We need fewer heroes: prioritize vulnerabilities using observability data

April 2024

DATADOG

Jb Aviat

Security Geek

Staff engineer at **Datadog**

Sqreen CTO & co-founder

Acquired by Datadog in 2021

Previously:

- Pentester
- Reverse Engineer @Apple
- Sqreen CTO & co-founder

I'm 🇫🇷 but I don't eat 🧀

Taken 10 years ago,
I know

DATADOG

Nobody cares about vulnerabilities (*rightfully!*)

People care about ***risk***.

Fixing vulnerabilities ***doesn't increase the value*** you provide to your customers.

But ***reducing risk*** is the baseline to keep customers data safe.

Remediate vulnerabilities with a huge risk

You’re a bank.

Let’s see systems with different characteristics…

- The customer facing API for the mobile app that receives wire orders
- The customer facing API to get an account’s balance
- The bank facing system that trigger wires
- A marketing landing page

Fix vulnerabilities that put you at risk

It can bring your systems down

→ customers can’t use their credit card

It can leak data

→ leak customer’s account balance and transactions

It can tamper with your systems or data

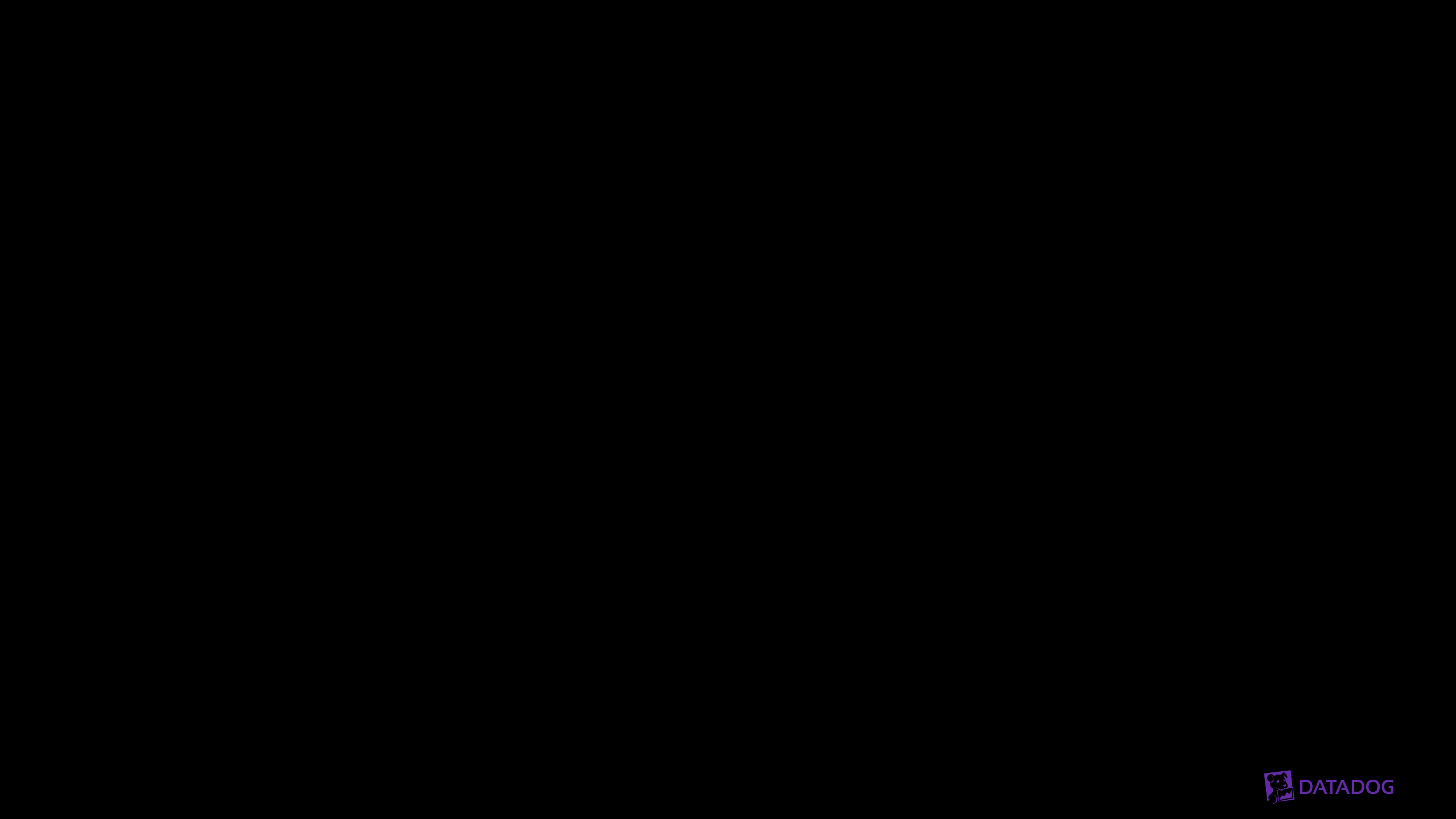
→ attackers can trigger unauthorized wires

