GTMARITIME

GT IDENTIFY

Fleet Summary Report

Kestral Marine (Demo)

April 2026

1. Executive Summary

During this reporting period, GT Identify provided continuous monitoring across 9 vessels, maintaining fleet-wide visibility of both managed and unmanaged onboard IT assets.

The platform identified changes within the onboard IT environment, including the introduction of new endpoints and software requiring validation, the presence of untrusted or unclassified assets affecting governance assurance, and known software vulnerabilities mapped to publicly disclosed CVEs.

Overall asset visibility and evidence quality remain sufficient to support audit and compliance requirements. Targeted remediation actions are recommended to strengthen endpoint management coverage, improve software change control, and reduce exposure to known vulnerabilities.

Based on current asset visibility and vulnerability exposure, the fleet IT security posture for this reporting period is assessed as:

At Risk

This posture reflects whether core onboard IT controls are operating effectively at a fleet-wide level, based on observed asset visibility, management coverage, configuration change, and known vulnerability exposure during the reporting period.

Posture is At Risk due to uncontrolled change, critical vulnerability exposure, and unsupported systems.

2. Key Results

IDENTIFY

145
Managed assets inventoried

247
Untrusted assets detected

8
New endpoints detected this month

32
New software discovered this month

145
Assets Untagged

DETECT

10
Software with vulnerabilities detected

8
Software with Critical / High CVEs detected

13
Endpoints with Critical / High vulnerabilities present

PROTECT

10
Unsupported operating systems detected

RESPOND

4
Priority remediation actions

RECOVER

3. Newly Detected Endpoints

The following endpoints were detected for the first time during the reporting period. These should be reviewed to confirm legitimacy, management status and classification.

Vessel Name	Hostname	IP Address	MAC Address	Manufacturer	Managed Status	First Seen	Tagging Set
Raven	ECR.raven.local	192.168.9.14	52-54-00-CF-10-C7	Dell	Unmanaged	2025-12-29	No
Eagle	COMMS.eagle.local	192.168.12.56	E8-6A-64-FD-76-D6	Vmware inc	Unmanaged	2025-12-05	No
Hawk	MASTER.hawk.local	192.168.11.84	52-54-00-D4-9A-25	Dell	Unmanaged	2025-12-05	No
Osprey	ECR.osprey.local	192.168.10.14	9C-7B-EF-3E-36-3D	Hewlett Packard	Unmanaged	2025-12-05	No
Osprey	MASTER. osprey.local	192.168.10.99	80-E8-2C-F7-BC-B3	Hewlett Packard	Unmanaged	2025-12-05	No
Osprey	BRIDGE. osprey.local	192.168.10.37	3C-A8-2A-07-20-32	Hewlett Packard	Unmanaged	2025-12-16	No
Osprey	OFFICE. osprey.local	192.168.10.84	2C-58-B9-95-B3-DE	HP Inc.	Unmanaged	2025-12-05	No
Osprey	SERVER.osprey.local	192.168.10.98	C8-D9-D2-32-8B-39	Hewlett Packard	Unmanaged	2025-12-05	No

4. Newly Detected Software

The following software changes where detected during the reporting period. This may indicate new installations, upgrades, or software previously outside of inventory visibility.

Publisher	Software	Version	Endpoint Count	Vessel Count
Adobe Systems Incorporated	Adobe Acrobat Reader MUI	25.001.20997	4	3
CrowdStrike, Inc.	CrowdStrike Sensor Platform	7.31.20309.0	5	5
CrowdStrike, Inc.	CrowdStrike Windows Sensor	7.31.20309.0	6	6
Google LLC	Google Chrome	143.0.7499.110	2	2
Google LLC	Google Chrome	143.0.7499.170	1	1
Google LLC	Google Chrome	143.0.7499.41	1	1
Microsoft	Microsoft Teams Meeting Add-in for Microsoft Office	1.25.28902	3	3
Microsoft Corporation	Microsoft Edge	143.0.3650.80	3	3
Microsoft Corporation	Microsoft Edge	143.0.3650.96	2	2
Microsoft Corporation	Microsoft Edge WebView2 Runtime	143.0.3650.80	3	3
Microsoft Corporation	Microsoft Edge WebView2 Runtime	143.0.3650.96	2	2

5. Vulnerability and CVE Exposure Summary

Metric	Value
Total vulnerabilities detected (CVE mapped)	10
Critical / High CVEs	8
Unique endpoints affected	13

The following vulnerabilities have been identified within the fleet during the reporting period.

