

Spécification Événements d'Audit

Schéma JSON & Taxonomie Complète — Toolbox Pentest Automatisée

Version: 1.0

Date: Janvier 2026

Auteur: Ingénieur Sécurité Opérationnelle

Client: Société de Cybersécurité Offensive

1. Schéma JSON Obligatoire

Tous les événements d'audit **DOIVENT** respecter ce schéma JSON. Chaque log est une ligne JSON valide, horodatée UTC.

Champs Obligatoires (7 champs core)

- timestamp** (string, ISO 8601 UTC) : Horodatage événement. Format strict : `2026-01-23T21:30:45Z`
- event_type** (string) : Type événement (ex: `USER_LOGIN`, `SCAN_LAUNCHED`). Voir section 2 pour liste complète.
- user_id** (string) : Identifiant utilisateur unique (ex: `alice`, `admin_01`)
- action** (string) : Description lisible action (ex: `"Connexion réussie"`, `"Scan lancé sur 192.168.1.100"`)
- resource** (string) : Ressource affectée (ex: `/scan/12345`, `/report/abc`, `/user/alice`)
- result** (string) : `SUCCESS` | `FAILURE` | `ERROR`
- severity** (string) : `CRITICAL` | `HIGH` | `MEDIUM` | `INFO` | `LOW`

Champs Optionnels (Context)

- ip_address** (string) : Source IP requête (ex: `192.168.1.50`)
- user_agent** (string) : User-Agent HTTP (ex: `Mozilla/5.0...`)
- duration_ms** (integer) : Durée exécution en millisecondes (ex: `1250`)
- details** (object) : Métadonnées supplémentaires (variable par event_type)
- error_code** (string) : Code erreur si `FAILURE/ERROR` (ex: `AUTH_FAILED`, `DB_CONNECTION_TIMEOUT`)
- correlation_id** (string) : ID requête pour traçabilité multi-systèmes

Exemple Minimal

```
{
  "timestamp": "2026-01-23T21:30:45Z",
  "event_type": "USER_LOGIN_SUCCESS",
  "user_id": "alice",
  "action": "Connexion réussie",
  "resource": "/login",
  "result": "SUCCESS",
  "severity": "INFO",
  "ip_address": "192.168.1.50"
}
```

Exemple Complet (Détails)

```
{
  "timestamp": "2026-01-23T21:35:12Z",
  "event_type": "SCAN_LAUNCHED",
  "user_id": "pentesteur_01",
  "action": "Scan Nmap lancé sur cible",
  "resource": "/scan/nmap_001",
  "result": "SUCCESS",
  "severity": "MEDIUM",
  "ip_address": "192.168.1.100",
  "user_agent": "Mozilla/5.0 (X11; Linux x86_64)",
  "duration_ms": 2500,
  "details": {
    "scan_id": "nmap_001",
    "target": "192.168.1.1",
    "scan_type": "SYN",
    "ports": "1-65535",
    "module": "nmap",
    "expected_duration": "45 minutes"
  },
  "correlation_id": "req_abc123xyz"
}
```

2. Taxonomie Événements (32 types)

Les événements sont groupés par **domaine métier**. Pour chaque domaine, indiquez le event_type exact à utiliser en logs.

2.1 Authentification & Accès (6 événements)

event_type	action (description)	severity	details
USER_LOGIN_SUCCESS	Connexion réussie	INFO	username, ip, timestamp
USER_LOGIN_FAILURE	Login échoué (mauvais mot de passe)	HIGH	username, ip, tentative_n, reason
USER_LOGIN_BLOCKED	Blocage après 5 tentatives échouées	HIGH	username, ip, locked_until
PASSWORD_CHANGED	Changement mot de passe	MEDIUM	username, changed_by (self/admin), ip
MFA_ENABLED	2FA activé sur compte	MEDIUM	username, method (TOTP/FIDO2), ip
MFA_DISABLED	2FA désactivé sur compte	HIGH	username, disabled_by, reason

