Modeling Application Risk At Scale @ Netflix

Shannon Morrison / Scott Behrens

5,500+ Applications

Problems

Broad risk categorization influenced by coffee and sleep

Inconsistencies in risk language with how we talk about risks

Uncertainty if we're recommending the most important security things

Our Goals

Better decision making

Improved security self-service

Improved strategic decision making

More confident incident response

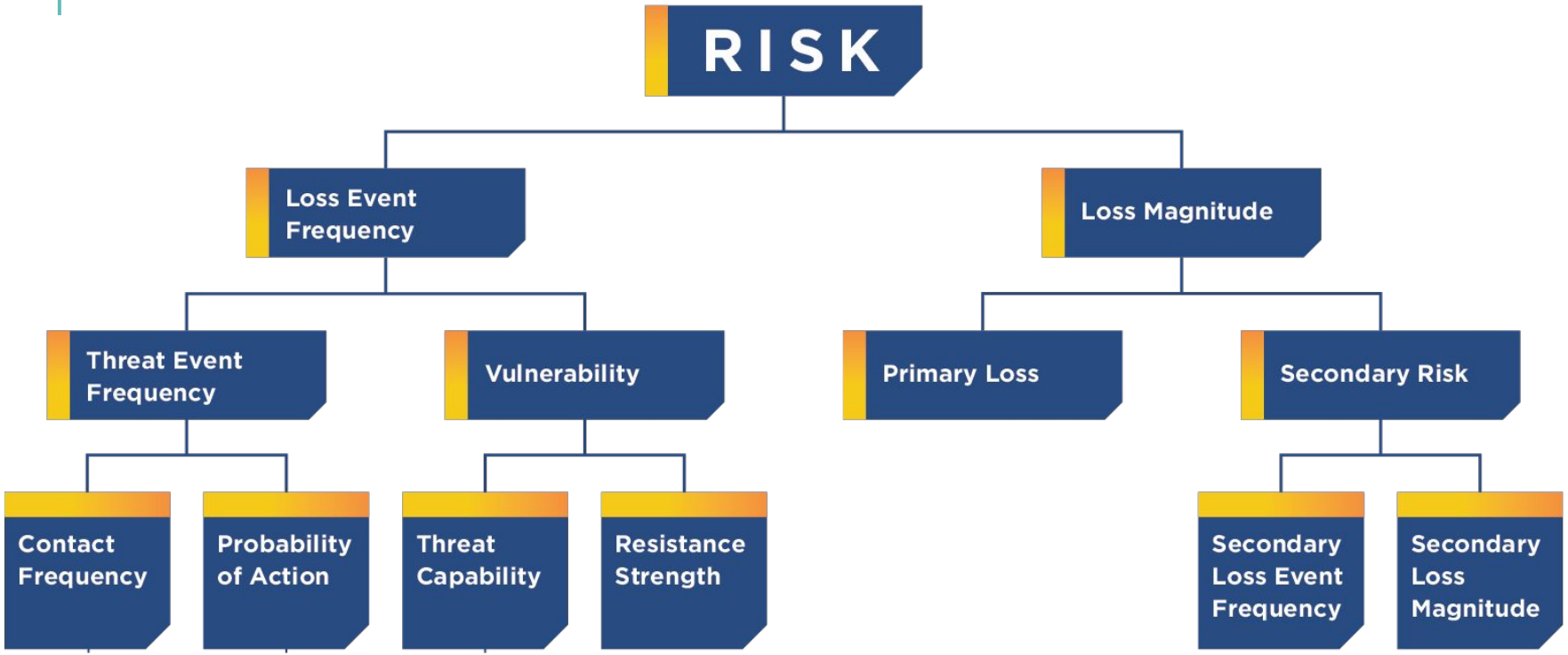
Risk Assessment

At Netflix we partner with risk practitioners who perform risk assessments

Risk assessment mitigate many of these concerns

Risk assessments are manual efforts that require time and people to conduct

FAIR Primer


RISK
Loss Event Frequency
Loss Magnitude
Threat Event Frequency
Vulnerability
Primary Loss
Secondary Risk
Contact Frequency
Probability of Action
Threat Capability
Resistance Strength
Secondary Loss Event Frequency
Secondary Loss Magnitude

