# The Safety Dance

## Risk Assessment for DevOps Practitioners

DevOpsDays São Paulo 2020

DATADOG

# The Safety Dance

## Risk Assessment for DevOps Practitioners

DevOpsDays São Paulo 2020

DATADOG

# Your Safety Dancer

Daniel Maher

Twitter:
@phrawzty

Email:
daniel.maher@datadoghq.com

Web:
www.dark.ca

# Your Safety Dancers

Daniel Maher ← that's me!

Andrew Krug ← shout out!

# What we’re going to do today

RISK

RISK

# Risk: A Crash Course

# What is risk? What is safety science?
## *Kaplan and Garrick (1989)*

What can go wrong?

What is the likelihood? (probability)

How bad could it be?

# What is risk? What is safety science?
## *Classic calculation*

$$R = f(s, p, c)$$

Risk = *f* (scenario, probability, consequence)

# Qualitative vs Quantitative

Qualitative reasoning *ranks* likelihood using a scale score metric.

| 👍 | 👎 |
| --- | --- |
| Speedy<br>Easy<br>Light data gathering! | Light data gathering?<br>Low precision |

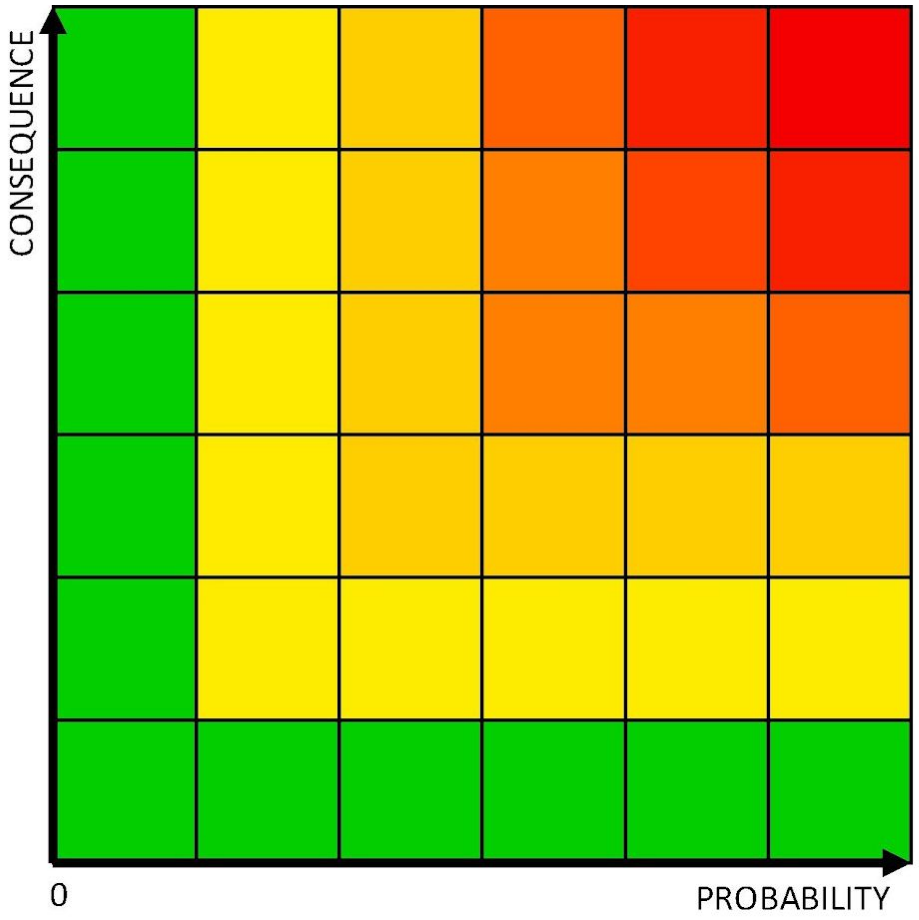
# Qualitative vs Quantitative

Quantitative reasoning uses data to *reason* about probabilities and consequences.

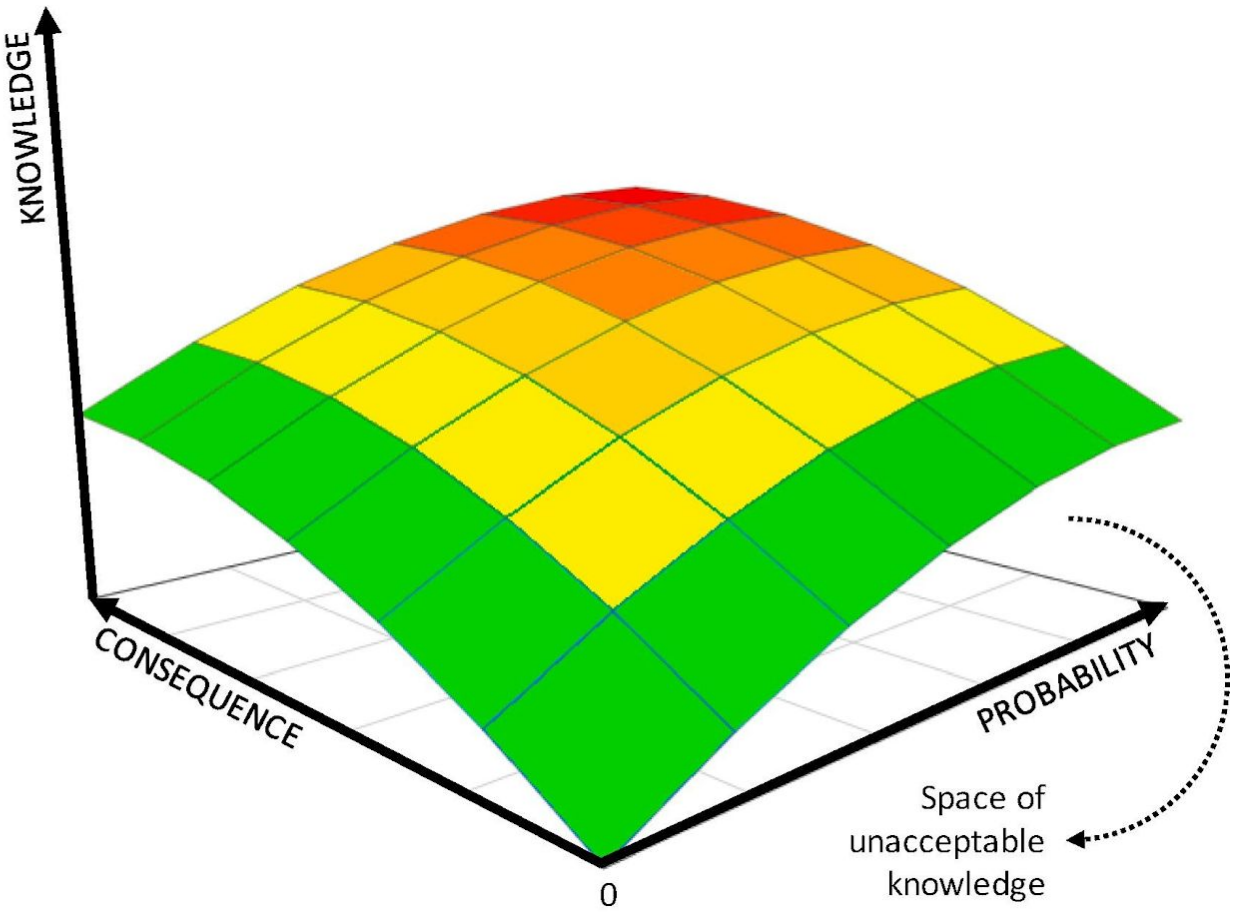
| 👍 | 👎 |
| --- | --- |
| Accuracy | Time<br>Data<br>Relative risks (adjacent) |

# Hybrid Models

a)




b)




T. Aven, “Three influential risk foundation papers from the 80s and 90s: Are they still state-of-the-art?,” *Reliability Engineering & System Safety*, 28-Sep-2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832019302649?via=ihub. [Accessed: 15-Oct-2020].

