DELEGATED AUTHORITY IN THE AGE OF MACHINE-SPEED THREATS

Brad Edwards

VIPSS, March 2026

The Clock is Already Running

Offensive AI

Criminal use is common.

Attacker Sophistication

Unsophisticated attackers have OSCP level agents.

Breach Speed

20% of 2025 breaches start → finish under 60 minutes.

APT AI Offense

Experimenting with very advanced, very high scale AI.

A Tale of Two Crises

Crisis 1: Proactive Delegation

Risk decisions are automated and delegated in advance.

Crisis 2: Reactive Delegation

Risk decisions are delegated at the time of crisis or not at all.

Automatic Home Invasion Remediation

Scenario: The Inexperienced Responder

23 year-old police officer, 6 months experience.

Life and Death Risk

Potential for fatal outcomes in high-stakes situation.

National Reputational Risk

Widespread negative publicity and loss of public trust.

Significant Legal Risk

Severe legal liabilities and regulatory consequences.

The Little Incident That Wouldn't

Scenario & Actor: The 23-Year-Old Incident Commander

23 year-old Incident Commander, limited experience in high-pressure events.

Significant Financial Risk

Potential for major monetary loss and resource drain.

National Reputational Risk

Widespread negative publicity and loss of public trust.

Significant Legal and Regulatory Risk

Severe compliance violations, fines, and legal action.

IRPs are Documentation, Not Governance

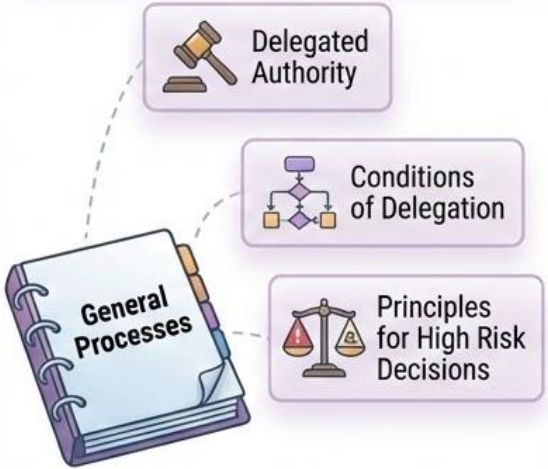
The Reality of IRPs

55%
No IRP

70%
Never Tested

Majority of organizations lack or fail to validate their Incident Response Plans.

Missing Governance Elements



Critical decision-making frameworks are often absent.

NIST & Real-World Context

67% of ransomware attacks start outside business hours.

Explicit authority and 24/7 readiness are essential.

Most SOC Capabilities Are Managed Not Governed

Strategic Engagement Gap

No strategic engagement to hone SOC leaders' risk judgement.

Tactical Operations Strategic Oversight

Misaligned Automation

Automation focused on labour savings not risk alignment.

Reactive vs. Strategic

SOC seen as tactical until strategic impacts surface during crisis.

Metric Myopia

SOC metrics assess tactical performance and control coverage.

What Has to be True to Move Fast

Operational Risk Appetite

Risk appetite expressed in operational, not abstract terms.

Clear Decision Criteria

Criteria for decision-making clearly defined.

Delegated Authority

Decision authorities delegated to specific roles and systems.

Legal Cover Established

Legal cover established in advance.

Judgment & Context Training

Training on judgement and business context.

Agents Make Governance Gaps Explicit

AI & Delegation Frameworks

AI without delegation frameworks just makes bad governance fail faster.

Automation Requires Understanding

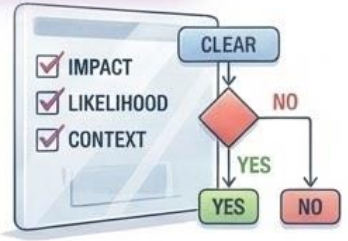
SOC leaders cannot automate what they do not understand.

Define Judgment

Define good **judgement**, or someone else will.

Clear Risk Criteria

Criteria for judging risk decisions must be understood.



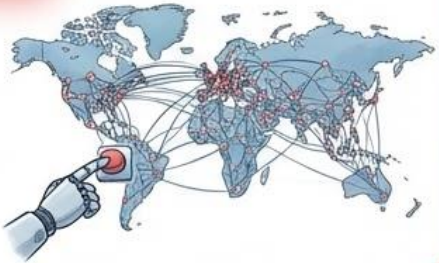
Delegating to Agents: Same Problem at Machine Speed

SPEED OF CONSEQUENCE

Actions have immediate, often irreversible, effects.

SCALE OF ACTION

Small decisions are amplified across vast systems instantly.

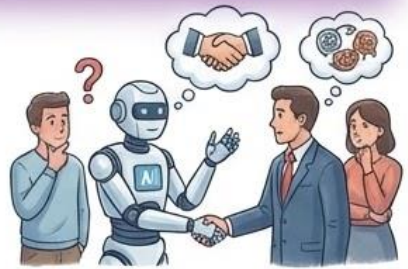


CASCADING DIVERGENCE

Minor deviations lead to widespread, unpredictable system failures.

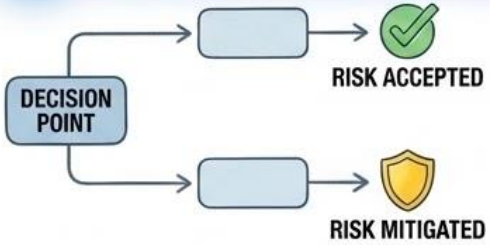
INABILITY TO INFER CONTEXT FROM CULTURE

AI lacks the nuanced understanding of human social and cultural context.



The Prerequisites Nobody Wants to Prioritize

Explicit definition of how to make appropriate risk decisions



Legal review of risk framework that preserve delegated authority

Risk framework delegated authority.

Protection for SOC leaders and engineers who act consistent with framework

Protection energy shield.

STRATEGIC AND BUSINESS CONTEXT

Strategic and business context coaching for SOC leadership and engineers

TABLETOP EXERCISES

Tabletop exercises to assess intended and unintended outcomes

Conversation Your Executive Team Needs to Have

RISK APPETITE

What is your risk appetite in operational terms?

AUTONOMOUS DECISIONS

What decisions can be made without escalation?

SYSTEM VS. LEADERSHIP DECISIONS

What decisions can made by the system? By SOC leadership? When?

PAINFUL LOSSES

Which losses are most painful and why?

Q&A

VIPSS, March 2026

OPTIV

paloalto NETWORKS