SoC

What's missing

SOC

NEED OF SOC

- Protection against threats
- Continuous monitoring and Incident responce
- Compliance with reulations
- Miminize damage from security incidents

SOC OPERATIONS

- Monitoring security events and logs
- Detecting analyzyes incidents
- Responding and recover from incidents

COMPONENTS OF SOC (PEOPLE, PROCESS, TECHNOLOGY)

PEOPLE

- SOC Level 1
- SOC Level 2
- Incident Responder
- Sublect Matter Expert/Hunter
- SOC Manager
- Chief Information Security Officer (CISO)

PROCESS

- Business Processes
- Technology Processes
- Operational Processes Analytical Processes

TECHNOLOGY

- SIEM Solutions
- Security Monitoring Tools
- Dashboard
- Ticketing system
- Automated assessment tool

SOC IMPLEMENTATION

SOC Key Performance indicators (KPI) and Metrics

TYPES OF SOC MODELS

In-House/Interinal SOC Model
Outsourced SOC Model
Hybrid SOC Model

TYPIS - MATURITY MODELS

- Completion time
- Response time
- Overtime
- First-time fix rate
- Client satisfaction
- Transfer rate
- Call service level compliance
- Operations audit
- Sustem ewauatilty and accessibility

SOC vs NOC

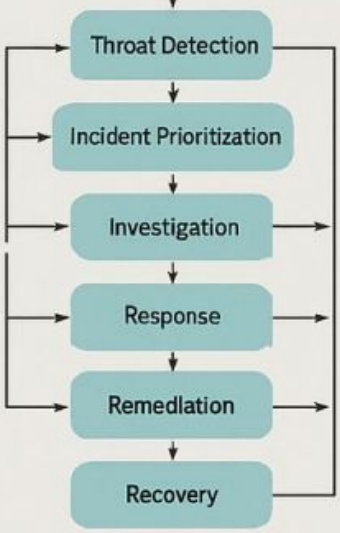
SOC

NOC

CHALLENGES IN IMPLEMENTATION OF SOC

BEST PRACTICES POR RUNNING

SOC WORFFVLOW



TYPES OF SOC MODELS

In-House/Internal SOC
Outsourced SOC Model
Hybrid SOC Model

3

TYPES OF MATURITY MODELS

SOC Capablity Maturity Model
Control Objectives for Information Technology (COBIT)