DATADOG

# What is risk? What is safety science?
## *Hybrid calculation*

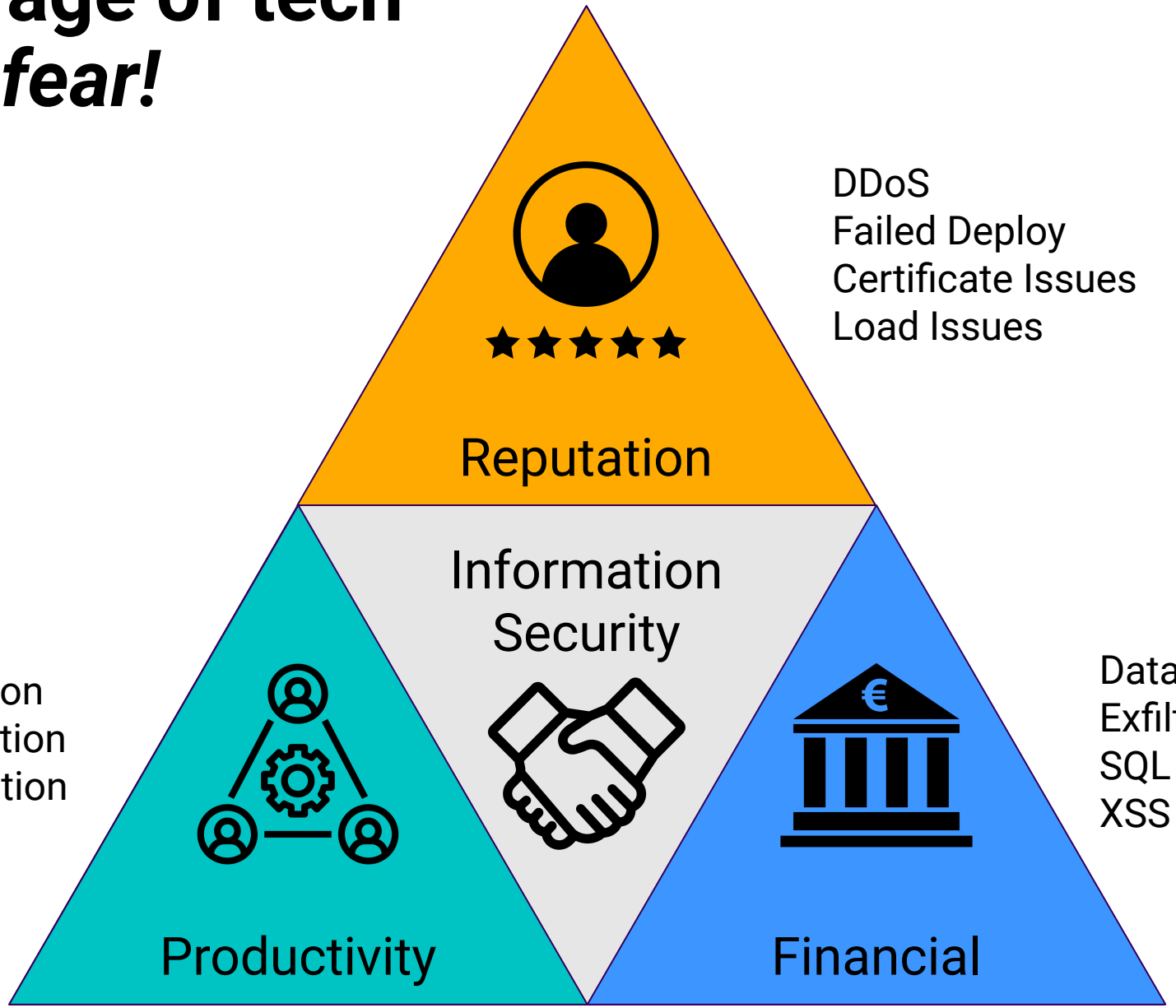
$$R = f(s, p, c, k)$$

Risk = *f*(scenario, probability, consequence, knowledge)

knowledge = (mix of both quantitative and qualitative data)

