Cybersecurity in Software Development

PRESENTER

Cat Easdon

Senior Privacy Engineer &
Team Captain

Who am I and why am I talking to you?

- Lead Dynatrace's Privacy Engineering team in close collaboration with our Product Security teams
- 🏔️-obsessed Brit based in Innsbruck
- Previously: also a Virtual Routes fellow!, Internet Society fellow, CPU security research at TU Graz, Palantir PCL
- No academic background in policy, but I try to contribute where I can

Disclaimer

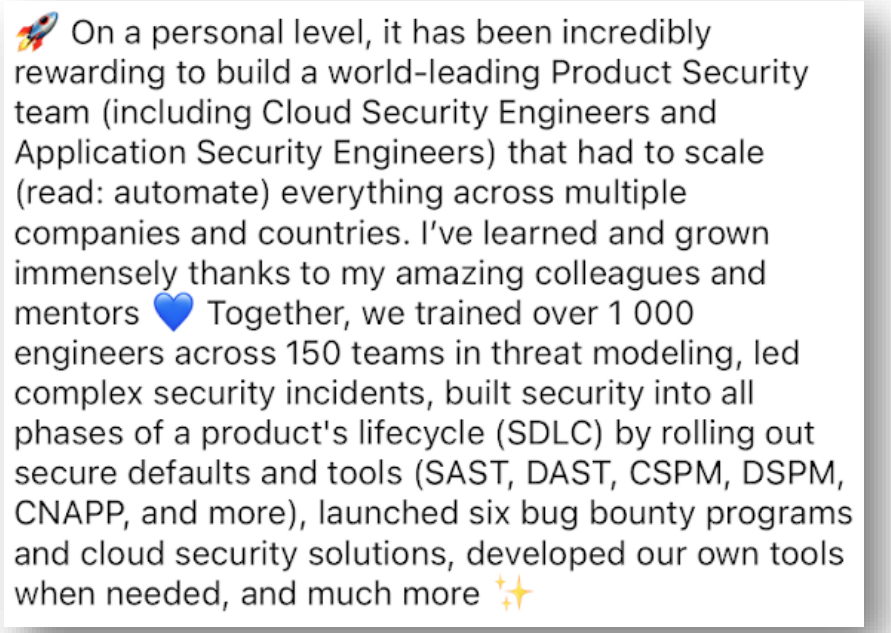
"If they've made a mistake, correct them gently and show them where they went wrong. If you can't do that, then the blame lies with you. Or no one." ~ Marcus Aurelius, Meditations, 10.4

- Opinions will be expressed in this presentation!
- Those opinions are my own, not Dynatrace's
- We'll look at case studies not to lay blame - because everybody makes security mistakes *(myself included!)* - but to understand how breaches occur and how we can reduce their likelihood

Warm-up

How comfortable do you feel with these concepts?

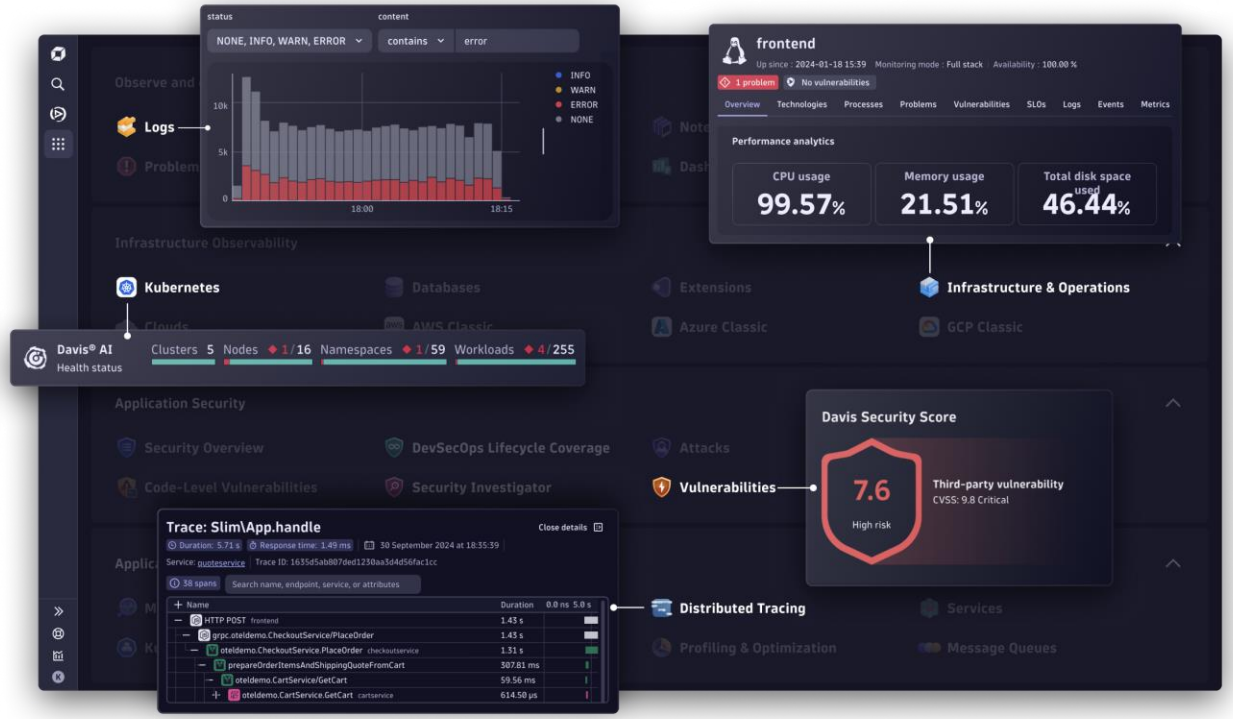
- Microservices
- Observability tooling
- The cloud shared responsibility model
- The software development lifecycle
- Software-level security and privacy controls ->



