0x40A57AD9

Cybersecurity Operations Centre

System Decomposition Report

Generated 2026-09-07 — Derive by AIRGen

derive.airgen.studio • info@airgen.studio

UNCLASSIFIED — SYNTHETIC DATA

About This Report

This report was generated autonomously by the Derive@AIRGen systems engineering platform. An AI agent decomposed the system into subsystems and components, classified each using the Universal Hex Taxonomy (a 32-bit ontological classification system), generated traced requirements in AIRGen, and built architecture diagrams — all without human intervention.

Every component and subsystem is assigned an 8-character hex code representing its ontological profile across 32 binary traits organised in four layers: Physical (bits 1–8), Functional (9–16), Abstract (17–24), and Social (25–32). These codes enable cross-domain comparison — components from unrelated systems that share a hex code or high Jaccard similarity are ontological twins, meaning they occupy the same structural niche despite belonging to different domains.

Duplicate hex codes are informative, not errors. When two components share the same code, it means UHT classifies them as the same kind of thing — they have identical trait profiles. This reveals architectural patterns: for example, a fire control computer and a sensor fusion engine may share the same hex because both are powered, synthetic, signal-processing, state-transforming, system-essential components. The duplication signals that requirements, interfaces, and verification approaches from one may transfer to the other.

Requirements follow the EARS pattern (Easy Approach to Requirements Syntax) and are traced through a derivation chain: Stakeholder Needs (STK) → System Requirements (SYS) → Subsystem Requirements (SUB) / Interface Requirements (IFC) → Verification Plan (VER). The traceability matrices at the end of this report show every link in that chain.

Referenced Standards

- ISO 27001 — Information security management systems

Contents

Acronyms & Abbreviations

Acronym	Definition
PII	usernames, IP addresses
SIEM	IFC-003
SLA	SYS-SYS-RESPOND-003
SOAR	IFC-009

Decomposition Tree

Cybersecurity Operations Centre	40A57AD9
├ Communications and Reporting Subsystem	40A57B58
├ Endpoint Detection and Response Subsystem	51F77B19
├ Identity and Access Monitoring Subsystem	41B77319
├ Network Security Monitoring Subsystem	40A53219
├ SIEM Engine	51F77B19
├ SOAR Platform	51B77B19
├ SOC Facility Infrastructure	DE851018
├ Threat Intelligence Platform	40F77319
├ Vulnerability Management System	41F77B19

Specification Tree

Requirement coverage by subsystem. Columns show count of requirements tagged to each subsystem across document types.

Subsystem	SUB	IFC	ARC	VER	Total
Communications and Reporting Subsystem	0	0	0	0	0
Endpoint Detection and Response Subsystem	0	0	0	0	0
Identity and Access Monitoring Subsystem	0	0	0	0	0
Network Security Monitoring Subsystem	0	0	0	0	0
SIEM Engine	0	0	0	0	0
SOAR Platform	0	0	0	0	0
SOC Facility Infrastructure	0	0	0	0	0
Threat Intelligence Platform	0	0	0	0	0
Vulnerability Management System	0	0	0	0	0

Stakeholder Requirements (STK)

Ref	Requirement	V&V	Tags
STK-STK-NEEDS-001	The Cybersecurity Operations Centre SHALL detect cyber threats targeting the organisation's IT and OT infrastructure with a mean time to detect (MTTD) not exceeding 15 minutes for high-severity incidents. Rationale: MTTD of 15 minutes for high-severity incidents derives from MITRE ATT&CK dwell-time analysis: adversaries completing lateral movement within 30-60 minutes of initial compromise means detection must occur in the first half of that window to enable effective containment. Exceeding 15 minutes significantly increases the probability of privilege escalation and data exfiltration.	Test	stakeholder, session-291
STK-STK-NEEDS-002	The Cybersecurity Operations Centre SHALL contain confirmed security incidents within 60 minutes of detection for critical-severity incidents and within 4 hours for high-severity incidents. Rationale: Containment timelines of 60 minutes (critical) and 4 hours (high) are derived from the NIST SP 800-61 incident response lifecycle and align with insurance underwriter expectations. Critical incidents (ransomware, active intrusion) require sub-hour containment to prevent encryption propagation or data exfiltration at scale.	Test	stakeholder, session-291
STK-STK-NEEDS-003	The Cybersecurity Operations Centre SHALL comply with NIST Cybersecurity Framework, ISO 27001, and all applicable sector-specific cyber security regulations in the jurisdictions where the organisation operates. Rationale: Regulatory compliance is a non-negotiable operational requirement. NIST CSF provides the detection and response framework, ISO 27001 the management system baseline, and sector-specific regulations (e.g., NIS2 for critical infrastructure, PCI-DSS for payment processing) impose additional controls with legal penalties for non-compliance.	Inspection	stakeholder, session-291
STK-STK-NEEDS-004	The Cybersecurity Operations Centre SHALL operate continuously 24 hours per day, 7 days per week, 365 days per year with no planned downtime exceeding 30 minutes per quarter. Rationale: Cyber attacks are not bounded by business hours; adversaries deliberately operate during off-peak periods when monitoring attention is lowest. The 30-minute quarterly maintenance window constrains planned downtime to what can be achieved with rolling upgrades and hot-standby failover, maintaining continuous threat detection coverage.	Demonstration	stakeholder, session-291
STK-STK-NEEDS-005	The Cybersecurity Operations Centre SHALL maintain visibility across all organisational IT assets, OT systems, cloud workloads, and remote access infrastructure, with no asset remaining unmonitored for more than 7 days after deployment. Rationale: Unmonitored assets are the primary vector for undetected compromise. The 7-day onboarding window balances operational reality (new asset provisioning, network registration, agent deployment) against the risk window. Complete asset visibility is foundational — detection rules and vulnerability scans are ineffective against assets the SOC cannot see.	Inspection	stakeholder, session-291