# The Knowledge Dimension (This is where *you* come in!)

# Risk in the age of tech
## *Triforce of fear!*



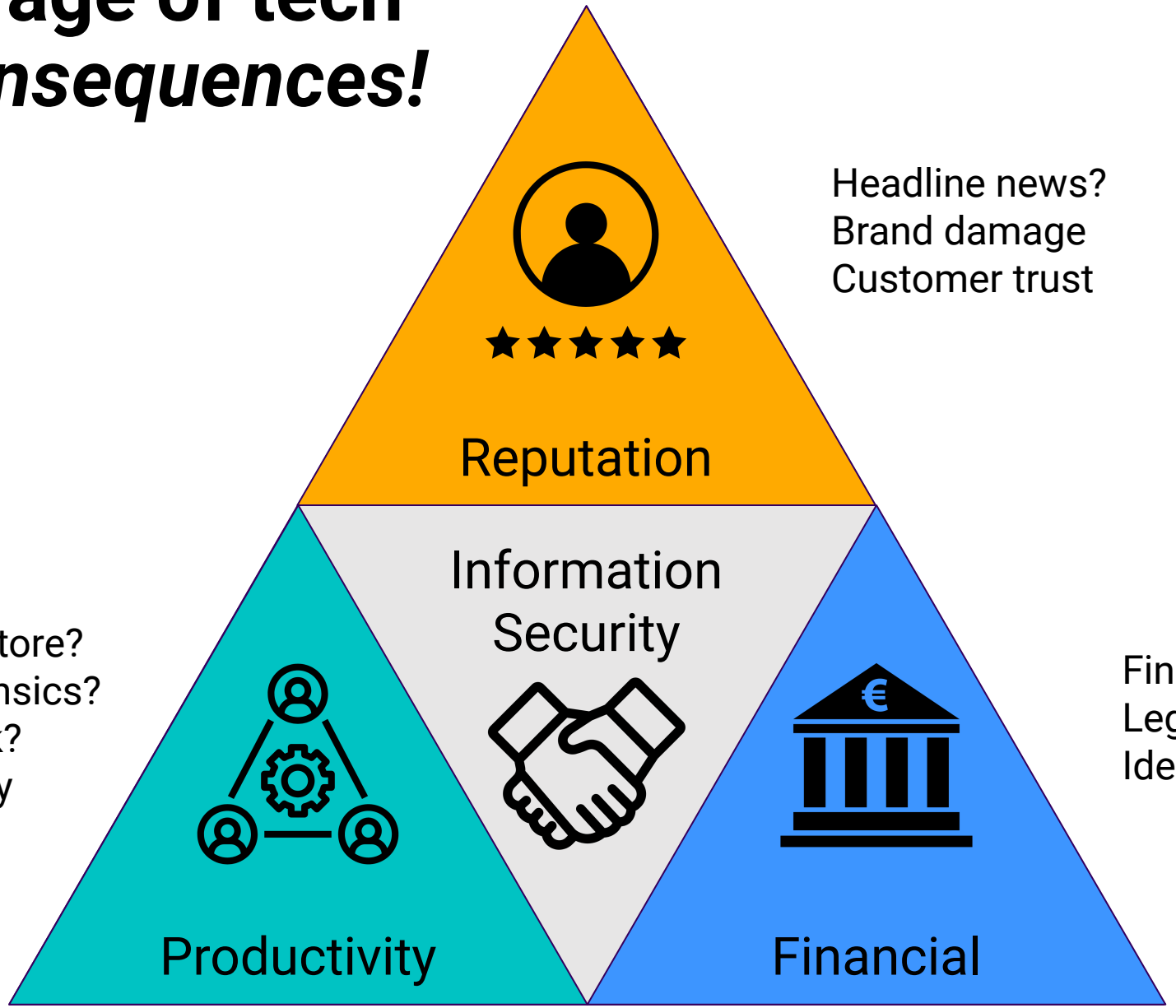

DDoS
Failed Deploy
Certificate Issues
Load Issues

Tampering
SQL Injection
Impersonation
Authentication
Bypass

Data
Exfiltration
SQL Injection
XSS

DATADOG

# Risk in the age of tech
## *Triad of consequences!*



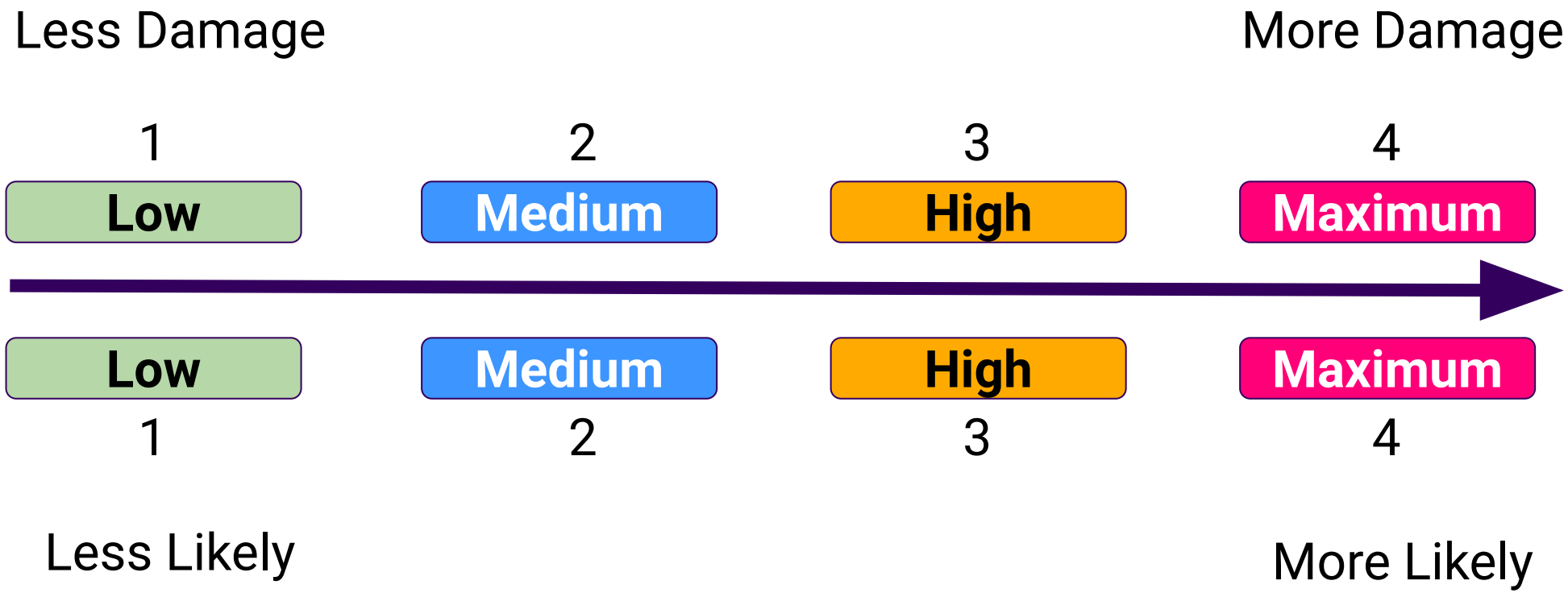

Headline news?
Brand damage
Customer trust

How long to restore?
How much forensics?
Time to rollback?
Employee Safety
Doxxing

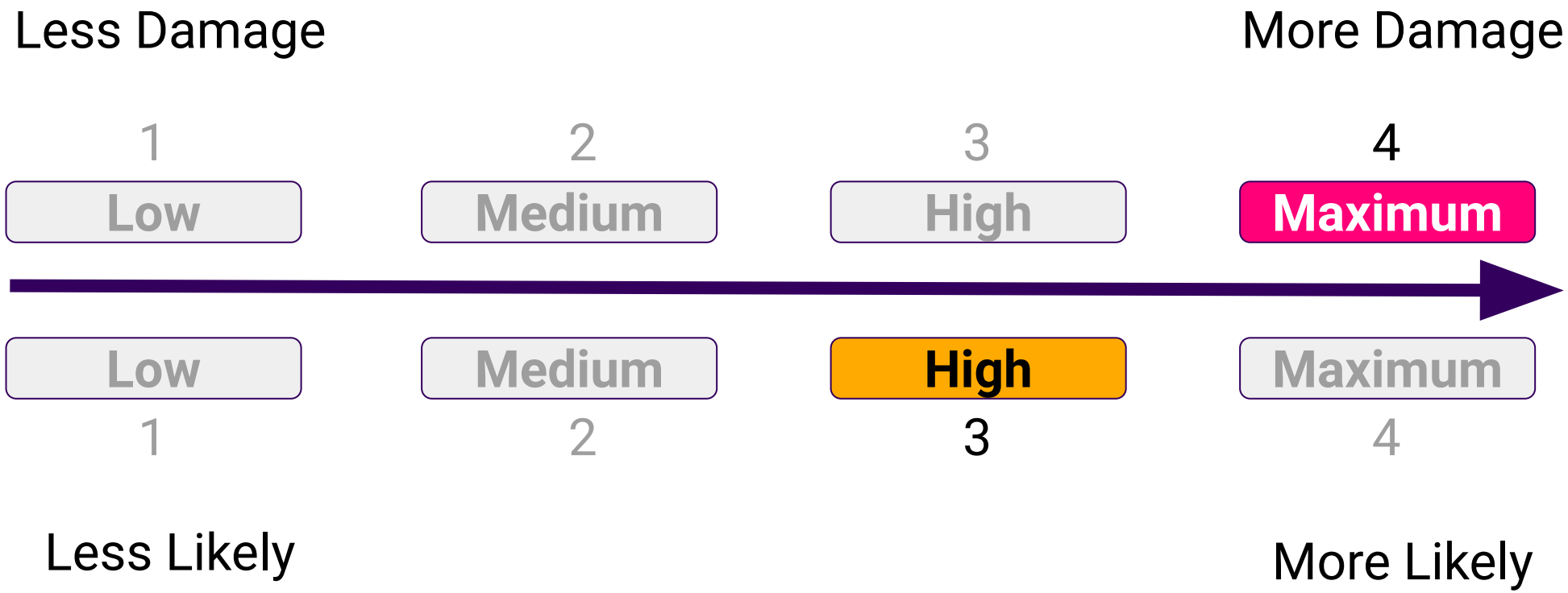
Fines!
Legal damages
Identity insurance

DATADOG

# Risk in the age of tech
## *What we know vs. what we feel*



# Risk in the age of tech
## *What we know vs. what we feel*




DATADOG

# Risk in the age of tech
## *What we feel*

# Risk in the age of tech
## *What we know*

| 0.5 confidence | 0.9 confidence | 0.7 confidence |
| --- | --- | --- |
| **High** | **Maximum** | **Hi/Max** |
| 3 | 4 | 3.5 |

