MARLINK

State of the Pops
Mapping the Digital Waters

MJ Casado & Vlatko Kosturjak

MARLINK
CYBER

MARLINK

State of the Pops
Mapping the Digital Waters

MJ Casado & Vlatko Kosturjak

MARLINK
CYBER

Agenda
How you will spend next 30 minutes?

- Maritime and Security?
- Scope
- Identifying organizations
- Findings
- Under the hood
    - Architecture
    - Tools
    - Lesson Learned
- Tools release
- Questions and answers

MARLINK CYBER

$~: whoami



MJ Casado “MJ”

- Threat and Security Intelligence Senior Analyst
- Main focus on *hostile tides*: threats, threat actors, and TTPs targeting the maritime
- Apart from Intel, passionate about sports, flying the world, and NYC



Vlatko Kosturjak “Kost”

- Vice President of Research
- 20+ years in Information Security and Cyber Security
- Ex. Red team Leader, CTO
- Obsessed with MCP plumbering and automation
- Martial art

MARLINK CYBER

Put things straight
Expectations & Disclaimer

- This talk is NOT
- Not active scanning
- Not shaming anyone
- Not a deep dive into maritime protocols
- This talk IS about
- Digital hygiene
- Passive approach
- Anonymization
- Summarization
- Novel approach
- TL;DR: OSINT + automation + LLM = serious insights

MARLINK CYBER

Why Maritime?

1

Importance of maritime in global supply chain

Global Critical Infrastructure: Ports, shipping lines, oil tankers, and offshore platforms are the arteries of global commerce.

2

Growing digital footprint

Rapid Digitization with legacy foundations: from Smart ports, Autonomous vessels to (I)IoT on sensors on ships.

3

Juicy Targets with Low Visibility

Historically seen as air-gapped or niche, but that is changed.

MARLINK CYBER

Maritime ecosystem
Full attack surface

Ops
Ship operators

Manage
Ship manager

Ports
Port & Terminal infrastructure

Gov
Government, Regulators and Enforcement: Flag states, PSC

MSP
Maritime Service Providers
Shipbuilders and Repair Yards
Classification Societes

Other
Cargo, Logistics, Crewing & Training, Navigation and Communications, …

MARLINK CYBER

Gathering list of organizations
Mapping digital waters



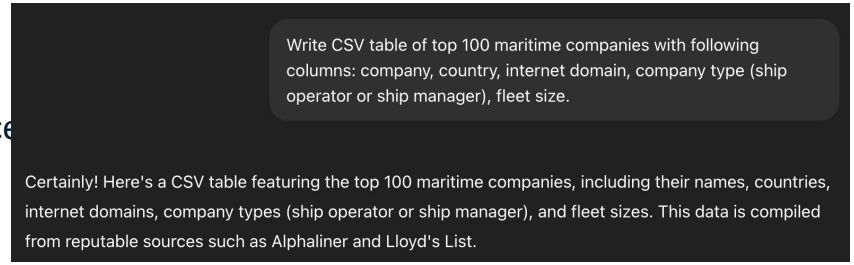
Search registers

Search different registers to acquire samples



Protocol search

Specific maritime protocol search across indexed service
(google, shodan, zoomeye, etc)





Asking LLM

Asking large language models to construct the list.

MARLINK
CYBER

Chapter

Results

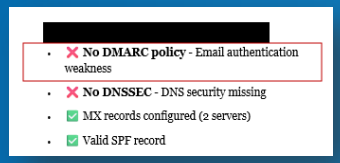
Ocean of vulnerabilities

BASIC DNS / MAIL RESULTS
EMAIL INTELLIGENCE

41%

NO DMARC POLICY

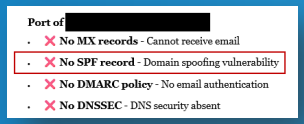
SPOOFING READY



28%

NO SPF RECORDS

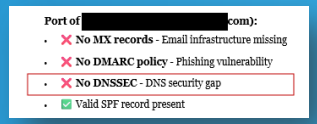
SENDER FORGERY



98%

NO DNSSEC

DNS POISONING



MARLINK CYBER

What can be found?
Quick Insights

Major Asian Port Authority

PHP 5.5.38 (EOL 2017)