2.2 Scans (8 événements)

event_type	action	severity	details
SCAN_CREATED	Nouveau scan créé	MEDIUM	scan_id, scan_name, target, module_type, created_by
SCAN_LAUNCHED	Scan lancé (exécution commence)	MEDIUM	scan_id, target, module, user, expected_duration
SCAN_IN_PROGRESS	Scan en cours	INFO	scan_id, progress_pct, elapsed_time_sec
SCAN_PAUSED	Scan mis en pause	MEDIUM	scan_id, reason, paused_by
SCAN_RESUMED	Scan repris	MEDIUM	scan_id, resumed_by, elapsed_pause_sec
SCAN_COMPLETED	Scan terminé avec succès	MEDIUM	scan_id, total_duration_sec, findings_count
SCAN_FAILED	Scan échoué (erreur exécution)	HIGH	scan_id, error_code, error_msg, failed_at_pct
SCAN_DELETED	Scan supprimé	HIGH	scan_id, deleted_by, reason

2.3 Données Sensibles Découvertes (5 événements)

event_type	action	severity	details
FINDING_LOGGED	Donnée sensible découverte pendant scan	HIGH	finding_id, type (credential/email/hash), count, scan_id, encrypted_preview
FINDING_ACCESSED	Accès donnée sensible consultée	HIGH	finding_id, user_id, access_type (view/download), duration_sec
FINDING_EXPORTED	Données sensibles exportées en rapport	HIGH	finding_id, export_format (PDF/CSV), exported_by, recipient
FINDING_DELETED	Donnée sensible supprimée	HIGH	finding_id, deleted_by, reason, retention_policy_triggered
CREDENTIAL_DECRYPTED	Credential chiffré déchiffré	CRITICAL	credential_id, decrypted_by, usage_reason, ip

2.4 Accès & Permissions (4 événements)

event_type	action	severity	details
PERMISSION_CHANGED	Rôle utilisateur modifié	HIGH	target_user, old_role, new_role, changed_by, reason
PRIVILEGED_ACCESS	Accès mode admin utilisé	HIGH	user_id, action_taken, authorized_by, approval_id
UNAUTHORIZED_ACCESS_ATTEMPT	Tentative accès ressource non autorisée	CRITICAL	user_id, target_resource, reason_denied, ip
ROLE_ESCALATION_ATTEMPT	Tentative escalade privilèges détectée	CRITICAL	user_id, current_role, target_role, method_attempted, ip

2.5 Rapports (3 événements)

event_type	action	severity	details
REPORT_GENERATED	Rapport pentest généré	MEDIUM	report_id, scan_id, format (PDF/HTML/JSON), generated_by, num_findings
REPORT_DOWNLOADED	Rapport téléchargé	MEDIUM	report_id, downloaded_by, ip, file_size_mb
REPORT_DELETED	Rapport supprimé	HIGH	report_id, deleted_by, reason

2.6 Gestion Utilisateurs (4 événements)

event_type	action	severity	details
USER_CREATED	Nouvel utilisateur créé	MEDIUM	new_user_id, role, created_by, email
USER_DELETED	Utilisateur supprimé	HIGH	deleted_user_id, deleted_by, reason, data_retention_days
USER_DISABLED	Compte utilisateur désactivé	HIGH	disabled_user_id, disabled_by, reason, reactivation_possible
USER_REACTIVATED	Compte utilisateur réactivé	MEDIUM	user_id, reactivated_by, reason

2.7 Configuration & Maintenance (4 événements)

event_type	action	severity	details
CONFIG_CHANGED	Configuration critique modifiée	HIGH	config_key, old_value, new_value, changed_by, impact
CERTIFICATE_EXPIRING	Certificat SSL bientôt expirant	CRITICAL	cert_cn, expires_in_days, renewal_date
BACKUP_COMPLETED	Sauvegarde effectuée	MEDIUM	backup_id, size_gb, duration_sec, destination
BACKUP_FAILED	Sauvegarde échouée	CRITICAL	backup_id, error_code, error_msg, retry_scheduled

