Cambridge Centre for Risk Studies

The Future of Cyber Risk Conference 2019

The Evolution of CyberSecurity Risk Ratings

Jasson Casey, CTO

Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

SecurityScorecard Company – Overview

- Founded in 2014, NYC HQ, offices worldwide
- Venture funded by **Sequoia Capital, Google**, Nokia, & others
- **#1 rated solution By Gartner Peer Insights, Forrester Wave leader**
- Use Cases: **VRM, Self Monitoring, Cyber Insurance, and others**
- **1,000,000+ rated companies** (10X any solution)
- Trusted by 650+ enterprise customers **engaging 150,000+ other companies**
- **Proprietary risk model** proving SSC grades linked to likelihood of breach

Basics of Cyber Security Risk Ratings

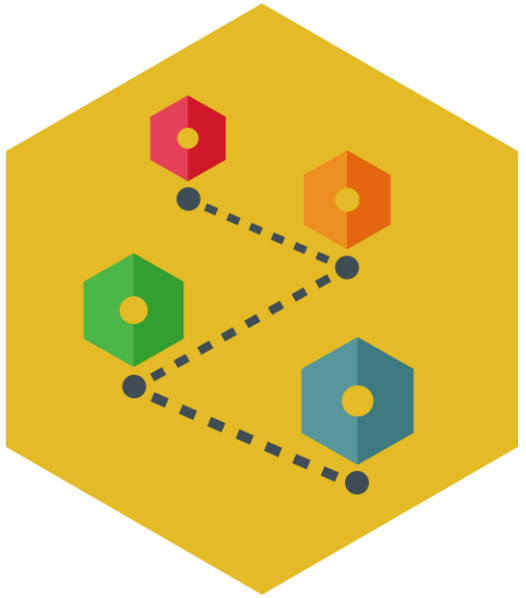
- **Data collection** – active & passive collection and asset discovery
- **Attribution** – relate digital assets to business entities globally
- **Measurement** – produce security judgements over observed hygiene, behavior & incidents
- **Scoring** – model building & entity rating

Collection – what is out there?

- **Rich data sources –** scanning, routing, registries & observations
- **Global presence –** regional collection necessary for comprehensive visibility
- **Contextualization –** deep analysis only possible with collection context
- **Adversarial tracking –** general and targeted threat intelligence

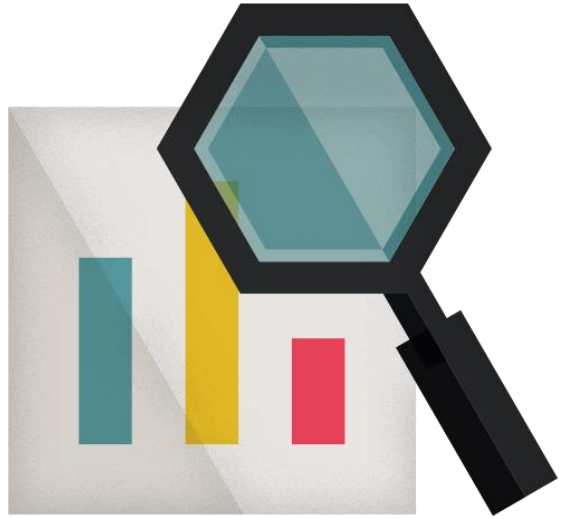
Attribution – who controls what?

- **Rich data sources –** scanning, routing, registries & observations
- **Probabilistic techniques –** signals provide estimates & error
- **Relationship analysis –** interaction between services is itself a signal
- **Signal compositing –** increase confidence to yield a conclusion



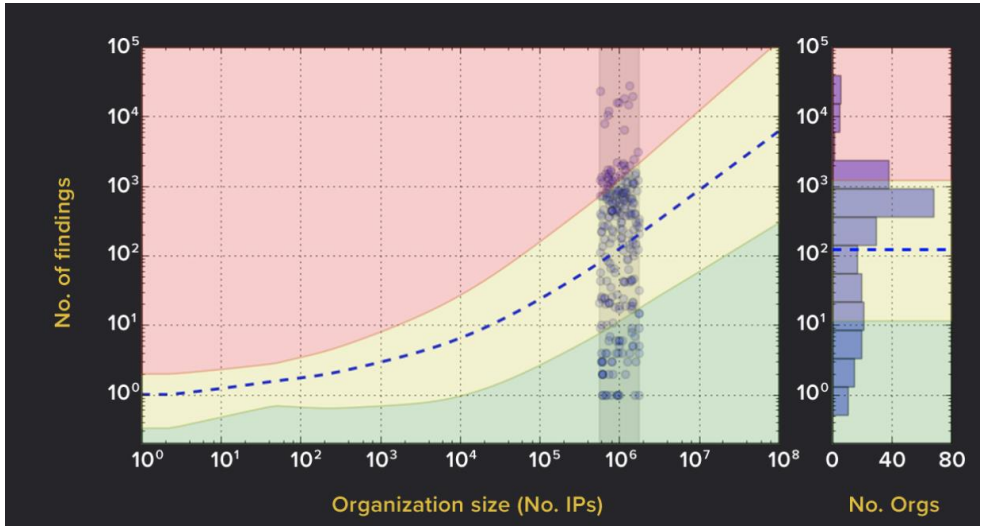
Measurements – what can we say?