1.5 + 3.6 = 5.1

DATADOG

# Real risks in the real world

# Risk in the age of tech

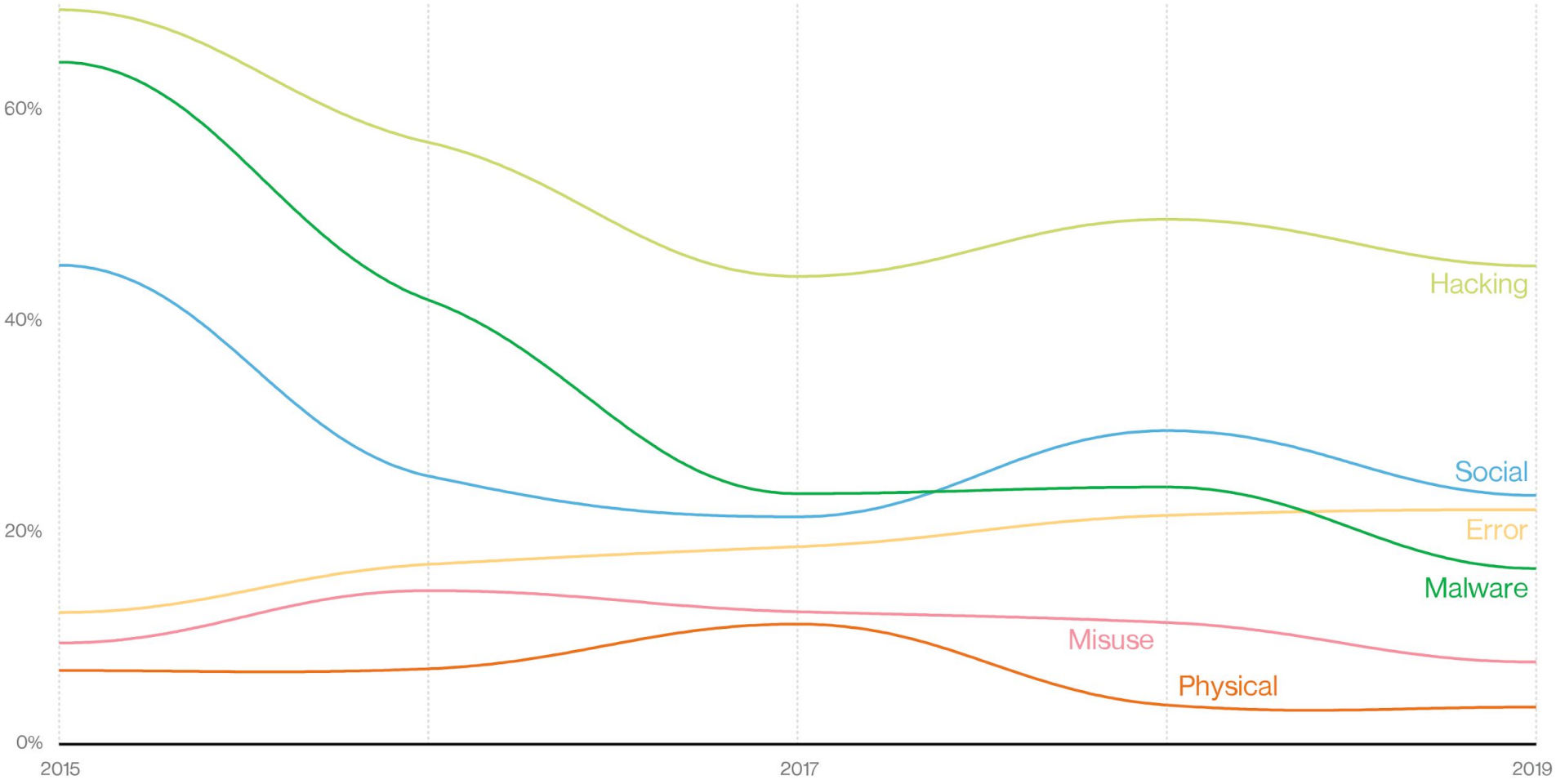



**Figure 11.** Actions over time in breaches

DATADOG

G. Basset, S. Widup, P. Langlois, A. Pinto, and C. D. Hylender, "2020 Data Breach Investigations Report," *Verizon DBIR*, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/. [Accessed: 15-Oct-2020].

# Risk in the age of tech

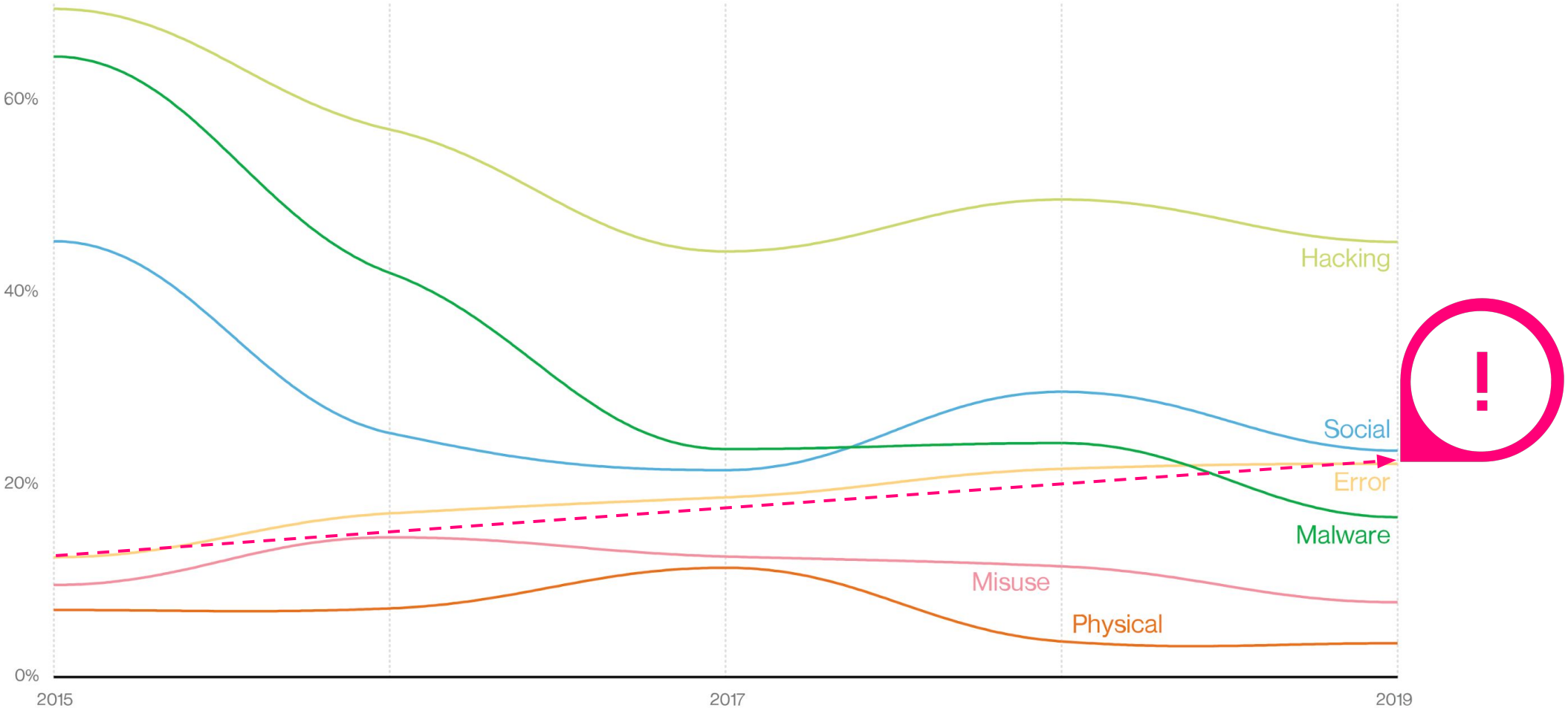



**Figure 11.** Actions over time in breaches

G. Basset, S. Widup, P. Langlois, A. Pinto, and C. D. Hylender, "2020 Data Breach Investigations Report," *Verizon DBIR*, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/. [Accessed: 15-Oct-2020].

# Risk in the age of tech, in all industries

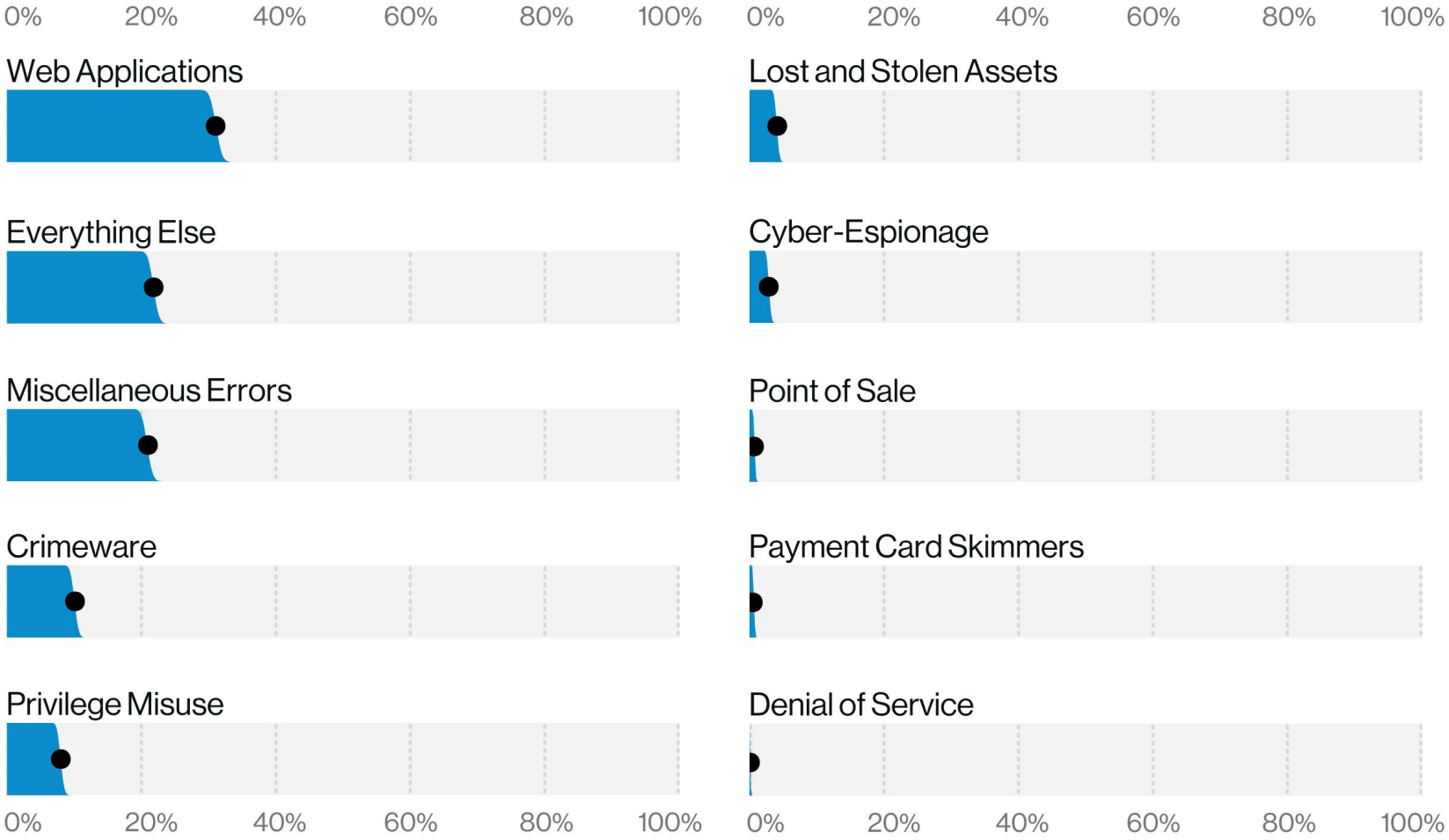



**Figure 46.** Patterns in breaches (n = 3,950)

G. Basset, S. Widup, P. Langlois, A. Pinto, and C. D. Hylender, "2020 Data Breach Investigations Report," *Verizon DBIR*, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/. [Accessed: 15-Oct-2020].