Ref	Requirement	V&V	Tags
STK-STK-NEEDS-006	The Cybersecurity Operations Centre SHALL incorporate current cyber threat intelligence from at least 10 independent sources to inform detection rules, prioritise vulnerabilities, and contextualise alerts with threat actor attribution. Rationale: Requiring 10+ independent intelligence sources ensures coverage diversity across commercial threat feeds (e.g., Recorded Future, Mandiant), open-source feeds (e.g., MISP communities, abuse.ch), government advisories (CISA, NCSC), and sector-specific ISACs. Single-source reliance creates blind spots for threats outside that vendor's collection aperture.	Inspection	stakeholder, session-291
STK-STK-NEEDS-007	The Cybersecurity Operations Centre SHALL generate regulatory breach notifications within the timeframes mandated by applicable law, including GDPR 72-hour notification and NIS2 24-hour early warning, and SHALL produce executive incident summaries within 4 hours of incident declaration. Rationale: GDPR Article 33 mandates 72-hour notification to supervisory authorities; NIS2 Article 23 requires 24-hour early warning. Failure to meet these timelines carries statutory penalties (up to 2% of global turnover under NIS2). The 4-hour executive summary enables incident commander decision-making during the critical early phase of response.	Demonstration	stakeholder, session-291
STK-STK-NEEDS-008	The Cybersecurity Operations Centre SHALL support monitoring of up to 100,000 endpoints and 500 network segments without degradation in detection performance, and SHALL accommodate 25% annual growth in monitored assets without architectural redesign. Rationale: 100,000 endpoints and 500 network segments represent a large enterprise baseline. The 25% annual growth accommodation prevents architectural redesign cycles that would introduce detection coverage gaps during migration. Without this headroom, SOC infrastructure becomes the bottleneck during acquisitions, cloud migrations, or rapid expansion.	Analysis	stakeholder, session-291

System Requirements (SYS)

Ref	Requirement	V&V	Tags
SYS-SYS-DETECT-001	The SIEM Engine SHALL correlate ingested security events against detection rules and produce alerts within 120 seconds of event ingestion for rule-based detections and within 300 seconds for behavioural anomaly detections. Rationale: The 120-second rule-based and 300-second behavioural detection windows derive from the 15-minute MTTD stakeholder requirement (STK-NEEDS-001). Correlation must complete well within the MTTD budget to leave time for alert triage, enrichment, and analyst notification. Behavioural analytics require longer windows due to baseline comparison computation.	Test	system, session-291
SYS-SYS-DETECT-002	The SIEM Engine SHALL sustain ingestion of at least 150,000 events per second at steady state and absorb bursts of up to 500,000 events per second for periods of up to 10 minutes without event loss or increased correlation latency. Rationale: 150K EPS steady-state derives from 100K endpoints generating an average of 1.5 events/sec each across OS telemetry, EDR, network flow, and authentication logs. The 500K EPS burst capacity accommodates incident-triggered log surges (e.g., mass scanning, worm propagation) when event volumes spike 3-4x. Event loss during these bursts would create detection blind spots precisely when they are most dangerous.	Test	system, session-291
SYS-SYS-DETECT-003	The Endpoint Detection and Response subsystem SHALL execute remote endpoint containment actions (network isolation, process termination) within 30 seconds of command issuance by the SOAR platform or analyst console. Rationale: 30-second containment execution derives from the 60-minute critical incident containment target (STK-NEEDS-002). Automated containment actions (network isolation, process kill) must execute near-instantly once the decision is made, as each second of delay allows additional lateral movement, data staging, or encryption. The 30-second ceiling accounts for agent communication latency across WAN-connected endpoints.	Test	system, session-291
SYS-SYS-DETECT-004	The SOAR Platform SHALL execute automated response playbooks for known alert categories within 60 seconds of alert receipt, and SHALL route alerts requiring human judgement to the appropriate analyst tier within 120 seconds. Rationale: 60-second automated playbook execution for known alert types reduces analyst cognitive load and ensures consistent response for high-volume, well-understood threats (phishing, malware beaconing, brute-force). The 120-second routing SLA for human-judgement alerts ensures tier-appropriate analyst engagement before the MTTD budget is consumed.	Test	system, session-291

Ref	Requirement	V&V	Tags
SYS-SYS-DETECT-005	The Threat Intelligence Platform SHALL ingest and normalise indicators from at least 20 intelligence feeds using STIX/TAXII 2.1, with feed update intervals not exceeding 4 hours for commercial feeds and 1 hour for critical advisories. Rationale: 20 feeds exceeds the 10-source stakeholder minimum (STK-NEEDS-006) to provide the TIP with sufficient indicator volume for cross-correlation. STIX/TAXII 2.1 is the OASIS standard for structured threat intelligence exchange, ensuring interoperability across commercial and government feeds. The 4-hour/1-hour update intervals balance API rate limits against indicator freshness for critical advisories (e.g., zero-day IOCs).	Test	system, session-291
SYS-SYS-DETECT-006	The Cybersecurity Operations Centre SHALL retain searchable security event logs for a minimum of 90 days in hot storage and 365 days in warm storage, with archived logs retrievable within 4 hours for forensic investigation. Rationale: 90-day hot storage enables immediate forensic investigation of incidents discovered during routine threat hunting or retrospective IOC matching. 365-day warm storage satisfies regulatory retention requirements (ISO 27001 A.12.4, PCI-DSS Requirement 10.7). The 4-hour retrieval SLA for archived logs supports investigation timelines without requiring cost-prohibitive all-hot architectures.	Test	system, session-291
SYS-SYS-DETECT-007	The Vulnerability Management System SHALL scan 100% of IT assets on a rolling 7-day cycle and 100% of OT assets on a rolling 30-day cycle, maintaining a real-time asset inventory with accuracy of 98% or greater. Rationale: 7-day IT scan cycle aligns with common vulnerability disclosure timelines and patch management SLAs. 30-day OT cycle reflects operational constraints — OT systems often cannot tolerate active scanning during production windows. 98% asset inventory accuracy ensures vulnerability coverage aligns with actual deployed infrastructure, preventing false confidence from scanning stale asset lists.	Test	system, session-291
SYS-SYS-DETECT-008	The Cybersecurity Operations Centre platform SHALL achieve 99.95% availability measured monthly, with no single point of failure in the detection and alerting pipeline from event ingestion through analyst notification. Rationale: 99.95% monthly availability allows approximately 22 minutes of unplanned downtime per month, consistent with Tier 3+ data centre SLAs and the 30-minute quarterly planned maintenance window (STK-NEEDS-004). The no-single-point-of-failure requirement ensures that component failure in the detection pipeline does not create an unmonitored window exploitable by adversaries.	Analysis	system, session-291