Introducing Sage: An Asset Risk Modeling Framework For Netflix

Enable at scale risk measurement across a broad range of risk scenarios,
so Netflix can achieve more efficient prioritization of security work

Example Risk Scenario

Analyze the risk of an **external actor(s)** impact the **confidentiality** of **sensitive data** via **[application] attack**?

What Features Do We Use for Modeling?

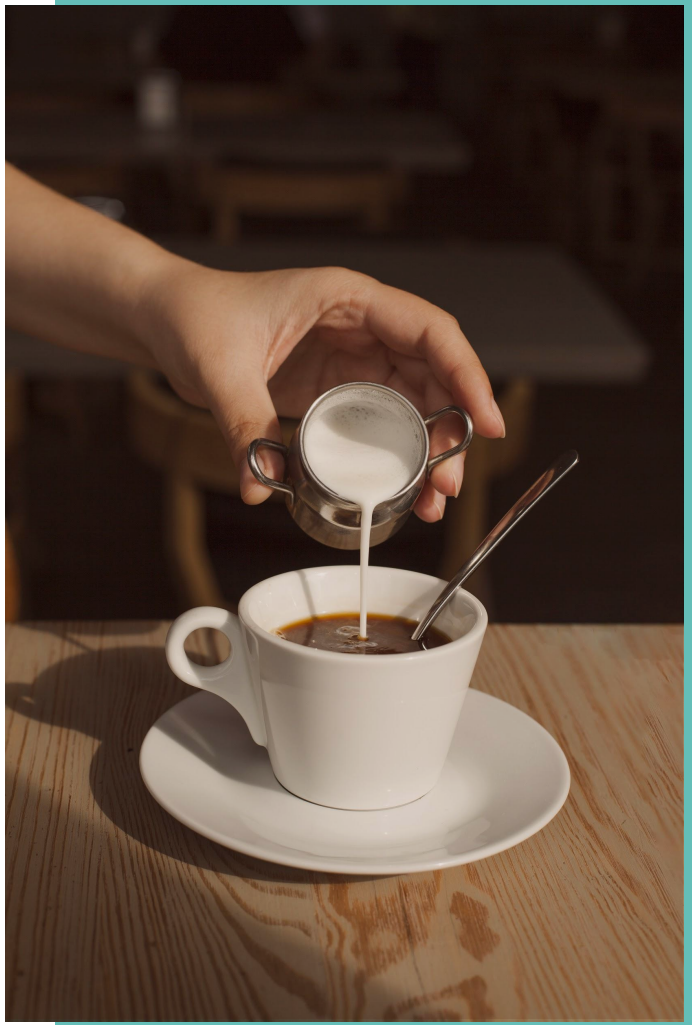
Controls

Observations

Incidents/Vulnerabilities

provide the expert with additional information to improve the accuracy of their forecasts

provide prior evidence of loss event frequency



Asset Inventory

Where do we ~~pour~~ store these features?

Asset Inventory

Asset Inventory provides a way to navigate and query relationships between disparate infrastructure data sources such as application metadata, laptops, databases, etc. to enable us to operate confidently on challenges that span our complex environment.

Asset Inventory Application Feature Examples

Example Risk Reduced Controls:

Internet facing

MFA

Secure database proxy

Updated AV

Critical application proxy

Non Employee access

Asset Inventory Demo

Data Model

How Do We Survey?

