/

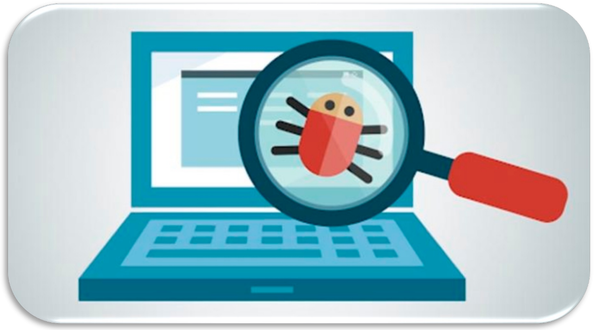
Tráfego de rede vertical nas portas TCP 80 e 443

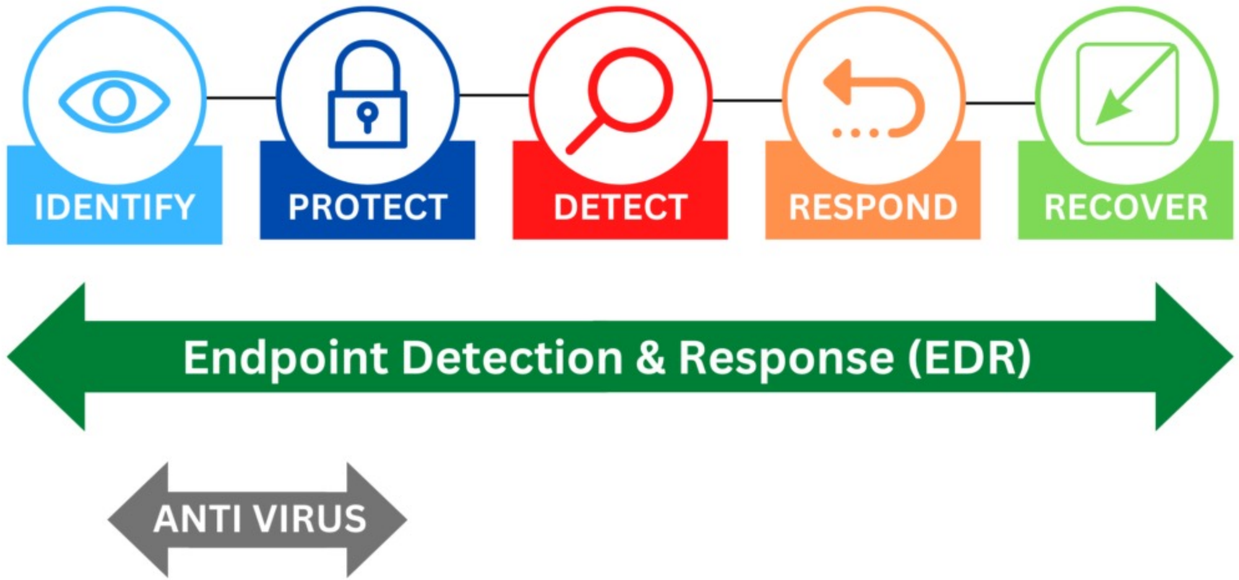
Tráfego de rede lateral na porta TCP 5555

Endpoint Protection

Endpoint Protection

- Antivírus Tradicional (*malwares*)
- *Endpoint Detection and Response* (**EDR**)
- *eXtended Detection and Response* (**XDR**)