- **Judgement – observations, assumptions, logic & conclusion**
- **Hygiene – claim against an asset: best common practices, weakness, vulnerability**
- **Behavior – model of interaction driving change over a collection of assets**
- **Incidents – highly suspicious signals emanating from an asset**



Scoring – what should we do?

- **Model – underlying mathematics that drive the scoring process**
- **Calibration – process for updating the scoring model**
- **Cadence – frequency of entity scoring**
- **Efficacy – claims of risk reduction, breach likelihood of entities and portfolios**



Principles for Fair and Accurate Security Ratings
U.S. Chamber of Commerce

- **Transparency**
  - Free scorecard for rated companies
  - Score planner tool to plan improvement
- **Dispute, Correction and Appeal Workflows**
  - Error reporting and dispute support
  - 24-hour turnaround on feedback
- **Accuracy and Validation**
  - Our models used by proxy advisories, baked into insurance underwriting models
  - Backed by 3rd party risk & loss firms
- **Model Governance**
  - Independence - grades are not impacted by customer relationships
  - Confidentiality - companies control distribution of their confidential information

So Now What?

Key Observations

- **Vulnerability Management Confusion**
- **Most exist in some state of compromise**
- **Effective security is a team sport**
- **Existing frameworks could be used to model a team's performance**

Traditional Vulnerability Scanners

- **Provide a laundry list of security issues of varying severity**
- **Intrusive, one-time : can only do it on your own company**
- **The companies are inundated with data and don't know what to focus on first**

You have an expired SSL certificate on 1.2.3.4

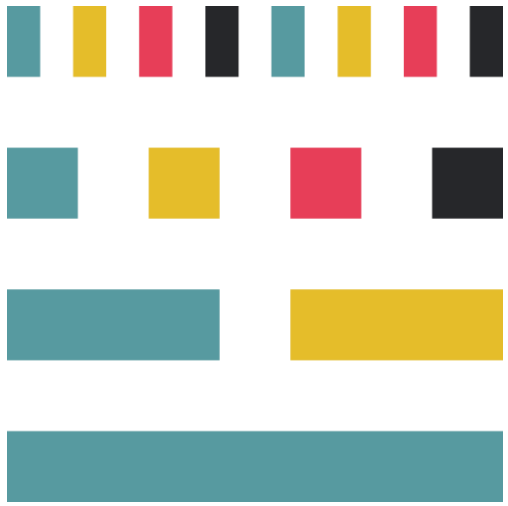
RDP port 3389 is exposed on 1.2.3.4 at 4/21/2019

This endpoint is vulnerable to CVE - CVE-2014-0160 Heartbleed vulnerability

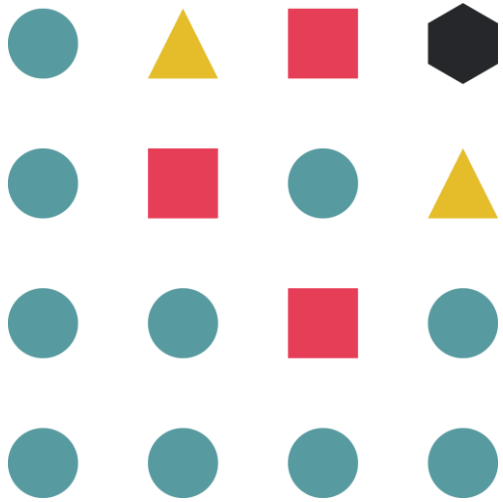
There is a Zeus botnet signature observed on 192.168.1.201 on 4/21/2019

Next Frontier : Focusing on Organizational Behavior Measurements

- **Measuring behavior is more meaningful than measuring absolute the number of issues**
- **Quick rate of response and high uniformity indicative of mature practices**



Rate of Response



Uniformity of Response

Modeling a Team – pick a framework!

