FIRELINKS BY PULSAR | BY PULSAR



THREAT PREVENTION, DETECTION AND RESPONSE

Every host.
Every event.
One defence.

Threat detection, file integrity, vulnerabilities, compliance and automatic response for servers, endpoints, cloud and containers, in one platform.

Endpoints | Servers | Cloud | Containers | Identity | Service desk

FIRELINKS BY PULSAR | BY PULSAR



ABOUT FIRELINKS

From first event to containment.

One platform that sees every host and acts before an attacker does.

FireLinks is the threat prevention, detection and response platform delivered and supported by Pulsar in Luanda. One agent on every server, workstation and cloud workload feeds a SIEM with thousands of detection rules mapped to MITRE ATT&CK, file integrity monitoring, vulnerability detection, CIS hardening checks and regulatory compliance reports, with automatic responses that contain an attack on detection. It runs in your data centre or is operated by Pulsar's SOC.

01

Detect

SIEM rules mapped to MITRE ATT&CK, on every host.

02

Protect

File integrity, vulnerabilities and CIS hardening checks.

03

Respond

Automatic containment and an incident timeline.

04

Prove

PCI DSS, GDPR, HIPAA, NIST and TSC evidence on demand.

11
modules in one platform

5
compliance frameworks

3
operating systems with the agent

100%
on-premises, your data



01 PLATFORM

Agents & log collection

One lightweight agent on every endpoint, every log in one place.

MODULE SCOPE

A single agent on Windows, Linux and macOS collects system and application logs, process and network inventory and security events, and ships them to the FireLinks manager over an encrypted channel. Agentless sources such as firewalls, switches and syslog devices are collected too.

WHAT YOU GET

- Agents enrolled in groups with central configuration.
- Syslog, Windows Event Log, auditd and application logs decoded out of the box.
- System inventory: packages, processes, ports, users and hardware.

BUSINESS VALUE

Complete visibility of the estate from day one, with no extra tooling on the endpoints.

WORKS WITH 02 Threat detection & SIEM · 03 File integrity monitoring · 11 Deployment & operations



02 DETECTION

Threat detection & SIEM

Thousands of rules, mapped to MITRE ATT&CK, scored by severity.

MODULE SCOPE

Events are normalised, correlated and matched against a rule set of thousands of detections, each mapped to MITRE ATT&CK tactics and techniques. Brute force, lateral movement, privilege escalation, web attacks and suspicious processes raise alerts with a severity level from 0 to 15.

WHAT YOU GET

- Rules and decoders you can extend for your own applications.
- Correlation across hosts and time windows.
- Threat intelligence lookups on IPs, hashes and domains.

BUSINESS VALUE

Attacks are seen while they happen, with the context an analyst needs to act.

WORKS WITH 08 Active response & incident handling | 10 Dashboards, reporting & threat hunting | 07 Malware & rootkit detection

03 ENDPOINT SECURITY

File integrity monitoring

Know who changed what, where and when.

MODULE SCOPE

Critical files, directories and Windows registry keys are watched in real time or on schedule. Every creation, change or deletion is recorded with the user and process responsible, the hash before and after and, when enabled, the exact difference.



WHAT YOU GET

- Real-time monitoring of system and application paths.
- Who-data: user and process behind each change.
- Alerts on unexpected binaries, web shells and configuration drift.

BUSINESS VALUE

Tampering and ransomware activity are caught at the first changed file.

WORKS WITH 07 Malware & rootkit detection | 08 Active response & incident handling | 02 Threat detection & SIEM



04 ENDPOINT SECURITY

Vulnerability detection

Every installed package checked against the CVE feeds, continuously.

MODULE SCOPE

The inventory of installed software on each agent is compared with vulnerability feeds from operating system vendors and the NVD. Each finding carries its CVE, CVSS score, affected package and the fixed version, and is closed automatically once the patch is applied.