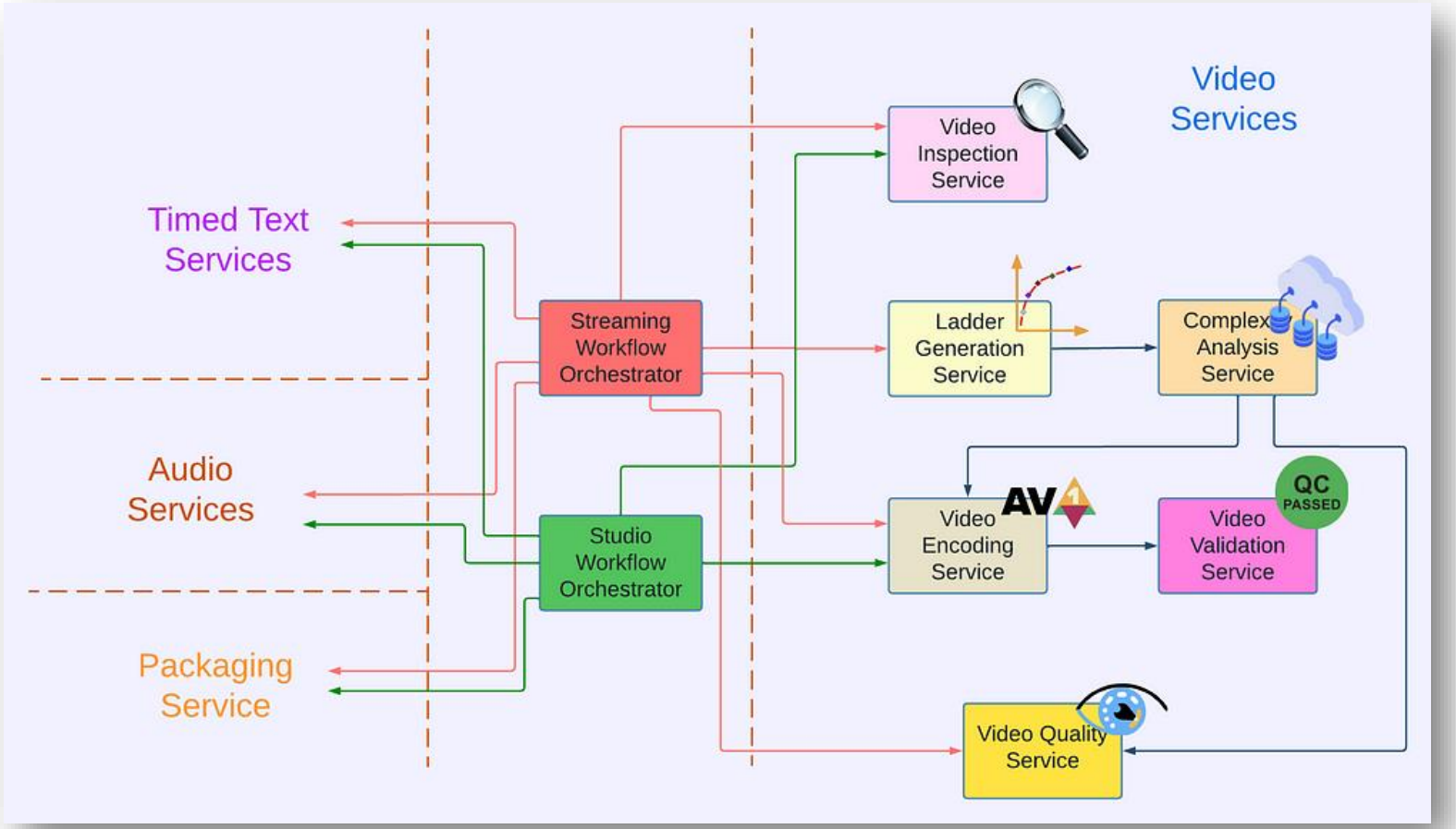
Source: Ståle Pettersen, LinkedIn. His accomplishments are a great summary of key topics that product security teams work on. Do you know all of these terms?

What does Dynatrace do?