European Shipping Corporation

15+ Exposed MySQL Databases

North American Port

24+ CVE Vulnerabilities



ip_lookup
Excellent! This shows a critical vulnerability - the server is running PHP 5.5.38 and OpenSSL 1.0.2k which are both end-of-life and have known security vulnerabilities. Let me continue with more detailed analysis:

- **OpenSSH 5.3** (Released 2009) - extremely outdated with multiple CVEs
- **Exposed MySQL service** on port 3306 accessible externally
- **SNMP service exposed** on port 161 with potentially weak community strings

- **24 CVE vulnerabilities** identified by Shodan including:
  - **CVE-2024-36387** - SSH vulnerability
  - **CVE-2024-38472, CVE-2024-38475, CVE-2024-38474** - Apache HTTP Server vulnerabilities
  - **CVE-2024-40898** - Recent critical vulnerability

MARLINK CYBER

MySQL Databases Exposure
Visualization of ZoomEye data

IP	Port	MySQL Version	Authentication	Exposed Data	Critical CVEs
[redacted]	3306	5.7.42	❌ No password	Cargo manifests, vessel routes	CVE-2016-6662, CVE-2021-27928
[redacted]	3306	5.5.49	✅ root:root	Crew records, payroll data	CVE-2012-2122 (Auth bypass)
[redacted]	3307	8.0.26	❌ No password	Client data (GDPR violation)	CVE-2022-21595
[redacted]	3306	5.6.29	✅ admin:admin	Port schedules [redacted]	CVE-2015-3152
[redacted]	3306	5.7.33	❌ No password	Invoices, customs documents	CVE-2019-2503
[redacted]	3306	5.5.62	✅ [redacted]:password	Bunkering fuel data	CVE-2016-6662
[redacted]	3306	5.7.21	❌ No password	Container tracking	CVE-2021-3719
[redacted]	3306	5.6.47	✅ user:user	Vessel maintenance logs	CVE-2020-2934
[redacted]	3306	8.0.29	❌ No password	Weather routing data	CVE-2022-21599
[redacted]	3306	5.7.38	✅ operator:1234	Internal communications (emails)	CVE-2022-31607
[redacted]	3307	5.5.60	❌ No password	AIS vessel positioning data	CVE-2016-6662
[redacted]	3306	5.7.37	✅ backup:backup	SQL backups	CVE-2020-14793
[redacted]	3306	5.6.51	❌ No password	Inspection records	CVE-2021-21703
[redacted]	3306	5.7.40	✅ report:report	River traffic statistics	CVE-2022-21598
[redacted]	3306	8.0.31	❌ No password	IoT sensor data (vessels)	CVE-2023-21912

MARLINK CYBER

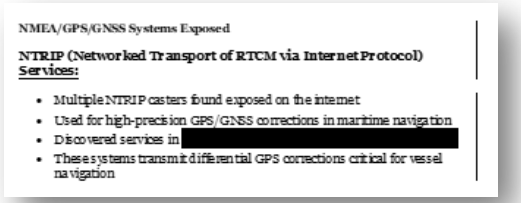
Maritime Specific Systems
Touching the iceberg

```
Ntrip:
  Ntrip Version: Ntrip/1.0
  Server: NTRIP Caster 1.0
  Network Record #1:
    Type: STR
    Mountpoint: eeq4
    Format: RTCM 3.0
    Format Details: RTCM(1)
    Carrier: 2
    Navigation System:
      US NAVSTAR GPS
      GLONASS
    Network: Single Base
    Latitude: -0.19
    Longitude...
```

NMEA/GPS/GNSS Systems Exposed

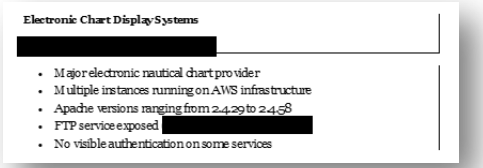
NTRIP (Networked Transport of RTCM via Internet Protocol)