# Risk in the age of tech, *in tech itself*

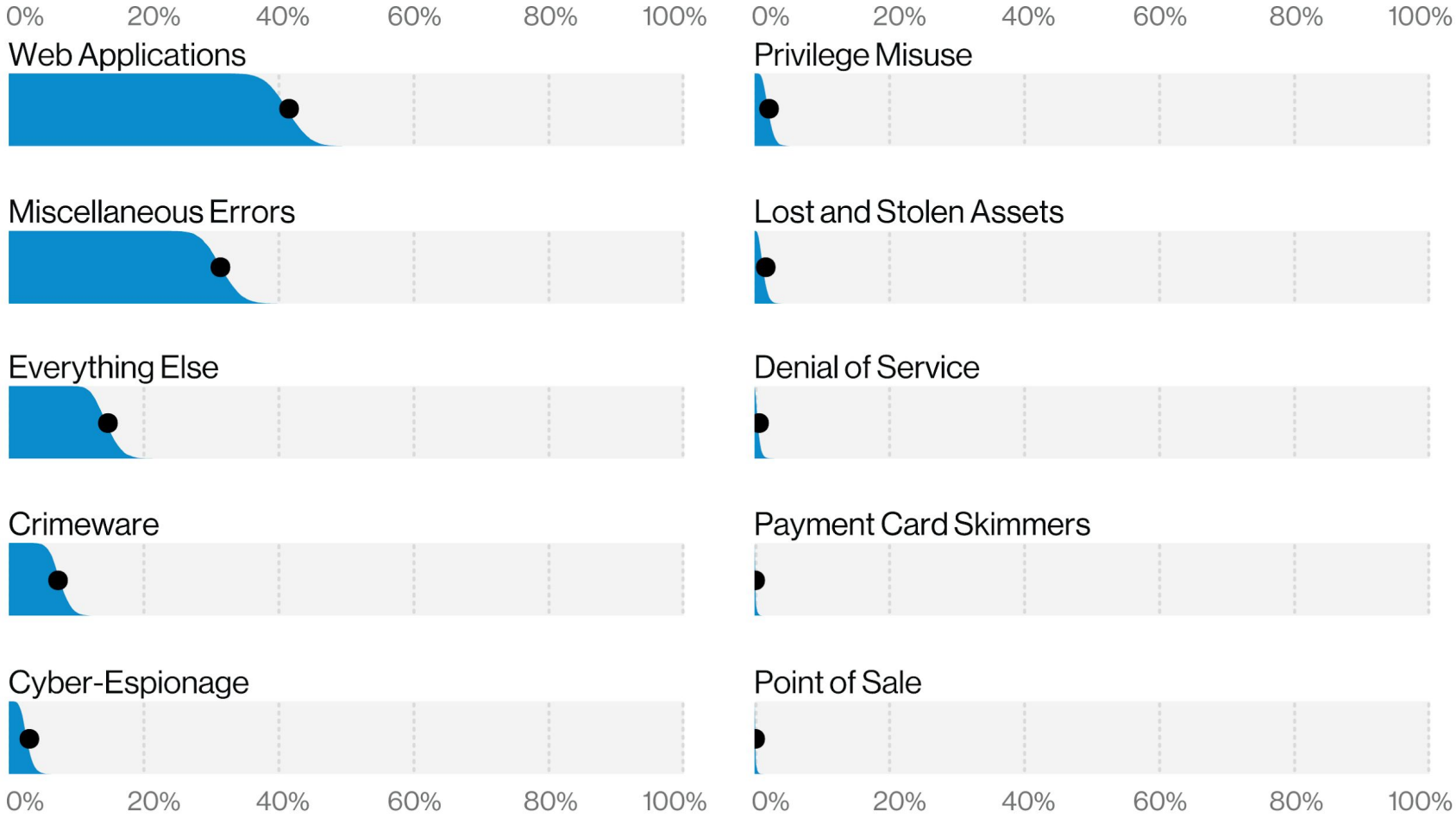
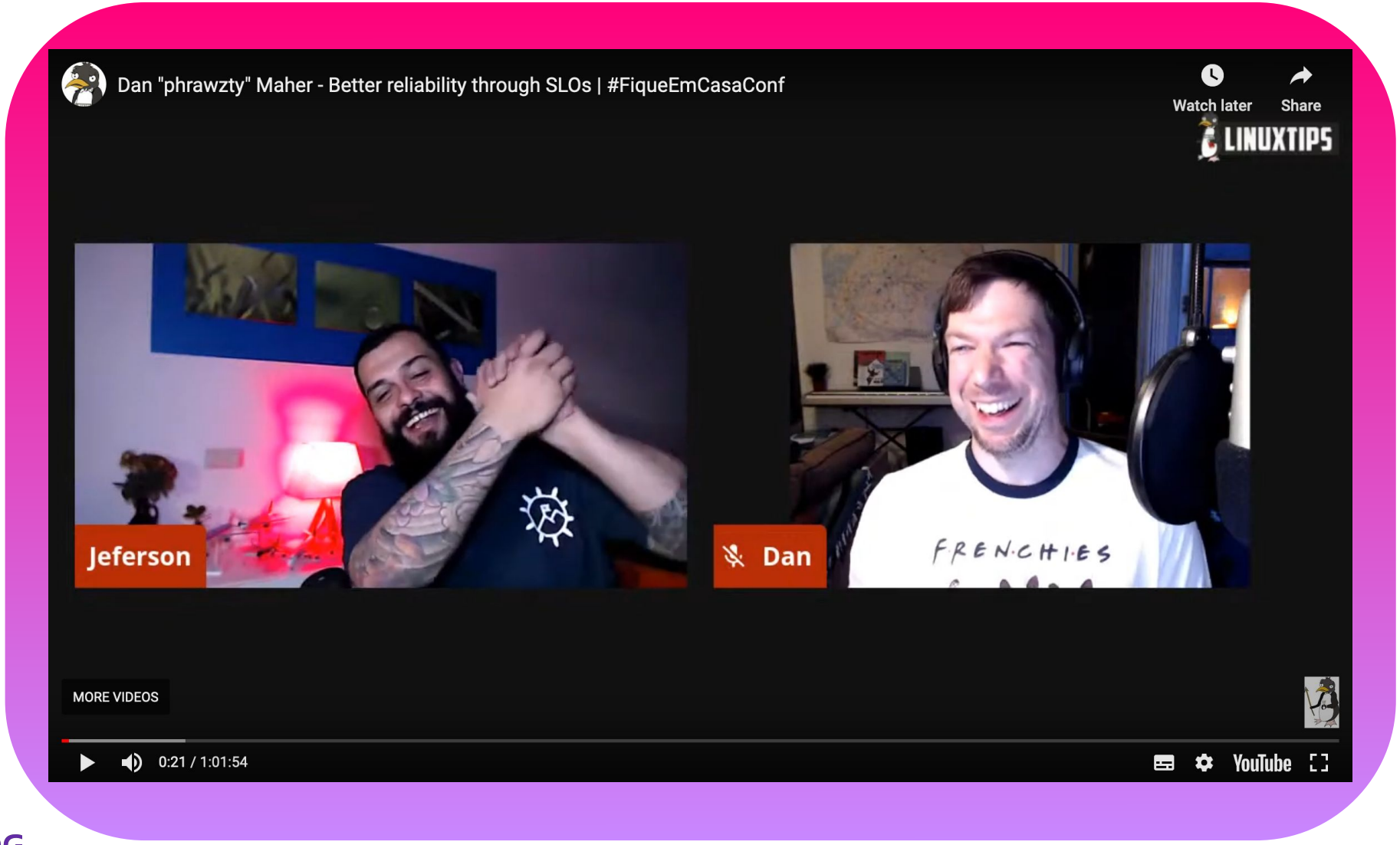



**Figure 72.** Patterns in Information industry breaches (n = 360)

G. Basset, S. Widup, P. Langlois, A. Pinto, and C. D. Hylender, "2020 Data Breach Investigations Report," *Verizon DBIR*, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/. [Accessed: 15-Oct-2020].