- Observability platform with SaaS and on-prem offerings
- ~$1.5 billion ARR, ~4000 customers, ~5000 employees
- Customers including BT, EDF Energy, National Grid, Deutsche Telekom, TSB, Allianz, Air Canada, Walmart, State of Minnesota

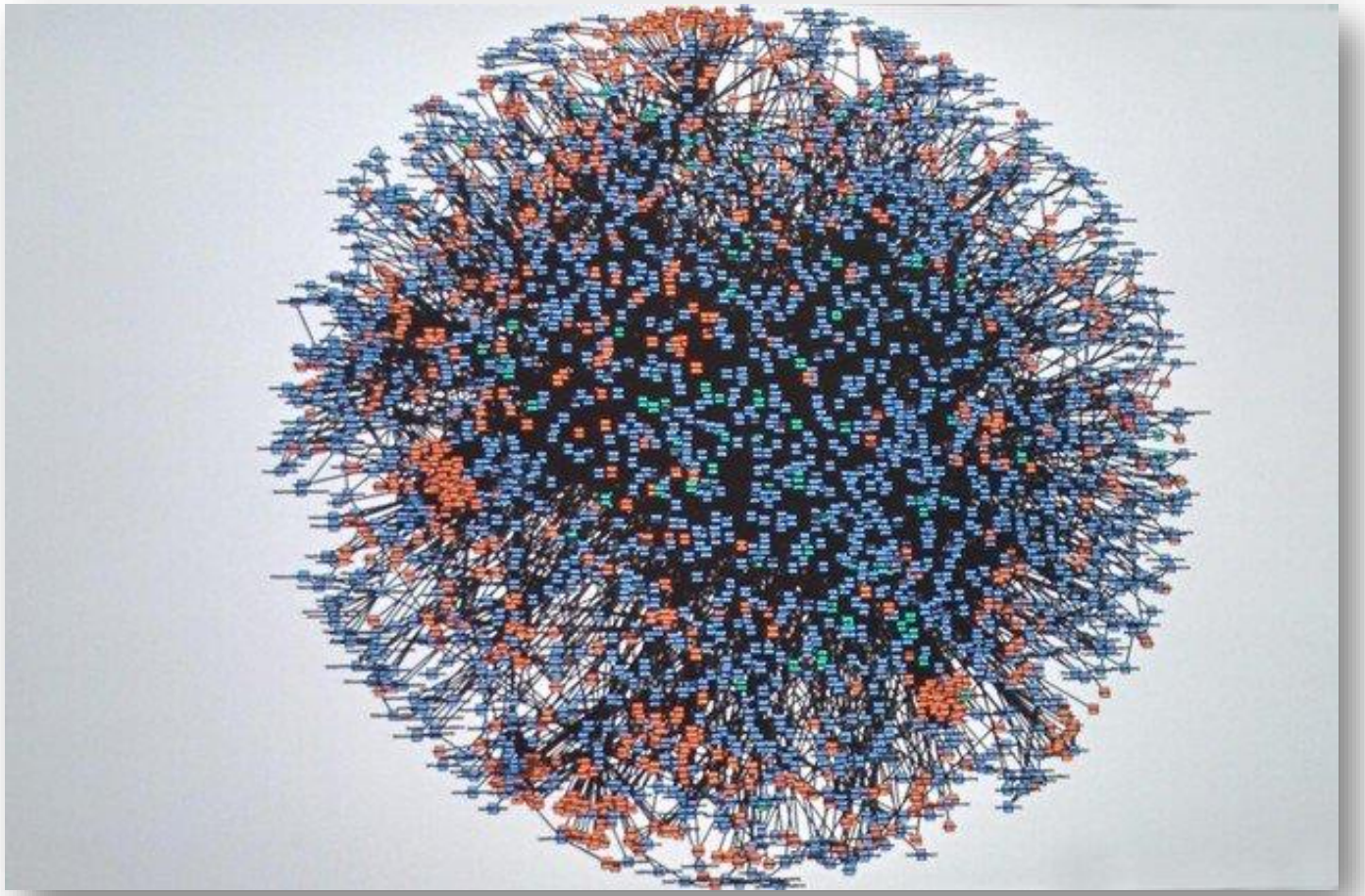


What's the point of observability tooling?



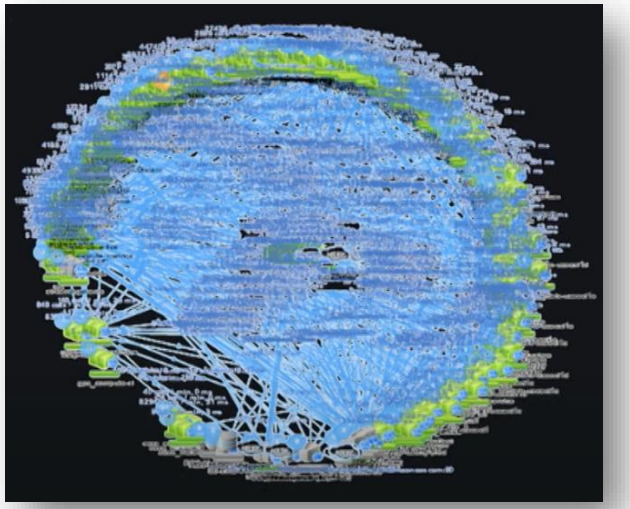
Netflix's microservices architecture for video processing. Source: [Netflix Technology Blog]

What’s the point of observability tooling?