Fix vulnerabilities that put you at risk

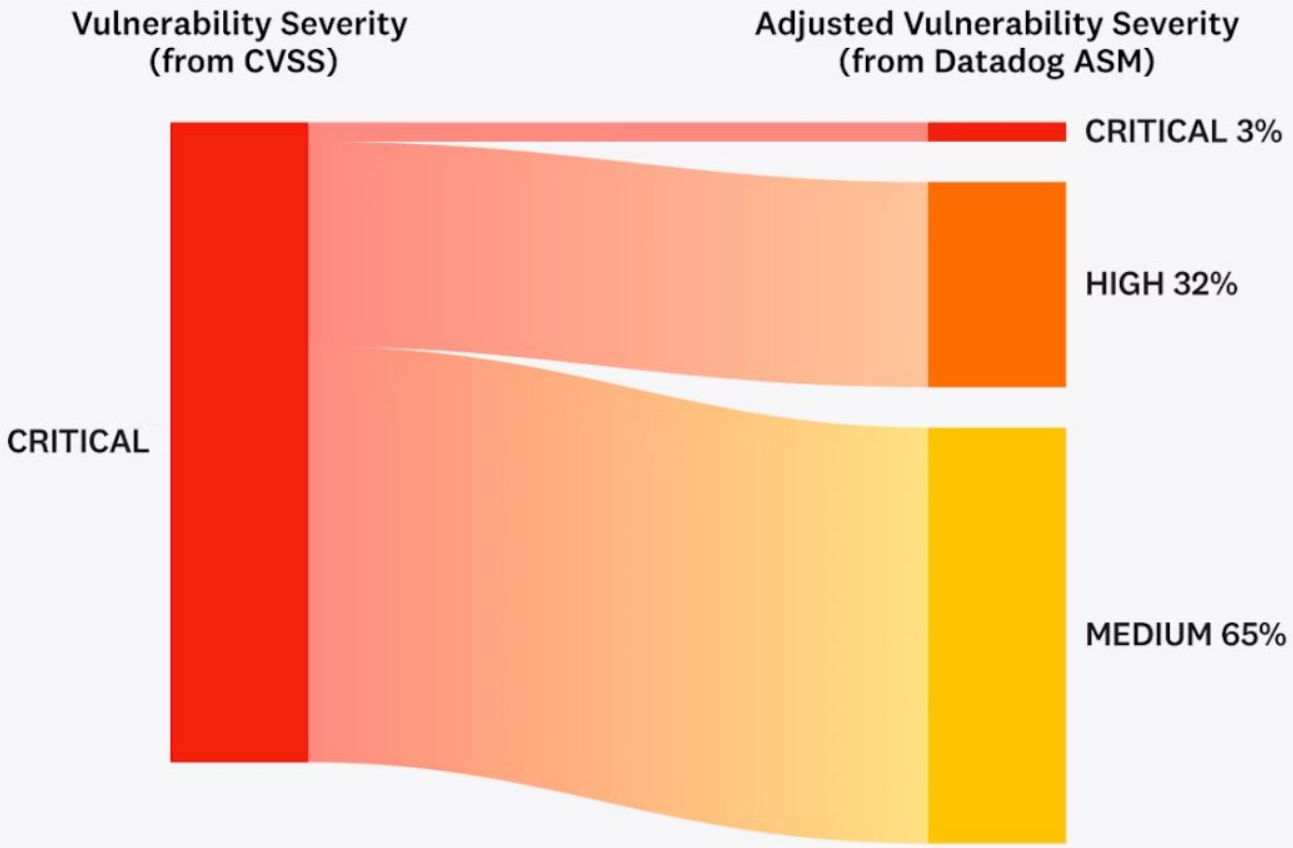
Ignore low risk vulnerabilities

Prioritize high risk vulnerabilities

→ a better outcome, in less time


DATADOG

Impact of Runtime Context on Vulnerability Severity



RUNTIME CONTEXT SHOWS THAT ONLY 3% OF CRITICAL VULNERABILITIES ARE WORTH PRIORITIZING

Source: Datadog

CVSS defines vulnerability severity

When a security research reports a vulnerability, they fill in related information

This generates a score between 0 and 10:

