AIRBUS

The Airbus Method: Transforming vulnerability noise into actionable intelligence

```
$ ./pipeline.py --input CVE-2025-53521 --mode demo
Continue ? (Y/n)_
```

Jérémy RICHARD & Paul VARGAS & Bertrand LECONTE & Eric CAUSSIN

Airbus · THCon 2026

—[AGENDA]—

AIRBUS

Flight Plan

03 | The team — Airbus
04 | Maintain Security Condition — Scope
05 | From scan to report — Architecture
06 | The real problem — Problem statement
07 | Plug & Play, Zero Friction — Workflow
08 | Day 0 — The CVE is born — Running thread 1/5
09 | Enrichment — Running thread 2/5
10 | Score contextualisation — Running thread 3/5
11 | Context is King — Contextualisation
12 | ThreatLevel — Running thread 4/5
13 | The reality test — Comparison
14 | Your Mileage May Vary — Configuration
15 | Pipeline output — Running thread 5/5
16 | The core of prioritization — Summary

AIRBUS

The Team

BL

Bertrand LECONTE

Airbus

Product Security Senior Expert

AIRBUS

EC

Eric CAUSSIN

Airbus

MCS Technical Team Leader

AIRBUS

PV

Paul VARGAS

Ferchau

Cybersecurity Engineer, Tech Lead

FERCHAU

JR

Jérémy RICHARD

Neverhack

Cybersecurity Engineer, Tech Lead

NEVERHACK

——[SCOPE]——

Maintain Security Condition

AIRBUS

01

Vulnerability Management

Detection, prioritization and tracking of CVEs affecting our systems.

presentation scope

02

Obsolescence Management

Lifecycle management of components and end-of-support tracking.

03

Audit & Pentest Management

Penetration testing and audit campaigns.

04

Incident Management

Response to security incidents.

05

Change Management

Validation, tracking of security-impacting changes and secure updates.

From Scan to Report

AIRBUS

01

Scan Pipeline

Architecture Dossier · Network scanners · Host agents · Ansible playbooks · Cyberwatch matching

→

02

Analysis Pipeline

Enrichment · Scoring · Prioritization · Threat level · Report generation

→

03

Processing

Decisions · Tickets · Remediation · Follow-up

Report
(Presentation scope)

Decisions

—[CONTEXT]—

The problem isn't the vuln.

AIRBUS

50 000 CVEs — NVD 2025

50 000 CVEs → matched against inventory (SBOM · Cyberwatch)

~2 500 CVEs → actually affect our systems

—[CLASSIC WORKFLOW — PER CVE]—

├─ Analyst review	~2h
├─ Ticket, decision and severity assessed	~4h
├─ Patch / mitigation / quarantine planned	~2 days
├─ Management approval, scheduling	~1 week
└─ Ticket resolution	???

× 1 250 CVEs/year. Workflow clearly improvable.

How do we automate CVE prioritization?

AIRBUS

Plug & Play, Zero Friction

from raw CVE to actionable report — zero human in the critical loop

— SCAN PIPELINE —

A routine that already cuts 95% of the noise.
5% go through analysis

— ANALYSIS PIPELINE —

Zero human intervention in the loop
Fully autonomous pipeline ***(internal SaaS + CI/CD)***.

AIRBUS

Day 0 — The CVE is born

—— CVE-2025-53521 ——

CVSS Base	**9.8**
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Product	F5 BIG-IP APM
CWE	CWE-121
Published	2025-10-14 — TODAY

—[WHAT WE KNOW]—

- ✓ A CVE number
- ✓ CVSS 9.8 — critical on paper
- ✓ Network, no auth, full impact
- ? Is there an exploit?
- ? Is it exploited IRL?
- ? Is our server reachable?

> 9.8 network, no auth: **panic**. But is it **really** urgent?

CVE-2025-53521
raw

AIRBUS

Enrichment — Who are you really?