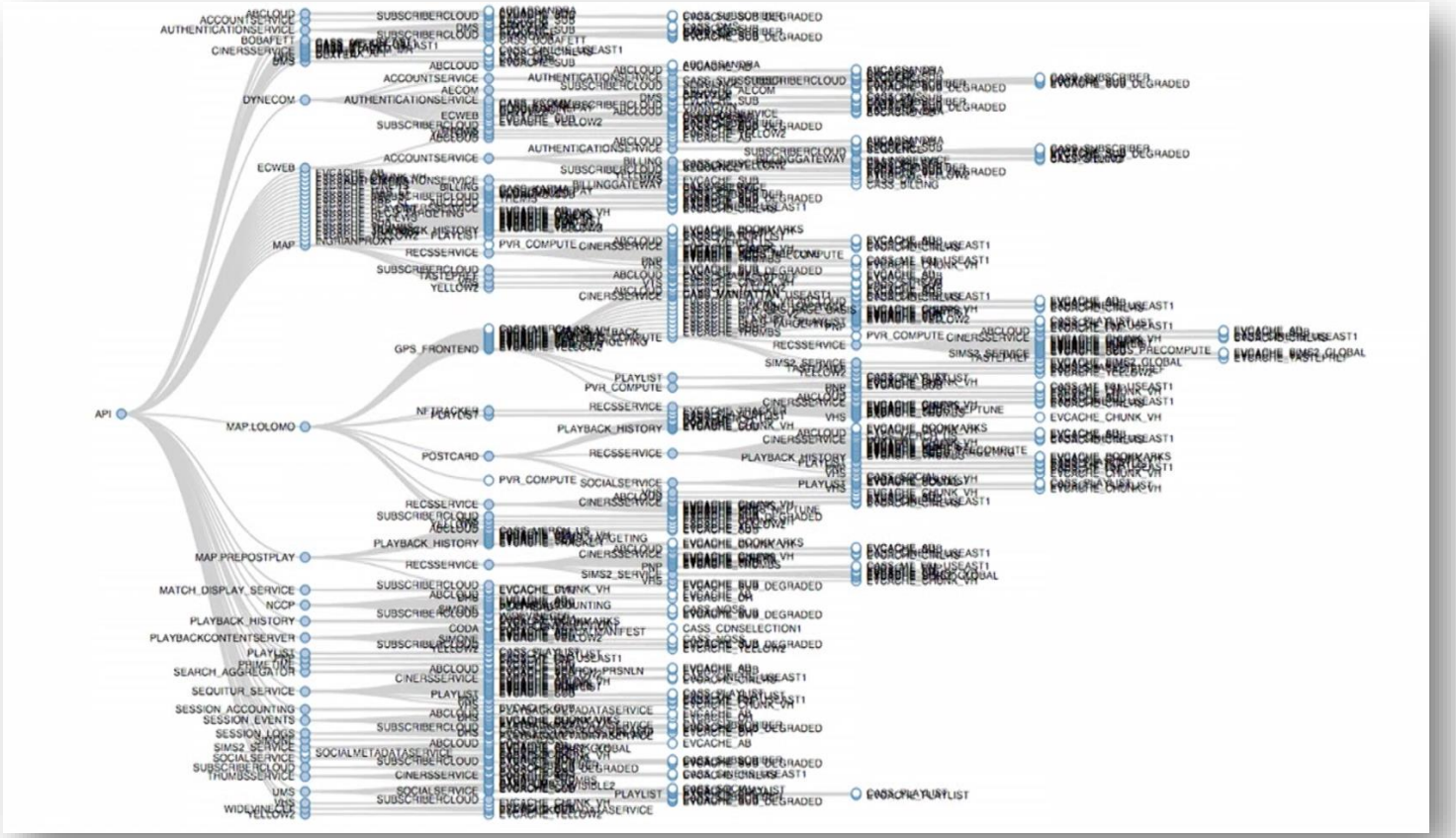
Visualization of dependencies between Amazon.com’s microservices in 2008. Source: Werner Vogels

What’s the point of observability tooling?