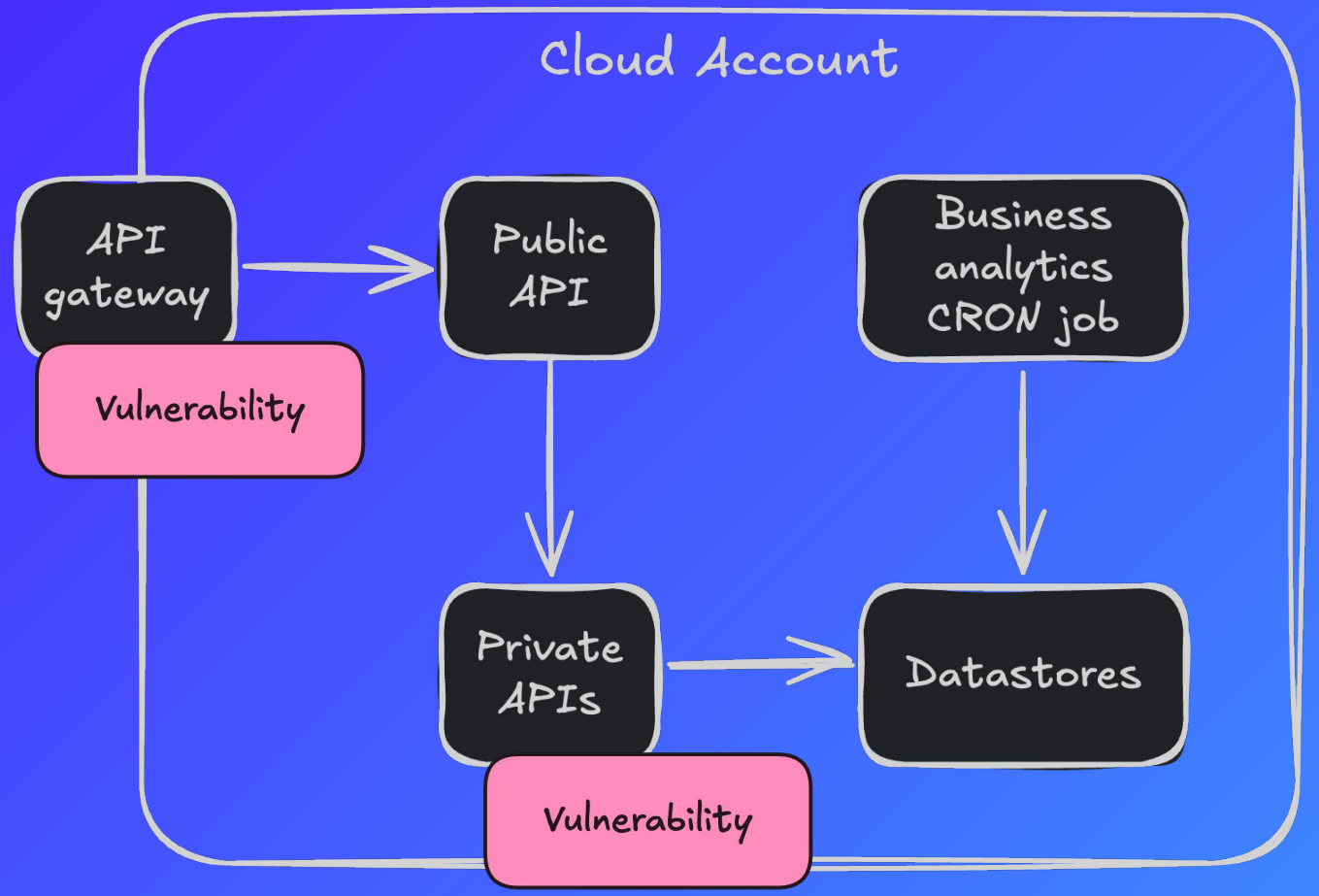
0 - the vulnerability is not important

10 - the vulnerability