Ref	Requirement	V&V	Tags
SYS-SYS-DETECT-009	The Communications and Reporting Subsystem SHALL generate pre-populated regulatory breach notification documents within 30 minutes of incident classification, covering GDPR Article 33, NIS2 Directive Article 23, and applicable sector-specific templates. Rationale: 30-minute notification document generation directly supports the GDPR 72-hour and NIS2 24-hour regulatory timelines (STK-NEEDS-007). Pre-populated templates eliminate the risk of incomplete mandatory fields under time pressure. GDPR Article 33, NIS2 Article 23, and sector templates must be maintained as living documents reflecting current regulatory interpretations.	Demonstration	system, session-291
SYS-SYS-DETECT-010	The Network Security Monitoring Subsystem SHALL capture full packet data on all monitored network segments at aggregate throughput of 10 Gbps, retaining packet captures for a minimum of 72 hours, and SHALL process IDS signatures with update latency not exceeding 4 hours from rule publication. Rationale: Full packet capture at 10 Gbps aggregate provides forensic evidence for incident investigation that metadata-only approaches cannot — payload inspection, protocol anomaly analysis, and malware sample extraction. 72-hour retention covers the typical investigation initiation window. 4-hour IDS rule update latency ensures signature coverage for newly disclosed vulnerabilities within the same operational cycle as vendor advisory publication.	Test	system, session-291
SYS-SYS-DETECT-011	The Identity and Access Monitoring Subsystem SHALL perform User and Entity Behaviour Analytics across all Active Directory, Azure AD, and PAM authentication events, detecting credential compromise indicators with a false positive rate not exceeding 5% of total identity alerts. Rationale: Identity is the primary attack surface in modern enterprise environments — over 80% of breaches involve credential compromise (Verizon DBIR). UEBA across AD, Azure AD, and PAM covers the full authentication surface. The 5% false positive ceiling ensures analyst trust in identity alerts; higher rates lead to alert fatigue and missed true positives in the identity domain.	Test	system, session-291
SYS-SYS-DETECT-012	The SOC Facility Infrastructure SHALL provide uninterruptible power for a minimum of 72 hours using UPS and backup generators, maintain physical access control with two-factor authentication, and sustain operations during loss of primary commercial power or primary internet connectivity. Rationale: 72-hour UPS/generator runtime covers extended utility outages during severe weather events or grid failures, maintaining SOC operations during the period when cyber threats may increase (adversaries exploit infrastructure disruptions). Two-factor physical access prevents unauthorised facility entry that could enable physical tampering with SOC infrastructure, keyboard loggers, or insider threat scenarios.	Demonstration	system, session-291

Ref	Requirement	V&V	Tags
SYS-SYS-DETECT-013	The SIEM Engine SHALL provide an interactive threat hunting interface supporting ad-hoc queries across all ingested telemetry with query response time not exceeding 30 seconds for searches spanning 7 days of data, and SHALL maintain a library of at least 50 reusable hunt hypotheses mapped to MITRE ATT&CK techniques. Rationale: Threat hunting addresses the detection gap between known-bad indicators (covered by detection rules) and novel adversary TTPs. The 30-second query response time over 7-day windows ensures analysts can iterate on hunt hypotheses without workflow disruption. The 50-hypothesis library mapped to ATT&CK ensures coverage of common adversary technique chains even with analyst turnover.	Demonstration	detection, validation, session-293
SYS-SYS-DETECT-014	The SIEM Engine SHALL implement alert suppression, deduplication, and correlation grouping to maintain a per-analyst alert volume not exceeding 25 actionable alerts per hour during steady-state operations, and SHALL provide tuning metrics showing false positive rates per detection rule category on a rolling 30-day basis. Rationale: Without alert tuning, SOC analysts face alert fatigue that degrades detection effectiveness. The 25-alert/hour/analyst ceiling is derived from cognitive load research showing analyst accuracy drops below 80% above this threshold. Rolling 30-day false-positive metrics per rule category enable evidence-based tuning decisions and prevent regression when new detection rules are deployed.	Test	detection, validation, session-293
SYS-SYS-DETECT-015	The Cybersecurity Operations Centre SHALL encrypt all security event data in transit using TLS 1.3 or later on all inter-subsystem and external communication channels, and SHALL encrypt data at rest using AES-256 or equivalent for all stored security events, threat intelligence, and incident case data. Rationale: Security event data contains PII (usernames, IP addresses), threat intelligence under TLP restrictions, and forensic evidence with legal chain-of-custody requirements. TLS 1.3 is mandated over TLS 1.2 to eliminate known downgrade attacks against inter-subsystem channels that carry high-value telemetry. AES-256 at-rest encryption is required by ISO 27001 control A.10.1.1 and by GDPR Article 32 for processing security-relevant personal data.	Inspection	infrastructure, validation, session-293