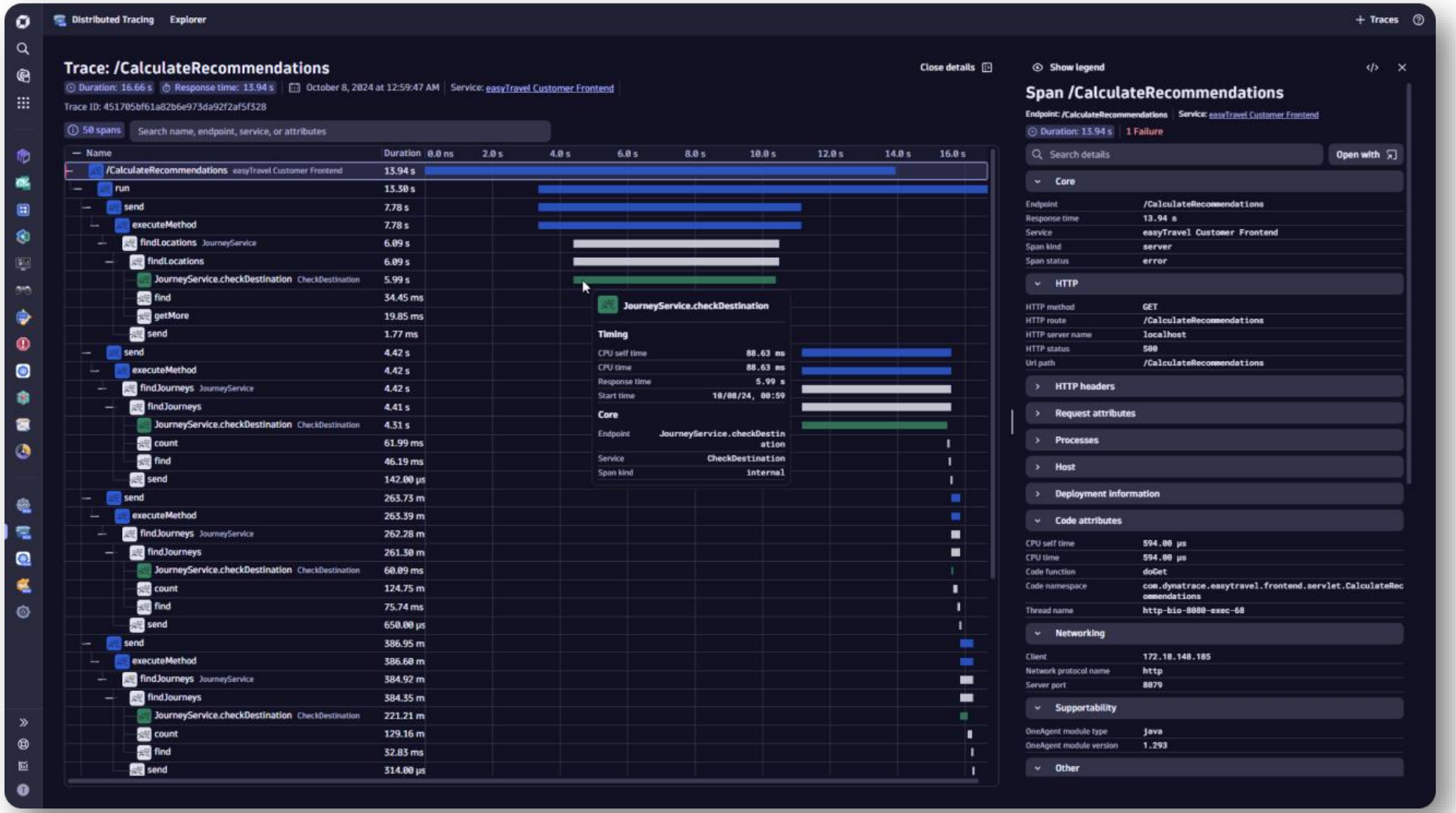
Netflix ecosystem

100s of microservices
1000s of daily production changes
10,000s of instances
100,000s of customer interactions per minute