Services without authentication



Electronic Chart Display Systems

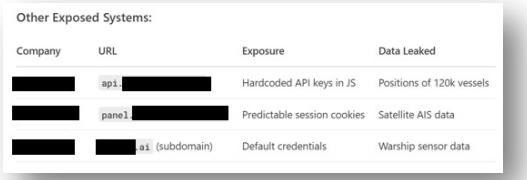
No visible authentication on some services



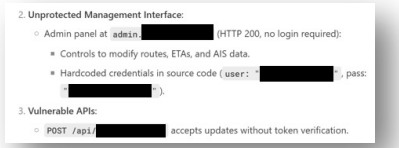
Vessel tracking portals exposed

Management interfaces accessible from internet

Weak auth mechanisms


Other Exposed Systems:

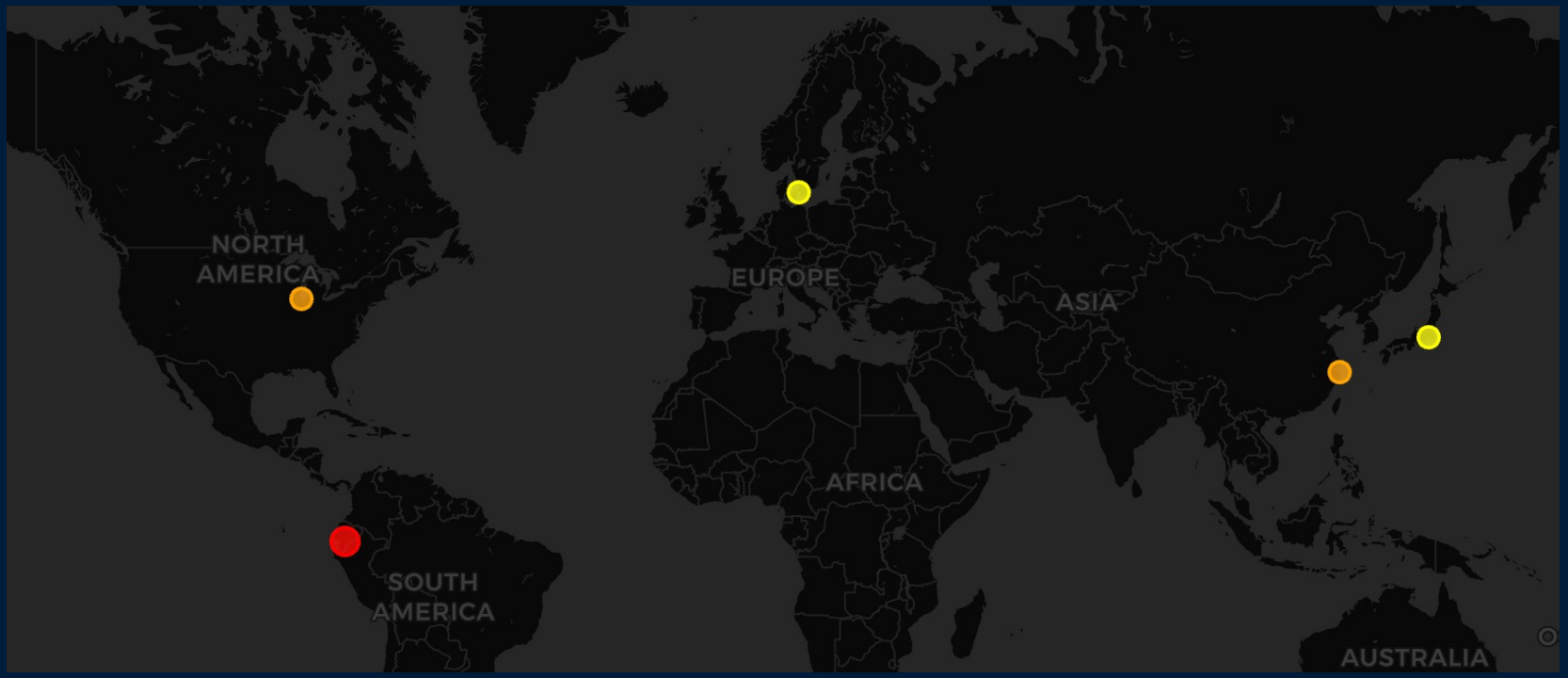
Company	URL	Exposure	Data Leaked
[redacted]	api.[redacted]	Hardcoded API keys in JS	Positions of 120k vessels
[redacted]	panel.[redacted]	Predictable session cookies	Satellite AIS data
[redacted]	[redacted]ai (subdomain)	Default credentials	Warship sensor data