Ref	Requirement	V&V	Tags
SYS-SYS-DETECT-016	The Cybersecurity Operations Centre SHALL maintain a documented disaster recovery capability with a recovery time objective of 4 hours and a recovery point objective of 1 hour for the detection and alerting pipeline, verified through quarterly DR exercises, and SHALL support geographic failover to an alternate facility. Rationale: A SOC must remain operational during regional infrastructure failures (power outages, natural disasters, physical security incidents) because adversaries actively exploit degraded defensive posture. The 4-hour RTO ensures detection pipeline restoration before typical adversary dwell times allow lateral movement. The 1-hour RPO limits telemetry data loss to a window recoverable via endpoint log replay. Geographic failover is required because single-site SOCs are a single point of failure for the entire organisation's security posture.	Demonstration	infrastructure, validation, session-293
SYS-SYS-DETECT-017	When the SIEM Engine becomes unavailable or operates at degraded capacity, the Cybersecurity Operations Centre SHALL maintain detection capability through direct alert forwarding from EDR, NSM, and IAM subsystems to the SOAR Platform, sustaining a minimum detection rate of 60% of high-severity alerts with mean time to detect not exceeding 30 minutes, until SIEM service is restored. Rationale: The SIEM-centric hub-and-spoke architecture creates a single point of failure in the detection pipeline, contradicting the no-SPOF requirement (SYS-INFRA-008). Cross-domain analogs from nuclear reactor protection and naval combat management implement diverse detection paths to maintain safety-critical alerting during primary system failure. The 60% detection floor and 30-minute MTTD represent minimum acceptable degraded performance during SIEM outage.	Test	degraded-mode, validation, session-297
SYS-SYS-DETECT-018	The Cybersecurity Operations Centre SHALL maintain a minimum staffing level of 2 Tier-1 analysts and 1 Tier-2 analyst per shift during 24/7 operations, with documented shift handover procedures including transfer of open incident context, pending playbook actions, and active threat hunt status, completed within 15 minutes of shift change. Rationale: STK-NEEDS-004 mandates 24/7 continuous operation but no system-level requirement defines the staffing model. Industry standards (NIST SP 800-61, FIRST CSIRT frameworks) recommend minimum dual-analyst coverage for Tier-1 triage to avoid single-analyst fatigue-induced detection gaps during overnight shifts. The shift handover requirement prevents context loss between shifts, which is a known root cause of delayed incident escalation in SOC operations.	Inspection	staffing, validation, session-297

Interface Requirements (IFC)

Ref	Requirement	V&V	Tags
IFC-IFC-INTERNAL-001	The SIEM Engine SHALL transmit correlated alert packages to the SOAR Platform via a message queue interface, with each package containing the triggering events, matched rule identifiers, affected asset inventory records, and threat intelligence enrichment data, delivered within 10 seconds of correlation completion. Rationale: The SIEM-to-SOAR alert handoff is the critical transition from detection to response. The 10-second delivery SLA ensures automated playbooks can execute within the 60-second response target (SYS-SYS-RESPOND-004). Including matched rule identifiers and threat intelligence enrichment in the package eliminates SOAR round-trip queries that would add latency and coupling.	Test	
IFC-IFC-INTERNAL-002	The Endpoint Detection and Response Subsystem SHALL stream endpoint telemetry to the SIEM Engine in Common Event Format (CEF) or Elastic Common Schema (ECS), including process creation, file modification, registry changes, and network connection events, at a sustained rate matching the endpoint fleet size without event loss. Rationale: Endpoint telemetry is the primary data source for host-based threat detection. CEF/ECS format standardisation enables correlation with network-layer events in the SIEM without per-vendor normalisation logic. Zero-loss streaming is required because adversary dwell-time indicators (process trees, registry modifications) are ephemeral and unrecoverable if dropped.	Test	
IFC-IFC-INTERNAL-003	The Threat Intelligence Platform SHALL push updated indicator-of-compromise watchlists to the SIEM Engine within 5 minutes of indicator ingestion, using STIX 2.1 bundle format, including indicator type, confidence score, TLP marking, and associated threat actor attribution where available. Rationale: IoC freshness directly determines detection effectiveness against active campaigns. The 5-minute push interval balances operational urgency with TIP processing overhead for deduplication, confidence scoring, and TLP compliance. STIX 2.1 is mandated by NIS2 information-sharing requirements and interoperability with government CERTs.	Test	
IFC-IFC-INTERNAL-004	The SOAR Platform SHALL issue containment commands to the Endpoint Detection and Response Subsystem via an authenticated REST API, supporting network isolation, process termination, and file quarantine actions, with command acknowledgement returned within 5 seconds and execution confirmation within the 30-second containment SLA. Rationale: Automated containment via SOAR-to-EDR API is the mechanism that achieves the 30-second containment SLA (SYS-SYS-RESPOND-003). The 5-second acknowledgement confirms the EDR agent received the command, distinguishing command delivery failures from execution failures. Network isolation, process termination, and file quarantine are the three containment primitives that cover 95% of MITRE ATT&CK response actions.	Test	