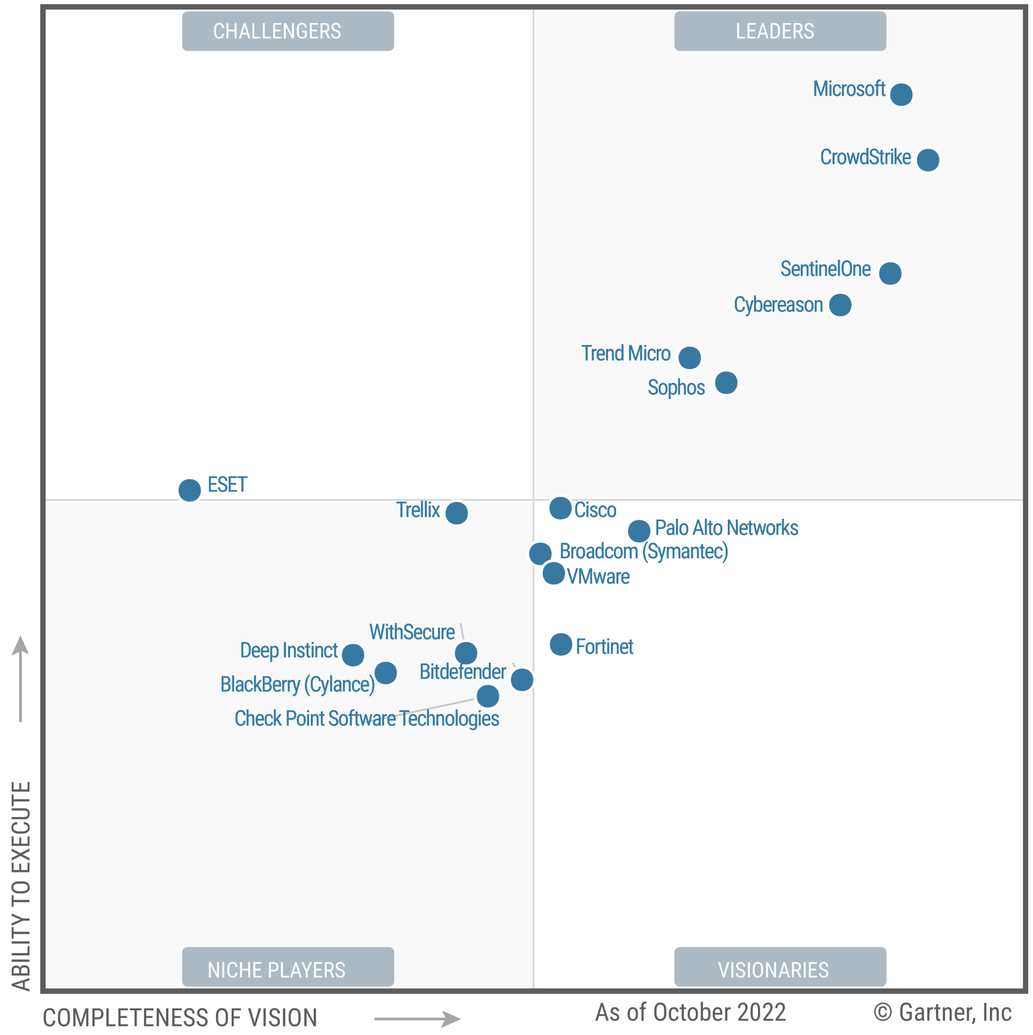




https://wirexsystems.com/resource/ndr-vs-edr/

Endpoint Protection

Figure 1: Magic Quadrant for Endpoint Protection Platforms



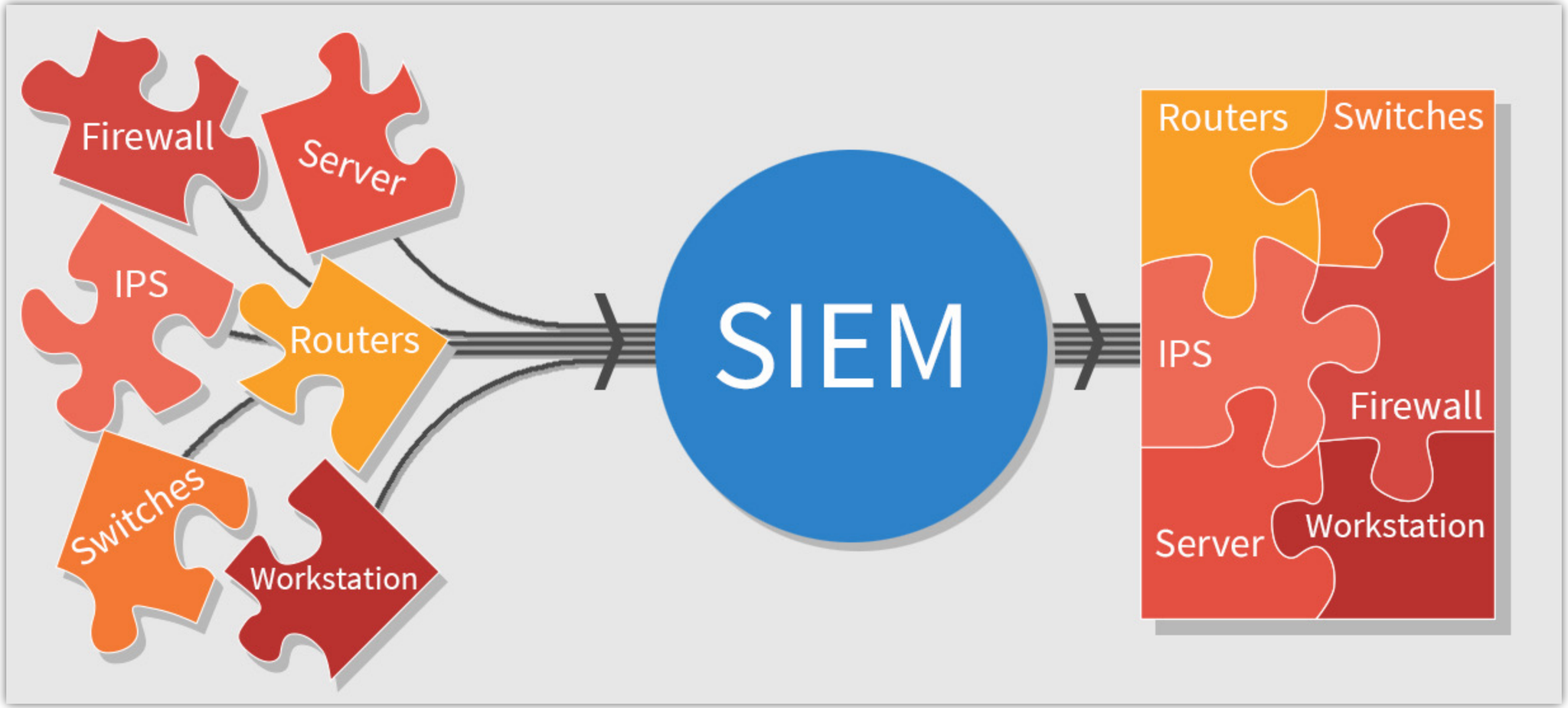
Source: Gartner (December 2022)

Agentes

- Agentes em *hosts* (estações de trabalho e servidores)
- Aumento da visibilidade na atividades de rede
- Auxílio na Resposta a Incidentes Cibernéticos
- Diversas soluções
  - ✓OSSEC
  - ✓Wazuh (EDR)
  - ✓Velociraptor