1. CWE / CAPEC | 2. Exploits | 3. References

src/processing/enrichment.py ⏮ 4 / 4 ⏭

```python
def enrich_cve_row(row, exploits_data,
                   cwes_data, capec_data):
    cve_id = row["CVE Code"]
    # Step 1: CWE / CAPEC
    cwe_key = extract_cwe_id(row["CWE"])
    cwe_info = cwes_data.get(cwe_key, {})
    capec_ids = cwe_info.get("Related_Attack_Patterns", [])
    # Step 2: Exploits
    exploits = lookup_exploits_for_cve(cve_id, exploits_data)
    # Step 3: References
    cisa_hit = cve_id in cisa_cve_set
    certfr_refs = get_certfr_refs(cve_id)
    return pd.Series({
        "CWE Name":   cwe_info.get("Name"),
        "CAPEC IDs":  capec_ids,
        "Exploits":   exploits,
        "CISA_KEV":   cisa_hit,
        "CertFR":     certfr_refs,
    })
```

cve_id="CVE-2025-53521"

cwe_key="CWE-121"

cwe_info=
{Name: "Stack Buffer Overflow"}

capec_ids=["CAPEC-100"]

exploits=
[{id:"none", maturity:"functional"}]

cisa_hit=True

cisa_due="2026-04-17"

certfr_refs="ALE-2026-XXXX"

// OUTPUT

CWE-121 → Stack Buffer Overflow

ExploitDB #none — functional RCE

CISA KEV — active exploitation

CERT-FR ALE — active French alert

→ return pd.Series({5 keys})

CALL STACK enrich_cve_row() ← enrich_dataframes() ← ReportGenerator.compute()

CVE-2025-53521

enriched

Score Contextualisation

AIRBUS

V3 COMPUTED

Base (NVD)	9.8
Computed	5.9

AV:N/AC:L/PR:N/UI:N
/S:U/C:H/I:H/A:H
+ E:F/RL:O/RC:C
+ MAV:A/MAC:H/MPR:L
+ CR:M/IR:H/AR:H

—— CVSS V3.1 — base (NVD) ——

```
base = "AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H"
CVSS3(base).scores()[0]  # → 9.8
```

—— get_temporals_vectors() ——

```
temporal = join_vectors(base, "E:F/RL:O/RC:C")
CVSS3(temporal).scores()[1]  # → 9.1
```

—— get_surface_vectors() — env. mitigations ——

```
surface  = "/MAV:A"  # AV:N → A  (Adjacent behind a FW)
surface += "/MAC:H"  # AC:L → H  (segmented network)
surface += "/MPR:L"  # PR:N → L  (auth required)
```

—— domain_vectors — business weighting ——

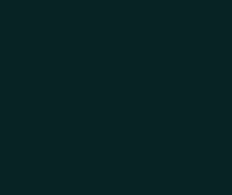
```
domain = "/CR:M/IR:H/AR:H"  # perimeter requirements
full   = join_vectors(base, temporal, surface, domain)
CVSS3(full).scores()[-1]  # → 5.9
```

CVE-2025-53521
scored

AIRBUS

Context is King

—— LB-DMZ-01 ——



Base (NVD)	9.8
Computed	5.9

lb-dmz-01

Network	**DMZ — adjacent**
Max Attack Vector	Adjacent (MAV:A)
Min Privileges	Low (MPR:L)

—— LB-PROD-EXT-01 ——

Base (NVD)	9.8
Computed	9.8

lb-prod-ext-01

Network	WAN — Internet-exposed
Max Attack Vector	Network (AV:N)
Min Privileges	None (PR:N)