- **Identify –** asset attribution and discovery
- **Protect –** asset hygiene
- **Detect –** collective asset behavior
- **Respond –** collective asset behavior
- **Recover –** not sure?

Reducing time to detect and time to respond will make companies more resilient to threats

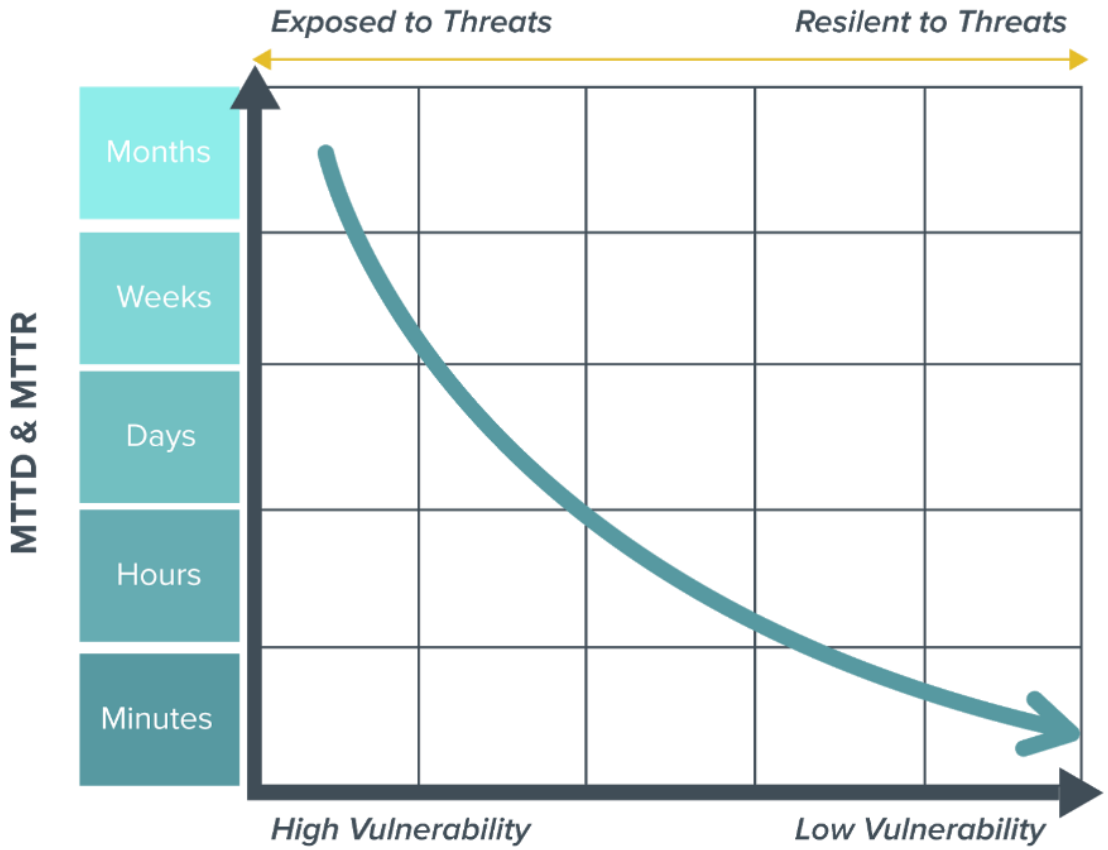


Image and statistics from LogRhythm: https://www.slideshare.net/LgRhythm/5-obstacles-to-faster-cyber-threat-detection-and-response-slideshare