SIEM

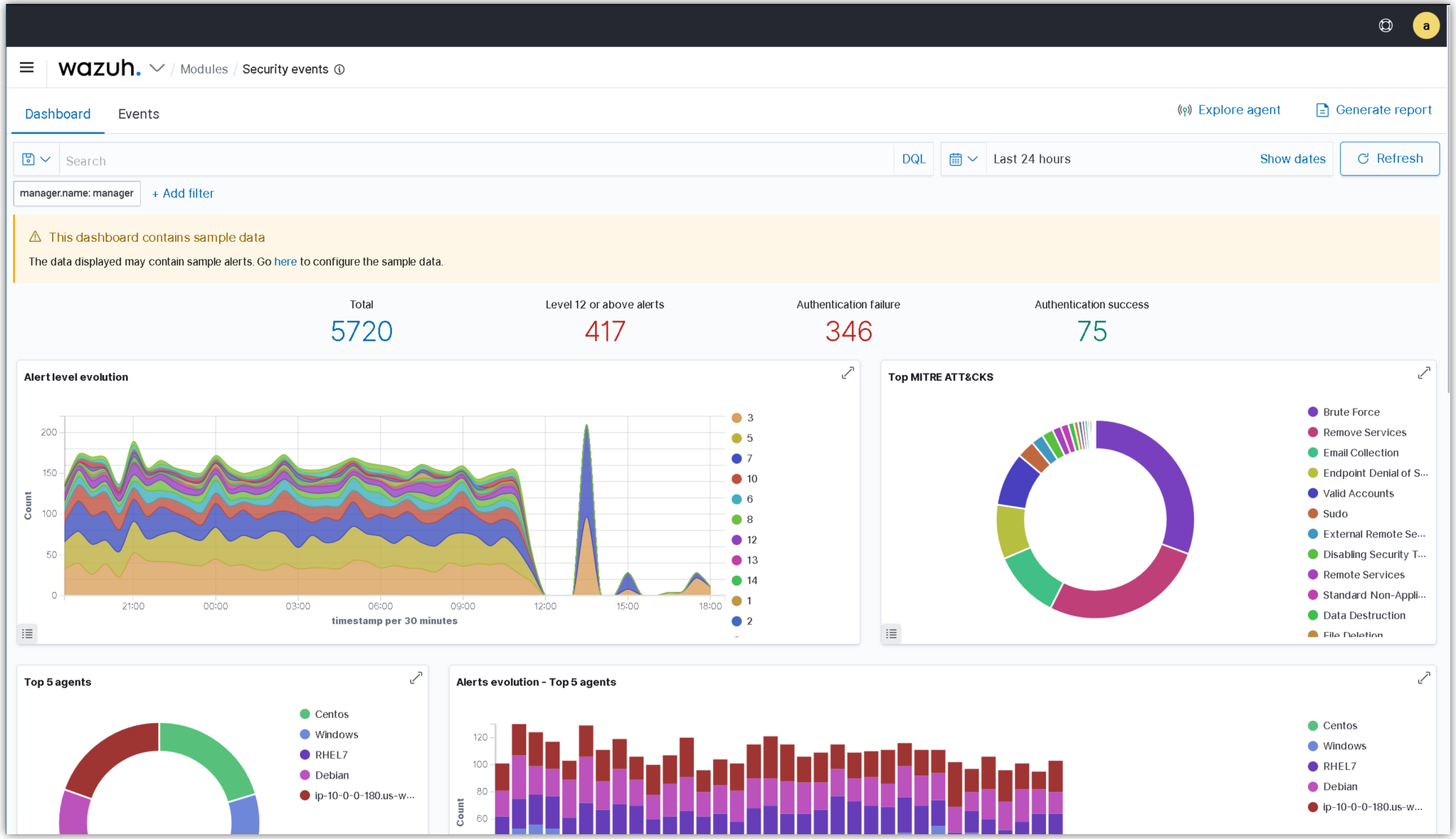
Security Information and Event Management