Ref	Requirement	V&V	Tags
IFC-IFC-INTERNAL-005	The Network Security Monitoring Subsystem SHALL forward IDS alerts, DNS query logs, and NetFlow metadata to the SIEM Engine in near-real-time with end-to-end latency not exceeding 30 seconds, tagging each event with the originating network segment identifier and sensor location. Rationale: Network-layer visibility provides detection coverage for threats invisible to endpoint agents (lateral movement, C2 beaconing, DNS exfiltration). The 30-second latency ceiling ensures IDS alerts reach the SIEM before automated response windows expire. Segment tagging is essential for correlating network events to asset inventory and establishing blast radius during incidents.	Test	
IFC-IFC-INTERNAL-006	The Identity and Access Monitoring Subsystem SHALL stream authentication events, privilege escalation attempts, and UEBA anomaly alerts to the SIEM Engine in Elastic Common Schema format, with event delivery latency not exceeding 15 seconds from event occurrence and including user principal name, source IP, authentication method, and risk score for each event. Rationale: Identity-based attacks (credential stuffing, privilege escalation, lateral movement via stolen tokens) account for over 60% of enterprise breaches. The 15-second delivery SLA ensures UEBA anomaly alerts reach the SIEM fast enough to correlate with concurrent network and endpoint indicators. ECS format ensures consistent schema with EDR telemetry for cross-domain correlation.	Test	interface, validation, session-293
IFC-IFC-INTERNAL-007	The Vulnerability Management System SHALL export vulnerability scan results and asset risk scores to the SIEM Engine via a scheduled API integration at intervals not exceeding 1 hour, with each record including CVE identifiers, CVSS base and environmental scores, affected asset identifiers, and remediation status. Rationale: Vulnerability context enriches SIEM correlation by linking observed exploit attempts to known vulnerable assets, enabling prioritised alerting. The 1-hour integration interval balances scan result freshness with API rate limits on vulnerability scanners. CVSS environmental scores (not just base) are required for risk-adjusted prioritisation against the organisation's specific attack surface.	Test	interface, validation, session-293
IFC-IFC-INTERNAL-008	The SOAR Platform SHALL create and update incident tickets in the IT Service Management system via a bidirectional REST API integration, with ticket creation occurring within 60 seconds of incident declaration, including severity, affected assets, containment actions taken, and remediation tasks, and SHALL receive ticket status updates to maintain incident timeline synchronisation. Rationale: ITSM integration is the boundary between SOC incident response and organisational IT remediation workflows. The 60-second ticket creation SLA ensures affected asset owners are notified before containment actions cause service disruptions. Bidirectional synchronisation prevents timeline divergence between the SOAR case record and the ITSM ticket, which undermines post-incident review accuracy.	Test	external, validation, session-293

Ref	Requirement	V&V	Tags
IFC-IFC-INTERNAL-009	The Threat Intelligence Platform SHALL expose a synchronous enrichment API to the SOAR Platform, accepting indicator queries (IP, domain, hash, URL) and returning confidence score, associated threat actor, TLP marking, and related indicators within 2 seconds per query, supporting a sustained query rate of at least 100 queries per minute during active incident response. Rationale: During incident response, SOAR playbooks need real-time indicator enrichment to make automated triage and containment decisions. Without a direct TIP-to-SOAR query interface, analysts must manually pivot to the TIP, adding minutes to response time. The 2-second SLA ensures playbook execution stays within the 60-second automated response target. The 100 qpm rate supports large-scale incidents.	Test	interface, validation, session-297
IFC-IFC-INTERNAL-010	The SOAR Platform SHALL issue network-level containment commands to the Network Security Monitoring Subsystem via an authenticated API, supporting IP address blocking, VLAN isolation, and DNS sinkhole actions, with command acknowledgement within 5 seconds and enforcement at the network perimeter within 30 seconds of command issuance. Rationale: Endpoint containment alone (IFC-INTERNAL-004) is insufficient for threats from unmanaged devices, IoT, or OT assets without EDR agents. Network-level containment through firewall rule insertion, VLAN isolation, or DNS sinkholing provides a complementary containment vector. The 30-second enforcement SLA matches EDR containment for consistent response timing. Cross-domain analog: naval CMS uses both close-in and area-defence engagement layers.	Test	interface, validation, session-297

Architecture Decisions (ARC)

Ref	Requirement	V&V	Tags
ARC-ARC-RAT-001	The Cybersecurity Operations Centre SHALL employ a SIEM-centric hub-and-spoke architecture where the SIEM Engine acts as the central correlation point, receiving telemetry from all detection subsystems (NSM, EDR, IAM, VMS) and forwarding correlated alerts to the SOAR Platform for automated and analyst-driven response. Rationale: Hub-and-spoke with SIEM as the central correlator was selected over a fully-meshed subsystem topology because it reduces integration complexity from O(n^2) to O(n) interfaces, concentrates log retention and forensic search in one store, and provides a single correlation context across all detection domains. The alternative — distributed correlation at each subsystem — was rejected due to increased latency for cross-domain detections and duplicated storage costs.	Analysis	

Verification Plan (VER)

Ref	Requirement	V&V	Tags
VER-VER-METH-001	The detection and alerting pipeline SHALL be verified through quarterly purple team exercises simulating at least 20 MITRE ATT&CK techniques across initial access, execution, persistence, lateral movement, and exfiltration tactics, with all test events required to produce alerts within the specified MTTD thresholds. Rationale: Purple team exercises are the only verification method that validates the end-to-end detection pipeline under realistic adversary conditions — from initial access through exfiltration. Quarterly cadence ensures detection coverage is verified after each detection rule update cycle. The 20-technique minimum across 5 ATT&CK tactic categories ensures breadth of coverage testing, not just depth against a single attack chain.	Test	verification, validation, session-293
VER-VER-METH-002	The SIEM Engine failover capability SHALL be verified through semi-annual failover exercises that simulate primary SIEM node failure and measure time-to-failover, event loss during switchover, and degraded-mode detection rate, with acceptance criteria of failover completion within 5 minutes, zero event loss exceeding 60 seconds, and degraded detection rate meeting the 60% minimum threshold. Rationale: SYS-REQS-017 introduces a degraded-mode detection requirement that must be verified independently of the quarterly purple team exercises (VER-METH-001). Failover testing validates both the SIEM HA architecture and the bypass alert paths from EDR/NSM/IAM to SOAR. Without dedicated failover exercises, the degraded-mode capability may exist on paper but fail under actual SIEM outage conditions.	Test	verification, validation, session-297
VER-VER-METH-003	The end-to-end detection and response pipeline from event ingestion through SIEM correlation to SOAR playbook execution and containment action SHALL be verified through monthly automated integration tests injecting synthetic events at each subsystem boundary, with each test validating end-to-end latency against SLA thresholds and confirming correct alert enrichment, routing, and containment command execution. Rationale: The verification plan currently covers only quarterly purple team exercises (VER-METH-001), which test detection effectiveness but not integration health. Monthly automated integration tests catch regression in inter-subsystem interfaces (message queue connectivity, API schema changes, TLS certificate expiry) before they impact real incident response. This mirrors the hospital patient monitoring approach where integration tests run continuously on the alerting pipeline.	Test	verification, validation, session-297

