



Oiseau Rouge

Rapport d'optimisation de la détection

Pour exporter le code d'une règle, se référer au guide de création et de modification de règles.

Règles proposées par l'équipe sécurité :

- Règle 1 : Détection de la connexion d'une IP privée (par exemple un poste de travail) à une IP publique sur les ports 80/443
- Règle 2 : Détection d'une connexion interactive * réussie d'un compte de service
- Règle 3 : Détection de nombreux accès à des fichiers publics différents sur un OneDrive*
- Règle 4 : Détection de l'espace disque d'un serveur rempli à 70%
- Règle 5 : Détection d'un scan de ports provenant d'une IP non autorisée à scanner

Règles non retenues :

Règle n°1 : **Connexion d'une IP privée à une IP publique sur les ports 80/443.**

- Justification : Risque élevé de faux positifs, car ces connexions sont fréquentes dans des activités légitimes (exemple : navigation sur Internet).

Règle n°3 : **Nombreux accès à des fichiers publics sur OneDrive.**

- Justification : Difficile à calibrer sans un baselining précis. Le OneDrive est déjà conçu pour un usage intensif par les utilisateurs.

Règle n°4 : **Espace disque rempli à 70%.**

- Justification : Cette règle relève davantage de la gestion des systèmes que de la sécurité.

Règles retenues :

Règle n°2 : **Détection d'une connexion interactive réussie d'un compte de service.**

- Justification : Les connexions interactives ne devraient pas avoir lieu pour des comptes de service. Cette règle aide à repérer les abus ou compromissions.



Voici le contenu de la règle exportée au format .ndjson :

```
{
  "id": "e99b3120-bb04-11ef-83fb-bd8ed20979ed",
  "updated_at": "2024-12-15T16:52:07.177Z",
  "updated_by": "analyst",
  "created_at": "2024-12-15T16:52:05.133Z",
  "created_by": "analyst",
  "name": "Connexion interactive - Compte de service",
  "tags": [
    "service-account",
    "interactive-login",
    "security"
  ],
  "interval": "5m",
  "enabled": true,
  "description": "Détection des connexions interactives réussies de comptes de service, ce qui est une anomalie pouvant indiquer une compromission.",
  "risk_score": 5,
  "severity": "high",
  "license": "",
  "output_index": "",
  "meta": {
    "from": "1m",
    "kibana_siem_app_url": "http://127.0.0.1:5601/app/security"
  },
  "author": [],
  "false_positives": [],
  "from": "now-360s",
  "rule_id": "c6688507-f009-4723-9319-557a3a5228c6",
  "max_signals": 100,
  "risk_score_mapping": [],
  "severity_mapping": [],
  "threat": [],
  "to": "now",
  "references": [],
  "version": 1,
  "exceptions_list": [],
  "immutable": false,
  "related_integrations": [],
  "required_fields": [],
```



```
"setup": "",
"type": "threshold",
"language": "kuery",
"index": [
  "winlogbeat-*"
],
"query": "event.category: \"authentication\" AND event.type: \"start\" AND
user.name: \"svc_*/\"",
"filters": [],
"threshold": {
  "field": [
    "user.name"
  ],
  "value": 1,
  "cardinality": []
},
"throttle": "no_actions",
"actions": []
},
{
  "exported_count": 1,
  "exported_rules_count": 1,
  "missing_rules": [],
  "missing_rules_count": 0,
  "exported_exception_list_count": 0,
  "exported_exception_list_item_count": 0,
  "missing_exception_list_item_count": 0,
  "missing_exception_list_items": [],
  "missing_exception_lists": [],
  "missing_exception_lists_count": 0,
  "exported_action_connector_count": 0,
  "missing_action_connection_count": 0,
  "missing_action_connections": [],
  "excluded_action_connection_count": 0,
  "excluded_action_connections": []
}
]
```



Oiseau Rouge

elastic Find apps, content, and more.

