HORIZON3.ai

Unifying SOC and ITSM

A Leadership Guide to Evidence-Driven Cyber Risk Management

Whitepaper

Executive Summary

Security Operations Centres (SOC) and IT Service Management (ITSM) teams are often set at cross-purposes.

The SOC is optimised to reduce cyber risk quickly. ITSM is optimised to maintain service stability and predictable change. Both objectives are legitimate, but the result is familiar friction around change management, ticket noise, ownership, and accountability for reducing cyber risk.

Over time this tension often becomes cultural. Security teams may view IT operations as slow to act or too tolerant of risk. IT operations may see security as disruptive to service delivery. In reality, the root problem is structural with SOC and ITSM teams frequently operating with different definitions of risk.

Scanning tools identify thousands of potential vulnerabilities drowning analysts with potential threats. ITSM teams prioritise service availability, service-level agreements, and operational stability. Without a shared understanding of which risks truly matter, disagreements are inevitable.

A more effective approach is to establish a shared operational view of exposure based on attacker-validated evidence rather than theoretical vulnerability severity which lacks the context of living and changing environment.

Offensive cyber platforms provide the operational mechanism for this shift.
By identifying exploitable attack paths in production, demonstrating potential business impact, and verifying remediation, they create a vital shared source of risk truth for both SOC and ITSM teams.

When this evidence is integrated into existing ITSM and SOC workflows, organisations move from debating theoretical risk to ruthlessly prioritising and fixing proven exposures that tangibly increase their security, resilience and reliability. The unified purpose the business seeks.

The Structural Challenge Between SOC and ITSM

Separation between security and IT operations exists for valid organisational reasons. Boards and executives distribute responsibilities across roles such as CIO, CISO, CTO, and CDIO to ensure focus and accountability.

However, operational effectiveness depends on how these functions interact across people, process, and technology.

Several structural differences commonly create friction between SOC and ITSM teams.

Dimension	Security Operations (SOC)	IT Service Management (ITSM)	Resulting Friction
Primary Objective	Reduce cyber risk quickly	Maintain service stability and uptime	Security pushes urgent changes while ITSM protects reliability
Key Metrics	Mean time to detect, respond, contain	SLA adherence, change success rate	Teams optimise for different outcomes
Primary Inputs	Alerts, vulnerability scans, threat intelligence	CMDB, incident tickets, service impact	Different data sources drive decisions
Risk Interpretation	Focus on attacker behaviour and exposure	Focus on operational impact and stability	Difficulty agreeing on urgency, priorities and focus
Operational Workflow	Investigate and escalate	Plan, schedule, approve change	Security urgency conflicts with change governance

These dynamics rarely stem from individual behaviour. They arise from the absence of a shared operational view of cyber risk to systems, services and the businesses vital data.

Schrödinger's Monkey: A New Operational Mindset

A useful way to think about this challenge is the combination of two concepts. One borrowed from physics (Schrödinger's Cat thought experiment) and one from chaos theory and resilience engineering (Chaos Monkey implementation).

Schrödinger's Monkey encapsulates two ideas. The first (Schrödinger's) is that every major operational issue should initially considered as both until proven otherwise:

+ a cybersecurity risk
+ an IT service risk

Modern attacks often exploit operational weaknesses such as misconfigurations, exposed credentials, or service dependencies. What appears to be a routine operational issue may in fact represent an exploitable attack path.

Conversely, what appears to be a security alert may ultimately be an operational fault. Treating incidents as both possibilities encourages joint investigation between SOC and ITSM teams, improving both cyber defence and operational resilience.

The second idea (Monkey) is that proactively conducting adversarial offensive cyber and service incident serials generates meaningful learning opportunities to consistently improve understanding, performance and resilience towards excellence. How can an organisation learn how to respond effectively to an attack or outage in the absence of repeated practice and validation?

This mindset reflects the growing use of autonomous tools by both defenders and attackers. As attack timelines accelerate, organisations have ever diminishing time to determine if an issue is operational or adversarial. Treating incidents as both from the outset improves response speed and coordination which is repeatedly tested and validated to consistently improve performance.

Establishing a Common Risk Perspective

Traditional vulnerability management tools identify the presence of weaknesses such as CVEs or misconfigurations. However, they do not demonstrate whether those weaknesses can actually be exploited in a given environment.

An organisation may have thousands of high-severity vulnerabilities on paper, yet in the context of their production environment, only a small subset enable attackers to move from an initial foothold to critical business systems.

Offensive cyber platforms take a different approach by adopting the attacker's perspective as the primary source of truth. Instead of cataloguing vulnerabilities in isolation, they identify and prove attack paths. These paths demonstrate how weaknesses can be chained together to achieve outcomes such as domain compromise, data theft, or service disruption. Each finding is supported by evidence of exploitation, such as captured credentials, demonstrated lateral movement, or privilege escalation.