Critical Metrics in Org Health

Level of preparedness

Time to Detect

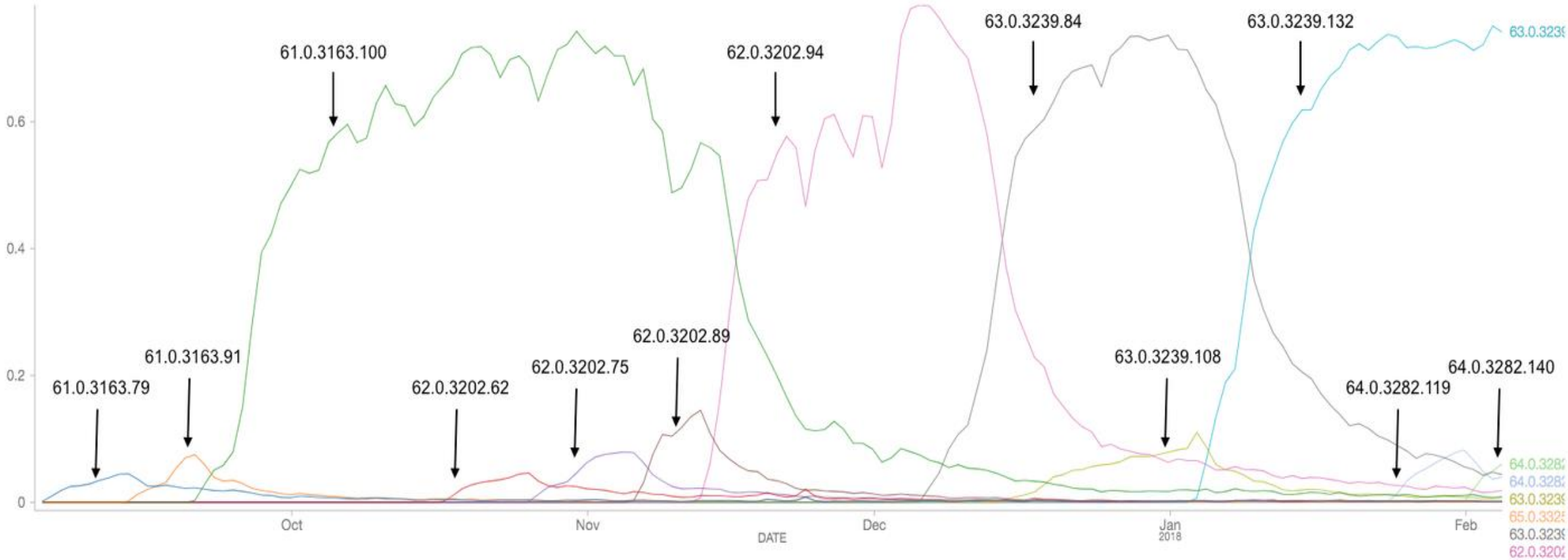
Time to respond

HACKER'S WINDOW OF OPPORTUNITY

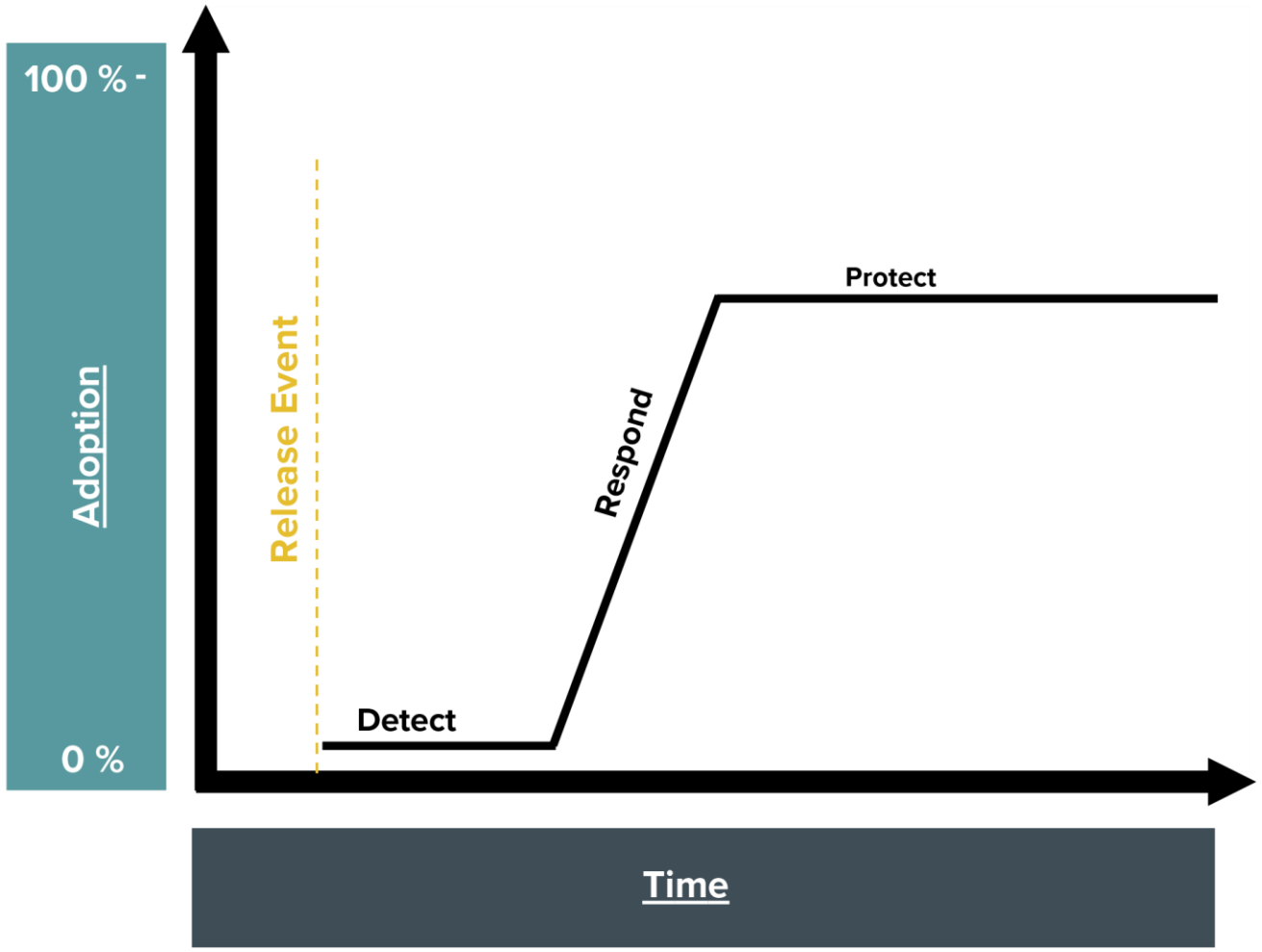
Image and statistics from LogRhythm: https://www.slideshare.net/LgRhythm/5-obstacles-to-faster-cyber-threat-detection-and-response-slideshare

