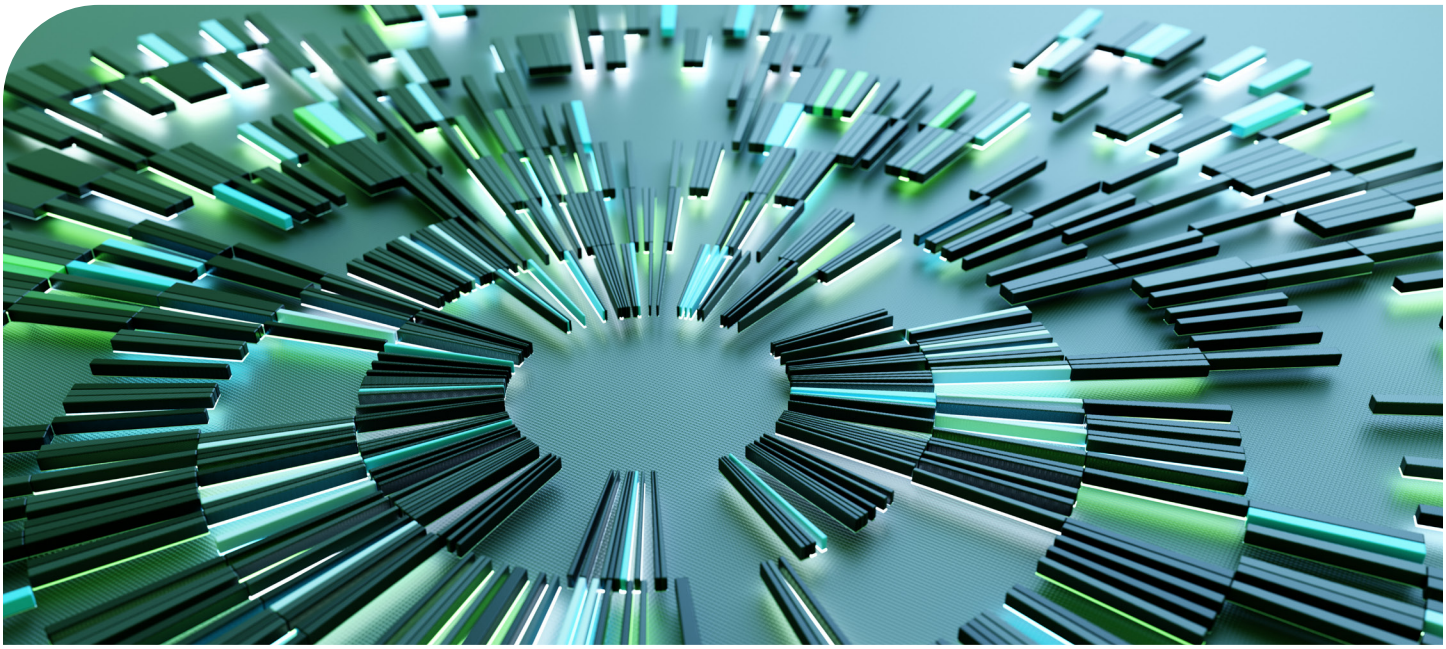

Info sheet

Rapid Value Assessment: Cybersecurity Detection Coverage

A focused assessment to validate your security detection coverage

Most organizations believe their security controls are working. The Cybersecurity Detection Coverage Rapid Value Assessment replaces that belief with evidence — measuring actual effectiveness, identifying the gaps, and translating them into business risk. Delivered as a fixed three-week engagement, the assessment is fast and non-disruptive, run with a read-only script with no persistent software installation and no data leaving your environment.

By directly interrogating your security information and event management (SIEM) and connected systems, we expose threat detection blind spots, validate your MITRE ATT&CK coverage (the industry-standard framework for classifying attacker behavior), and benchmark your environment against industry standards, delivering clear, prioritized findings to close gaps before they become breaches or violations. The findings are quantified in business terms, translating technical gaps into potential risks, including financial and operational exposure. They are also mapped to recognized security and regulatory frameworks, providing audit-ready evidence that supports compliance and governance requirements.