Platforms such as the NodeZero® Proactive Security Platform operationalise this model by continuously identifying exploitable attack paths and producing attacker-validated evidence of exposure.

This evidence fundamentally changes the conversation between security and operations. Rather than asking ITSM teams to prioritise theoretical risk, security can demonstrate precisely how an attacker would compromise critical assets.

Traditional Vulnerability Management vs Evidence-based Exposure

Traditional Approach	Evidence-based Exposure
Large lists of vulnerabilities	**Prioritised exploitable attack paths**
CVSS severity drives prioritisation	**Demonstrated exploitability drives prioritisation**
Thousands of tickets created	**Fewer high-value remediation actions**
Debate over theoretical risk	**Evidence-backed decisions**
Limited validation of remediation	**Verified closure through retesting**

This shared evidence becomes the foundation for aligning SOC and ITSM priorities.

SOC–ITSM Integration Maturity Model

Organisations often evolve through stages as they integrate security and operational workflows.

Level	Characteristics	Operational Outcome
Level 1 Isolated Functions	SOC and ITSM operate independently	Security alerts rarely translate into operational action
Level 2 Information Sharing	Security findings passed to ITSM manually	Limited prioritisation and high ticket noise
Level 3 Evidence-Driven Prioritisation	Exploitable attack paths inform remediation	Reduced noise and improved prioritisation
Level 4 Integrated Operations	Shared metrics and verification workflows	Security and IT operations jointly reduce exposure
Level 5 Proactive test and evaluation of response	Continuously measure and improve people, process and technology integration	Consistent cadence to evaluate and drive increased system resilience and security

Most organisations operate between Levels 1 and 2.

Evidence-based exposure management enables progress toward Levels 3 and 4.

Only a mindset of continuous improvement and devotion to excellence can take you to Level 5.

Leadership Actions for SOC–ITSM Integration

Leaders seeking to integrate security and IT operations should focus on a small number of operational changes. These changes strengthen the connection between cyber risk management and service management rather than replacing existing governance frameworks.

1. Align SOC and ITSM Around Evidence-Based Risk

When security teams prioritise vulnerabilities solely based on severity scores and ITSM teams prioritise changes based on service stability, both sides lack a common decision framework. Evidence-based exposure changes this dynamic. If system weaknesses are validated through real attack paths, both teams can focus on the same operational question:

How quickly should we remove this proven route to compromise?
This approach reduces noise dramatically. Thousands of potential vulnerabilities collapse into a smaller number of exploitable attack paths that truly matter. The result is a prioritised backlog shared by both SOC and ITSM.

2. Establish Shared Metrics for Risk Reduction

SOC and ITSM teams are frequently measured independently. This reinforces organisational silos. A more effective approach is to adopt metrics that reflect the full lifecycle of risk reduction.

Metric	What it Measures	Why it matters
Time from exploit discovery to ticket creation	Speed of translating security findings into operational work	Ensures exposure quickly becomes operational work
Time from ticket creation to remediation	Operational responsiveness	Aligns security priorities with change execution
Time from remediation to verified closure	Effectiveness of remediation	Confirms exploit paths are removed
Number of exploitable attack paths to critical assets	Real exposure to high-value systems	Focuses leadership attention on meaningful risk
Recurrence of previously fixed attack paths	Sustainability of remediation	Identifies systemic configuration issues

These metrics shift the focus from activity to actual risk reduction.

3. Integrate Security Findings Directly Into ITSM Workflows

Security findings should enter the same operational systems that manage service delivery. Offensive testing platforms can integrate directly with ITSM tools such as ServiceNow or Jira. Validated exposures are then automatically translated into structured tickets containing:

+ affected assets
+ exploit evidence
+ attack path context
+ remediation guidance

Status updates in ITSM systems synchronise back to the security platform, ensuring both teams share a consistent view of progress.

This eliminates manual handoffs and ensures remediation activity occurs within existing operational workflows.

4. Make Security Verification Part of Change Management

In many organisations, change management confirms that systems continue to operate correctly after modifications. However, it rarely verifies whether security exposure has actually been removed.

Offensive testing enables a closed-loop verification model. Once remediation actions are implemented, targeted retesting confirms that the previously exploited attack path is no longer possible.

Capabilities such as those provided by offensive security platforms allow organisations to revalidate previously identified attack paths and confirm whether remediation has successfully removed the exposure. Changes are not complete until exposure is proven to be resolved.