Show me!

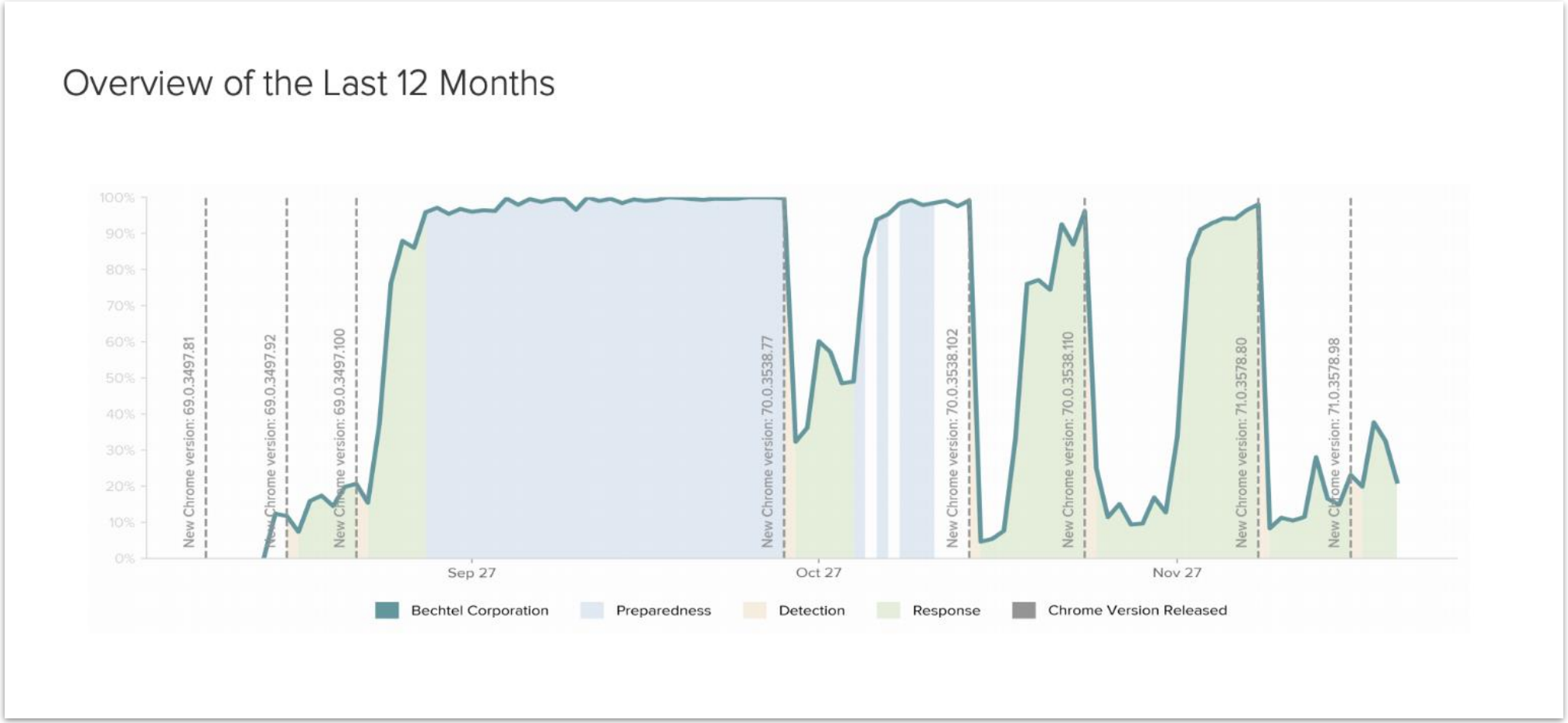
Browsers – Lets start with endpoints



Applying the NIST Framework to Evaluations of Third Parties

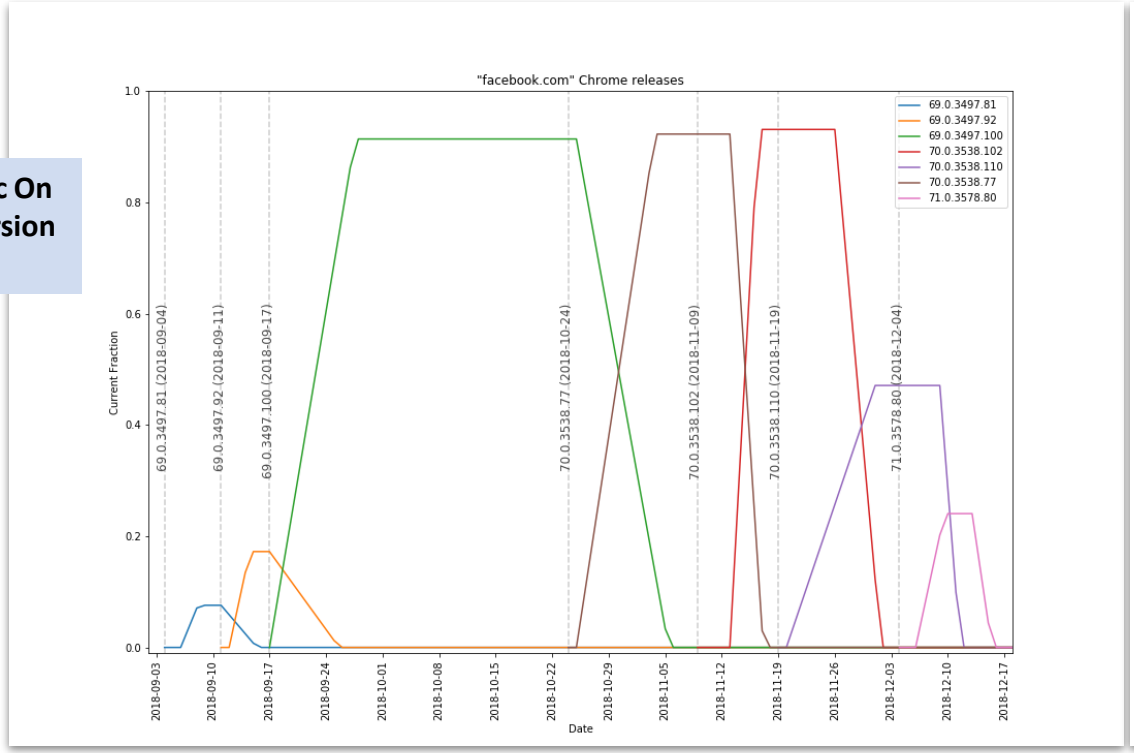


Historical Trend for that Supermarket Chain

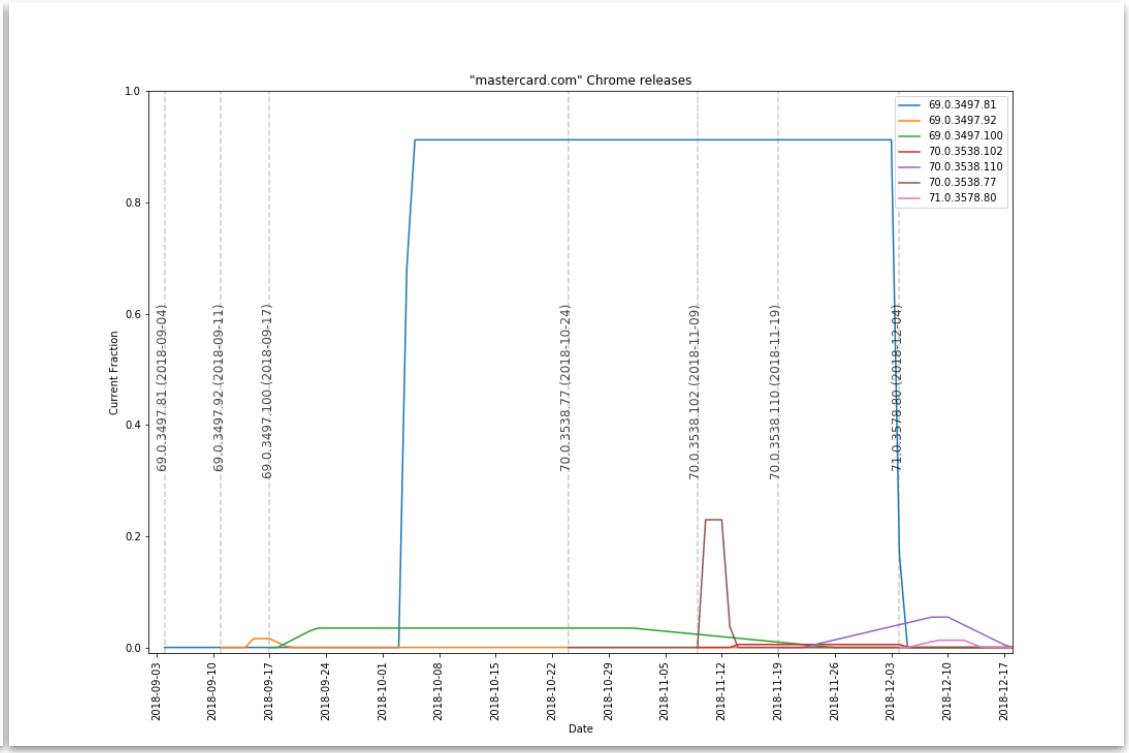


Tracking Against Public Release Cycle

