WEEKLY CYBER OPERATIONS SUMMARY

Cyber SOC

Cyber SOC

ISSUE	OPERATIONS WEEK 00
CADENCE	WEEKLY
HANDLING	CLIENT CONFIDENTIAL

BOTTOM LINE UP FRONT

The Cyber SOC triaged 2,310 alerts this week and opened 14 cases, three of which moved to incident response. A credential stuffing wave against the client web portal was contained within two hours. Dark web chatter about client infrastructure remained low.

2.3K
ALERTS TRIAGED

14
CASES OPENED BY ANALYSTS

38m
MEDIAN TIME TO CONTAIN

WEEKLY CYBER THREAT LEVEL

3 / 5

ELEVATED

LOW — CRITICAL

Scored on TAM-C's 1 to 5 risk method. Up one level on the portal credential stuffing wave.

01 Key cases

ACCOUNT ABUSE — HIGH

Credential stuffing on client portal

Login failures on the [redacted] customer portal spiked to 40 times baseline from a rotating proxy pool. Analysts enabled rate limits and forced resets on 212 accounts that logged in successfully.

SOURCE · ARGO NG TELEMETRY

DARK WEB — ELEVATED

VPN access offered on a forum

A broker on a [redacted] forum offered VPN access to a firm matching the client profile. The team confirmed the account was dormant, disabled it, and opened a case to review remote access logs.

SOURCE · DARK WEB FEEDS

PHISHING — MODERATE

Invoice lure aimed at finance staff

Nine finance staff received invoice emails spoofing the vendor [redacted]. Two users clicked; the linked page was blocked at the proxy, sessions were revoked, and the sender domain was sinkholed.

SOURCE · EMAIL GATEWAY

02 Cyber operations watch

INDICATOR	TREND	EXPOSURE
Credential stuffing against web portals	▲ Rising	HIGH
Access broker listings matching client	▲ Rising	ELEVATED
Invoice and payroll phishing lures	■ Steady	MODERATE
Malware detections on endpoints	▼ Easing	MODERATE

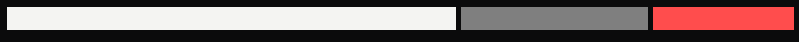
03 Analyst recommendations

01 Add bot detection and phishing-resistant MFA to the customer portal login flow.

02 Retire dormant VPN accounts older than 90 days and review remote access policy.

03 Run a short invoice fraud refresher for finance staff before quarter close.

DETECTION SOURCES THIS WEEK



Telemetry 58% · Dark web 24% · Email 18%

WHAT THE CLIENT RECEIVES

→ Analyst-staffed cyber monitoring

→ ARGO NG and dark web correlation

→ Incident response workflows

→ Weekly cyber operations summary

ILLUSTRATIVE SAMPLE. ORGANIZATIONS, ACCOUNTS AND FIGURES ARE ANONYMIZED OR REDACTED.
FULL SUMMARIES ARE DELIVERED TO CLIENTS ONLY.

OPERATIONS@TAMCINTEL.COM · +1.202.922.0068