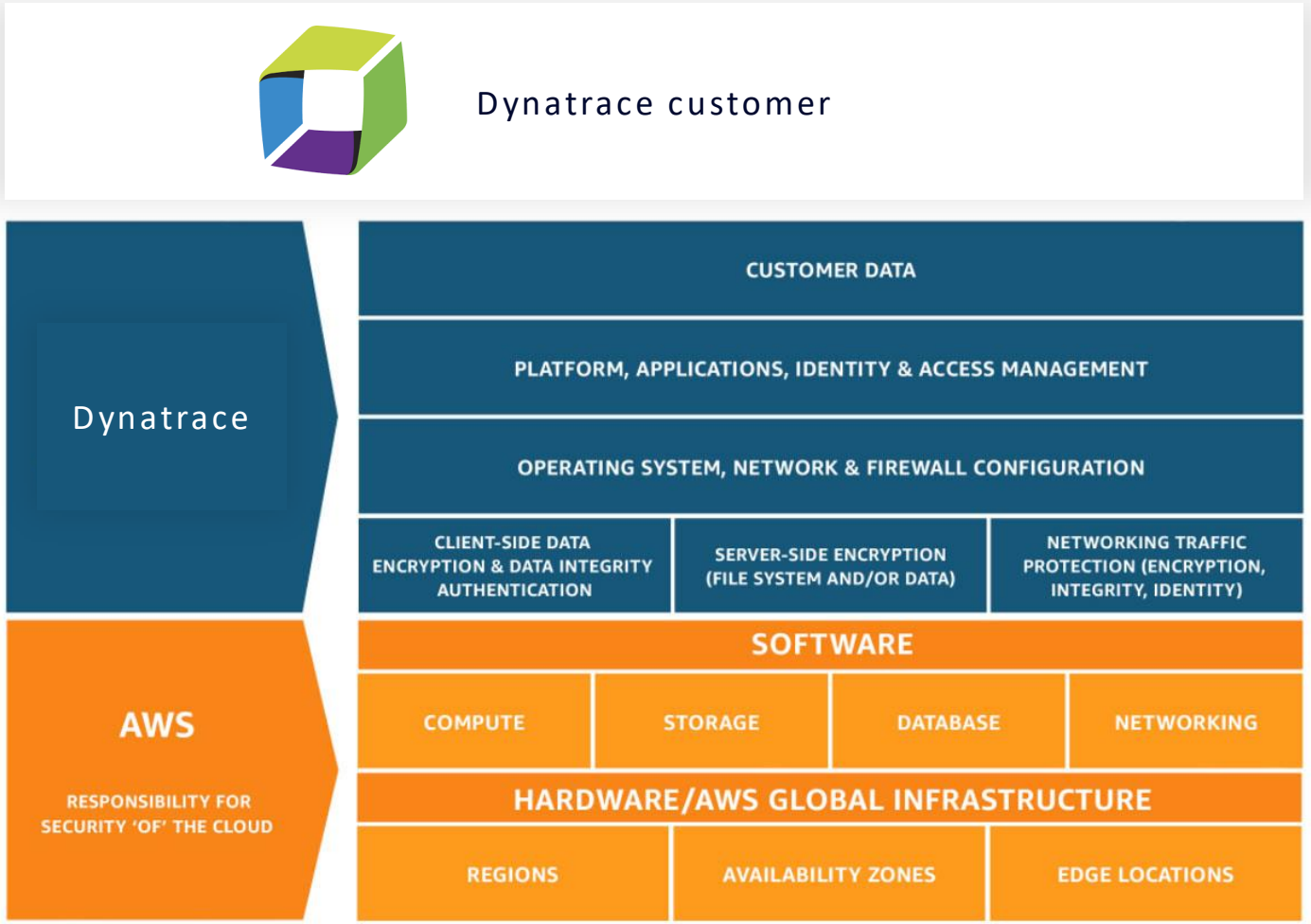


Source: [Dave Hahn, AWS re:Invent 2015](). Recommended read: [How Netflix works]()

Navigating Microservice Complexity



Cloud Shared Responsibility Model: B2B SaaS



Google Cloud

HETZNER
SERVER · CLOUD · HOSTING

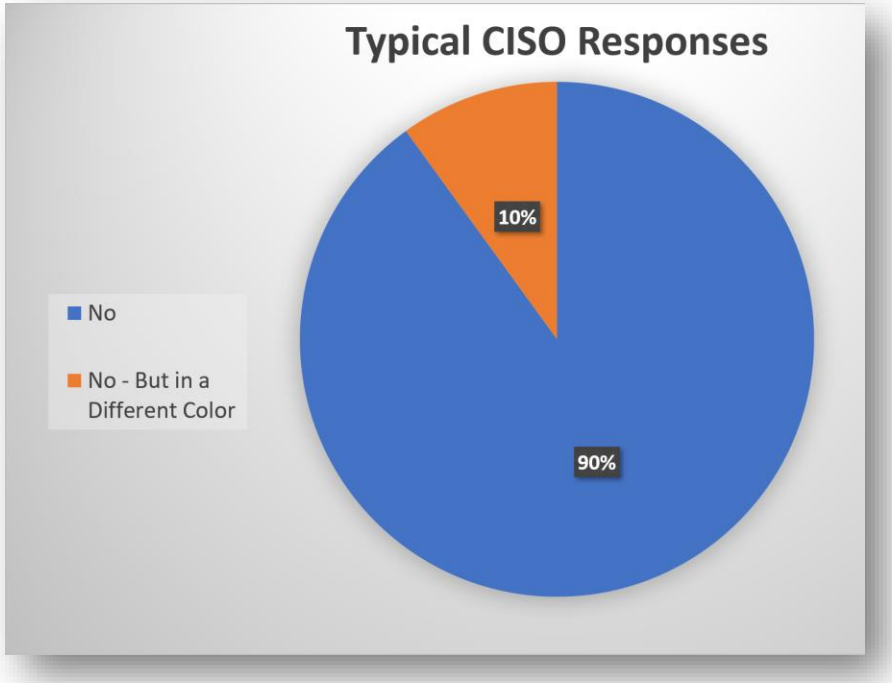
How do software companies reason about security?

- Customer expectations and perceptions
- Security posture of competitors
- Known risks and vulnerabilities; prior incidents
- Security posture of vendors that the company uses
- Existing and emerging legislation, enforcement cases
- Security maturity frameworks, e.g. NIST CSF
- *(depending on size)* Threat intelligence and geopolitical risk

How do software companies reason about security?