should be fixed ASAP

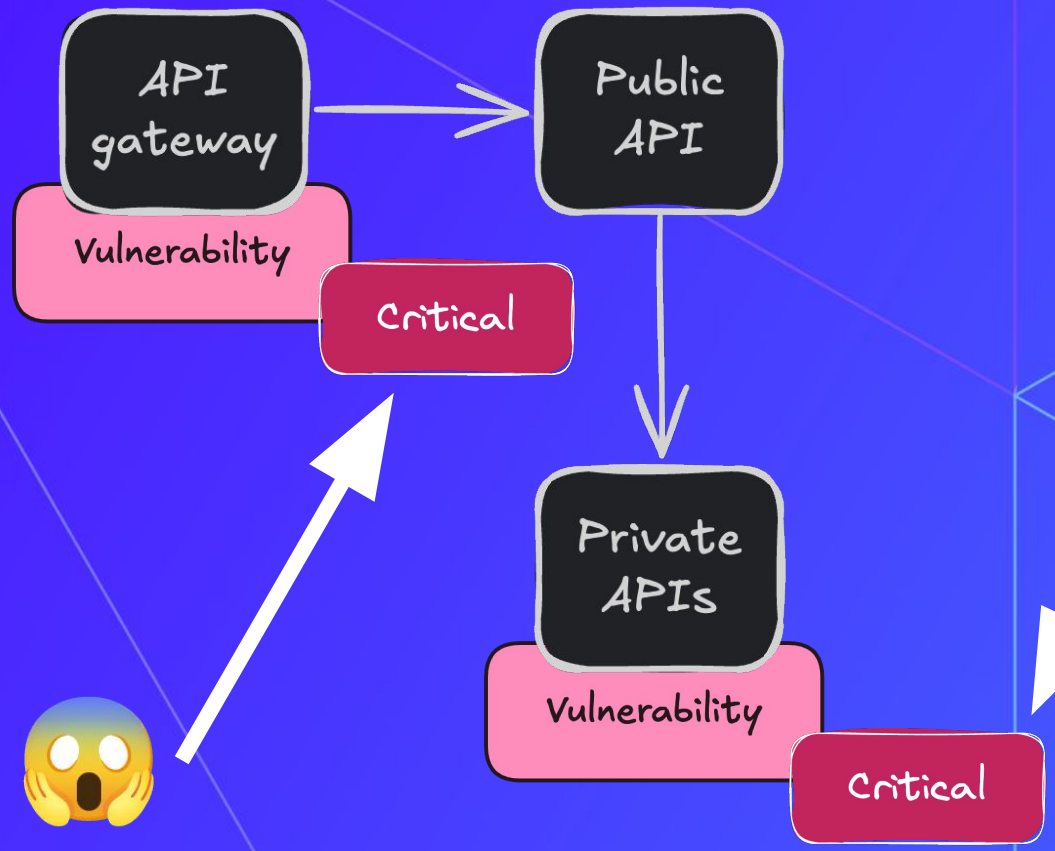
This scoring mechanism is named “CVSS”