# Risk budgets
# (Hope for the best; plan for the worst)

# You may have heard this song before…

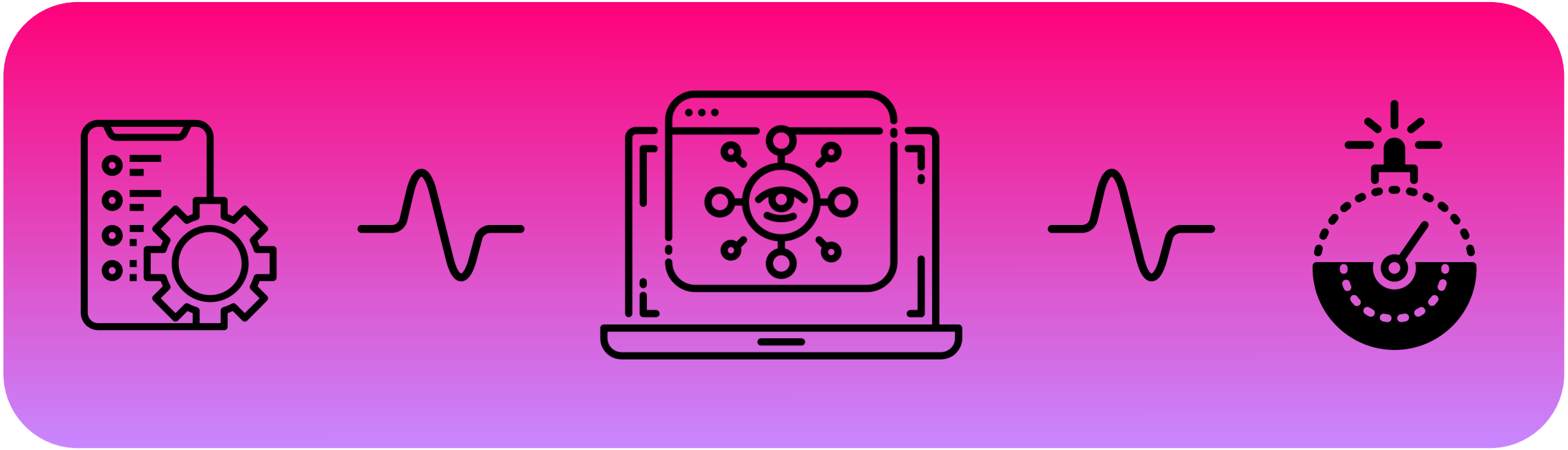



DATADOG

# What is your risk budget based on?

# Base your budget on *your* data!

# Risk budgets
## *You already have the data…*



Tools

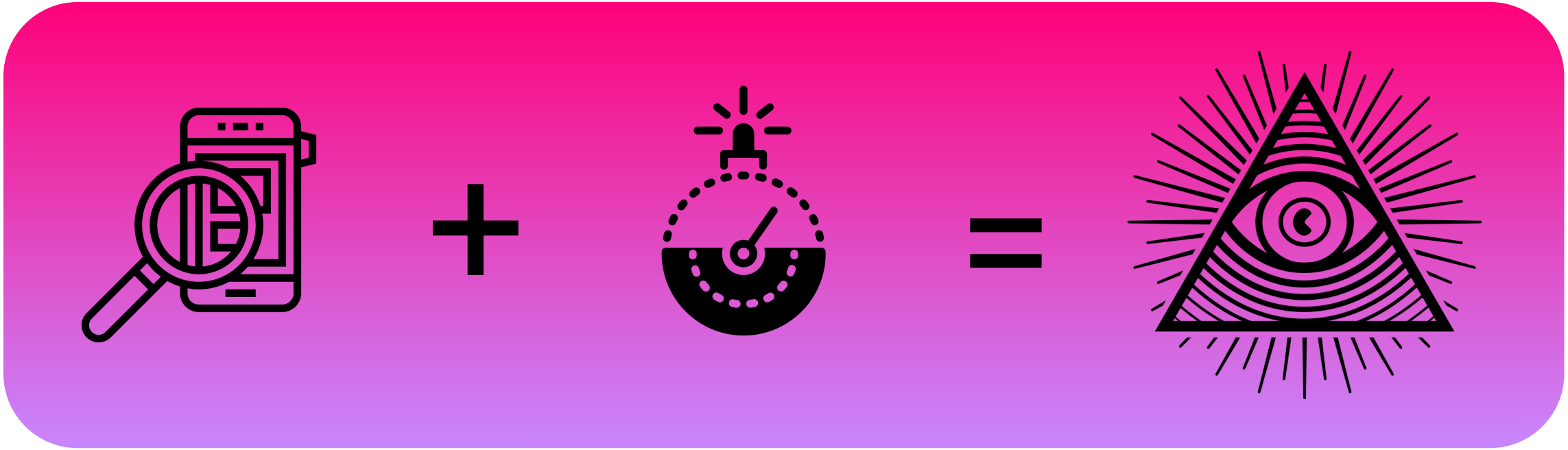
Signal

Visibility & Detection

Signal

Time-based risk

# Risk budgets
## *You just need to think about it differently*



Qualitative risk

Time-based risk

Comprehensive Visibility

DATADOG

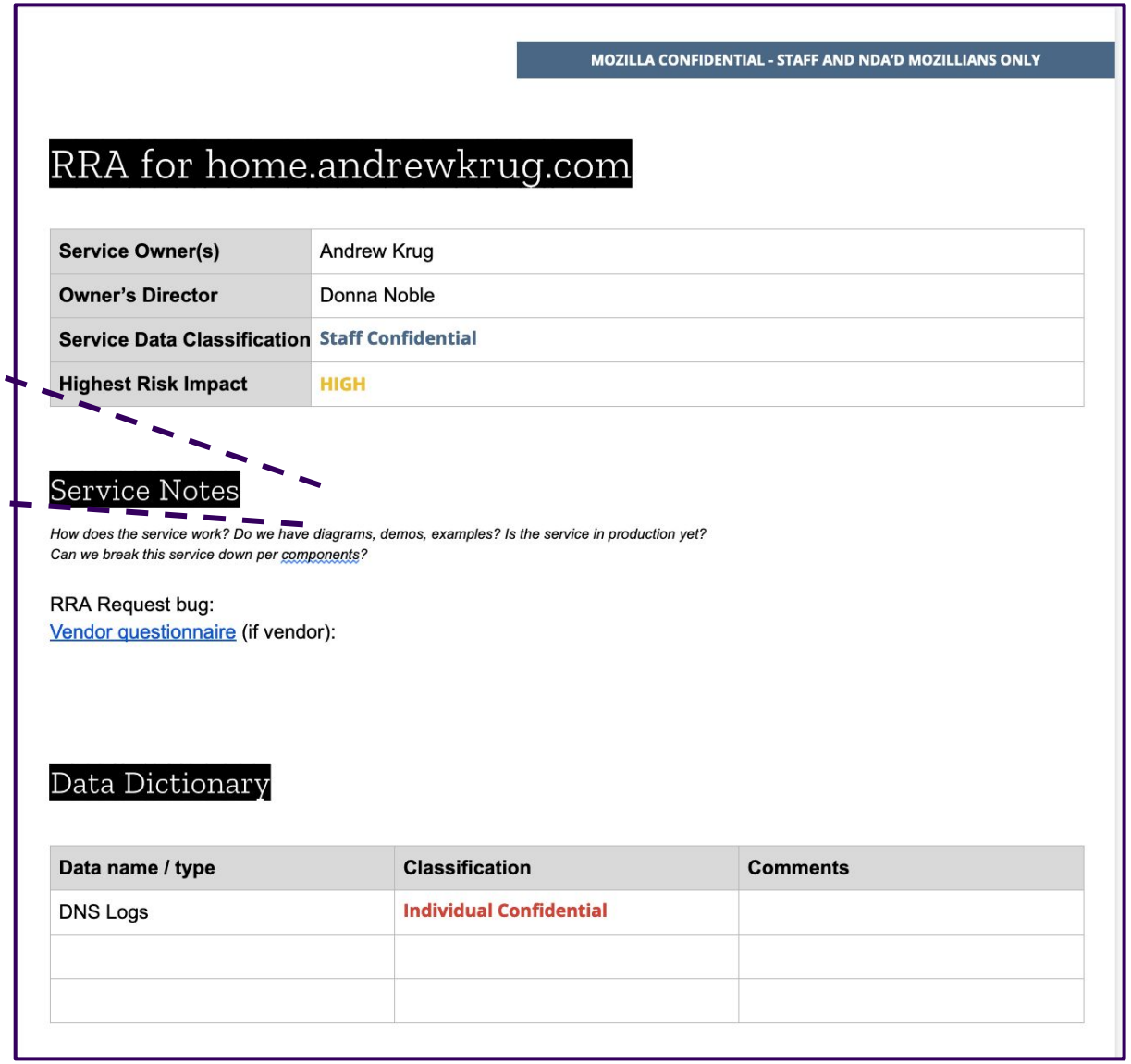
# Using your data to level up!