5. Build Joint Operational Practices Between SOC and ITSM

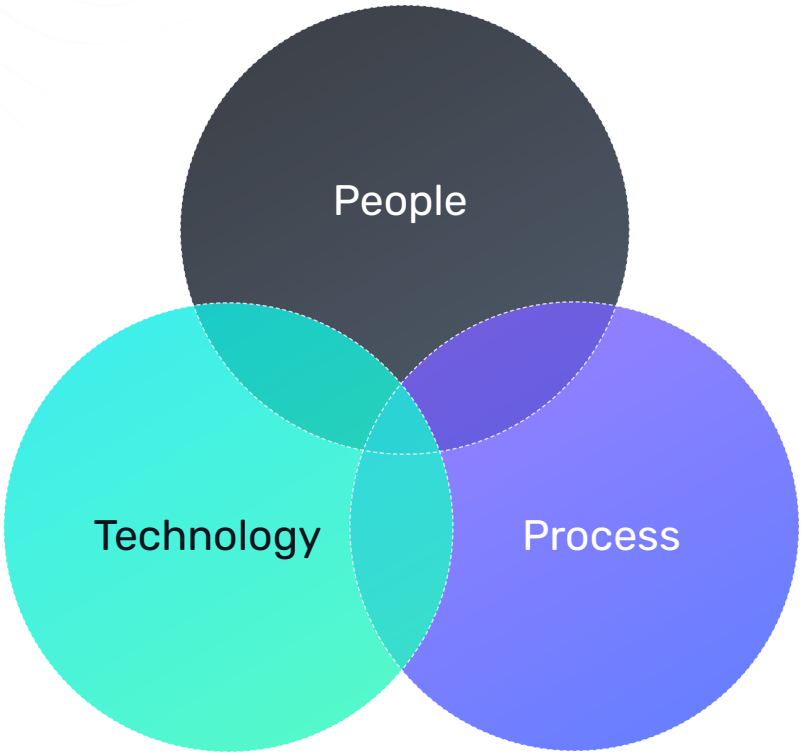
Tools alone cannot resolve organisational friction. Integration must also occur through shared operational practices. Examples include:

+ joint triage for high-impact findings
+ shared incident reviews combining SOC telemetry and ITSM timelines
+ collaborative workshops exploring attack paths and remediation strategies

These activities build mutual understanding and improve response effectiveness.

Integrating People, Process, and Technology

Sustainable SOC–ITSM integration requires alignment across people, processes, and supporting technologies.



People
Joint exercises and operational reviews help both teams understand each other's responsibilities and constraints. Attack path analysis provides a practical foundation for cross-training.

Process
Security validation can be embedded within core ITSM processes including incident management, problem management, and change management.

Technology
Offensive security platforms integrate with existing security and operational tooling, creating a unified operational picture of exposure across infrastructure, cloud environments, identity systems, and external attack surfaces.

Aligning With Cyber Risk Management Frameworks

The UK National Cyber Security Centre cyber security risk management framework provides a useful structure for understanding how these capabilities support broader governance objectives.

The framework outlines eight steps:

1. Establish organisational context
2. Identify decision-makers and governance structures
3. Define the cyber risk challenge
4. Select appropriate approaches
5. Understand and manage risks
6. Communicate and consult
7. Implement and assure
8. Monitor and review

Offensive validation supports several of these stages directly by identifying exploitable paths to critical assets, informing remediation decisions, and confirming whether risk treatments are effective.

Leadership Checklist for SOC–ITSM Integration

Leadership Question	What Good Looks Like
Do SOC and ITSM share a common view of cyber risk?	**Exploitable attack paths visible to both teams**
Are validated exposures tracked in ITSM systems?	**Tickets automatically created with exploit evidence**
Are remediation actions verified?	**Retesting confirms attack paths are closed**
Are remediation tickets only closed after validation?	**Tickets remain open until retesting confirms the exposure has been removed**
Do both teams use shared metrics?	**Exposure lifecycle metrics tracked**
Are incidents reviewed jointly?	**SOC telemetry and ITSM timelines analysed together**

Conclusion

SOC and ITSM teams are not adversaries. They are responsible for different aspects of organisational resilience.

Security reduces the likelihood of compromise. IT operations maintains reliable services. The challenge arises when both teams operate from different views of risk.

Offensive security platforms provide a practical mechanism for aligning those views by demonstrating which weaknesses are actually exploitable and how they impact critical services.

When this evidence is integrated with ITSM workflows and governed through established cyber risk management frameworks, security and operations can work toward a shared objective.

Organisations stop debating theoretical vulnerabilities and start removing proven attack paths while verifying that fixes remain effective.

This is how organisations move from assumed security to demonstrable resilience and from competing operational silos to a unified defence of mission and service.

About the Author

Daniel Bird MBE is the Field Chief Technology Officer for EMEA at Horizon3.ai, where he works with organisations across government and industry to strengthen cyber resilience through operational security practices. Prior to joining Horizon3.ai, Daniel spent more than two decades in the UK Ministry of Defence delivering and operating critical information and communications systems, including leadership roles in large-scale IT service delivery, operational planning, and international technology cooperation.

His career has focused on integrating technology, operations, and risk management to support mission outcomes. Daniel holds postgraduate qualifications in Defence Technology from Cranfield University and was awarded the Member of the Order of the British Empire (MBE) for his service to UK defence.