[See https://www.first.org/cvss/calculator/3-1](https://www.first.org/cvss/calculator/3-1)

Same vulnerability *but* different systems = different risks



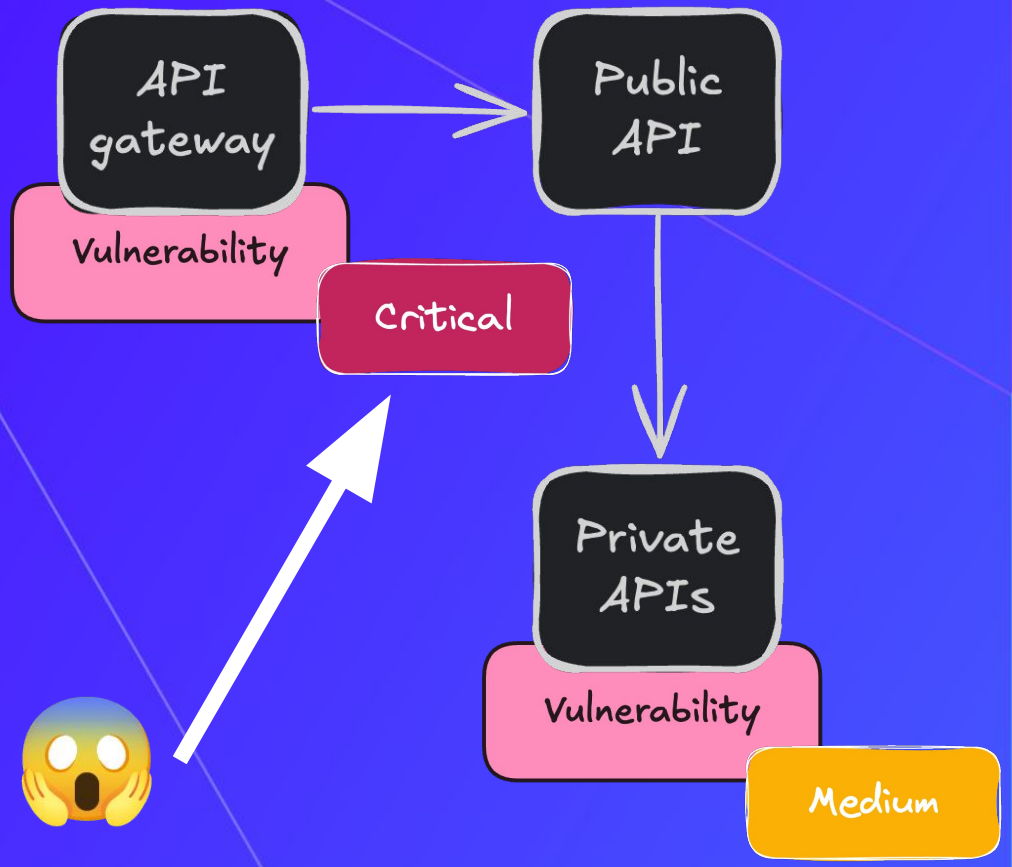
Base CVSS is *too* generic



Too dramatic 🤨

Fair 😱

Enrich CVSS with context



Fair 😱

Fair 😮‍💨

What have we learnt so far?