In Person Meeting

We introduce forecasters to the process

Calibration

Risk team offers optional calibration training to improve accuracy

Survey

On their own time, they fill out a 50 question survey

Refine

We revisit results, work through outliers, and collect feedback on the process

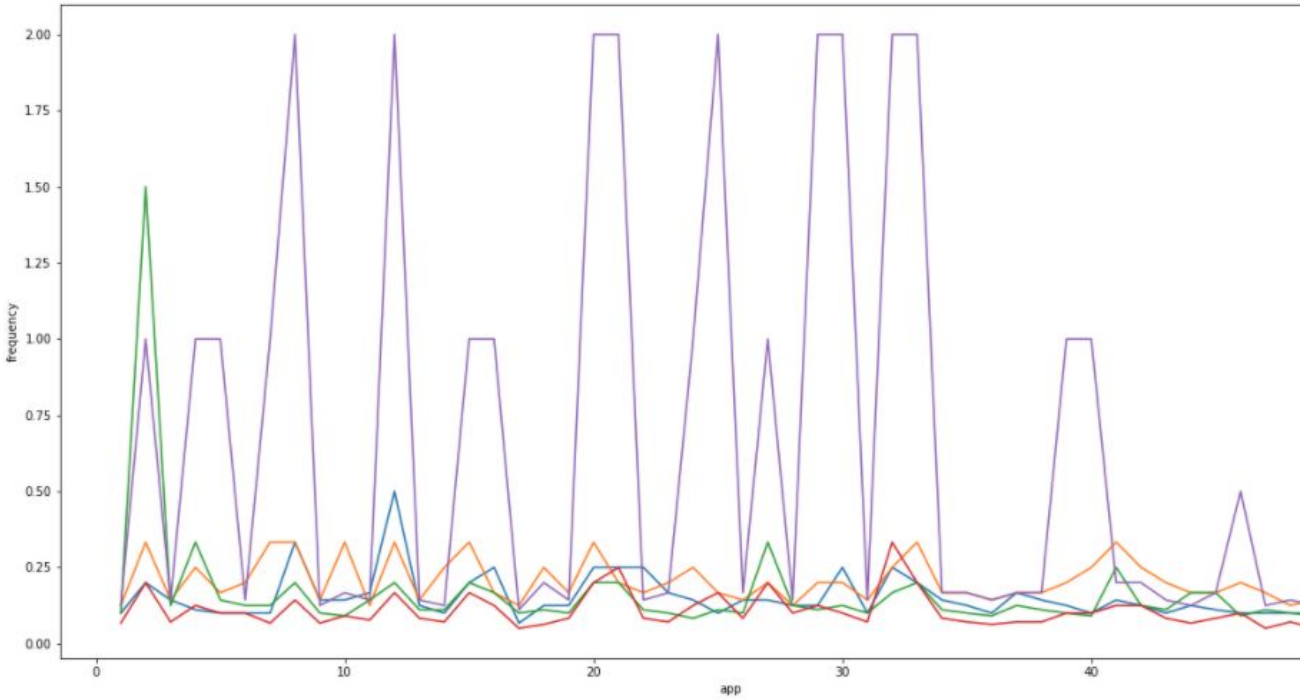
App 0

Feature	Score
Internet Facing	TRUE
Uses Secure Application Gateway	FALSE
Missing SSO	FALSE
Missing Authorization Evidence	TRUE
Uses Secure Database Gateway	TRUE
Missing Application Firewall	FALSE
Missing mTLS API Protection	FALSE
Critical Vulnerabilities	0
Non-Employee Access	0
Employee Accss	32
Oldest Instance Age in Days	35
Frequency	