% Traffic On that Version



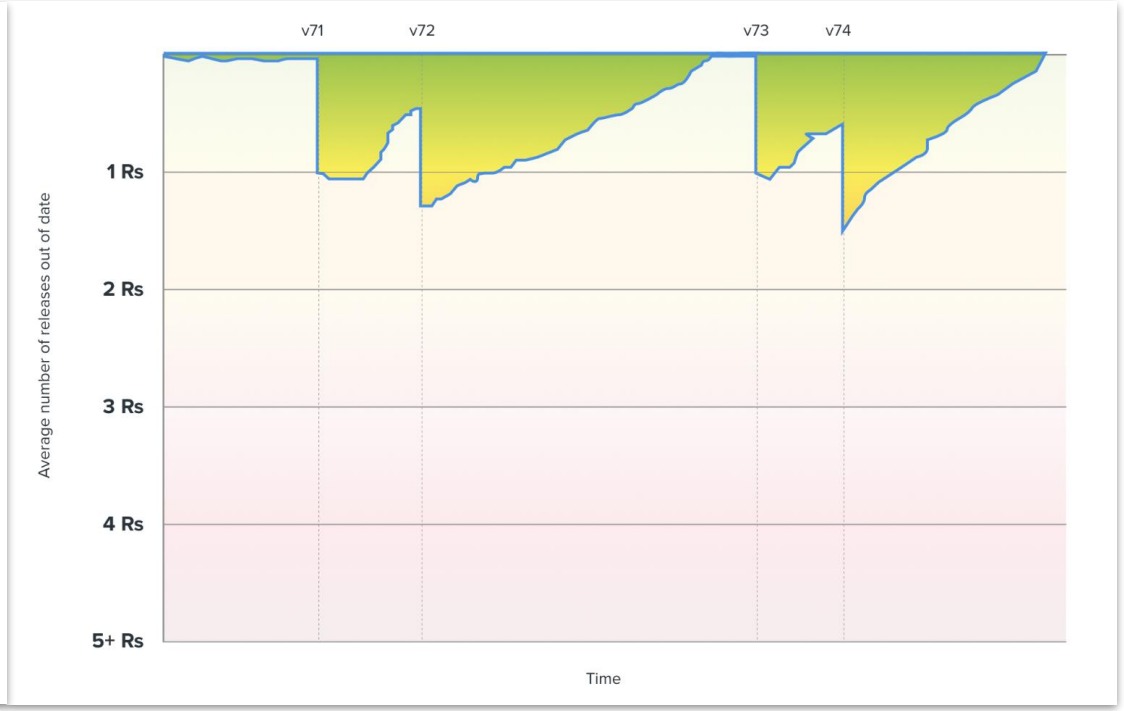
Follows the public release cycle



Doesn't follow public release cycle

Browser Age: A Reflection of Cybersecurity Posture

 # releases out of date



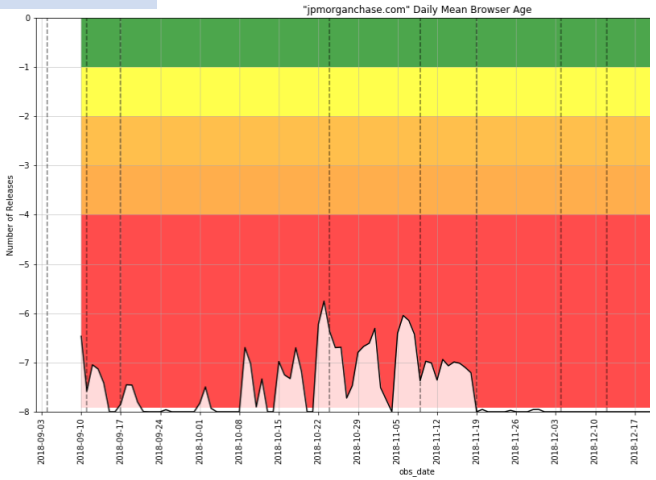
Slow Adopters

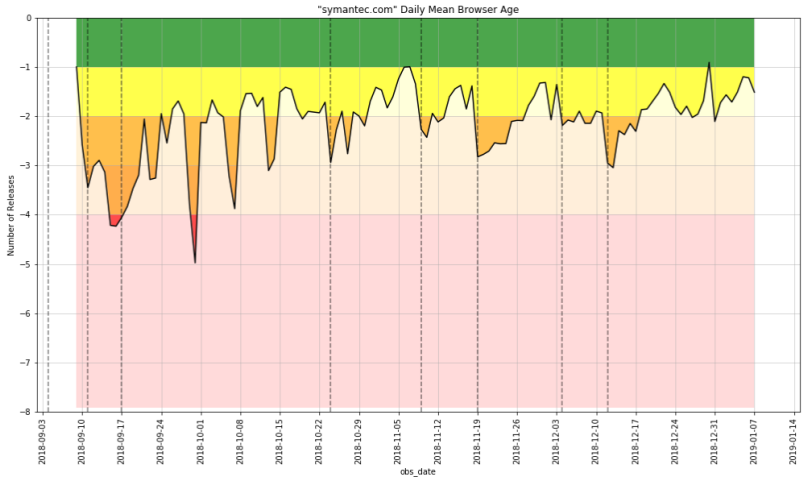
