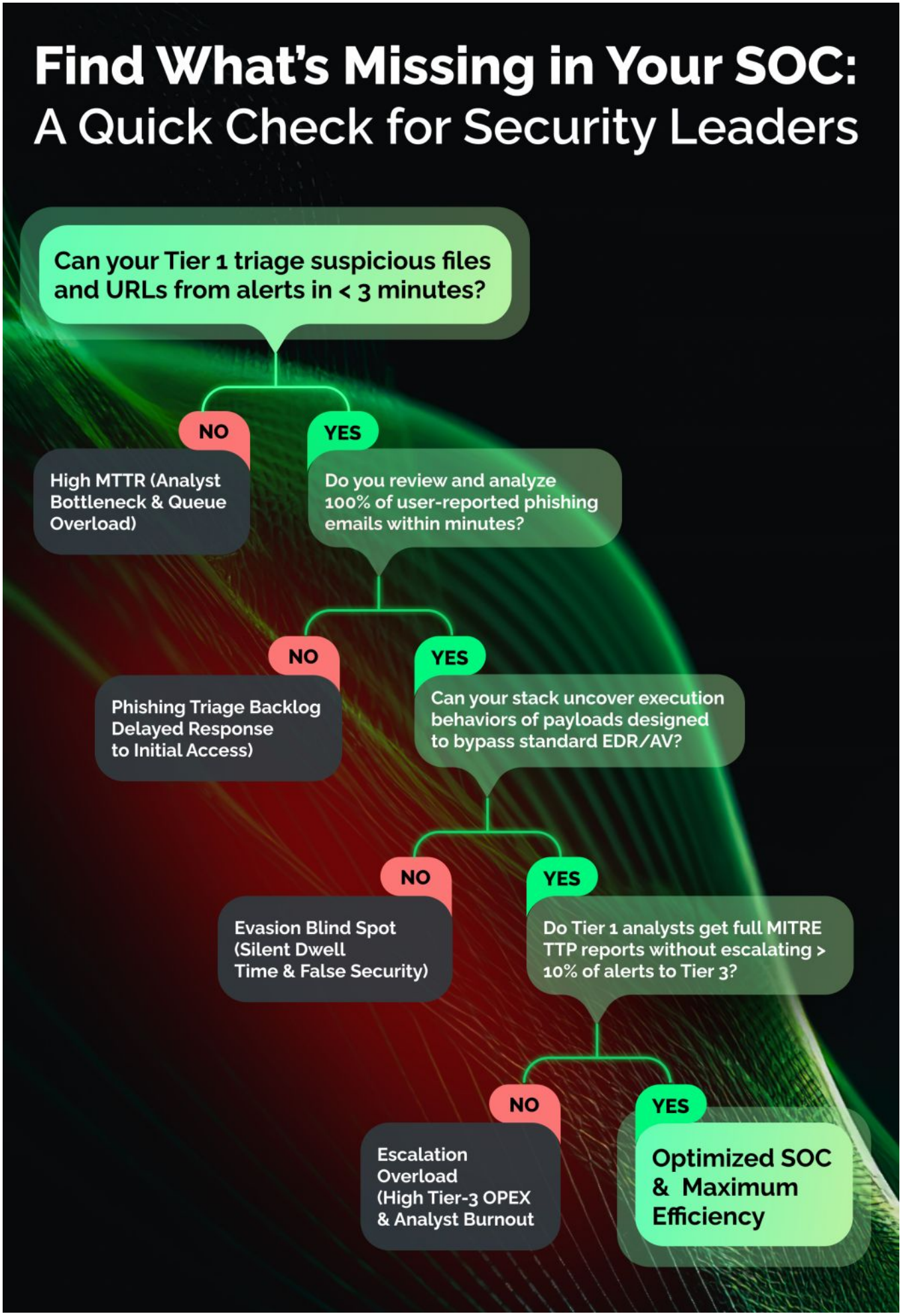
SoC

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

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**