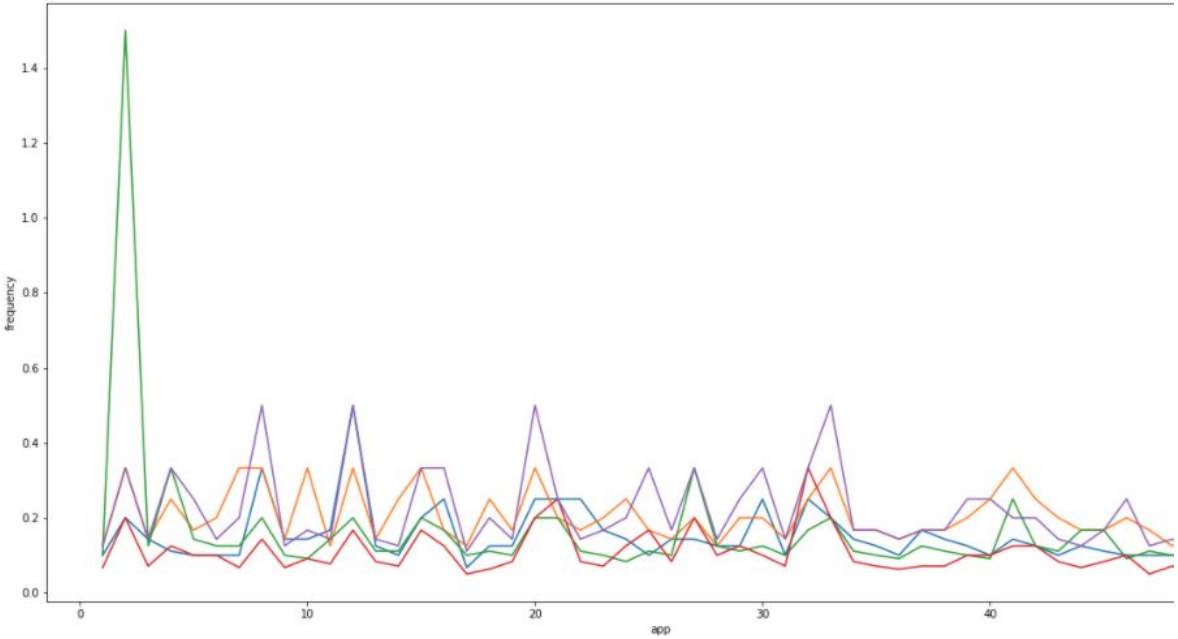
Loss Event Frequency

One time in the next 5 years: 0.2

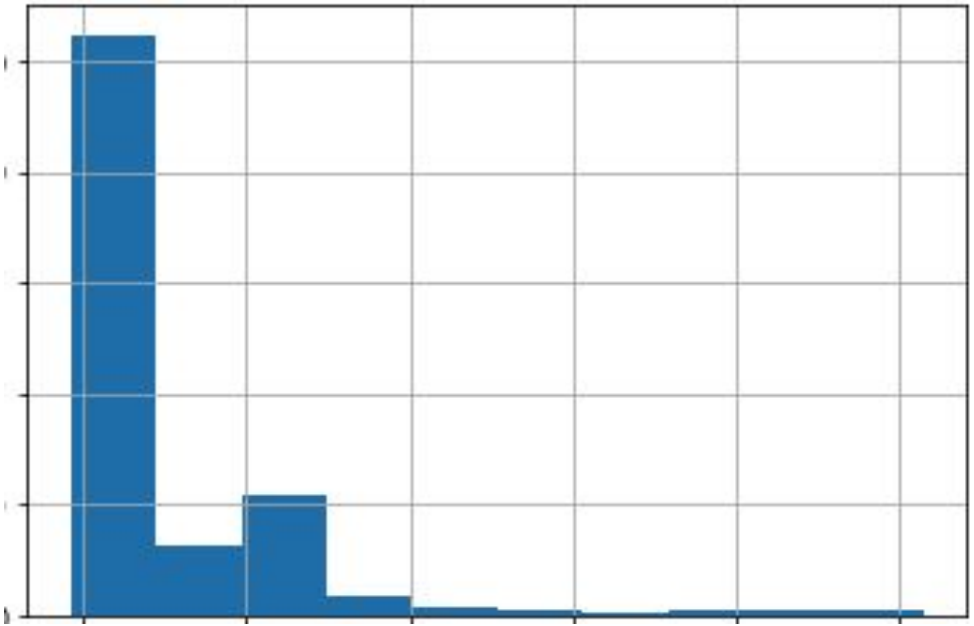
Review Loss Event Frequency by Application and Forecaster