Fast Adopters

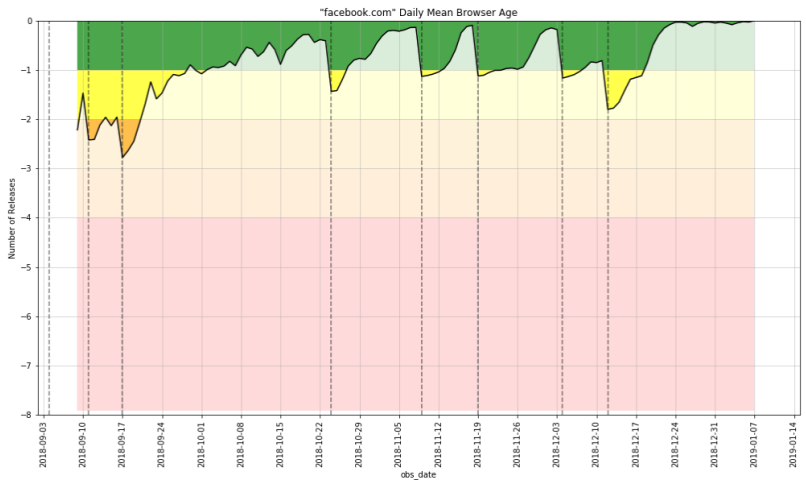
UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for Risk Studies

Spectrum of Organizational Health

 # releases







A large investment bank

Browsers are rarely up-to-date; frequently hit the -8 release limit.

A security company

While some updates require a little longer than we should expect, this is behavior is fairly good.

A social media platform

While some updates require a little longer than we should expect, this is behavior is fairly good.

Cybersecurity Program Maturity

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School