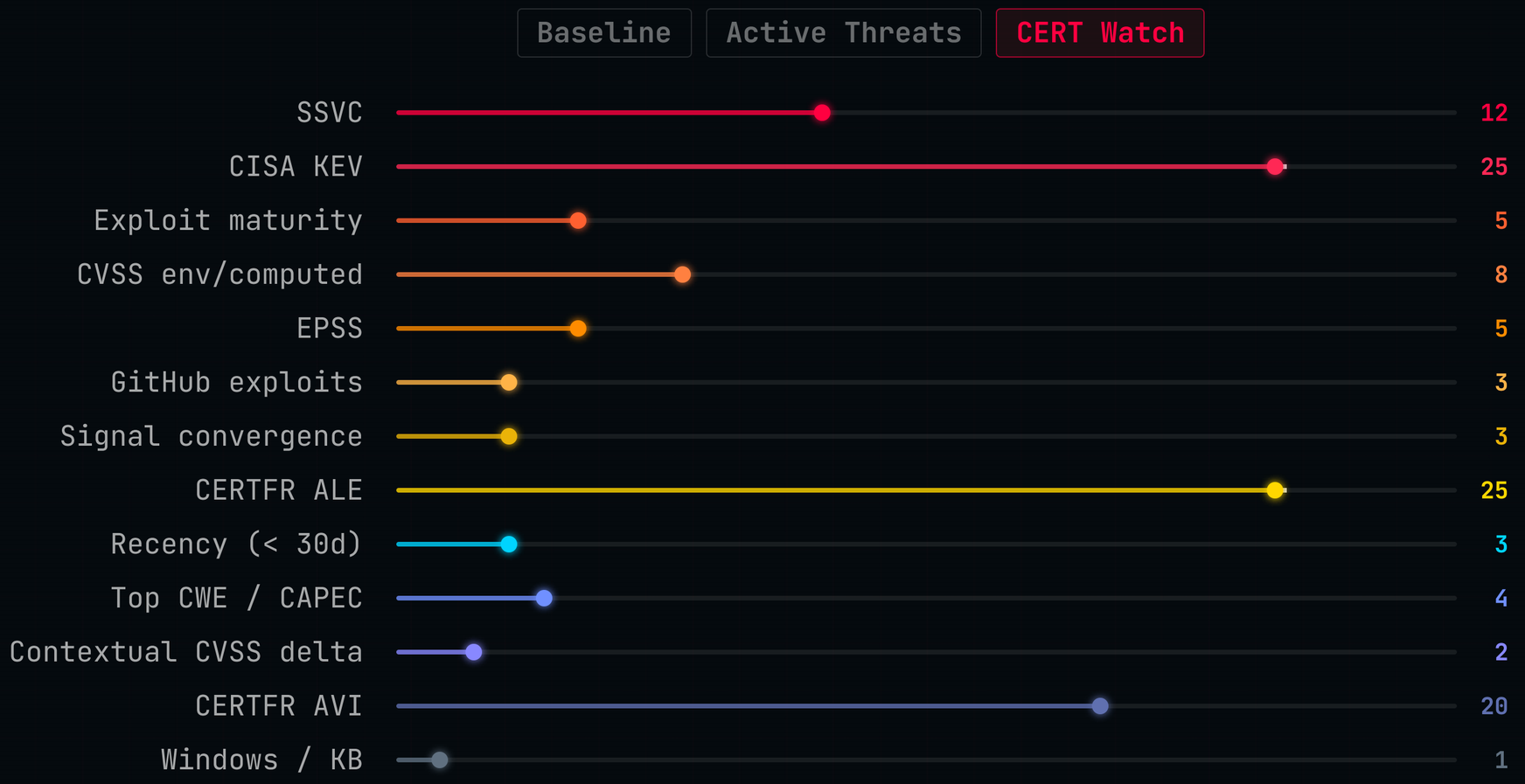
Same CVE-2025-53521 · Same BIG-IP APM · Same pipeline · **5.9** vs 9.8 · The network zone changes everything.

CVE-2025-53521
scored

AIRBUS

ThreatLevel — composite scoring

Adjust weights · add your sources · the score adapts to your context



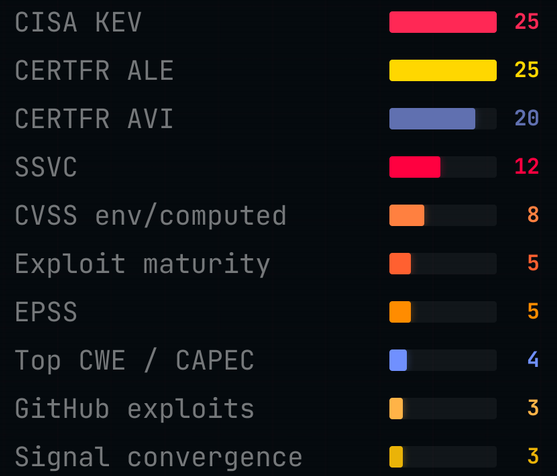
Theoretical max

116

pts

→ capped at 100 by min()

— TOP SIGNALS —



13 signals · 13 active

AIRBUS

The Reality Test

— CVE-2025-53521 (F5 BIG-IP APM) —

Base CVSS **9.8** CRITICAL — computed → 5.9

✓	SSVC	Active · Auto…	+25
✓	CISA KEV	2026-03-26	+18
✓	Exploit maturity	PoC (mat. 2)	+10
✓	CVSS env/computed	5.9 ↓ (surfac…	+5
✓	EPSS	19%	+2
✗	GitHub exploits	0 public PoC	—
✓	Convergence	2 strong sign…	+2
✗	CERTFR ALE	not published	—
✗	Recency (<30d)	>90d	—
✓	Top CWE / CAPEC	Capec-100	+4
✗	Delta CVSS	computed < ba…	—
✓	CERTFR AVI	2025-AVI-0886	+3
✗	Windows / KB		—