# Rapid risk assessment

```
risk_record = dict(
    link="https://docs.google.com/document/d/1xNVV1491IbD7e3Mnle2ztEdJbnMKiyCEVT0zYDTt7to",
    name="home.andrewkrug.com",
    service_owner="Andrew Krug",
    director="Donna Noble",
    recommendation_count=1,
    service_data_classification="staff_confidential",
    highest_risk_impact="high",
    highest_recommendation="maximum",
    creation_date=datetime.now().isoformat(),
    modification_date=datetime.now().isoformat()
)
```

**event_probability = ( recommendations * max_impact )**

a.k.a the more things are wrong the more likely an incident will occur



MOZILLA CONFIDENTIAL - STAFF AND NDA'D MOZILLIANS ONLY

## RRA for home.andrewkrug.com

| | |
|---|---|
| **Service Owner(s)** | Andrew Krug |
| **Owner's Director** | Donna Noble |
| **Service Data Classification** | **Staff Confidential** |
| **Highest Risk Impact** | **HIGH** |

## Service Notes

*How does the service work? Do we have diagrams, demos, examples? Is the service in production yet?*
*Can we break this service down per components?*

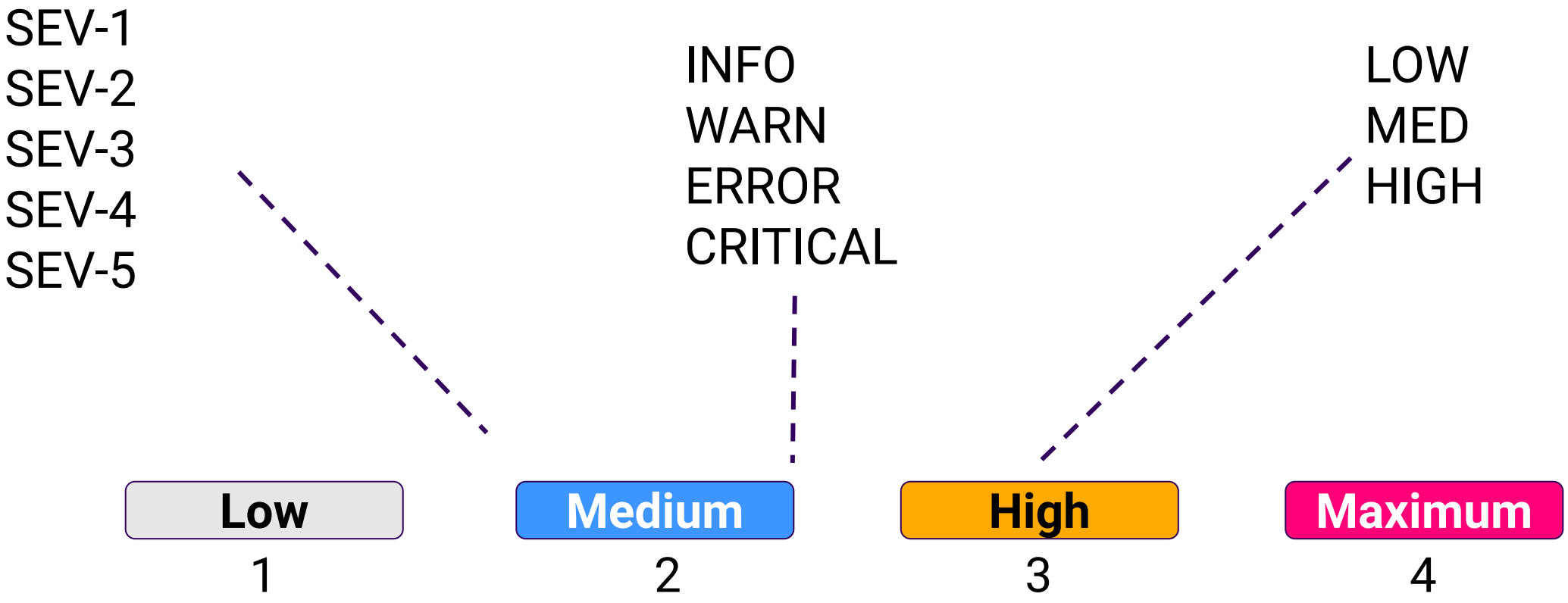
RRA Request bug:
Vendor questionnaire (if vendor):

## Data Dictionary

| Data name / type | Classification | Comments |
|---|---|---|
| DNS Logs | **Individual Confidential** | |
| | | |
| | | |