The result is an objective, evidence-based scorecard that removes guesswork and gives your team a clear, defensible view of current detection effectiveness without adding operational overhead or unreasonable cost.

The assessment provides

- **SIEM environment scorecard** with overall and domain-level security ratings benchmarked against industry averages, highlighting control gaps that impact compliance readiness, operational efficiency, and financial exposure
- **MITRE ATT&CK coverage heat map** showing where your detection rules hit, where they miss, and what remediation to prioritize first
- **Blind-spot inventory** identifying unmonitored assets, misconfigured connectors, untested detection rules, and alert noise masking real threats
- **Prioritized remediation** findings that are mapped to leading industry frameworks (MITRE ATT&CK, NIST Cybersecurity Framework (CSF), and Critical Security Controls (CIS Controls)) and ranked by business impact through automated analysis and correlation
- **Business risk context** that translates technical and defense gaps into financial and breach risk exposure, giving your management a clear and defensible business case to remediate security gaps

How the assessment works

The assessment automatically correlates detection data across your security stack, including assets your team may not know are unmonitored, turning raw signals into actionable intelligence. This reduces noise, focusing attention on the detections that matter most. Working through four structured phases, it requires approximately 4 to 6 hours of your team's time.

Scoping and access (Days 1–2)	Align on assessment objectives and IT landscape. Provision read-only access to your SIEM, configuration management database (CMDB), IT service management (ITSM), and Active Directory. No data or logs leave the environment.
Data collection (Days 3–5)	Our data collection (logs, events, security incidents, asset details, etc.) methodology interrogates your SIEM and connected systems, inventorying data sources, detection rules, MITRE ATT&CK coverage, and platform health. The script is read-only with no persistent installation.
Expert analysis (Days 6–12)	Unisys security specialists leverage a proprietary detection coverage analysis tool that automatically evaluates gathered data against industry benchmarks and frameworks such as MITRE ATT&CK, NIST CSF, and CIS Controls, eliminating the need for manual assessment. Risk is ranked by business impact, not just technical severity.
Findings workshop (Day 15)	Collaboratively, we review your comprehensive scorecard and prioritized findings in a workshop to define a plan to increase coverage and optimize response and remediation. Walk away knowing exactly where your detection coverage stands and what to do about it.

Why participate in the assessment

- **Replace assumptions with evidence:** Most organizations assume their SIEM is working. This assessment validates whether it is, surfacing unmonitored assets, misconfigured connectors, untested rules, and alert noise that obscures real risk, revealing findings no standard vulnerability scan will detect.
- **Act on expert guidance:** Get practical recommendations from security specialists with deep enterprise experience, mapped to frameworks your leadership and compliance teams already recognize.
- **Prioritize with confidence:** Risk-ranked findings help you direct resources where they reduce business exposure the most, improving operational focus and reducing wasted investigative effort without relying on fear-based or speculative risk narratives.
- **Accelerate compliance readiness:** Assessments focus on SIEM/SOC (security operations center) coverage and detection health, with findings mapped to global frameworks (NIST CSF, PCI DSS, HIPAA, etc.) based on industry and geolocation, providing documented evidence for audit readiness and board-level reporting.
- **Build a clear business case:** The scorecard quantifies savings across log costs, analyst labor, and breach risk reduction, complete with ROI and payback period, giving security teams the financial evidence needed to justify investment and giving management a credible answer to the question that matters most: "Are we prepared for cyber attack?"
- **Create a path forward:** Assessment findings connect directly to Unisys Security Managed Services for ongoing detection, protection, and response, so momentum continues after the engagement ends.

Why Unisys?

Unisys delivers a detection assessment that replaces assumed coverage with measured evidence. Our security team operates global security operations centers staffed by analysts who understand both technical vulnerabilities and business risks. We partner with leading technology providers, including Microsoft and Dell, and bring industry-specific overlays for public sector, higher education, manufacturing, financial services, and healthcare.

Unlike assessment-only providers, Unisys combines automated, evidence-based detection analysis with practitioners who run enterprise SOCs every day. Findings are not just accurate but operationally actionable.

Know your gaps before attackers do

Request your Cybersecurity Detection Coverage Rapid Value Assessment at unisys.com/cyber.

unisys

unisys.com

04/26 6494-12105