SIEM Gratuito

- Elastic Stack
- Graylog
- Wazuh
- OSSIM

SIEM Gratuito

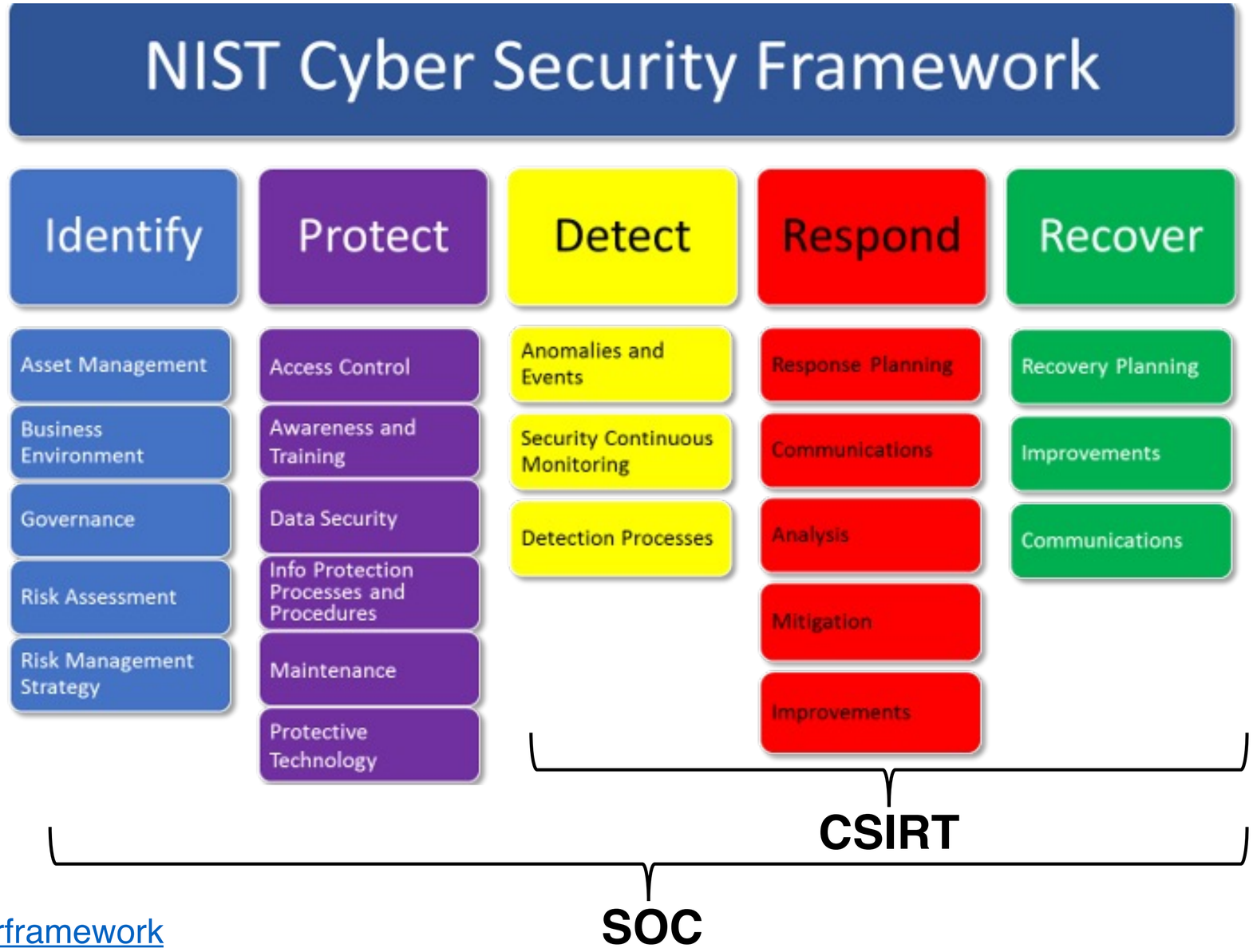


SIEM Comercial

- Splunk
- QRadar IBM
- ArcSight
- LogRhythm

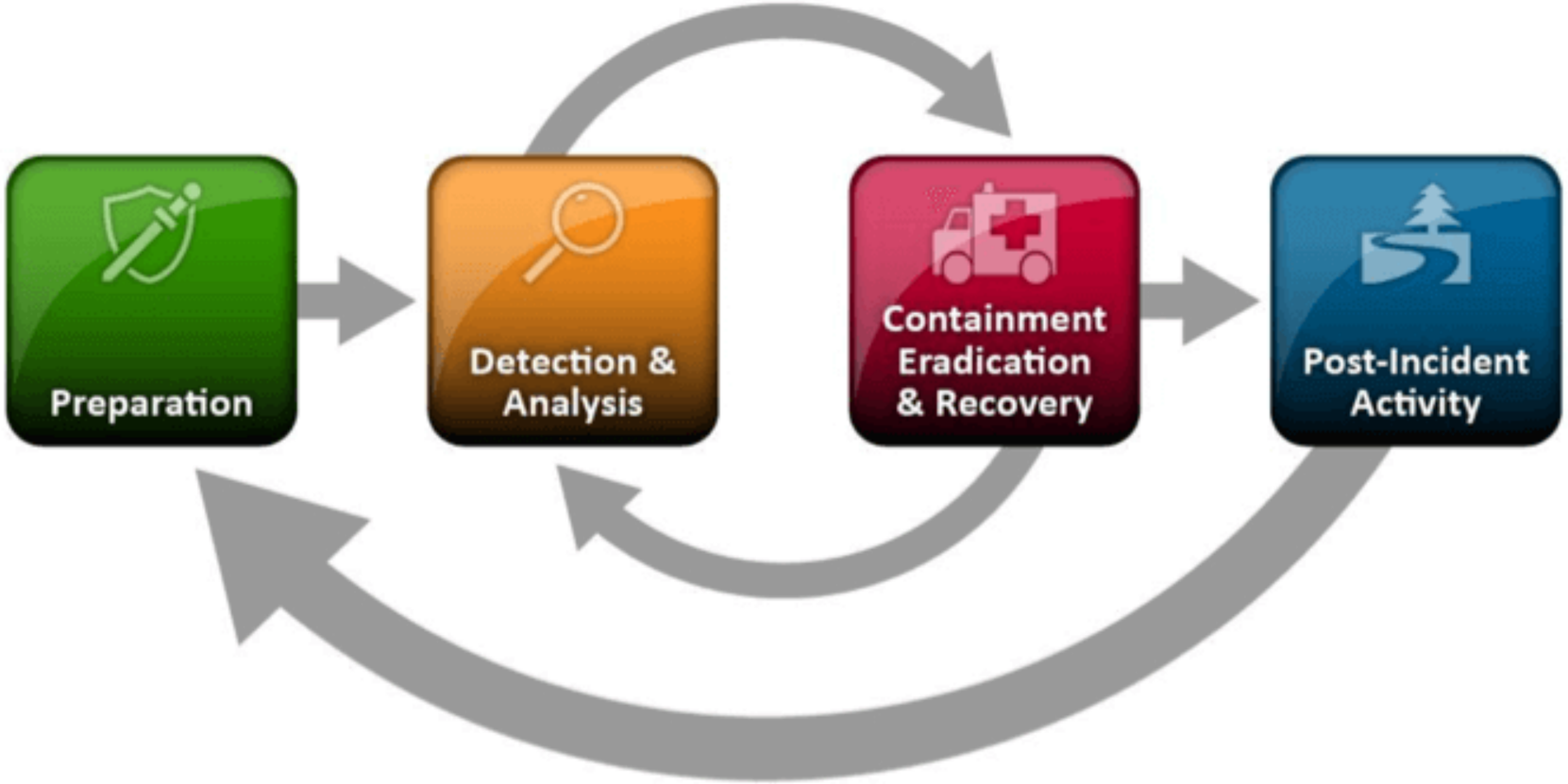
SOC/CSIRT

SOC/CSIRT



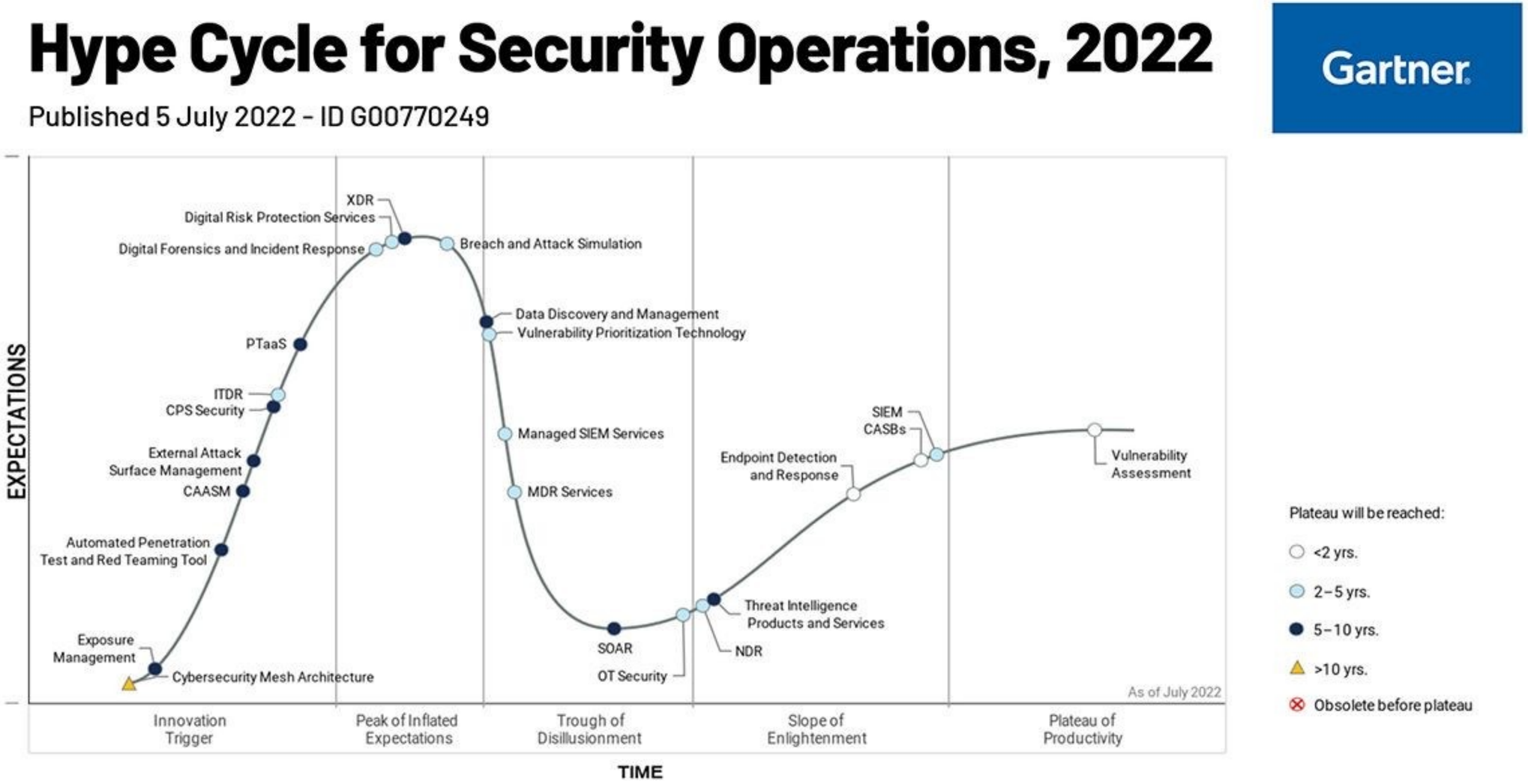
https://www.nist.gov/cyberframework

SOC/CSIRT



NIST SP 800-61 Rev.2 – Computer Security Incident Handling Guide

SOC/CSIRT


Hype Cycle for Security Operations, 2022
Published 5 July 2022 - ID G00770249
Gartner
EXPECTATIONS
XDR
Digital Risk Protection Services
Digital Forensics and Incident Response
Breach and Attack Simulation
Data Discovery and Management
Vulnerability Prioritization Technology
PTaaS
ITDR
CPS Security
Managed SIEM Services
SIEM
CASBs
External Attack
Surface Management
CAASM
MDR Services
Endpoint Detection
and Response
Vulnerability
Assessment
Automated Penetration
Test and Red Teaming Tool
Threat Intelligence
Products and Services
Exposure
Management
SOAR
NDR
Cybersecurity Mesh Architecture
OT Security
As of July 2022
Innovation
Trigger
Peak of Inflated
Expectations
Trough of
Disillusionment
Slope of
Enlightenment
Plateau of
Productivity
TIME
Plateau will be reached:
<2 yrs.
2–5 yrs.
5–10 yrs.
>10 yrs.
Obsolete before plateau

FIM

GoHacking

CYBER SECURITY TRAININGS