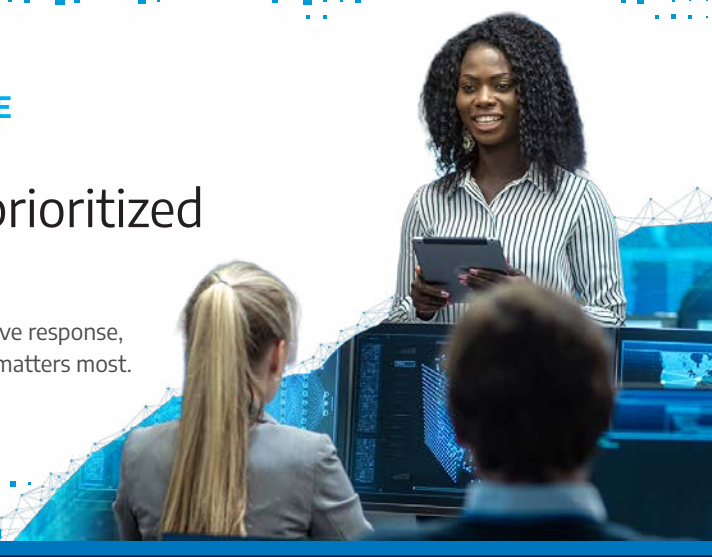
MODERN INFRASTRUCTURE AND MULTICLOUD

Adopting a Risk-prioritized Security Model

A practical approach to cut noise, improve response, and focus security operations on what matters most.



When everything feels urgent, nothing gets prioritized.

Most security teams are not struggling because they lack visibility. They are struggling because they lack prioritization. Without clear visibility into critical assets and alerts with the most business impact, time is spent sifting through low-value activity while real threats compete for attention.

Up to **62%** of security alerts ultimately go unactioned due to volume.[1]

Move from alert volume to business impact.

A risk-prioritized security model focuses less on collecting and processing every alert the same way and more on identifying which risks create the greatest business impact. Success is measured not by how many alerts are processed, but by how effectively teams act on the alerts that matter most.

Up to **70%** of security alerts may be false or low-value.[2]

Build the model around risk, exposure, and response.

The shift starts with a Strategic Security Evaluation and Security Assessment Suite to identify critical assets, map dependencies, and align technical findings to business risk. External and Internal Penetration Testing then validates exposure by showing how attackers could realistically move through the environment and exploit weaknesses. This creates a clear view of which vulnerabilities and attack paths deserve immediate attention.

Assess
SECURITY ASSESSMENT SUITE

Map business risk and dependencies
STRATEGIC SECURITY EVALUATION

Validate exposure and attack paths
PENETRATION TESTING

Align monitoring and response to high-value alerts
MANAGED XDR

Prioritization needs governance, not just technology.

Technology alone doesn't ensure effective alert prioritization. A Virtual Chief Information Officer-led or -aligned governance framework is needed to translate technical findings into business risk, align investments to key exposures, and provide clear operational priorities for the SOC.

> "Security teams aren't just drowning in volume; they're operating without a clear sense of what matters most."[3]

What organizations gain from adopting the model.

When Managed XDR monitoring and response are aligned to business-critical assets, organizations can reduce unnecessary investigations, improve response focus, and strengthen operational resilience. Teams can improve consistency in responding to threats with the greatest business impact even when overall alert volume remains high.

- Reduced noise (fewer unnecessary investigations)
- Improved analyst focus on high-impact threats
- More consistent response
- Stronger operational resilience
- More informed security decisions

How Connection Can Help

It's not about processing more alerts. It's about prioritizing the ones that matter. Connection helps organizations assess risk, validate exposure, establish governance, and operationalize prioritized detection and response through Strategic Security Evaluations, Penetration Testing, Virtual Chief Information Officer services, and Managed XDR.

Explore our Solutions and Services

- Cybersecurity
- Strategic Security Evaluations
- Penetration Testing
- Virtual Chief Information Officer
- Managed XDR

1.800.998.0019

Connection®
we solve IT®

Sources
1. Dark Reading, SOC Teams: Threat Detection Tools Are Stifling Us
2. CIO, Report Reveals Tool Overload Driving Fatigue and Missed Threats in MSPs
3. Forbes, Your SOC Doesn't Need More Alerts—It Needs A Brain