WHAT YOU GET

- Coverage for Windows, Linux distributions and macOS packages.
- Prioritisation by CVSS and by hosts affected.
- Reports per host, per package and per severity.

BUSINESS VALUE

Patching driven by real exposure instead of guesswork.

WORKS WITH 05 Security configuration assessment | 10 Dashboards, reporting & threat hunting | 11 Deployment & operations



05 COMPLIANCE

Security configuration assessment

Hardening checked against CIS benchmarks, host by host.

MODULE SCOPE

Each agent runs configuration checks based on CIS benchmarks and Pulsar policies: password rules, services, permissions, logging, network settings. Every check reports pass or fail with the remediation, and the score per host is tracked over time.

WHAT YOU GET

- Benchmarks for Windows Server, Linux, Docker, Kubernetes and databases.
- Custom policies written in the same format.
- Remediation guidance on every failed check.

BUSINESS VALUE

Hardening becomes a measurable number instead of a one-off project.

WORKS WITH 06 Regulatory compliance | 04 Vulnerability detection | 11 Deployment & operations

06 COMPLIANCE

Regulatory compliance

PCI DSS, GDPR, HIPAA, NIST 800-53 and TSC evidence, generated by the platform.

MODULE SCOPE

Alerts and checks are tagged with the controls of PCI DSS, GDPR, HIPAA, NIST 800-53 and the Trust Services Criteria. Dashboards show coverage per framework and reports collect the evidence an auditor asks for: access control, integrity, logging and vulnerability management.



WHAT YOU GET

- Dashboards per framework and per control.
- Scheduled PDF reports for auditors and management.
- Retention of the events behind each control.

BUSINESS VALUE

Audit evidence comes from the platform, not from spreadsheets.

WORKS WITH
- 05 Security configuration assessment
- 10 Dashboards, reporting & threat hunting
- 03 File integrity monitoring



07 ENDPOINT SECURITY

Malware & rootkit detection

Signatures, behaviour and file scans on every host.

MODULE SCOPE

Rootkit checks look for hidden processes, ports and files; YARA rules and VirusTotal lookups scan new and changed files; anomalies in system calls and known malicious behaviour raise alerts. Suspicious files can be quarantined by an active response.

WHAT YOU GET

- Rootcheck for hidden processes, ports and kernel-level anomalies.
- YARA scanning of new and modified files.
- VirusTotal and threat-feed hash lookups.

BUSINESS VALUE

Malware is caught by what it does, not only by what it is called.

WORKS WITH 08 Active response & incident handling | 03 File integrity monitoring | 02 Threat detection & SIEM



08 RESPONSE

Active response & incident handling

Block, isolate or quarantine automatically, then investigate.

MODULE SCOPE

Alerts trigger automatic actions on the host: block an IP in the firewall, disable an account, kill a process, quarantine a file or isolate the endpoint. Every action is logged, reversible after a timeout and tied to the alert that caused it, with the timeline analysts need to close the incident.

WHAT YOU GET

- Built-in responses for Windows and Linux, plus your own scripts.
- Timeouts and allow-lists so responses stay safe.
- Incident timeline with the alert, the action and the analyst notes.

BUSINESS VALUE

Containment starts at detection, without waiting for someone to log in.

WORKS WITH 02 Threat detection & SIEM | 07 Malware & rootkit detection | 10 Dashboards, reporting & threat hunting

09 CLOUD

Cloud & container security

AWS, Azure, Google Cloud, Microsoft 365, Docker and Kubernetes in the same view.

MODULE SCOPE

Cloud audit trails and security services are pulled through their APIs: CloudTrail, GuardDuty, Azure Activity, Google Cloud logs, Microsoft 365 and GitHub audit. Docker and Kubernetes events, images and running containers are monitored with the same rules as hosts.



WHAT YOU GET

- Cloud configuration checks against CIS benchmarks.
- Container runtime events and image inventory.
- Identity events: logins, privilege changes, key creation.

BUSINESS VALUE

One rule set and one dashboard for on-premises, cloud and containers.