ThreatLevel **69** /100

— CVE-2025-58034 (FORTINET) —

Base CVSS **7.2** HIGH — computed → 7.7 ↑

✓	SSVC	Active · No a…	+20
✓	CISA KEV	2025-11-17	+18
✓	Exploit maturity	Weaponized (m…	+15
✓	CVSS env/computed	7.7 ↑ (env am…	+7
✓	EPSS	51%	+2
✓	GitHub exploits	4 PoCs	+2
✓	Convergence	4 strong sign…	+5
✗	CERTFR ALE	not published	—
✗	Recency (<30d)	>90d	—
✓	Top CWE / CAPEC	CWE-78 (cmd i…	+4
✓	Delta CVSS	+0.5 env > ba…	+1
✓	CERTFR AVI	2025-AVI-1023	+3
✗	Windows / KB		—

ThreatLevel **77** /100

Base CVSS **9.8** vs **7.2** · ThreatLevel **65** vs **73** → **Priority inversion**

—[CONFIGURATION]—

AIRBUS

Customisation

Same CVE. Four teams. Four decisions.

PROD Critical Production

Critical assets in production — zero tolerance

CISA KEV · SSVC · Exploit mat. · CVSS env

ThreatLevel P1 87

DEV Active Development

No env context yet — reduced signals

CVSS base · EPSS · CISA KEV

ThreatLevel P4 52

CI/CD Release Candidate

Pre-release — exploit maturity is critical

Exploit mat. · SSVC · Delta CVSS · GitHub

ThreatLevel P2 71

SOC SOC / Threat Intel

Watch mode — real-time signals

EPSS · Recency · Convergence · CERTFR ALE

ThreatLevel P2 64

CVE-2025-53521
contextualizing

AIRBUS

Pipeline output

——[CVE REPORT — DETAILED ANALYSIS]——

ASSET	CVE	PRODUCT	BASE	COMP.	EPSS	EXPLOIT	PATCH	PRIORITY
fw-core-01	**CVE-2025-58034**	FortiOS	7.2	7.7↑	51%	Weaponized	*in progress…*	[P1 — CRITICAL]
lb-prod-ext	**CVE-2025-53521**	F5 BIG-IP APM	9.3	9.3	19%	CISA KEV	v17.1.2.1	[P1 — CRITICAL]
lb-dmz-01	**CVE-2025-53521**	F5 BIG-IP APM	9.3	5.9↓	19%	CISA KEV	v17.1.2.1	[P2 — CRITICAL]
lb-prod-ext	**CVE-2026-31431**	Linux Kernel	8.1	7.8	34%	PoC	6.12.31	[P2 — CRITICAL]
lb-dmz-01	CVE-2026-31431	Linux Kernel	8.1	5.2↓	34%	PoC	6.12.31	[P3 — HIGH]
wks-linux-12	CVE-2026-31431	Linux Kernel	8.1	3.9↓	34%	PoC	6.12.31	[P4 — HIGH]
app-srv-03	CVE-2021-44228	Apache Log4j	10.0	7.4	2%	#46805	v2.17.2	[P3 — HIGH]
wks-lan	CVE-2025-99999	Chrome Browser	7.2	7.2	31%	N/A	*pending*	[P7 — MEDIUM]

Sorted by **ThreatLevel**, not CVSS — FortiOS 7.2 above BIG-IP 9.3. Zone and exploit maturity make the difference.

CVE-2025-53521
prioritized

The core of prioritization

—— SOVEREIGNTY · FULL AUTOMATION ——

- European Cyberwatch + internal scripts.
- **Internal SaaS + CI/CD** — zero human intervention in the loop.
- One-click report — accessible to every team, zero friction.
- Autonomous, reproducible, scalable pipeline.
- **6 months ahead** of SSVC at time of implementation.

SOVEREIGNTY
INTEGRATION
ACCESSIBILITY
AUTONOMY

ENRICHISSEMENT

CISA · CERT-FR · EPSS · ExploitDB · MITRE

Cross-referencing, not cherry-picking.

CONTEXTUALISATION

A 9.8 can become 5.9. A 5.9 can be P1.

Raw CVSS means nothing without context.

LEVELING

Active threats always go first.

No drowning in weak signals.

AIRBUS

Report generated

```
$ ./pipeline.py --status CVE-2025-53521
→ [P1] Immediate action. Isolation recommended.
```

Thanks for listening

Jérémy RICHARD & Paul VARGAS & Bertrand LECONTE & Eric CAUSSIN