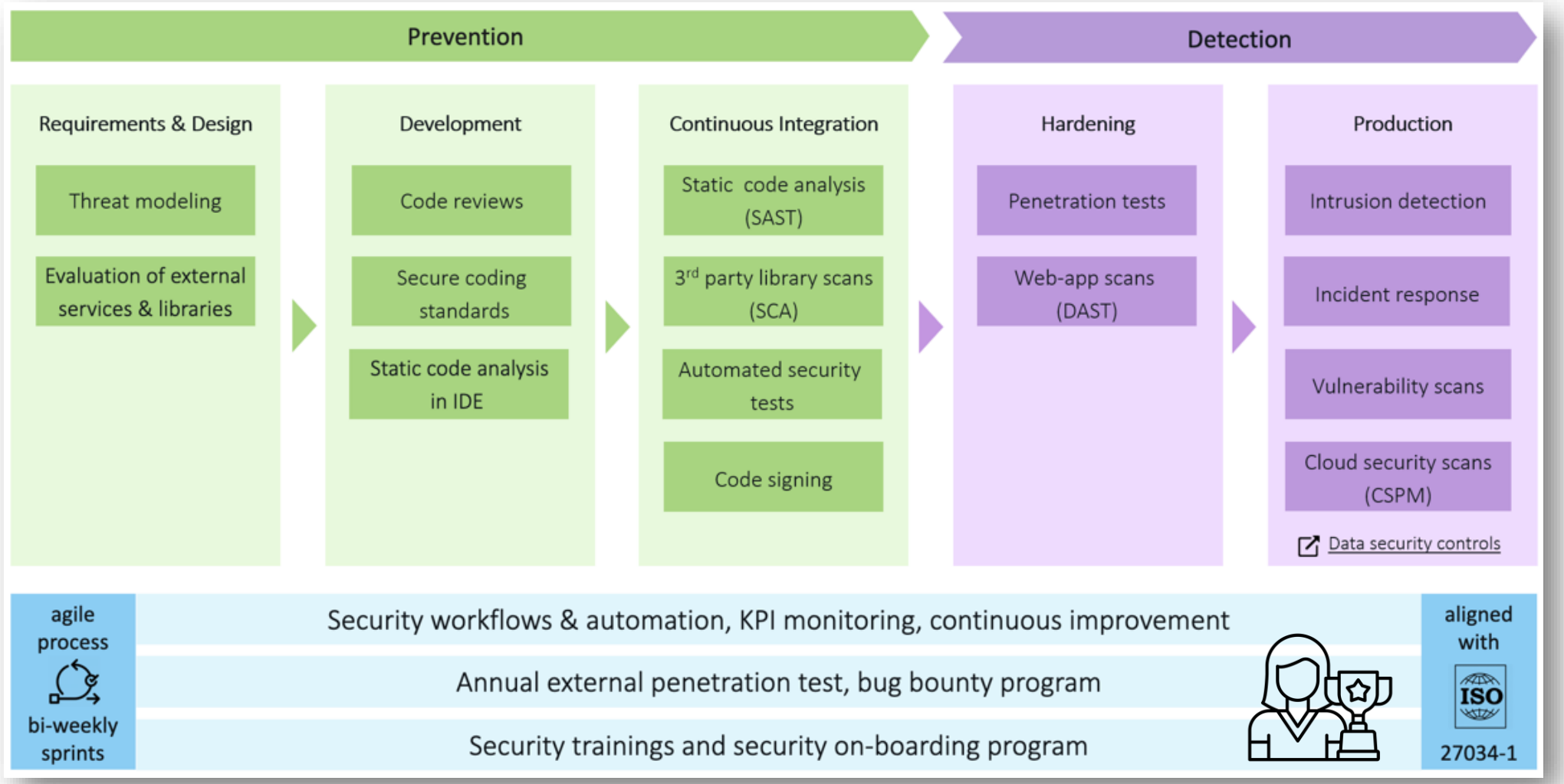
- Security is just one of many risks the business needs to manage; never the highest priority
- Availability and integrity are usually higher priority than confidentiality
- Brutal prioritization is essential; you never have sufficient resources
- Security teams try to avoid making enemies

Even Google struggles to manage vulnerabilities, particularly in open-source dependencies. They're betting on AI to tackle this



"Security as Department of No"
Source: Rami McCarthy

Secure Development Lifecycle: Dynatrace Edition

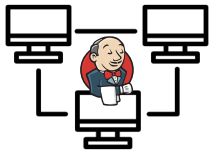


Supply Chain Security

SAST, DAST, CSPM, DSPM, CNAPP…

Data Loss Prevention

Observability Platform



Endpoint Security Tooling

Cloud Security Posture Management

Static Application Security/privacy Testing (SAST):

- Code
- Container
- Infrastructure as code

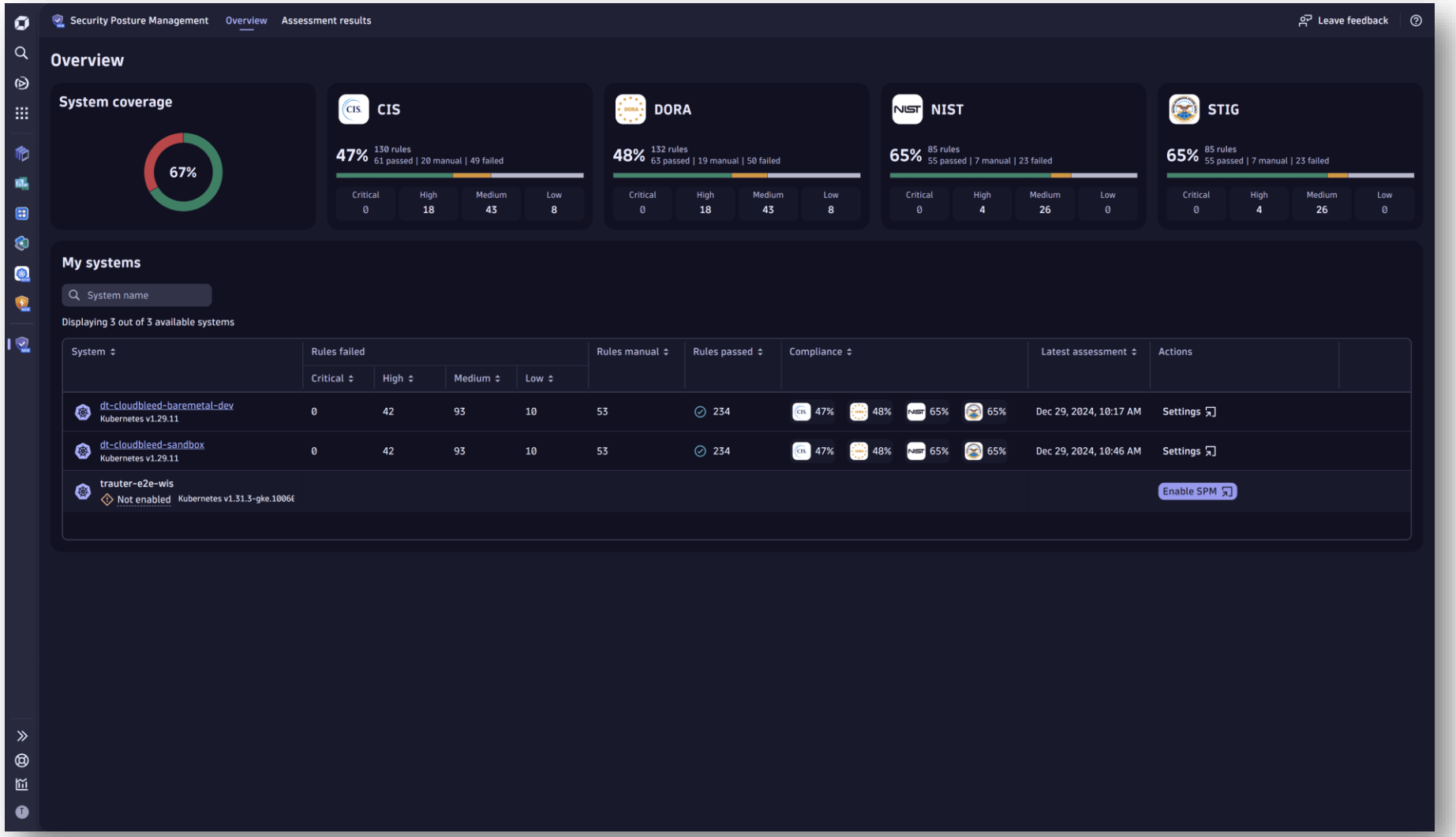
Software composition analysis and software bills of materials (SBOMs)

