

SoC

What's missing

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

SOC METRICS EVERY CISO SHOULD TRACK

1 VISIBILITY & RECONNAISSANCE



Deep analytical tools

- Identify & Map critical assets & dependencies; Gap Analysis of data sources; OSINT and threat intelligence integration.

2 EFFICIENCY & TRIAGE (THE TRIAGE FUNNEL)



MTTR (Mean Time to Respond/Remediate)

- Measure analysis, isolation, and remediation speed.



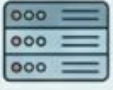
False Positive Rate

- Analyze alert fidelity and reduce noise.

Alert Volume & Fidelity

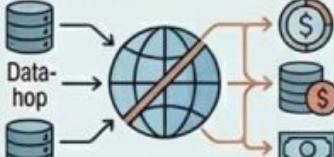
- Measure signal-to-noise ratio.

3 ZERO TRUST SOC METRICS



- Categorize alerts by risk; Measure signal-to-noise ratio.

4 OPERATIONAL IMPACT & ROI



- Exfiltration Prevention Efficiency; Minimize operational downtime; ROI of security tools & automation.

5 COMPARATIVE SECURITY ANALYSIS

	Traditional SOC	Zero Trust SOC
Access Control	Protect security access Perimeter	SQL injection, target phishing
Trust Model	Lateral Movement in discentration	Quality Trust Trust model
Lateral Movement Protection	Lateral Movement Protection	Date lateral Movements
Verification	Security actual auto verification	Security natio verification
Compliance	Quality compliane, quality technical	Compined technical

6 ORCHESTRATION & AUTOMATION (SOC TO CISO)



AUTOMATION EFFICIENCY PATCH DEPLOYMENT SPEED QUARANTINE MALICIOUS FILES

IDENTITY-CENTRIC IS THE NEW PERIMETER

- Verify identity explicitly; implement strong MFA; apply continuous adaptive access

TRADITIONAL (LEGACY) SOC METRICS VS ZERO TRUST SOC METRICS

ATTACKS SPREAD WIDELY VS NEVER TRUST, VERIFY EXPLICITLY

TRUST INSIDE, DENY OUTSIDE VS ATTACKS LOCALIZED TO COMPROMISED IDENTITY

VPN ALLOWS LATERAL SPREAD VS ZTNA LOCALIZED MODEL

HISTORICAL ATTACKS IS HE NEW PERIMETER

- e.g. target phishing, e.g. SQL injection, SQL injection, e.g., snap conformations

2 DEPLOYING BACKDOORS



Remote server

- Establish reverse shell or C2 connection; modify system settings; inject code into processes.

3 ZERO TRUST SOC METRICS



Hidden servers

Data filtering

- Verify identity explicitly; use ZTNA segment attacks.

6 ORCHESTRATION & AUTOMATION (SOC TO CISO)



AUTOMATION EFFICIENCY PATCH DEPLOYMENT SPEED QUARANTINE MALICIOUS FILES

IDENTITY-CENTRIC IS THE NEW PERIMETER

- Verify identity explicitly; implement strong MFA; apply continuous adaptive access

STAY VIGILANT. ADOPT ZERO TRUST. PROTECT BUSINESS ASSETS.

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

Permanent link:
<https://wiki.fortier-family.com/cybersecurity/soc?rev=1790062549>

Last update: 2026/09/22 09:35