We want to fix vulnerabilities that pose an **actual** risk

The risk is **system dependent,** not generic

But CVSS is **generic** and “assumes worst case”

To the rescue: CVSS environmental

What we call CVSS score is actually “CVSS base score”

CVSS is extensible and offers “CVSS environmental score”

The initial severity **can be adjusted depending on system’s characteristics**

Log4shell - base:	Critical
Non-production system	High
Non-public & non-production	Medium

CVE-2021-26691 - base:	Critical
(httpd)	
Non-public network	High
Non-public & non-production	Medium

Environmental Score

10.0 (Critical)

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Modified Attack Vector (MAV)

Not Defined (X) | Network | Adjacent Network | Local | Physical

Modified Attack Complexity (MAC)

Not Defined (X) | Low | High

Modified Privileges Required (MPR)

Not Defined (X) | None | Low | High

Modified User Interaction (MUI)

Not Defined (X) | None | Required

Modified Scope (MS)

Not Defined (X) | Unchanged | Changed

Modified Confidentiality (MC)

Not Defined (X) | None | Low | High

Modified Integrity (MI)

Not Defined (X) | None | Low | High

Modified Availability (MA)

Not Defined (X) | None | Low | High

first.org/cvss/calculator/

Environmental Score

9.4
(Critical)

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Modified Attack Vector (MAV)

Not Defined (X) | Network | Adjacent Network | Local | Physical

Modified Attack Complexity (MAC)

Not Defined (X) | Low | High

Modified Privileges Required (MPR)

Not Defined (X) | None | Low | High

Modified User Interaction (MUI)

Not Defined (X) | None | Required

Modified Scope (MS)

Not Defined (X) | Unchanged | Changed

Modified Confidentiality (MC)

Not Defined (X) | None | Low | High

Modified Integrity (MI)

Not Defined (X) | None | Low | High

Modified Availability (MA)

Not Defined (X) | None | Low | High

first.org/cvss/calculator/

Environmental Score

8.3
(High)

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Modified Attack Vector (MAV)

Not Defined (X) | Network | Adjacent Network | Local | Physical

Modified Attack Complexity (MAC)

Not Defined (X) | Low | High

Modified Privileges Required (MPR)

Not Defined (X) | None | Low | High

Modified User Interaction (MUI)

Not Defined (X) | None | Required

Modified Scope (MS)

Not Defined (X) | Unchanged | Changed

Modified Confidentiality (MC)

Not Defined (X) | None | Low | High

Modified Integrity (MI)

Not Defined (X) | None | Low | High

Modified Availability (MA)

Not Defined (X) | None | Low | High

first.org/cvss/calculator/

Environmental Score

6.8
(Medium)

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Modified Attack Vector (MAV)

Not Defined (X) | Network | Adjacent Network | Local | Physical

Modified Attack Complexity (MAC)

Not Defined (X) | Low | High

Modified Privileges Required (MPR)

Not Defined (X) | None | Low | High

Modified User Interaction (MUI)

Not Defined (X) | None | Required

Modified Scope (MS)

Not Defined (X) | Unchanged | Changed

Modified Confidentiality (MC)

Not Defined (X) | None | Low | High

Modified Integrity (MI)

Not Defined (X) | None | Low | High

Modified Availability (MA)

Not Defined (X) | None | Low | High

first.org/cvss/calculator/

Environmental Score

0.0
(None)

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Modified Attack Vector (MAV)

Not Defined (X) | Network | Adjacent Network | Local | Physical

Modified Attack Complexity (MAC)

Not Defined (X) | Low | High

Modified Privileges Required (MPR)

Not Defined (X) | None | Low | High

Modified User Interaction (MUI)

Not Defined (X) | None | Required

Modified Scope (MS)

Not Defined (X) | Unchanged | Changed

Modified Confidentiality (MC)

Not Defined (X) | None | Low | High

Modified Integrity (MI)

Not Defined (X) | None | Low | High

Modified Availability (MA)

Not Defined (X) | None | Low | High

first.org/cvss/calculator/

Build a more accurate risk using system's data

Public accessibility

Is the system publicly accessible (from cloud configuration)?

Is it exposed to attacks?

Is it receiving traffic from public IPs?

Confidentiality & Integrity

Is the system processing sensitive information?

Is it connected to datastore with sensitive information?

Has it a login endpoint?

Availability

Is the system a dependency of many other systems?

Is it forwarding traffic to many others systems?