Ref	Requirement	V&V	Tags
VER-VER-METH-004	The data retention and regulatory compliance capabilities SHALL be verified through quarterly audits confirming that hot storage retains 90 days of searchable events, warm storage retains 365 days of retrievable events, case data is retained for 2 years, and regulatory notification templates produce complete and accurate documents for GDPR Article 33 and NIS2 Article 23 reporting. Rationale: Multiple requirements specify data retention periods (SYS-DATA-006, REQ-SECYBERSECOPSCENTRE-003, REQ-005) and regulatory notification generation (SYS-DATA-009), but no verification activity confirms these capabilities are maintained over time. Storage tier migration, schema changes, or capacity pressure can silently break retention compliance. Quarterly audit frequency aligns with the 90-day hot retention window, ensuring at least one audit covers each retention boundary.	Inspection	verification, validation, session-297
VER-VER-METH-005	The incident response and containment pipeline SHALL be verified through quarterly tabletop exercises and semi-annual live containment tests, simulating endpoint isolation via EDR, automated playbook execution via SOAR, and network-level containment via NSM, with acceptance criteria of endpoint isolation within 30 seconds, playbook execution within 60 seconds, and full incident lifecycle closure including post-incident review within 4 hours of detection. Rationale: The response pipeline spans EDR containment (REQ-007), SOAR playbook execution (REQ-004/005), and SOAR-to-EDR/NSM command interfaces (IFC-004, IFC-010). Without end-to-end response testing, individual subsystem tests may pass while the integrated containment workflow fails under realistic incident conditions. Quarterly tabletop plus semi-annual live test balances operational disruption against verification confidence.	Test	session-298, verification
VER-VER-METH-006	The network security monitoring and identity monitoring subsystems SHALL be verified through quarterly sensor coverage audits confirming IDS deployment on all monitored segments at 10 Gbps aggregate, and through semi-annual UEBA accuracy assessments measuring false positive rate against a baseline of normal authentication patterns, with acceptance criteria of 100% segment coverage, PCAP retention of 72 hours minimum, and UEBA false positive rate not exceeding 5% of generated alerts. Rationale: Network monitoring (REQ-009) and identity monitoring (REQ-010) are passive detection subsystems whose effectiveness degrades silently — a missing sensor or drifted UEBA baseline produces no visible failure signal. Periodic coverage audits and accuracy assessments are the only way to maintain confidence that these subsystems are detecting threats across the full monitored surface.	Test	session-298, verification

Ref	Requirement	V&V	Tags
VER-VER-METH-007	The threat intelligence ingestion and enrichment pipeline SHALL be verified through monthly feed health checks confirming that all configured intelligence feeds are active and delivering indicators within specified latencies, and through quarterly enrichment accuracy tests measuring the proportion of SIEM alerts correctly enriched with TIP context, with acceptance criteria of at least 20 active feeds, indicator delivery within 5 minutes of publication, and enrichment coverage of at least 90% of correlated alerts containing at least one TIP-sourced IOC match. Rationale: The TIP subsystem (REQ-008) and its interfaces to SIEM (IFC-003) and SOAR (IFC-009) form a critical enrichment chain — without current intelligence, SIEM correlation operates on signatures alone and SOAR playbooks lack threat context for triage prioritisation. Feed health degrades silently (expired API keys, deprecated endpoints), so proactive verification is essential.	Test	session-298, verification

Subsystem Requirements (SUB)

Other

Ref	Requirement	V&V	Tags
SUB-SUB-SIEM-001	The SIEM Engine SHALL provide an ad-hoc threat hunting query interface supporting structured and unstructured searches across all ingested telemetry types, with query response time not exceeding 30 seconds for searches spanning the full 90-day hot storage window, and SHALL support saved hunt hypotheses linked to MITRE ATT&CK technique identifiers. Rationale: Derives from SYS-SYS-DETECT-013 threat hunting requirement. 30-second query latency matches the parent requirement and is driven by analyst workflow studies showing that interactive threat hunting degrades when query round-trip exceeds 30 seconds. Saved hypothesis linkage to ATT&CK enables systematic coverage tracking across hunt campaigns.	Test	session-298
SUB-SUB-SIEM-002	The SIEM Engine SHALL implement alert suppression, deduplication, and correlation grouping to reduce raw alert volume by at least 80% before analyst presentation, maintaining a per-analyst actionable alert queue not exceeding 25 active alerts per 8-hour shift, with suppression rules configurable per detection rule and auditable for false negative review. Rationale: Derives from SYS-SYS-DETECT-014. The 25-alert-per-analyst threshold is based on cognitive load research showing SOC analyst effectiveness drops sharply above 3-4 alerts per hour. 80% reduction target reflects industry benchmarks for mature SIEM tuning. Auditability of suppression rules is critical to prevent false negatives from hiding in suppression logic.	Analysis	session-298
SUB-SUB-SIEM-003	When the SIEM Engine is unavailable or operating at degraded capacity, the SOAR Platform SHALL activate direct alert ingestion channels from the EDR, NSM, and IAM subsystems, maintaining detection capability for at least the top 50 MITRE ATT&CK techniques at a minimum 60% detection rate relative to nominal SIEM-mediated operation, with analyst notification within 2 minutes of SIEM degradation onset. Rationale: Derives from SYS-REQS-017 degraded-mode detection requirement. The 60% detection floor and top-50 ATT&CK technique scope match the parent requirement. Placing this capability in the SOAR subsystem reflects the SOAR's role as the operational workflow engine — it must be able to receive alerts even when the SIEM correlation backbone is down. The 2-minute notification threshold ensures analysts know they are operating in degraded mode.	Test	session-298