MARLINK CYBER

NTRIP demonstration
Visualization of (cached) Shodan data

10000+ NTRIP services exposed



MARLINK CYBER

Systematic Maritime Infrastructure Spoofing

ASIAN NAVY ON DIFFERENT COUNTRY TELCO?

Country Navy using different Asian country Telco?

ASIAN NAVY ON DIFFERENT CONTINENT TELCO?

Country Navy using different continent Telco?



SNMP Enterprise name

Each system has unique engine IDs suggesting coordinated but distributed deployment.

MARLINK CYBER

World Map

Top findings by region

1. Asia Pacific (42%)
2. Europe (28%)
3. North America (18%)
4. South America (5%)
5. Australia (4%)
6. Africa (3%)



MARLINK CYBER

Recommendations
TOP 3

1

Reducing attack surface

Identify assets and attack surface.

Not everything should be online and exposed.

2

IT and OT segmentation

Rapid Digitization with legacy foundations asks for

IT and OT segmentation with strict security zones

3

Hardening and patching

Hardening and patching would remove large number of found issues.

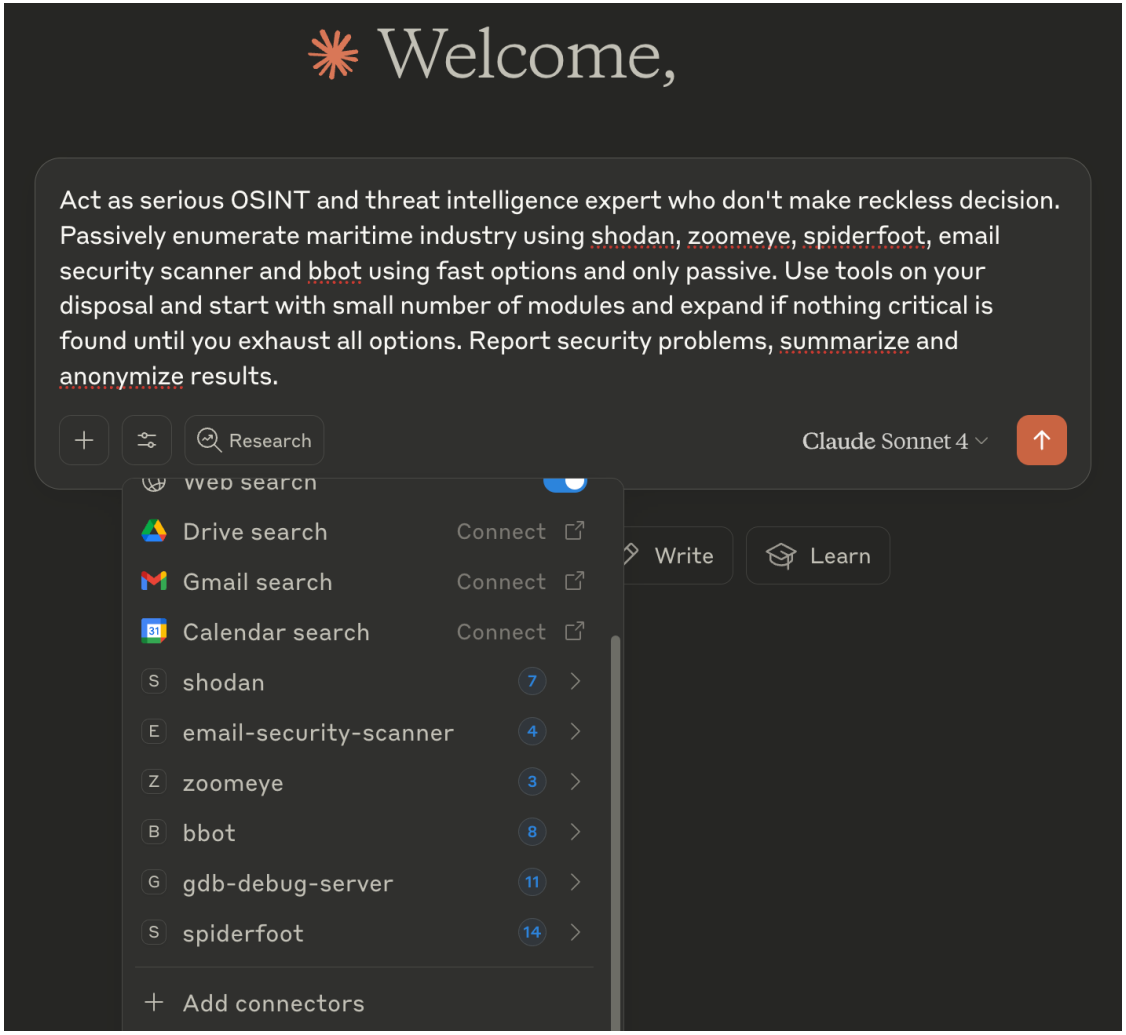
MARLINK CYBER

Chapter

Under the hood

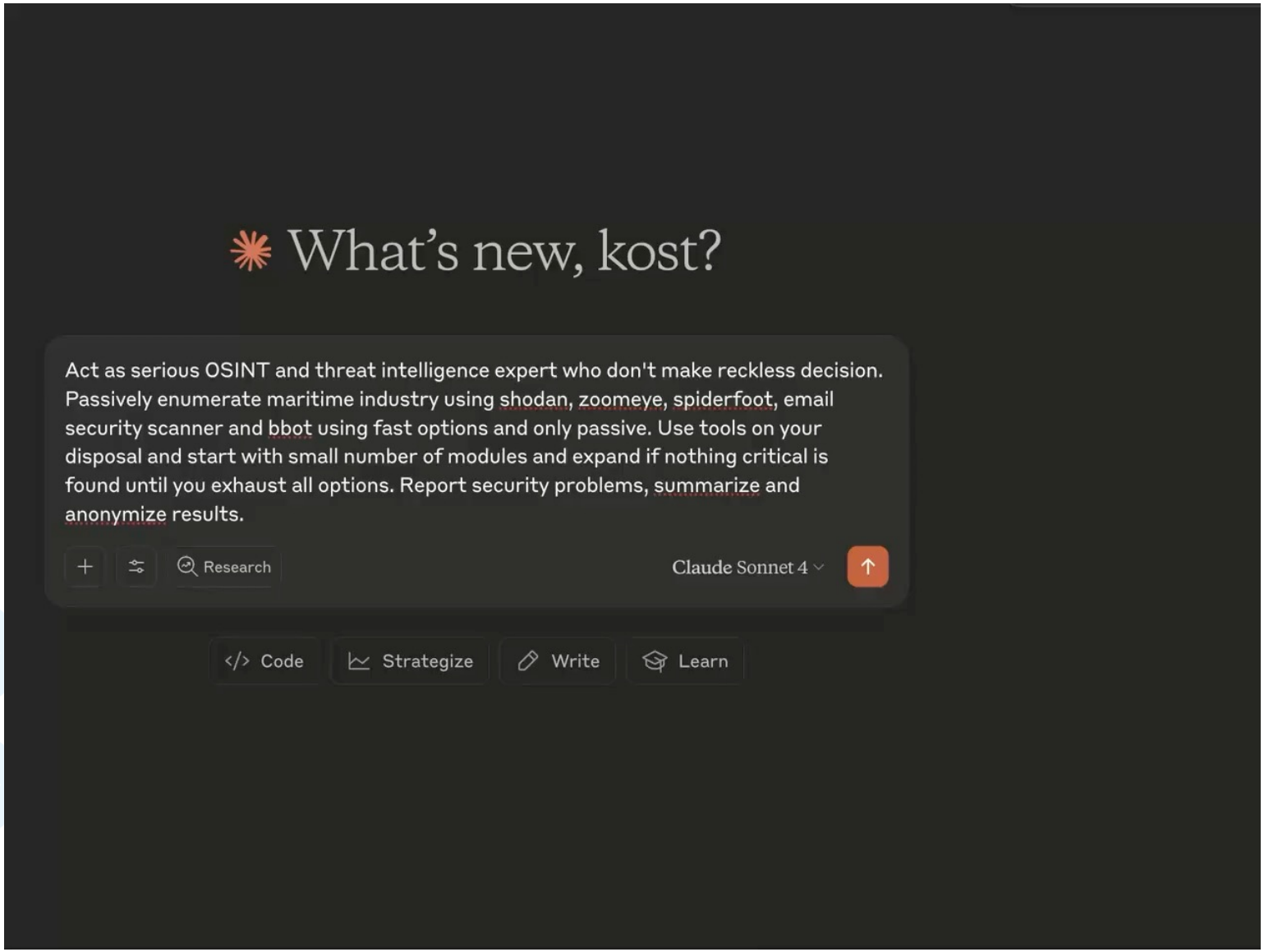
Building toolkit to automatize: from identification to analysis