SOC GENERATIONS

First-generation SOC: 1973–1995

Second-generation SOC: 1996–2001

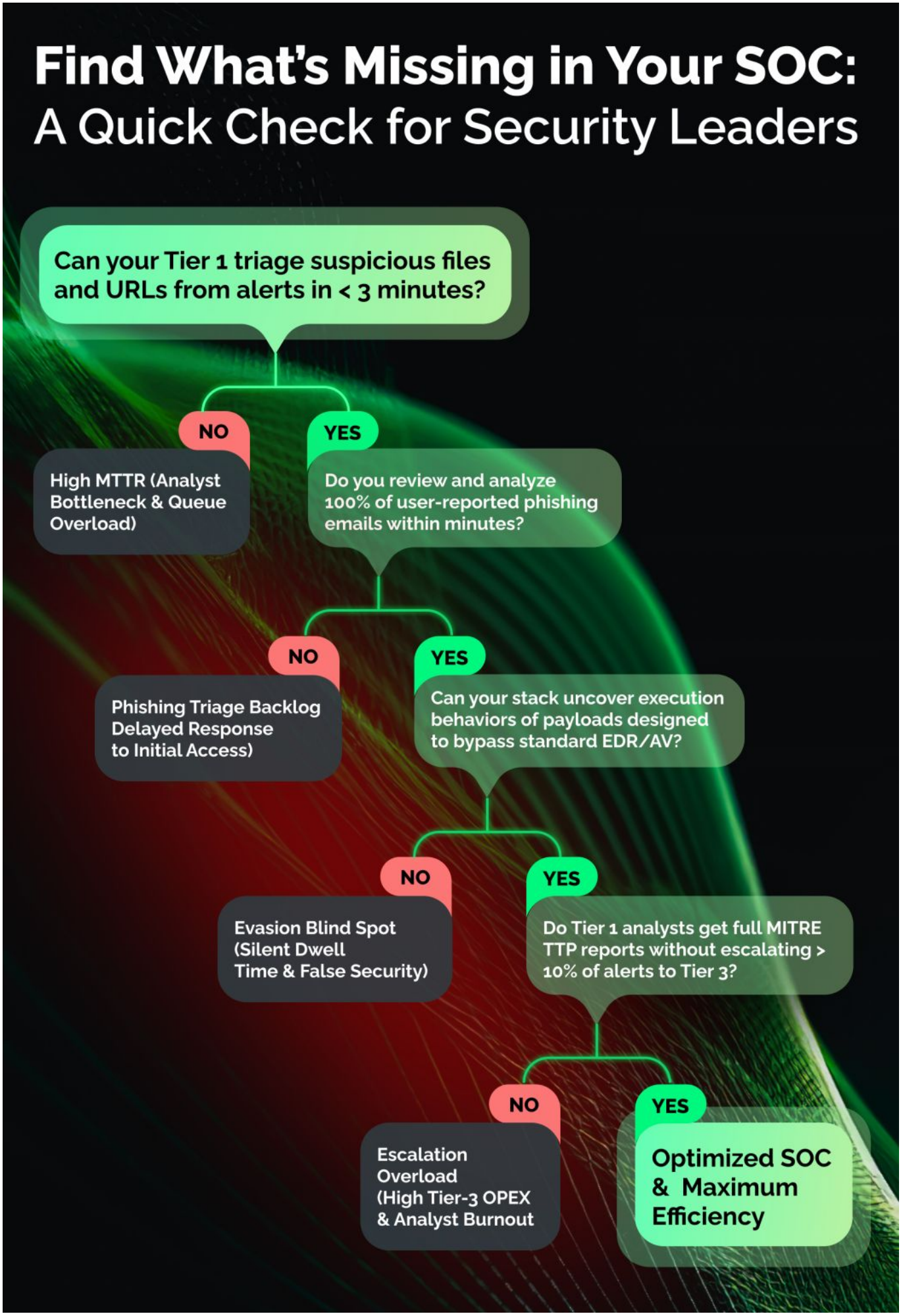
Third-generation SOC: 2002–2006

Fourth-generation SOC: 2007–2012

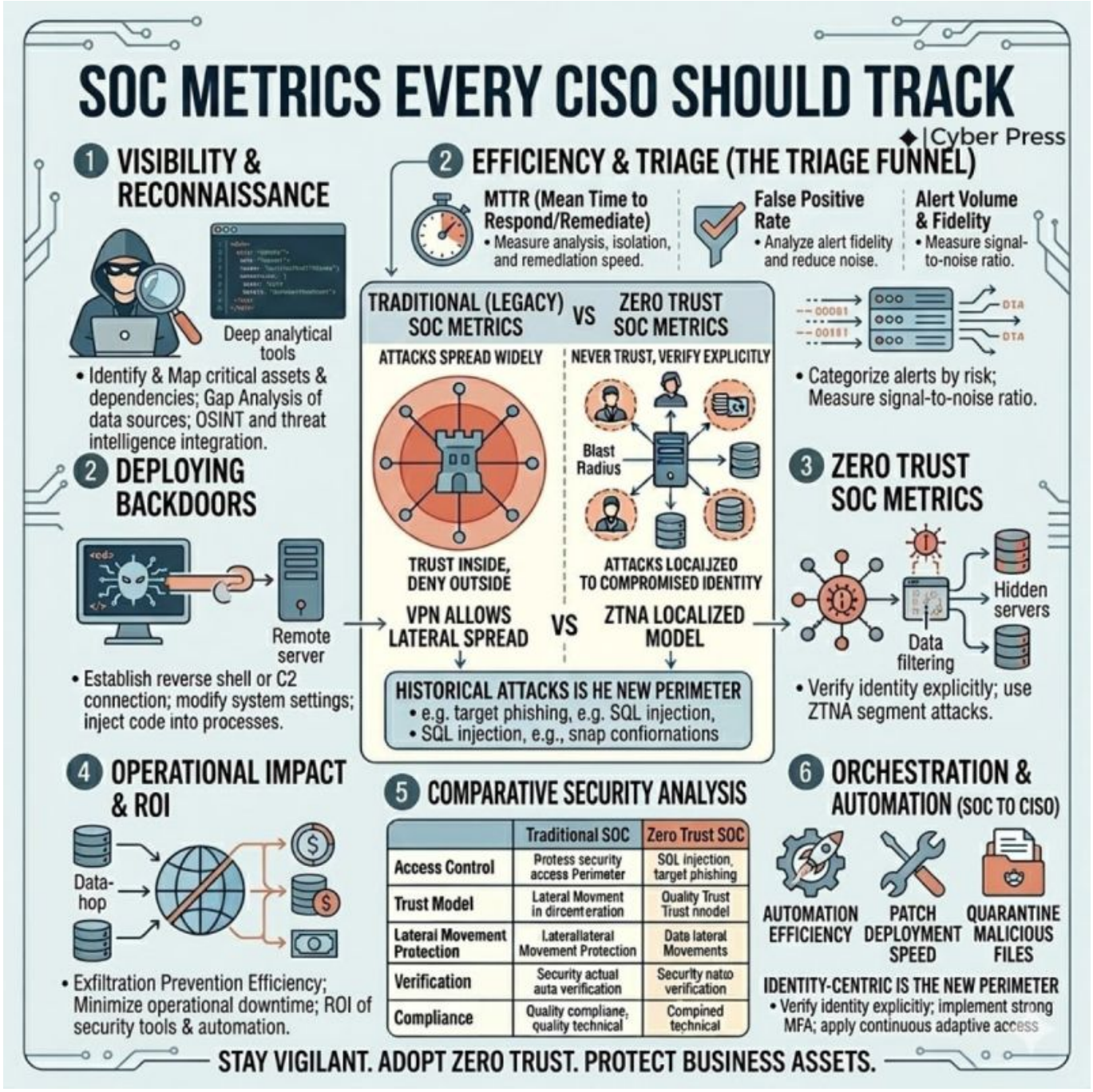
Fifth-generation SOC: 2013–till date

SOC KEY PERFORMANCE INDICATORS (KPI) AND METRICS

- Completion time
- Response time
- Overtime


Find What's Missing in Your SOC:
A Quick Check for Security Leaders
Can your Tier 1 triage suspicious files and URLs from alerts in < 3 minutes?
NO
High MTTR (Analyst Bottleneck & Queue Overload)
YES
Do you review and analyze 100% of user-reported phishing emails within minutes?
NO
Phishing Triage Backlog Delayed Response to Initial Access)
YES
Can your stack uncover execution behaviors of payloads designed to bypass standard EDR/AV?
NO
Evasion Blind Spot (Silent Dwell Time & False Security)
YES
Do Tier 1 analysts get full MITRE TTP reports without escalating > 10% of alerts to Tier 3?
NO
Escalation Overload (High Tier-3 OPEX & Analyst Burnout
YES
Optimized SOC & Maximum Efficiency


How Business Risk Escalates Across the SOC
SOC Layer
What Should Happen
Where It Breaks Down
Business Impact
Monitoring
Suspicious signal detected early
Signal lost in noise or not prioritized
No action taken
Tier 1: Triage
Alert validated & contextualized
Unclear signal delayed or ignored
Attacker gains foothold
Tier 2: Investigation
Behavior analyzed, risk confirmed
Lack of context, inconclusive analysis
Lateral movement begins
Incident Response
Threat contained early
Escalation happens late
Full incident impact
Detection Engineering
Patterns identified, detections updated
No feedback loop, gap remains
Repeated exposure



From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/cybersecurity/soc

Last update: **2026/09/22 10:56**