Ref	Requirement	V&V	Tags
SUB-SUB-SIEM-004	The SOC Facility Infrastructure SHALL maintain a documented disaster recovery capability including a secondary SOC site or cloud-hosted failover environment, achieving a recovery time objective of 4 hours and recovery point objective of 1 hour for all SIEM correlation data, SOAR case state, and detection rule configurations, with DR procedures tested semi-annually. Rationale: Derives from SYS-SYS-INFRA-016 disaster recovery requirement. The 4-hour RTO and 1-hour RPO match the parent requirement. Recovery must preserve SIEM correlation data, SOAR case state, and detection rules because loss of any one of these renders the SOC operationally blind (data), uncoordinated (cases), or undefended (rules). Semi-annual testing is the minimum cadence for DR validation in security-critical infrastructure.	Test	session-298

Classified Entities

Communications and Reporting Subsystem `40A57B58`

Secure communications and reporting subsystem providing internal SOC collaboration, external stakeholder notification, and regulatory reporting capabilities. Internal channels include encrypted instan

Cybersecurity Operations Centre `40A57AD9`

Enterprise-grade Security Operations Centre (SOC) providing 24/7 cyber defence for a large organisation's IT and OT infrastructure. Integrates Security Information and Event Management (SIEM), Network

Endpoint Detection and Response Subsystem `51F77B19`

Agent-based endpoint detection and response (EDR) subsystem deployed across 50,000+ Windows, Linux, and macOS endpoints including servers, workstations, and virtual machines. Agents collect process te

Identity and Access Monitoring Subsystem `41B77319`

Specialised monitoring subsystem focused on identity-based threats across the enterprise identity fabric. Integrates with Active Directory, Azure AD/Entra ID, LDAP directories, and Privileged Access M

Network Security Monitoring Subsystem `40A53219`

Passive and active network security monitoring subsystem covering 200+ network segments across enterprise LAN, WAN, DMZ, and OT networks. Deploys network TAPs and SPAN ports feeding full-packet-captur

SIEM Engine `51F77B19`

Security Information and Event Management engine serving as the central data processing backbone of the SOC. Ingests structured and unstructured log data from 50,000+ endpoints, network devices, firew

SOAR Platform `51B77B19`

Security Orchestration, Automation and Response (SOAR) platform serving as the operational workflow engine of the SOC. Executes 150+ automated playbooks for common alert types (phishing, malware detec

SOC Facility Infrastructure `DE851018`

Purpose-built physical facility housing the Security Operations Centre, designed to Tier III data centre standards for the server room and secure operations area. Includes redundant UPS and diesel gen

Threat Intelligence Platform `40F77319`

Cyber threat intelligence (CTI) aggregation and management platform that ingests, normalises, and correlates intelligence from 20+ commercial and open-source feeds (STIX/TAXII 2.1, CSV, JSON). Maintai

Vulnerability Management System `41F77B19`

Continuous vulnerability management subsystem maintaining a real-time asset inventory of all IT and OT assets (servers, endpoints, network devices, cloud instances, containers, IoT). Performs authenti

Traceability Matrix — Derivation

Source	Target	Type	Description
SUB-SUB-SIEM-004	VER-VER-METH-002	derives	SOC DR infrastructure requirement to failover verification
SUB-SUB-SIEM-001	VER-VER-METH-001	derives	SIEM threat hunting subsystem requirement to purple team verification
SUB-SUB-SIEM-003	VER-VER-METH-002	derives	SOAR degraded-mode detection requirement to SIEM failover verification
IFC-IFC-INTERNAL-003	VER-VER-METH-007	derives	TIP-to-SIEM watchlist interface to TIP enrichment verification
SUB-SUB-SIEM-008	VER-VER-METH-007	derives	TIP indicator processing subsystem requirement to feed health verification
SUB-SUB-SIEM-010	VER-VER-METH-006	derives	IAM UEBA subsystem requirement to UEBA accuracy verification
SUB-SUB-SIEM-009	VER-VER-METH-006	derives	NSM subsystem requirement to sensor coverage audit verification
IFC-IFC-INTERNAL-004	VER-VER-METH-005	derives	SOAR-to-EDR containment interface to response pipeline verification
SUB-SUB-SIEM-004	VER-VER-METH-005	derives	SOAR playbook execution subsystem requirement to response pipeline verification
SUB-SUB-SIEM-007	VER-VER-METH-005	derives	EDR containment subsystem requirement to response pipeline verification
SYS-SYS-DETECT-016	SUB-SUB-SIEM-004	derives	System-level DR requirement decomposed to facility infrastructure DR capability
SYS-SYS-DETECT-017	SUB-SUB-SIEM-003	derives	System-level degraded-mode detection decomposed to SOAR direct alert ingestion bypass
SYS-SYS-DETECT-014	SUB-SUB-SIEM-002	derives	System-level alert volume management decomposed to SIEM subsystem suppression and deduplication
SYS-SYS-DETECT-013	SUB-SUB-SIEM-001	derives	System-level threat hunting requirement decomposed to SIEM subsystem hunting query capability
SUB-SUB-SIEM-001	VER-VER-METH-001	derives	SIEM correlation subsystem requirement to purple team detection verification
SUB-SUB-SIEM-003	VER-VER-METH-004	derives	SIEM storage tier requirement to data retention compliance audit
SUB-SUB-SIEM-001	VER-VER-METH-002	derives	SIEM correlation subsystem requirement to failover verification
IFC-IFC-INTERNAL-010	VER-VER-METH-003	derives	SOAR-NSM containment interface to end-to-end integration testing
IFC-IFC-INTERNAL-009	VER-VER-METH-003	derives	TIP-SOAR enrichment interface to end-to-end integration testing
SYS-SYS-DETECT-004	SUB-SUB-SIEM-005	derives	System SOAR response automation to SOAR case management subsystem requirement
STK-STK-NEEDS-004	SYS-SYS-DETECT-018	derives	Continuous operation stakeholder need to SOC staffing and shift handover
STK-STK-NEEDS-004	SYS-SYS-DETECT-017	derives	Continuous operation stakeholder need to degraded-mode detection capability
SYS-SYS-DETECT-004	IFC-IFC-INTERNAL-010	derives	System automated response to SOAR-NSM network containment interface
SYS-SYS-DETECT-005	IFC-IFC-INTERNAL-009	derives	System intel ingestion capability to TIP-SOAR enrichment interface
SYS-SYS-DETECT-012	SUB-SUB-SIEM-013	derives	System infrastructure availability to facility physical security