Security Manage Rules ML job settings Add integrations

Rules

Rules Rule Monitoring

Import value lists Import rules Create new rule

Rule name, index pattern (e.g., "filebeat-*"), or MITRE ATT&CK tactic or technique (e.g., "Defense Evasion" or "TA0005") Tags Elastic rules (0) Custom rules (3) Enabled rules Disabled rules

Showing 1-3 of 3 rules Selected 0 rules Select all 3 rules Bulk actions Refresh Refresh settings

Rule	Risk score	Severity	Last run	Last response	Last updated	Enabled
Détection d'un scan de ports - IP non autorisée	80	High	58 seconds ago	Succeeded	24 minutes ago	Enabled
Multiples échecs de connexion Windows	47	Medium	22 seconds ago	Succeeded	2 hours ago	Enabled
Connexion Interactive - Compte de service	5	High	4 seconds ago	Succeeded	2 hours ago	Enabled

Rows per page: 20

127.0.0.1:5601/app/security/alerts?sourcer=(default:[idsecurity-solution-default,selectedPatterns:([alerts-security.alerts-default]))&timeline=(activeTab:query... Confirmer votre identité

Stream Soifège Sacré, fréq... Mon Wecode Dev JSON Schema Valid... InfoTrad - l'informat... Ventusky Happy Scribe: Audi... Cideo - Outils vid... Excalidraw | Hand... Nouveau dossier

elastic Find apps, content, and more.

Security Alerts ML job settings Add integrations Data view Alerts

Alerts

Open Acknowledged Closed

Updated 45 seconds ago

Summary Trend Counts Treemap

Severity levels

Levels	Count
High	2
Medium	1

3 alerts

Alerts by name

Rule name	Count
Connexion interactive - Compte de service	2
Multiples échecs de connexion Windows	1

Top alerts by

host.name

No items found

Columns 1 field sorted 3 alerts Fields

Actions	@timestamp	Rule	Severity	R.	Reason	host.name	user.name	pro...	file.name	source.ip	destination.ip
	Dec 23, 2024 @ 16:20:30.600	Multiples échecs de connexion Windows	medium	47	event by Administrator c...	—	Administrator	—	—	—	—
	Dec 23, 2024 @ 16:15:44.796	Connexion interactive - Co...	high	5	event by svc_test create...	—	svc_test	—	—	—	—

GET STARTED

Manage



Règle n°5 : **Détection d'un scan de ports provenant d'une IP non autorisée.**

- Justification : Les scans de ports sont une étape préalable aux attaques. Cette règle est essentielle pour identifier et prévenir ces tentatives.

Voici le contenu de la règle au format .ndjson :

```
[
  {
    "id": "83a78000-f423-11ef-8534-e3ff3b8d9671",
    "updated_at": "2025-02-26T12:09:23.101Z",
    "updated_by": "analyst",
    "created_at": "2025-02-26T09:24:44.664Z",
    "created_by": "analyst",
    "name": "Scan de ports - IP non autorisé",
    "tags": [
      "scan de ports",
      "détection",
      "analyse réseau",
      "sécurité"
    ],
    "interval": "5m",
    "enabled": true,
    "description": "Détection des scans de ports effectués sur les ports bien connus (1 à 1024) depuis des IP non autorisées. Les IP internes et connues sont exclues.",
    "risk_score": 73,
    "severity": "high",
    "license": "",
    "output_index": "",
    "meta": {
      "from": "1m",
      "kibana_siem_app_url": "http://127.0.0.1:5601/app/security"
    },
    "author": [],
    "false_positives": []
  }
]
```



```
"from": "now-360s",
"rule_id": "a6ce0707-ee59-4c78-9ff1-e968a0007f39",
"max_signals": 100,
"risk_score_mapping": [],
"severity_mapping": [],
"threat": [],
"to": "now",
"references": [],
"version": 9,
"exceptions_list": [],
"immutable": false,
"related_integrations": [],
"required_fields": [],
"setup": "",
"type": "threshold",
"language": "kuery",
"data_view_id": "logs-*",
"query": "source.ip: * AND NOT source.ip:(\"192.168.9.10\" OR \"192.168.10.215\")",
"filters": [],
"threshold": {
  "field": [
    "source.ip"
  ],
  "value": 20,
  "cardinality": []
},
"throttle": "no_actions",
"actions": []
},
{
  "exported_count": 1,
  "exported_rules_count": 1,
  "missing_rules": [],
  "missing_rules_count": 0,
  "exported_exception_list_count": 0,
  "exported_exception_list_item_count": 0,
  "missing_exception_list_item_count": 0,
  "missing_exception_list_items": [],
  "missing_exception_lists": [],
  "missing_exception_lists_count": 0,
  "exported_action_connector_count": 0,
  "missing_action_connection_count": 0,
```



```
"missing_action_connections": [],  
"excluded_action_connection_count": 0,  
"excluded_action_connections": []  
}  
]
```