Publisher	Software	Version	Max CVE Score	Endpoint Count	Vessel Count
Adobe Systems Incorporated	Adobe AIR	27.0.0.124	10.0	1	1
Google LLC	Google Chrome	139.0.7258.128	9.8	1	1
Google LLC	Google Chrome	140.0.7339.128	9.8	1	1
Google LLC	Google Chrome	141.0.7390.108	8.8	1	1
Google LLC	Google Chrome	141.0.7390.76	8.8	1	1
Google LLC	Google Chrome	143.0.7499.110	8.8	1	2
Google LLC	Google Chrome	143.0.7499.170	8.8	1	1
Google LLC	Google Chrome	143.0.7499.193	8.8	2	4
Google LLC	Google Chrome	143.0.7499.41	8.8	1	1
Intel Corporation	Intel(R) Chipset Device Software	10.1.17968.8131	6.7	1	1
Intel(R) Corporation	Intel(R) Chipset Device Software	10.1.17968.8131	6.7	1	1
Microsoft	Microsoft Teams Meeting Add-in for Microsoft Office	1.24.25702	6.5	1	1
Microsoft	Microsoft Teams Meeting Add-in for Microsoft Office	1.25.18302	6.5	1	2
Microsoft	Microsoft Teams Meeting Add-in for Microsoft Office	1.25.24601	6.5	1	2
Microsoft	Microsoft Teams Meeting Add-in for Microsoft Office	1.25.28902	6.5	1	7
Microsoft Corporation	Microsoft Edge	139.0.3405.102	9.8	1	1
Microsoft Corporation	Microsoft Edge	140.0.3485.66	9.8	1	1
Microsoft Corporation	Microsoft Edge	141.0.3537.57	9.8	1	1
Microsoft Corporation	Microsoft Edge	141.0.3537.85	9.8	1	1
Microsoft Corporation	Microsoft Edge	143.0.3650.139	9.8	1	3
Microsoft Corporation	Microsoft Edge	143.0.3650.80	9.8	1	3
Microsoft Corporation	Microsoft Edge	143.0.3650.96	9.8	1	2
Microsoft Corporation	Microsoft Edge WebView2 Runtime	139.0.3405.102	9.8	1	1
Microsoft Corporation	Microsoft Edge WebView2 Runtime	140.0.3485.66	9.8	1	1
Microsoft Corporation	Microsoft Edge WebView2 Runtime	141.0.3537.57	9.8	1	1

Microsoft Corporation	Microsoft Edge WebView2 Runtime	141.0.3537.92	9.8	1	1
Microsoft Corporation	Microsoft Edge WebView2 Runtime	143.0.3650.139	9.8	1	3
Microsoft Corporation	Microsoft Edge WebView2 Runtime	143.0.3650.80	9.8	1	3
Microsoft Corporation	Microsoft Edge WebView2 Runtime	143.0.3650.96	9.8	1	2
Microsoft Corporation	Microsoft OLE DB Driver for SQL Server	18.2.3.0	7.8	1	5

6. Remedial Actions

Based on the findings from this reporting period, the following actions are recommended to maintain compliance, improve asset governance and reduce onboard cyber risk.

1. Review Newly Detected Endpoints and Untrusted Devices

- Action: Validate ownership, purpose and legitimacy of newly detected endpoints and any untrusted devices.
- Why: New and unmanaged devices can introduce uncontrolled change and reduce audit readiness.
- Outcome: Confirmed inventory accuracy and reduction of unknown device exposure.
- Recommended Next Step: Review devices flagged as "New" and "Untrusted", confirm classification and apply tagging.

2. Improve Managed Endpoint Coverage

- Action: Install GTDeploy agent on all endpoints expected to be managed.
- Why: Devices without the agent do not provide full inventory, software and service status evidence.
- Outcome: Stronger compliance evidence and improved vulnerability visibility.
- Recommended Next Step: Prioritise agent deployment on critical systems (Bridge, Communications, Admin and Navigation support devices).

3. Verify Software Changes

- Action: Review software changes and confirm approval status.
- Why: New software can introduce licensing issues, security risk or unapproved tooling.
- Outcome: Better governance over onboard application inventory and reduced risk from unknown software.
- Recommended Next Step: Confirm whether new software is expected and ensure patching / version standards are met.

4. Remediate Critical Vulnerabilities

- Action: Patch or upgrade applications affected by Critical and High severity CVEs.
- Why: Known vulnerabilities create avoidable exposure and may breach cyber control requirements.
- Outcome: Reduced vulnerability footprint and stronger cyber posture across the fleet.
- Recommended Next Step: Apply remediation priorities based on severity, asset criticality and vessel impact and track completion.