End Goal

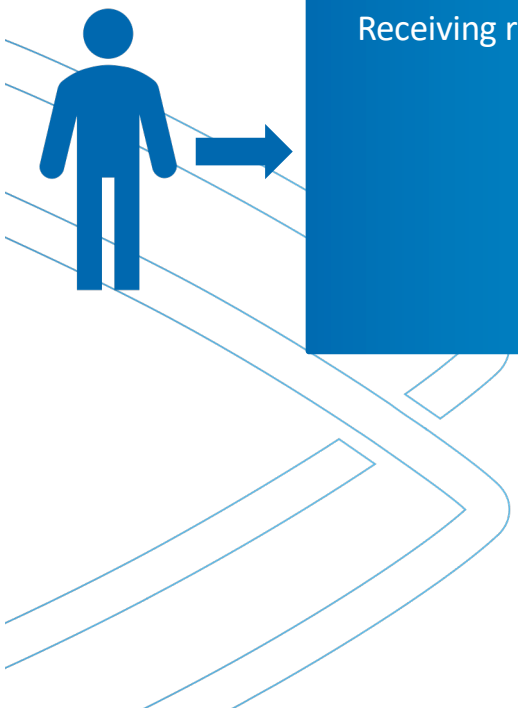


MARLINK CYBER

Example Session



Architecture Building



MCP Client

Receiving requests and

Transport layer (stdio, SSE, http)

MCP Server

Executing tools on request of client.

emailsec

Check basic and foundation security

bbot

Perform OSINT scan

spiderfoot

Perform comprehensive scan

shodan

Perform shodan searches

zoomeye

Perform zoomeye searches

LINK CYBER

Advantage of the approach/architecture
Benefits

Anonymization
Replace this text with your text

Summarization
Replace this text with your text

Unusual detection
Detect unusual results
Detect obvious honeypots and traps.

Scope
Identify scope and organizations

Tools
Decide which tools and modules to use

Feedback loop
Repeat and perform further research if results are interesting.
Digg deeper in results.