Blast radius

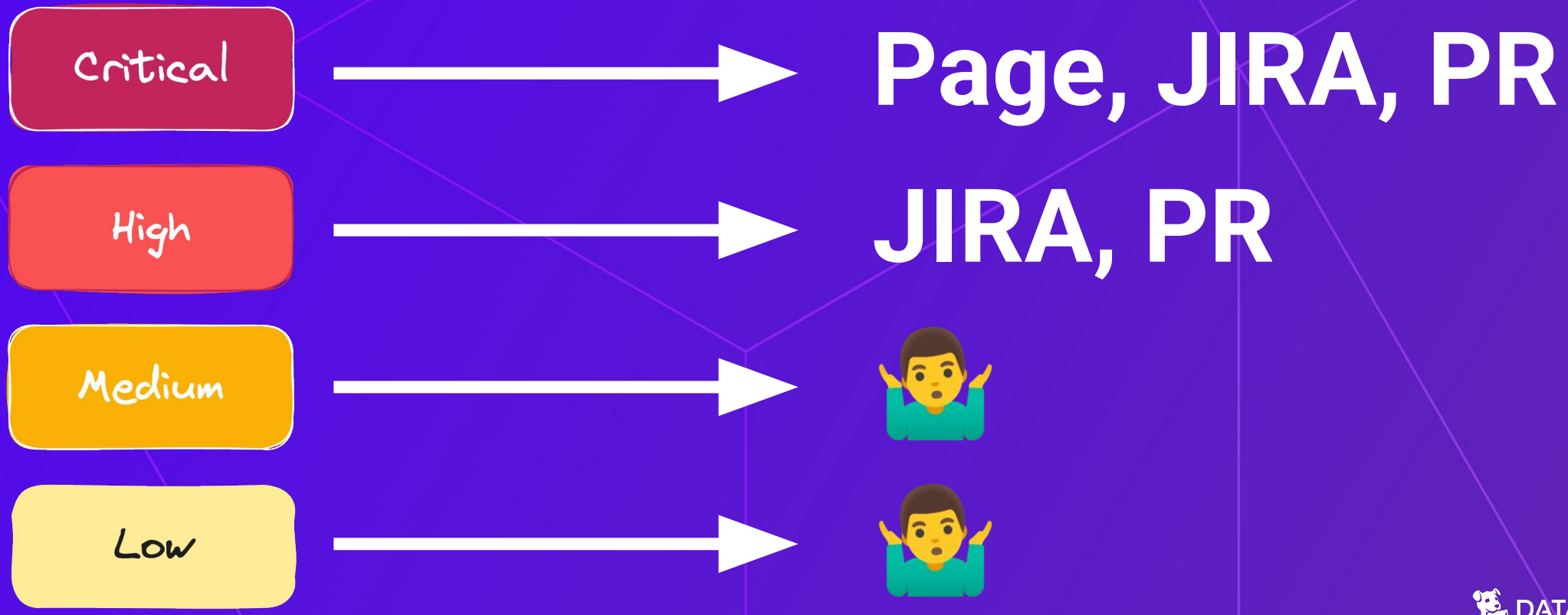
What can an attacker do if they take over this system?

Escape the container to the host?