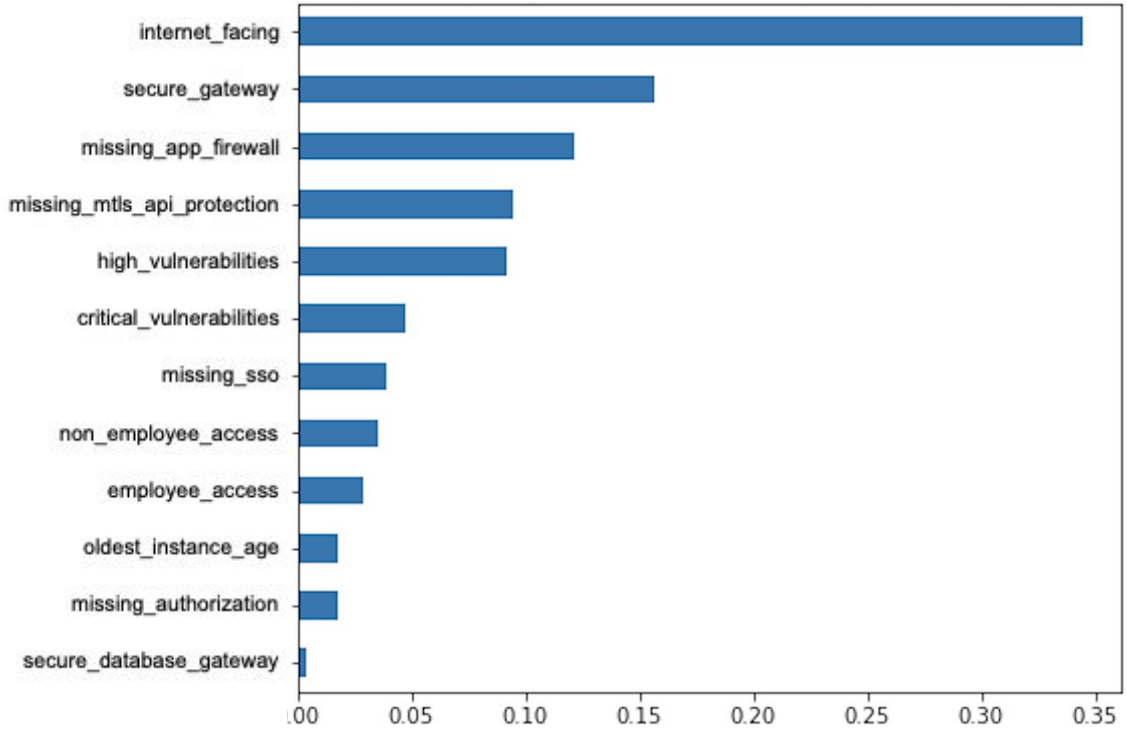
Outliers



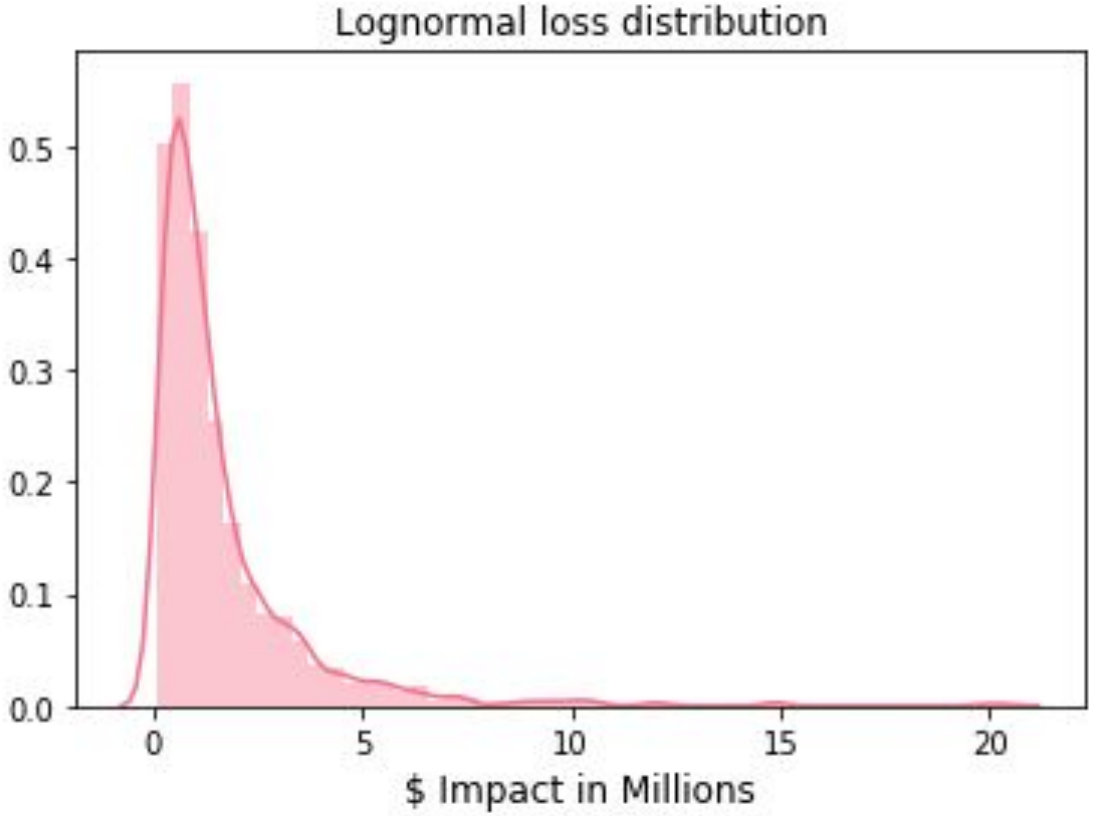
Build Model of Loss Event Frequency



Feature Importance



Magnitude


Lognormal loss distribution
0.5
0.4
0.3
0.2
0.1
0.0
0
5
10
15
20
$ Impact in Millions

Magnitude Distribution Mean x Frequency = $Annualized Loss