WORKS WITH 02 Threat detection & SIEM · 05 Security configuration assessment · 10 Dashboards, reporting & threat hunting

Full-text
SEARCH

PDF
REPORTS



10 VISIBILITY

Dashboards, reporting & threat hunting

Every event searchable; every indicator on a board.

MODULE SCOPE

The FireLinks dashboard shows alerts by severity, host, rule and MITRE technique, with drill-down to the raw event. Analysts search months of events, build their own boards and schedule reports; management receives weekly summaries.

WHAT YOU GET

- Pre-built boards for security events, integrity, vulnerabilities and compliance.
- Full-text search over the retained events.
- Scheduled PDF reports and alert routing by email, Slack or ticket.

BUSINESS VALUE

Decisions on facts the whole team can see and query.

WORKS WITH 02 Threat detection & SIEM | 06 Regulatory compliance | 08 Active response & incident handling



11 PLATFORM

Deployment & operations

In your data centre or run by Pulsar's SOC.

MODULE SCOPE

FireLinks runs on premises on one node or as a high-availability cluster, with the indexer sized to your retention. Pulsar installs it, keeps rules and feeds up to date, and can operate it from its SOC. Data never leaves your network unless you decide it should.

WHAT YOU GET

- Single node or cluster with indexer replication.
- Role-based access, single sign-on and API for integrations.
- Updates, rule feeds and backups handled by Pulsar.

BUSINESS VALUE

Enterprise-grade monitoring with the operating burden where you want it.

WORKS WITH 01 Agents & log collection | 10 Dashboards, reporting & threat hunting | 08 Active response & incident handling

FROM KICK-OFF TO FIRST ALERT

Delivery with clear criteria.

01 Discover

Assets, operating systems, cloud accounts, log sources and compliance goals.

02 Deploy

Manager, indexer and dashboard installed; agents enrolled by group.

03 Tune

Rules, integrity policies, vulnerability feeds and active responses adjusted.

04 Operate

Dashboards, reports and alert routing handed to your SOC or to Pulsar.

DEPLOYMENT OPTIONS

On-premises

Manager, indexer and dashboard in your data centre. Events, alerts and evidence never leave your network.

Pulsar SOC

Installed on premises and monitored by Pulsar analysts.

Hybrid

Platform on premises, rules and feeds maintained by Pulsar, your team on the dashboard.

Licensing by monitored agent. Project, subscription or managed SOC service: the model and indicators are defined in the proposal.

DELIVERED WITH

Agents deployed

Agents on servers, workstations and cloud workloads, enrolled and reporting.

Rules tuned

Detection rules, integrity policies and compliance checks adjusted to your estate.

Training

SOC analysts and administrators, in Portuguese.

Support agreement

Rule updates, platform updates and a named Pulsar contact.

MODULE MAP

11 modules. One defence.

01	Agents & log collection PLATFORM	03
02	Threat detection & SIEM DETECTION	04
03	File integrity monitoring ENDPOINT SECURITY	05
04	Vulnerability detection ENDPOINT SECURITY	06
05	Security configuration assessment COMPLIANCE	07
06	Regulatory compliance COMPLIANCE	08
07	Malware & rootkit detection ENDPOINT SECURITY	09
08	Active response & incident handling RESPONSE	10
09	Cloud & container security CLOUD	11
10	Dashboards, reporting & threat hunting VISIBILITY	12
11	Deployment & operations PLATFORM	13

COVERAGE

Endpoints | Servers | Cloud | Containers | Identity | Service desk

LET'S TALK

Your next line of defence starts here.

Book a demonstration. We will enrol agents on your servers, run the first hardening checks and show you the alerts in one session.

EMAIL
info@isoft.ao

PHONE
+244 937 777 777

WEBSITE
https://isoft.ao

www.isoft.ao Request a demo

APP

FIRELINKS BY PULSAR

Avenida Comandante Gika, n.º 114, Alvalade
Luanda, Angola