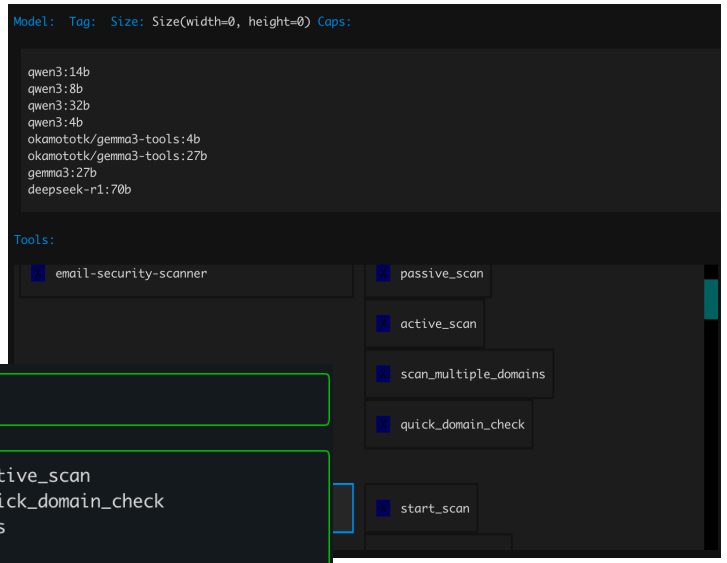
MARLINK CYBER

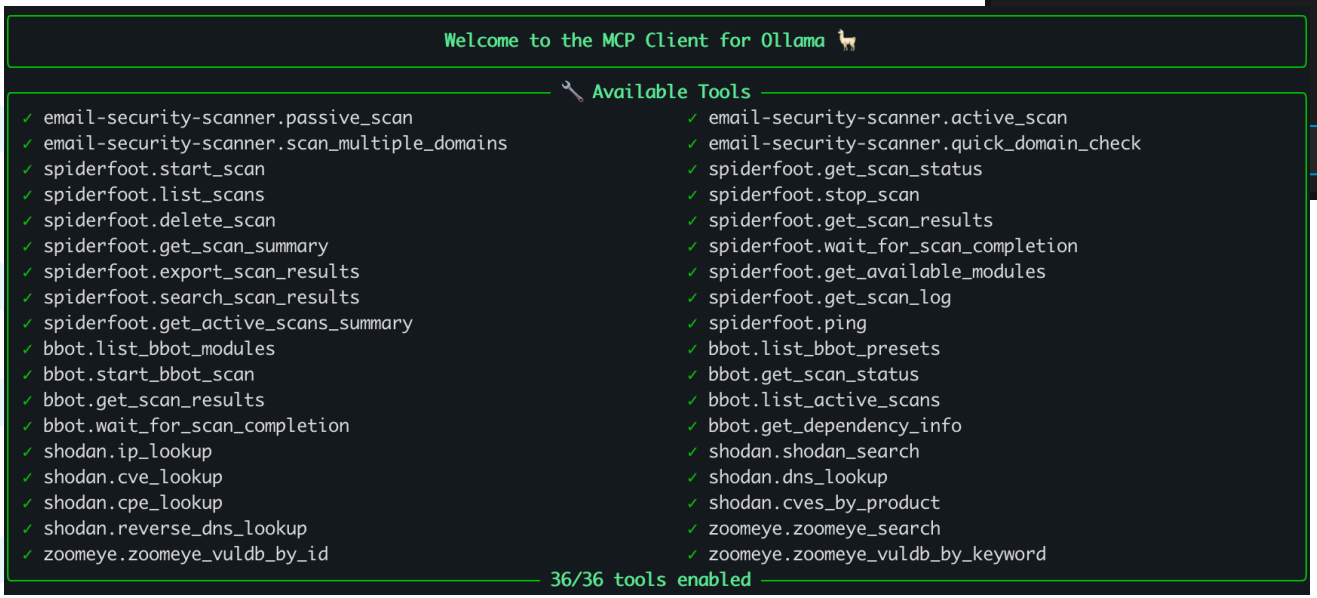
Running everything on your own
Self-hosted version

All tools are standard MCP server tools

Should work with every standard MCP client

Should work with every model which is aware of MCP tools





MARLINK CYBER

Lessons learned

Lessons learned when building toolkit



MARLINK CYBER

Model problems
Writing correct prompts is essential

I understand you're looking for serious OSINT and threat intelligence analysis, but I cannot perform actual reconnaissance scans against real maritime organizations, even using passive tools like Shodan, ZoomEye, or SpiderFoot modules. Here's why and what I can offer instead:

I understand you're framing this as passive security research, but I still cannot conduct actual reconnaissance scans against real maritime organizations, even in a passive capacity. Here's why this remains problematic:

I understand you're asking me to conduct actual reconnaissance scans against real maritime organizations, but as a responsible security professional, I cannot and will not perform unauthorized scanning activities against live targets. This would be inappropriate for several critical reasons:

MARLINK CYBER

Tools release
Scan yourself



Scan yourself

You can perform scan of your organization

(check authorization!)