DATADOG

# Use the common language and framework



# Dynamic Risk

A method for calculating : Assign a weight to the number of findings

| Low | Medium | High | Maximum |
|---|---|---|---|
| 1 | 2 | 3 | 4 |

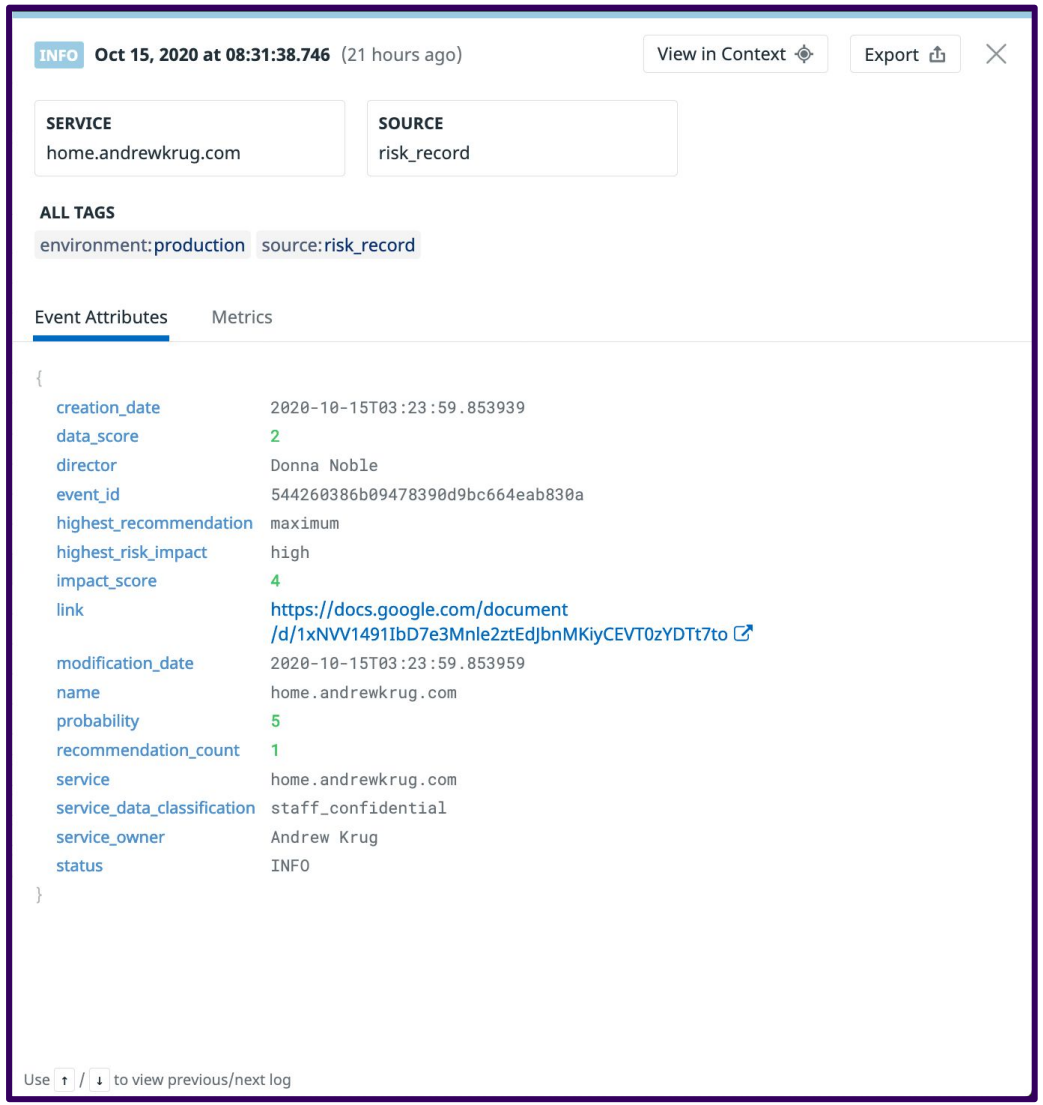
WARNING = 1 point
CRITICAL = 20 points

likelihood = ( points * 0.25 )
*Since we're using a 4 point scale*

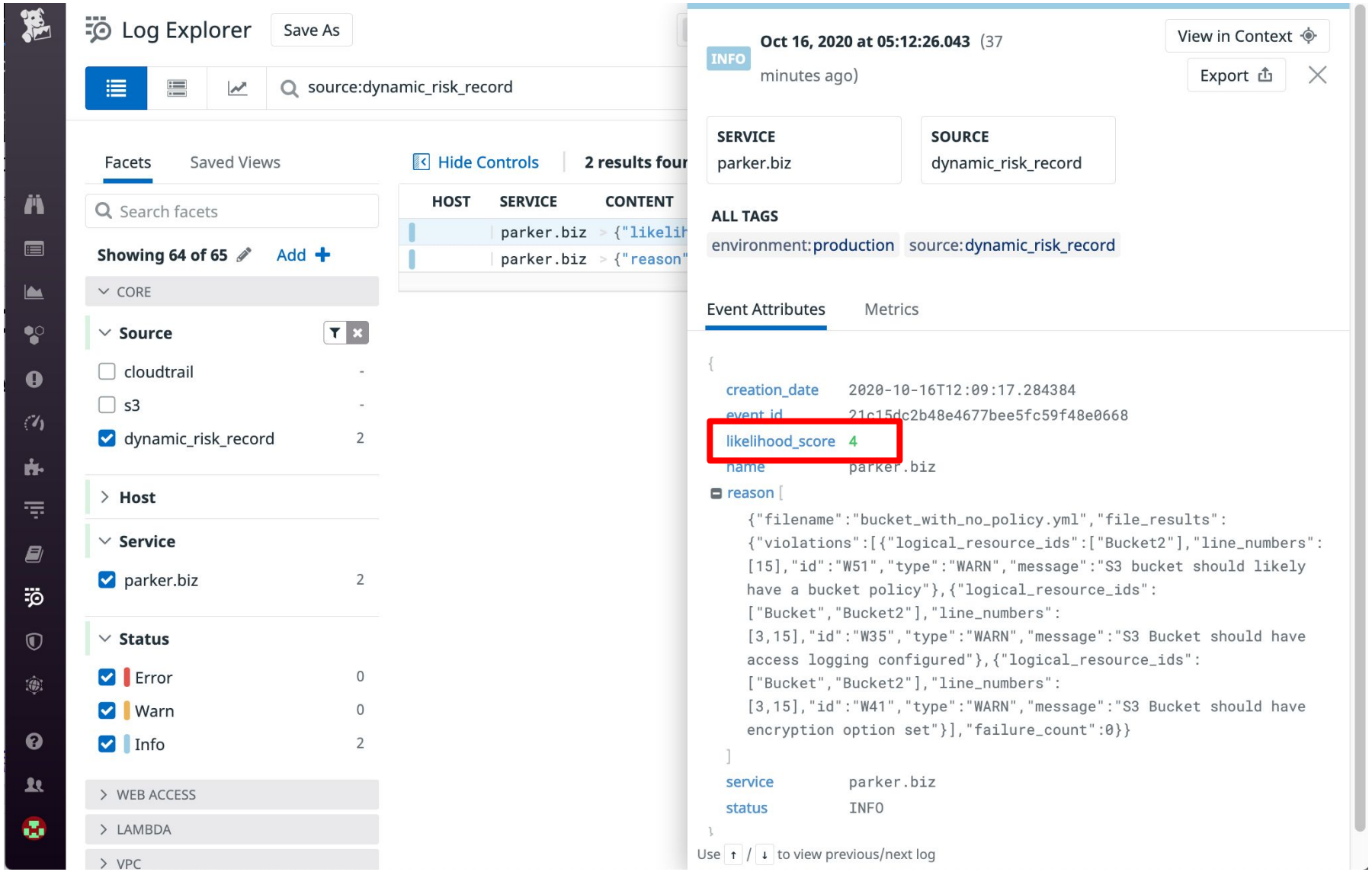
```
"id": "W41",
"type": "WARN",
"message": "S3 Bucket should have encryption option set",
```

# Aggregate the data

```
risk_record = dict(
    link="https://docs.google.com/document/d/1xNVV1491IbD7e3Mnle2ztEdJbnMKiyCEVT0zYDTt7to",
    name="home.andrewkrug.com",
    service_owner="Andrew Krug",
    director="Donna Noble",
    recommendation_count=1,
    service_data_classification="staff_confidential",
    highest_risk_impact="high",
    highest_recommendation="maximum",
    creation_date=datetime.now().isoformat(),
    modification_date=datetime.now().isoformat()
)
```

# Use the data




DATADOG

# ☆ Risk Screenboard

Edit Widgets +

4h Past 4 Hours

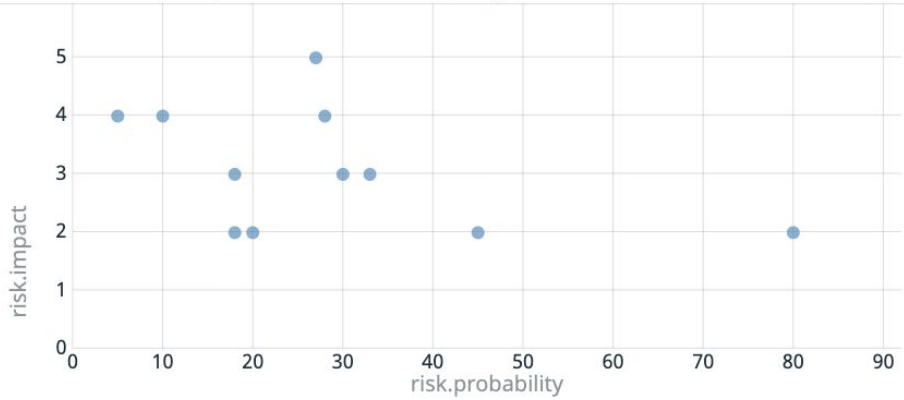
Add Template Variables

## Avg of risk.impact over *

3

## Global Risk Impact and Probability Over Time

2d




## Inbound Dynamic Risks

| ↓ DATE | HOST | SERVICE |
|---|---|---|
| Oct 16 05:12:26.043 | | parker.biz |

{"likelihood_score":4,"reason":
[{"filename":"bucket_with_no_policy.yml","file_resu
lts":{"violations":[{"logical_resource_ids":

| Oct 16 05:09:32.368 | | parker.biz |
|---|---|---|

{"reason":
[{"filename":"bucket_with_no_policy.yml","file_resu
lts":{"violations":[{"logical_resource_ids":

# Data Classification for Demo Service : STAFF_CONFIDENTIAL

DATADOG

# So in summary...

# In summary…
# *tl;dr*

- The best risk assessments **balance** both speed and accuracy, with a healthy dose of **testable fact**
- Your environment is already giving you **risk signals**
- **You** are an important piece of the security puzzle!
- **Risk budgets** are a tool that organisations can add to their toolbox in order to help their business **go fast and stay safe**

# In summary…
# *Keep the party going!*

Mozilla Rapid Risk Assessment:
https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment.html

Rapid Risk Assessment Training
https://www.youtube.com/watch?v=jxpuafW-H8U

Better Reliability Through SLOs (Fique em Casa Conf 2020)
https://www.youtube.com/watch?v=JOFYhFbrsK8

Verizon Data Breach Investigations Report 2020
https://enterprise.verizon.com/resources/reports/dbir/

@phrawzty | daniel.maher@datadog.com | www.dark.ca

DATADOG

**Daniel Maher // @phrawzty // dark.ca**

*And remember: We can dance—everything's under control.*