2.8 Erreurs Système (2 événements)

event_type	action	severity	details
SYSTEM_ERROR	Erreur système critique	CRITICAL	service, error_code, error_msg, stack_trace (truncated)
DATABASE_ERROR	Erreur connexion/requête base de données	HIGH	query_type (SELECT/INSERT/UPDATE), error_code, affected_rows

2.9 Sécurité Infrastructure (1 événement)

event_type	action	severity	details
CONTAINER_VIOLATION	Violation sécurité Docker/conteneur détectée	CRITICAL	container_id, violation_type (privileged/root_run/secret_in_env), details

3. Règles de Sévérité

Mapping Severity par Domaine

Domaine	INFO	MEDIUM	HIGH	CRITICAL
Auth	Login réussi	MFA changes	Login failure x5	—
Scans	In-progress	Start/complete	Deletion	Failure
Données	—	—	Access/export	Credential decrypted
Permissions	—	—	Role change	Escalation attempt
Infra	—	Backup success	Config change	Cert expiring, Backup fail
Erreurs	—	—	DB error	System error

Alerting Rules (Actions SecOps)

- **CRITICAL** → Email + Escalade immédiate
- **HIGH** → Email + Dashboard alerte + Enquête dans 1h
- **MEDIUM** → Dashboard + Logs archivés
- **INFO** → Logs archivés uniquement

4. Exemples Concrets par Événement

Authentication

```
{
  "timestamp": "2026-01-23T09:15:00Z",
  "event_type": "USER_LOGIN_SUCCESS",
  "user_id": "alice",
  "action": "Connexion réussie",
  "resource": "/login",
  "result": "SUCCESS",
  "severity": "INFO",
  "ip_address": "192.168.1.50",
  "details": {
    "method": "password+totp",
    "totp_verified": true
  }
}
```

Scan Lancé

```
{
  "timestamp": "2026-01-23T10:45:30Z",
  "event_type": "SCAN_LAUNCHED",
  "user_id": "pentesteur_02",
  "action": "Scan Nmap lancé sur 10.0.1.0/24",
  "resource": "/scan/nmap_20260123_001",
  "result": "SUCCESS",
  "severity": "MEDIUM",
  "details": {
    "scan_id": "nmap_20260123_001",
    "target": "10.0.1.0/24",
    "module": "nmap",
    "flags": "-sV -sC -O",
    "expected_duration_min": 90,
    "num_hosts_estimated": 254
  }
}
```

Donnée Sensible Découverte

```
{
  "timestamp": "2026-01-23T11:20:15Z",
  "event_type": "FINDING_LOGGED",
  "user_id": "system",
  "action": "Identifiant administrateur découvert",
  "resource": "/finding/ADM_CRED_001",
  "result": "SUCCESS",
  "severity": "HIGH",
  "details": {
```

```
"finding_id": "ADM_CRED_001",
"finding_type": "credential",
"scan_id": "nmap_20260123_001",
"source_ip": "10.0.1.5",
"username": "[ENCRYPTED]",
"password": "[ENCRYPTED]",
"severity_rating": "critical",
"cvss_score": 9.2
}
}
```

Accès Données Sensibles

```
{
"timestamp": "2026-01-23T14:30:00Z",
"event_type": "FINDING_ACCESSED",
"user_id": "alice",
"action": "Consultation credential découverte",
"resource": "/finding/ADM_CRED_001",
"result": "SUCCESS",
"severity": "HIGH",
"ip_address": "192.168.1.50",
"details": {
"finding_id": "ADM_CRED_001",
"access_type": "view_decrypted",
"duration_sec": 180,
"data_sensitivity": "critical"
}
}
```