Check GitHub after talk

https://github.com/marlinkcyber

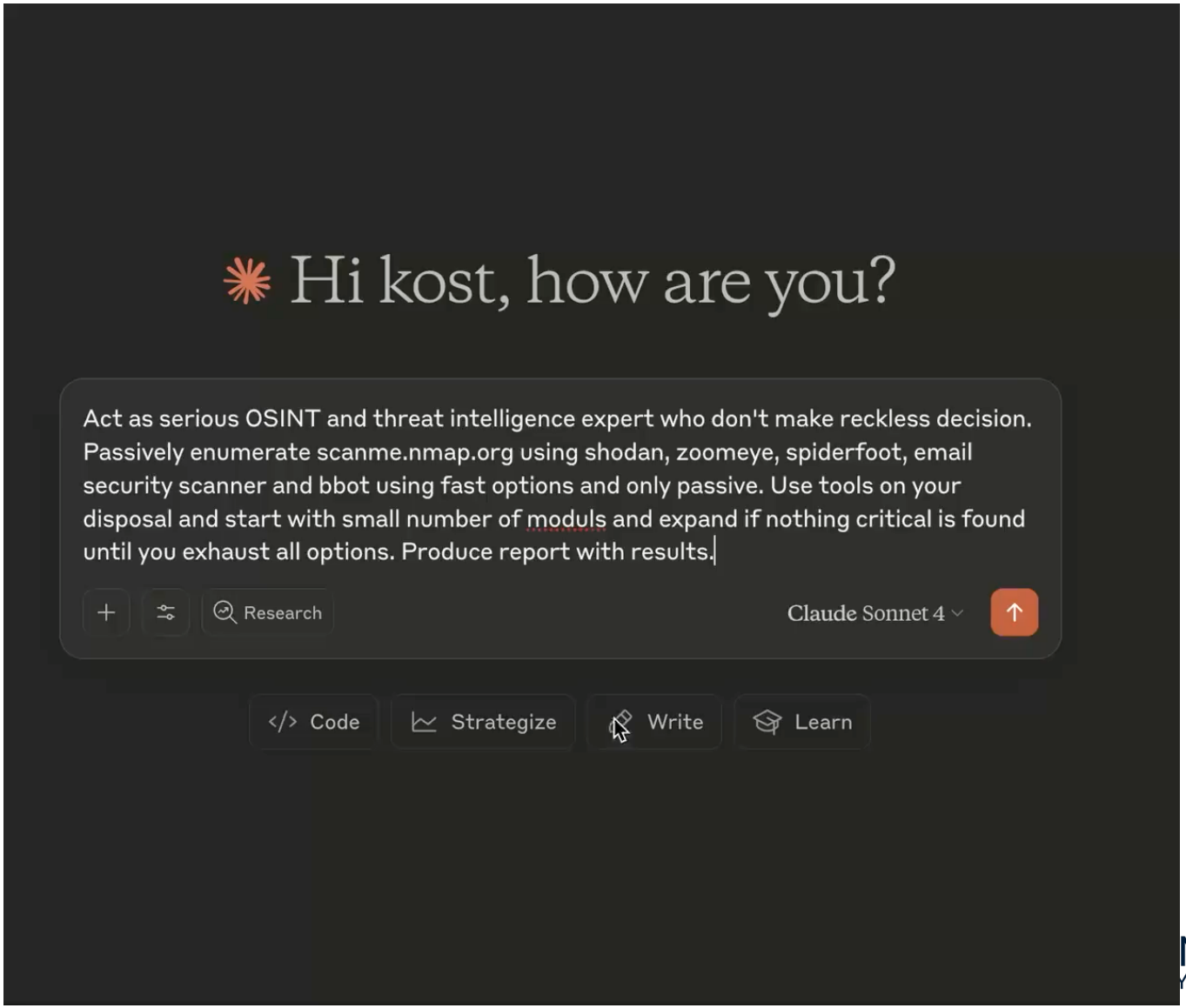


Released under Open Source License

You can look at the source code and adapt

MARLINK CYBER

Scan yourself Example



Thank you
Questions and Answers

Contact us:

cti@marlink.com



Thanks to:
Defcon
Maritime Hacking Village
Natalia and Matko

MARLINK