Source	Target	Type	Description
SYS-SYS-DETECT-001	SUB-SUB-SIEM-006	derives	System detection capability to EDR agent telemetry collection
SYS-SYS-DETECT-009	SUB-SUB-SIEM-012	derives	System reporting SLA to Comms subsystem pipeline
SYS-SYS-DETECT-007	SUB-SUB-SIEM-011	derives	System vuln scanning to VMS prioritisation model
SYS-SYS-DETECT-011	SUB-SUB-SIEM-010	derives	System identity monitoring to IAM UEBA baselining
SYS-SYS-DETECT-010	SUB-SUB-SIEM-009	derives	System network monitoring to NSM sensor deployment
SYS-SYS-DETECT-005	SUB-SUB-SIEM-008	derives	System intel ingestion to TIP processing pipeline
SYS-SYS-DETECT-003	SUB-SUB-SIEM-007	derives	System containment SLA to EDR isolation
SYS-SYS-DETECT-004	SUB-SUB-SIEM-004	derives	System response automation to SOAR playbook engine
SYS-SYS-DETECT-006	SUB-SUB-SIEM-003	derives	System data retention to SIEM storage tier
SYS-SYS-DETECT-002	SUB-SUB-SIEM-002	derives	System ingestion capacity to SIEM normalisation pipeline
SYS-SYS-DETECT-001	SUB-SUB-SIEM-001	derives	System detection SLA to SIEM correlation module
STK-STK-NEEDS-003	SYS-SYS-DETECT-015	derives	
STK-STK-NEEDS-004	SYS-SYS-DETECT-016	derives	
STK-STK-NEEDS-001	SYS-SYS-DETECT-014	derives	
STK-STK-NEEDS-001	SYS-SYS-DETECT-013	derives	
SYS-SYS-DETECT-004	IFC-IFC-INTERNAL-008	derives	
SYS-SYS-DETECT-007	IFC-IFC-INTERNAL-007	derives	
SYS-SYS-DETECT-011	IFC-IFC-INTERNAL-006	derives	
SYS-SYS-DETECT-001	IFC-IFC-INTERNAL-002	derives	
SYS-SYS-DETECT-010	IFC-IFC-INTERNAL-005	derives	
SYS-SYS-DETECT-005	IFC-IFC-INTERNAL-003	derives	
SYS-SYS-DETECT-003	IFC-IFC-INTERNAL-004	derives	
SYS-SYS-DETECT-001	IFC-IFC-INTERNAL-001	derives	
STK-STK-NEEDS-001	SYS-SYS-DETECT-002	derives	
STK-STK-NEEDS-003	SYS-SYS-DETECT-009	derives	
STK-STK-NEEDS-008	SYS-SYS-DETECT-007	derives	
STK-STK-NEEDS-008	SYS-SYS-DETECT-002	derives	
STK-STK-NEEDS-007	SYS-SYS-DETECT-009	derives	
STK-STK-NEEDS-006	SYS-SYS-DETECT-005	derives	
STK-STK-NEEDS-005	SYS-SYS-DETECT-010	derives	
STK-STK-NEEDS-005	SYS-SYS-DETECT-007	derives	
STK-STK-NEEDS-004	SYS-SYS-DETECT-012	derives	
STK-STK-NEEDS-004	SYS-SYS-DETECT-008	derives	
STK-STK-NEEDS-003	SYS-SYS-DETECT-006	derives	
STK-STK-NEEDS-002	SYS-SYS-DETECT-004	derives	
STK-STK-NEEDS-002	SYS-SYS-DETECT-003	derives	
STK-STK-NEEDS-001	SYS-SYS-DETECT-011	derives	
STK-STK-NEEDS-001	SYS-SYS-DETECT-010	derives	

Source	Target	Type	Description
STK-STK-NEEDS-001	SYS-SYS-DETECT-001	derives	

Orphan Requirements

1 requirement(s) have no trace links (neither derivation nor verification). These should be reviewed for traceability gaps.

Ref	Text (excerpt)	Document
ARC-ARC-RAT-001	The Cybersecurity Operations Centre SHALL employ a SIEM-centric hub-and-spoke architecture where the SIEM Engine acts as	architecture-decisions