Erreur Scan

```
{
"timestamp": "2026-01-23T12:15:45Z",
"event_type": "SCAN_FAILED",
"user_id": "pentesteur_02",
"action": "Scan échoué - timeout réseau",
"resource": "/scan/nmap_20260123_001",
"result": "FAILURE",
"severity": "HIGH",
"details": {
"scan_id": "nmap_20260123_001",
"error_code": "TIMEOUT_EXCEEDED",
"error_msg": "Connexion cible perdue après 45 min",
"failed_at_pct": 65,
"retry_attempted": true,
"retry_successful": false
},
"error_code": "TIMEOUT_EXCEEDED"
}
```

5. Politique de Rétention

Log Type	En Ligne	Archive Froide	Suppression
AUTH (login/2FA)	90 jours	2 ans	Destruction physique
SCAN (lancé/complété)	90 jours	2 ans	Destruction physique
FINDING (découverte)	90 jours	2 ans + RGPD	Destruction sécurisée + masquage
ACCÈS (données sensibles)	90 jours	2 ans	Destruction physique
CONFIG/ADMIN	90 jours	2 ans	Destruction physique
ERREURS	30 jours	1 an	Destruction physique

Immuabilité obligatoire : Logs archivés = WORM (Write-Once-Read-Many), pas de modification/suppression retroactive.

6. Requêtes ELK/Graylog (Exemples)

Recherche : Tous les logins échoués (dernières 24h)

```
event_type:"USER_LOGIN_FAILURE" AND timestamp:[now-24h TO now]
```

Recherche : Accès données sensibles par utilisateur

```
(event_type:"FINDING_ACCESSED" OR event_type:"FINDING_EXPORTED")  
AND user_id:"alice"  
AND timestamp:[now-7d TO now]
```

Recherche : Tentatives escalade privilèges

```
event_type:"ROLE_ESCALATION_ATTEMPT"  
OR event_type:"UNAUTHORIZED_ACCESS_ATTEMPT"  
AND severity:"CRITICAL"
```

Recherche : Timeline incident (reconstitution)

```
correlation_id:"req_abc123xyz"  
OR user_id:"pentesteur_02"  
AND timestamp:[2026-01-23T11:00Z TO 2026-01-23T14:00Z]
```

7. Checklist Implémentation

Contrôle	Preuve	Test
Format JSON valide	Validation schema en pipeline	python -m json.tool logs.json
ISO 8601 timestamp	Exemple : 2026-01-23T21:30:45Z	date -u +%Y-%m-%dT%H:%M:%SZ
event_type existant	Logs parsing sans erreur	grep event_type logs.json \ sort -u
7 champs obligatoires présents	100% des logs contiennent tous les 7	Script validation
Pas credentials en clair	Grep "password", "api_key" → zéro résultat	grep -i "password\ secret\ token" logs.json
Severity correct	Mapping règles appliquées	Audit aléatoire 10 logs
Logs immuables	Tentative modif → échouée	Test suppression log ancien
Rétention appliquée	Logs >90j transférés archive	Vérifier /archive vs /online

8. Intégration Outils

Systemd/Syslog → JSON :

rsyslog config

```
$template JsonFormat, "{\"timestamp\":\"%timestamp:::date-rfc3339\",\"host\":\"%HOSTNAME%\",\"msg\":\"%msg%\"}\\n\"
.action(type="omfile" file="/var/log/app.json" template="JsonFormat")
```

Python Application :

```
import json, logging
from datetime import datetime, timezone

def log_event(event_type, user_id, action, result, severity, **details):
    log = {
        "timestamp": datetime.now(timezone.utc).isoformat() + "Z",
        "event_type": event_type,
        "user_id": user_id,
        "action": action,
        "result": result,
        "severity": severity,
        **details # Spread optional fields
    }
    print(json.dumps(log)) # ou vers ELK/Graylog
```