BROADCOM

Executive Summary

From Tools to Telemetry: A Playbook for Modern Detection and Response in Resource-Constrained Teams

For years, midsize organizations believed they were too small to attract sophisticated cyberattacks. That assumption no longer holds. Ransomware-as-a-service (RaaS), supply chain attacks, and credential theft have dramatically lowered the cost of launching enterprise-grade attacks, allowing adversaries to target organizations with only a handful of security personnel.

Many organizations have responded by purchasing more security tools. Yet a security team of 3 to 10 generalists cannot realistically manage 15 or more separate consoles; manually correlate alerts across endpoint, identity, cloud, and network environments; and respond quickly enough to stop today's attacks. More technology alone does not create stronger security.

Modern detection and response requires a different approach—one that prioritizes visibility across security domains, correlates telemetry into a unified picture of attacker behavior, and automates high-confidence response actions before adversaries can establish persistence or move laterally.

Three capabilities distinguish effective resource-constrained security programs:

- **Telemetry fusion** that correlates endpoint, identity, email, SaaS, cloud, and network activity into a unified attack story.
- **Threat-informed detection** that measures coverage against MITRE ATT&CK® techniques rather than raw alert volume.
- **Decision-ready response** that automates containment for validated threats while providing analysts with complete investigative context.

Rather than advocating another point solution, the paper presents a practical four-phase operating model: *Audit*, *Consolidate*, *Automate*, and *Validate*. Organizations that continuously execute this cycle improve visibility, reduce analyst workload, and demonstrate measurable security maturity to customers, insurers, regulators, and executive leadership.

The Modern Detection Challenge

Enterprise-grade attacks now routinely target midsize organizations.

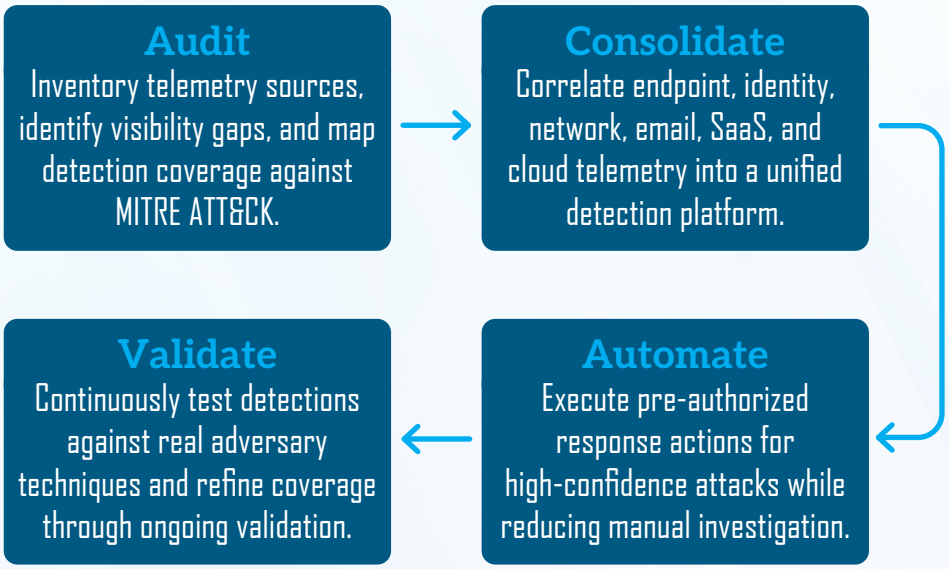
Security teams often manage dozens of disconnected tools with limited staff.

Critical attack signals remain isolated across endpoint, identity, cloud, and network platforms.

Manual investigation slows response while attackers move in minutes.

RESULT:
More tools don't create better security—better correlation does.

The Detection and Response Lifecycle



Key Capabilities of Modern Detection and Response

- Unified telemetry across endpoint, identity, network, cloud, and SaaS
- Native correlation of attacker activity across security domains
- MITRE ATT&CK–aligned detection coverage
- Automated, policy-driven response actions
- Continuous validation through adversary emulation and testing
- Visibility designed for lean security teams

Modern Detection and Response Strengthens Existing Security Investments

- Maximizes value from existing security tools through correlation
- Reduces analyst time spent pivoting between consoles
- Improves ransomware and credential attack detection
- Accelerates containment through automated response
- Produces measurable evidence for cyber insurance, audits, and compliance

Bottom Line for Executives

Today's attackers operate faster than resource-constrained security teams can manually investigate disconnected alerts. Success no longer depends on adding more security tools—it depends on unifying the telemetry organizations already collect, automating response where confidence is high, and continuously validating detection coverage against modern adversary techniques.

Organizations that adopt an **Audit → Consolidate → Automate → Validate** operating model improve visibility, reduce analyst workload, strengthen resilience, and create a security program that scales with both business growth and the evolving threat landscape.

What's at Stake

Security Risk

Disconnected telemetry allows attackers to exploit identity, cloud, and endpoint gaps before defenders recognize the full attack.

Operational Burden

Small security teams spend valuable time manually correlating alerts instead of responding to incidents.

Business Risk

Delayed detection increases the likelihood of ransomware, business disruption, financial loss, and reputational damage.

Compliance & Customer Trust

Organizations increasingly must demonstrate validated detection capabilities to regulators, insurers, and enterprise customers.

Competitive Advantage

Security maturity has become a differentiator in procurement, cyber insurance, and business resilience.

SANS | Research Program