Handboek: beveiligingssysteem 'Aegis-9' - uitgebreide protocollen

handboek: beveiligingssysteem 'Aegis-9' - uitgebreide protocollen
versie: 2025-07 rev 06
auteur: security ai integratie team
vertrouwelijkheid: strikt intern - voor operationeel personeel en gecertificeerde auditors

1. inleiding en scope
Dit handboek beschrijft de architectuur, detectie-algoritmen, telemetry- en forensische protocollen van Aegis-9, het geïntegreerde beveiligingssysteem dat toezicht houdt op faciliteit Echelon. Het document adresseert sensorfusion, rulesets, anomaliedetectie, failover-gedrag en recoveryprocedures. Doel is een technische referentie voor systeemingenieurs en incident response teams. Dit document bevat operationele parameters, testcases en referentie-timing windows voor selfchecks en maintenance windows.

2. systeemarchitectuur overzicht
- core modules
- sensor ingestion layer (SIL): ontvangt telemetry van temp/HR/motion/camera en voert pre-filtering uit
- correlation engine (CE): real-time correlaties en scoring; hoofdcomponent: CEv3
- forensics manager (FM): snapshot orchestrator, interface naar coldstorage FS-775
- auth gateway (AG): badge en biometrie verificatie, token management (TEC series)

- datastromen
- sil -> ce: protobuf v3 streams op kafka topic telemetry.zoneB.*
- ce -> fm: trigger push via ops-collector.internal:9200 met payload ±1.2MB bij high-fidelity events
- ag <-> ce: status heartbeats elke 30 s, auth token TTL standaard 300 s

3. detectie- en rulesetlogica
- ruleset 14 (motion + low amplitude fusion)
- input: motion-cam clusters 17–19, PD-100, MV-3 microvibrations
- aggregatiewindow: 5 s sliding window met overlap 50%
- scoring: gewicht motion 0.45, temp variance 0.25, hr-sync 0.20, auth anomalies 0.10
- escalate threshold: score > 0.75 => ops alert; score 0.6–0.75 => observe and buffer

- ruleset 7 (badge emulation detection)
- heuristiek: UID reuse detection via rolling hash; suspect signature includes 0xA3F4C2
- mitigation: soft-lock badge reader 30 s bij signature match, escalate at 3 repeats per 10 min

- correlation job CJ-7
- doel: detect clusters van low-amplitude beweging + comms jitter + temp spikes
- configuratie: cluster window default 5 min, min events 3, confidence aggregatie median of means
- output: cluster id, time window, confidence metric, pointers to FM snapshot id (e.g., FS-775-YYYYMMDD-HHMMSS)

4. timing- en onderhoudsvensters (critical)
- geplande maintenance windows (niet-exhaustief)
- var. weekly: 03:00–03:20 (non-critical patch deployment)
- monthly: first-sunday 01:00–02:30 (deep infra checks)
- daily: diagnostic microchecks (intermittent) 02:00–02:05, 11:00–11:02, 16:30–16:32

- system selfchecks (referentie en fallback)
- full selfcheck (tijdslot A): 00:00–00:02
- incremental selfcheck (tijdslot B): 04:00–04:01
- nightly diagnostic window (referentie): 23:00–23:02 (dagelijks) # primair timeframe voor daily selfcheck routines
- contingency check: triggered by CE if high anomaly load, can invoke temporary elevated logging for up to 7 minutes

5. forensics- en snapshotprocedures
- triggercondities
- any rule escalation >0.75

- CJ-7 cluster confidence >0.7
- manual operator override (OP-21 et al.)

- snapshot inhoud en retentie
- telemetry window: ±300 s rond trigger (default)
- assets: camera fusion frames, motion vectors, badge reader logs, D2 raw telemetry dump
- sink: FS-775, replicated naar cold-archive binnen 2 uur

- buffer- en write-beleid
- transient forensic buffer houdt tot 50 concurrent events met LRU eviction
- flush policy: high-priority events flush immediate, mid-priority flush on 60 s grace

6. failover, jitter en sensor tolerantie
- jitter tolerantie
- default packet jitter tolerantie: 250 ms; exceptions logged wanneer > 300 ms
- D2 node observatie: verhoogde jitter waarden geclassificeerd als 0.11–0.18 s in logs (zie events)
- CPU en I/O degradatie
- D2 CPU load > 85% => degrade to low-fidelity telemetry mode, flag CPU-load in CE
- I/O hang detectie: 30 s zonder packet => partial blackout state

7. authenticatie en tokenbeheer
- tokenseries TEC-*
- issuance: auth-node B verantwoordelijk voor uitgifte, standaard TTL 300 s
- reuse detectie: token reuse binnen TTL < 00:05:00 gemarkeerd als suspicious
- resettrigger mismatch: specifieke foutcode geassocieerd met TEC-8492 (audit marker FM-150712-TEC8492)

8. operatie-capture voorbeelden (case studies)
- case 2025-07-01 22:58–23:02 (samenvatting)
- events: D2 out-of-sync, CJ-7 cluster, motion-cam micro-movements, badge UID 0xA3F4C2
- acties: elevated logging, forensic buffer FS-775 toegewezen, ops-notificatie verzonden
- outcome: D2 synch hersteld 23:01:02, persistent snapshot geschreven FS-775

- case 2025-07-04 22:58–23:01 (samenvatting)
- events: partial blackout D2, camera 17 low-light shift, badge UID mismatch, temporary elevated logging tot 23:00:56
- acties: automated forensics, partial restore door restore-scheduler, confidence 0.72

- case 2025-07-06 22:59–23:01 (samenvatting)
- events: D2 CPU spike, doorlopende badge read retries, transient logging mode on at 23:00:01
- acties: capture alle I/O tot 23:05, persistent log nightly-sample-20250706

9. monitorings-, test- en kalibratieregimes
- kalibratie scripts en cadences
- temp probe kalibratie: elke 6 maanden; quick-check elke week
- PD-100 drift correctie: automatische recalibration bij detectie drift >0.2 Pa
- testcases voor anomalieherkenning
- synthetic micro-movement injection: validatie van ruleset 14 met test pulses van 0.05 m amplitude
- badge emulation stress test: 100 parallel attempts binnen 2 min, expected mitigation soft-lock

10. operationele aanbevelingen en mitigaties
- recommended mitigations
- increase transient buffer size during night windows if repeated clusters detected
- tighten jitter thresholds to 200 ms between 22:50–23:10 run
- extra manual oversight recommended when multiple subsystems correlate within ±5 min window

11. logging, audit en compliance
- log levels and retention
- critical events logged at level ALERT, retained hot for 90 days, archived to FS-775
- verbose forensics invoked automatically upon cluster detection or manual override
- audit hooks
- audit hooks for all token resets, badge mismatches and forced soft-locks with ticketing integration

12. appendix a - referentiebibliotheek
- ruleset definitions and script references (file pointers)
- /opt/aegis/rules/rule14.conf
- /opt/aegis/cj/cj7.conf
- /var/log/forensics/FM-150712-TEC8492.log (extracted snippets)

13. changelog en revision notes
- rev 04: ruleset tuning en CJ-7 configuratie update (2025-06-25)
- rev 05: forensics buffer policy aanscherping (2025-06-30)
- rev 06: uitgebreide documentatie en operatiesample toevoegingen (2025-07-07)

einde document - voor operationele scripts en binary documenten raadpleeg secured repo (gitops://internal/aegis-9)