Magnitude Distribution Mean x Frequency = $Annualized Loss

Impact: [$100,000, $1,000,000]

Lognormal distribution mean: $400,400

Magnitude Distribution Mean x **Frequency** = $Annualized Loss

One time in the next 5 years: 0.2

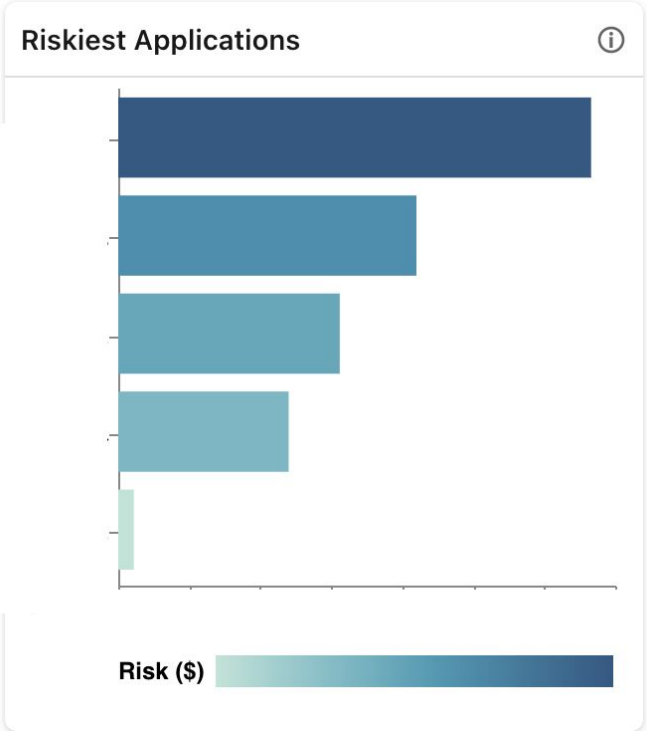
Magnitude Distribution Mean x Frequency = $Annualized Loss