The screenshot shows the Elastic Security console interface. The left sidebar contains navigation links for Security, Dashboards, Alerts, Findings, Timelines, Cases, Explore, and Intelligence. The main content area displays the configuration for a rule named "Scan de ports - IP non autorisé".

About

Détecte les scans de ports effectués sur les ports bien connus (1 à 1024) depuis des IP non autorisées. Les IP internes et connues sont exclues.

Severity

High

Risk score

73

Tags

scan de ports, détection, analyse réseau, sécurité

Definition

Data View

logs-*

Custom query

source.ip: "*" AND NOT source.ip:("192.168.0.0/24" OR "10.0.0.0/24")

Rule type

Threshold

Timeline template

None

Threshold

Results aggregated by source.ip >= 20

Schedule

Runs every

5m

Additional look-back time

1m

The screenshot shows the Elastic Security console interface, specifically the Alerts page. The left sidebar contains navigation links for Security, Dashboards, Alerts, Findings, Timelines, Cases, Explore, and Intelligence. The main content area displays a summary of alerts.

Alerts

Open Acknowledged Closed

Updated 10 seconds ago

Summary Trend Counts Treemap

Severity levels

Levels	Count
High	3

Alerts by name

Rule name	Count
Scan de ports - IP non autorisé	3

Top alerts by

host.name

No items found

Columns 1 field sorted 3 alerts Fields

Actions	@timestamp	Rule	Severity	Risk Score	Reason	host.name	username	process.n...	file.name	source.ip	de
	Feb 26, 2025 @ 13:14:25.814	Scan de ports - IP non auto...	High	73	event with source 10.65.50.33 created high alert Scan de ports - IP non a...	---	---	---	---	10.65.50.33	---
	Feb 26, 2025 @ 13:04:04.291	Scan de ports - IP non auto...	High	73	event with source 10.65.50.33 created high alert Scan de ports - IP non a...	---	---	---	---	10.65.50.33	---
	Feb 26, 2025 @ 13:04:04.291	Scan de ports - IP non auto...	High	73	event with source 10.65.50.33 created high alert Scan de ports - IP non a...	---	---	---	---	10.65.50.33	---



Détails sur l'infrastructure :

Le compte svc_test est un compte de service. C'est celui qui sera utilisé pour nos tests. Dans le futur, on pourra imaginer créer une liste de nos comptes de service, mais aujourd'hui cette liste n'existe pas.

Nos postes de travail utilisateurs sont sur le réseau 192.168.1.0/24.

L'IP 192.168.9.10 est un de nos outils de sécurité.

L'IP 192.168.10.215 est notre contrôleur de domaine.

*L'entreprise possède un OneDrive permettant de partager des fichiers entre collaborateurs. Ce OneDrive est accessible publiquement et les collaborateurs peuvent le synchroniser sur leur poste de travail.

***Connexions utilisateur interactives :** Connexions où un utilisateur fournit un facteur d'authentification, tel qu'un mot de passe, une réponse via une application MFA, un facteur biométrique ou un code QR.

Connexions utilisateur non interactives : Connexions établies par un client pour le compte d'un utilisateur. Ces connexions ne nécessitent ni interaction, ni facteur d'authentification de la part de l'utilisateur. L'authentification et l'autorisation se font à l'aide de jetons d'accès et d'actualisation et ne nécessitent pas que l'utilisateur entre des informations d'identification.