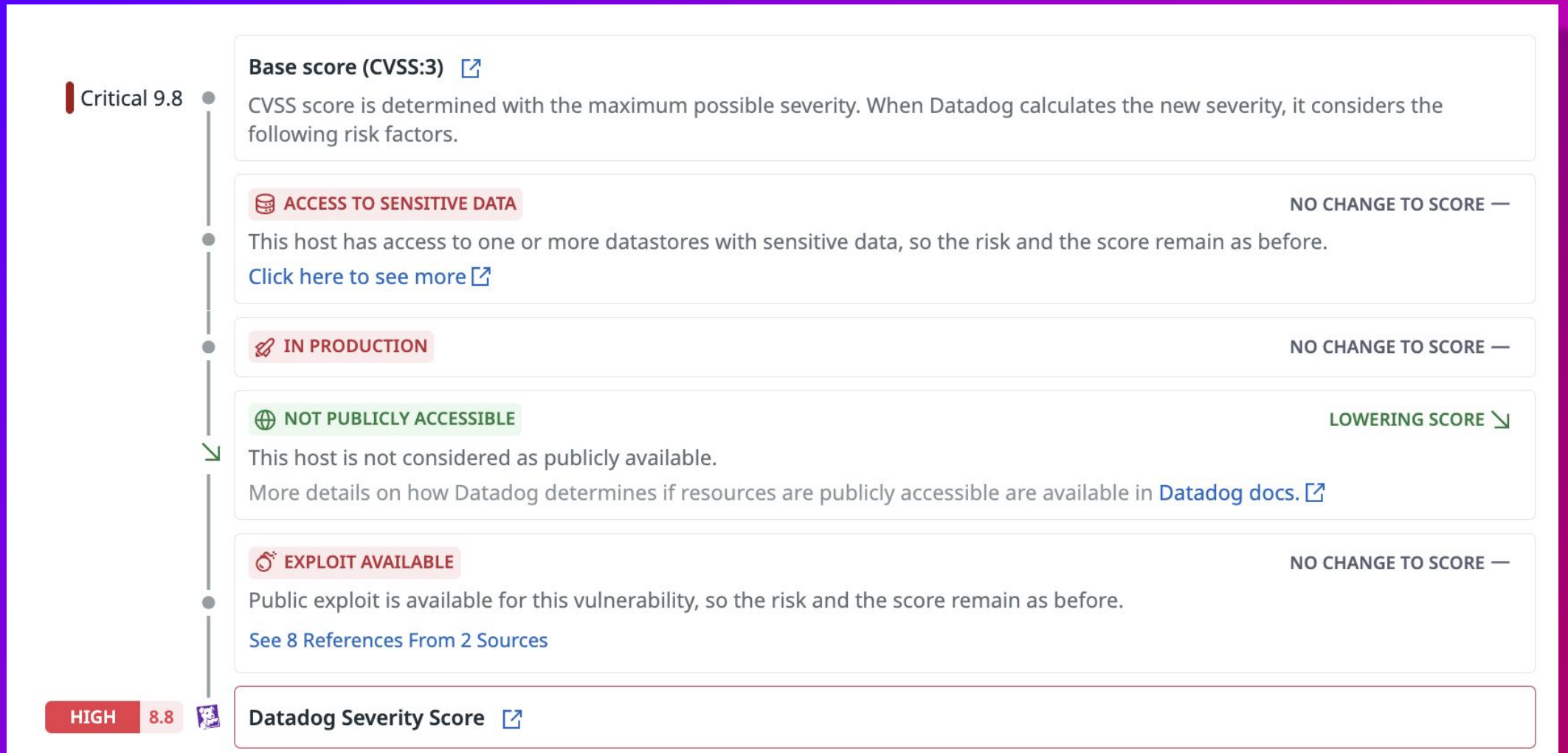
Pivot to other systems in my cloud account?

Pivot to other cloud accounts?

Trust scoring. Prioritize vulnerabilities accordingly.



DATADOG



Resurfacing to users

How do you fix vulns?

Automate pull requests / libraries updates in Cursor

Review / test

Merge

Deploy

When are we done?

When vulnerable systems stop running.

Going beyond observability data

Reachability analysis

Are the vulnerable methods used in my code?

Are the vulnerable methods called in production?

Attack protection

Can I block attacks trying to exploit this vulnerability?

Can I just prevent the sensitive method from being called?

Fixed build already available

Is there a fixed container image already available?

Don’t fix, just deploy!

Deeper system characteristics

Is my architecture impacted (e.g. CPU)?

Is my app impacted (e.g. frontend vs backend vuln)?

What does future looks like? (aka Jb crystal-balling)

More vulnerabilities will be discovered

    Amongst which new categories of vulnerabilities

But it will become easier to upgrade (easy for AI tools)

Though, deploying code using an upgraded library **will still be risky**

→ that's where a difference can be made

Questions time