$400,400 x 0.2 = $80,800

Write to Asset Inventory


```
{
  "data": {
    "applications": [
      {
        "isActiveGuess": true,
        "languageList": [
          "java"
        ],
        "applicationCommunicatesWithDatabasesBySubject": [],
        "fw_has_risk_factor": [ ↔ ],
        "fw_has_paved_road_practice": [ ↔ ],
        "applicationHasRiskScoresBySubject": [
          {
            "riskScoreByObject": {
              "riskInDollars": "7200",
              "riskMagnitudeDistribution": {
                "mode": 0,
                "median": 0,
                "minimum": 0,
                "tenth_percentile": 0,
                "ninetieth_percentile": 40000
              },
              "frequency": "0.18"
            }
          }
        ]
      },
      {
        "isActiveGuess": true,
        "languageList": [
          "java"
        ],
```

Security Guide and Dashboard Demo



94%

App risk model accuracy from 2020 to 2021

10%

Every application with an incident or bug bounty payout was in the top 10% by frequency from 2020 to 2021

What Did We Get Wrong?

Too precise

Too many features

Feature confusion

Unclear scenario

Data reliability

Not enough coffee

Sage Limitations

Emphasis on Paved Road

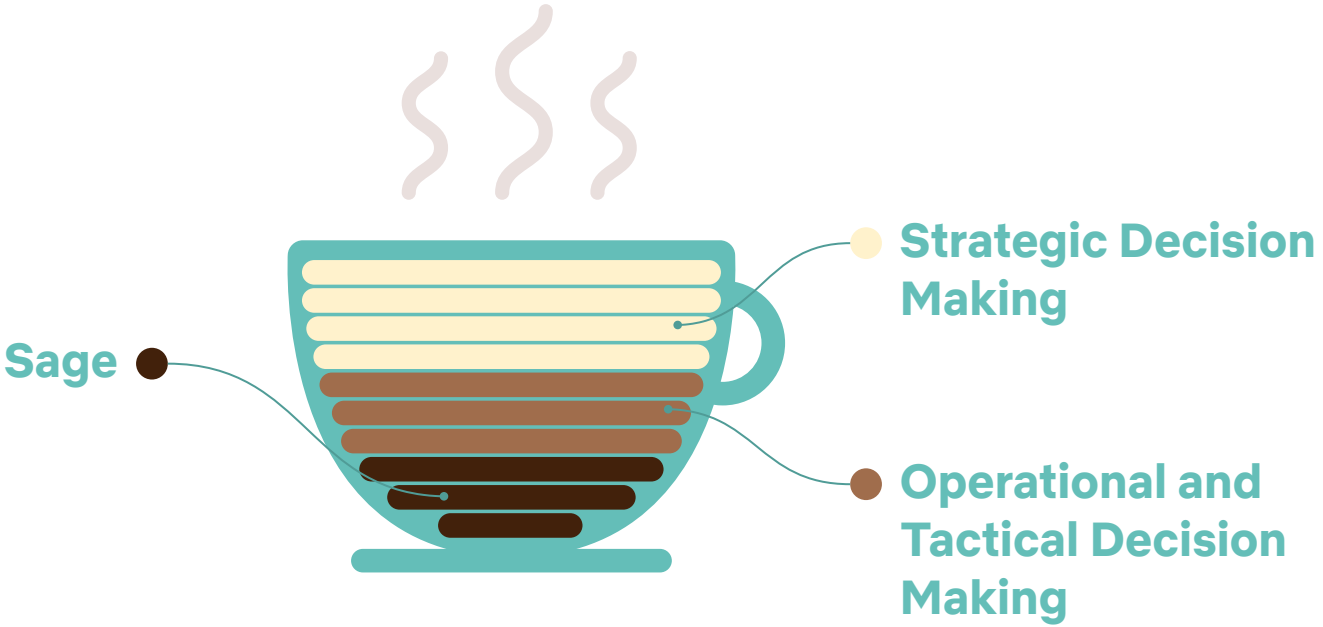
Magnitude uncertainty

Data incongruities

Experts can be wrong

Many risk scenarios happen infrequently

Conclusion


Strategic Decision Making
Sage
Operational and Tactical Decision Making

Thanks

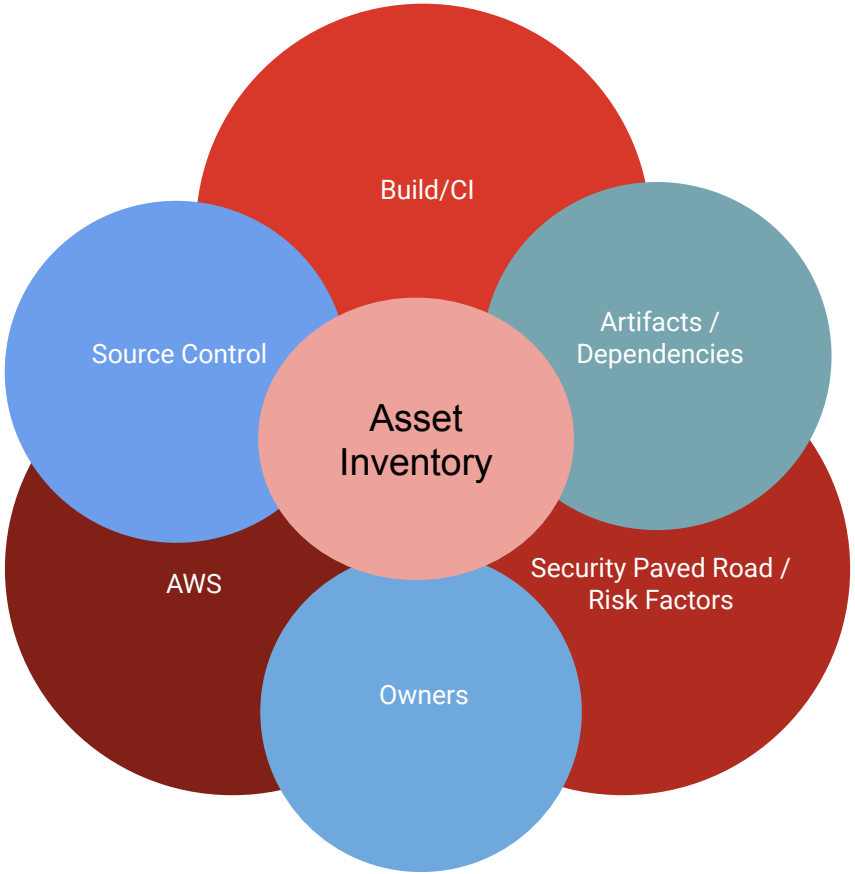
Dave King
Paul McMillan
Tony Martin-Vegue
Aubrey Sharwarko
Jai Balani
Felipe Munera Savino
Amit Patil
Markus De Shon

Questions?

Riskquant library

Quantifying Risk QCon Presentation

Asset Inventory



Which applications are Internet Facing and have employee access events?

What is the risk score for the appfoo application?

What applications are owned by Bryan Payne's org which are written in Java?

Which applications talk to RDS?