Data Security Posture Management

- Dynamic Application Security Testing (DAST)
- Penetration testing

CNAPP (minus endpoints) -> “we can do everything” 🪄 ✨

SAST, DAST, CSPM, DSPM, CNAPP…



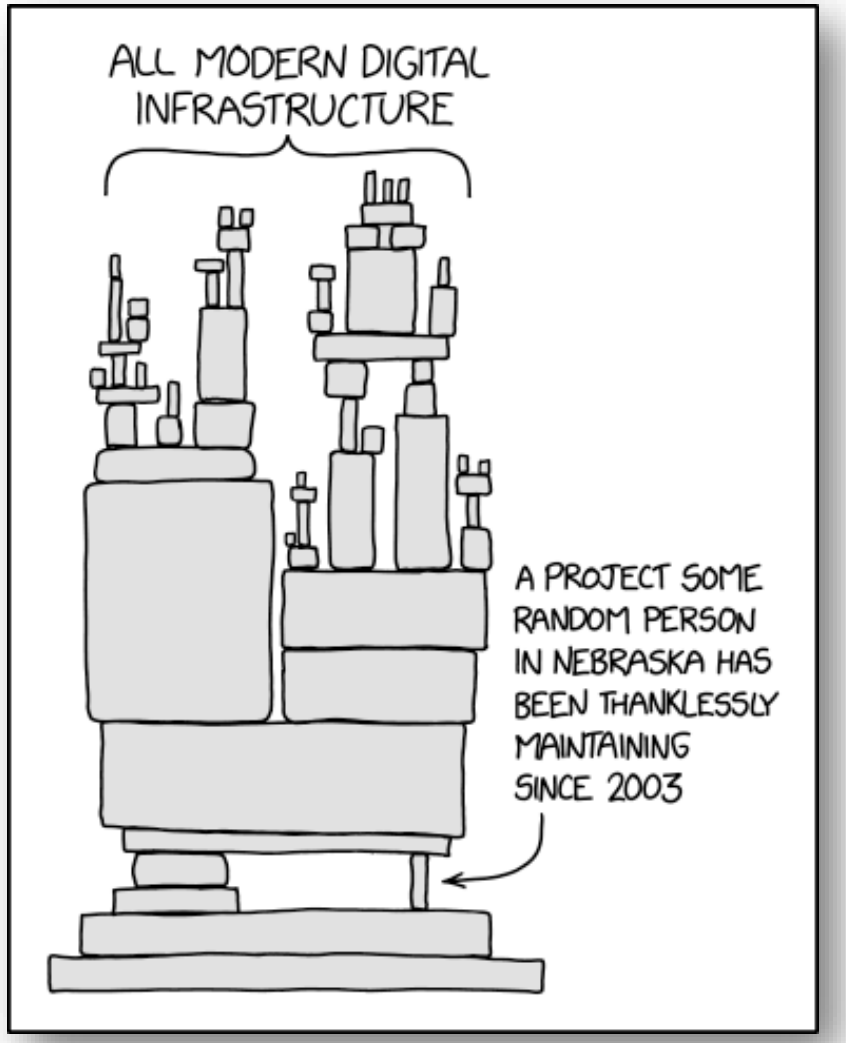
SBOMs and VEX

"Understanding the supply chain of software, obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk."

~ *US Executive Order 14028, Improving the Nation's Cybersecurity (2021)*

SBOMs and VEX

Sources: XKCD, Signal-Desktop on GitHub




```
{
 "$schema": "./package.schema.json",
 "name": "signal-desktop",
 ...
 "dependencies": {
    "@formatjs/fast-memoize": "2.2.3",
    "@formatjs/icu-messageformat-parser": "2.9.3",
    "@formatjs/intl-localematcher": "0.2.32",
    "@indutny/dicer": "0.3.2",
    "@indutny/mac-screen-share": "1.0.13",
    "@indutny/range-finder": "1.3.4",
    "@indutny/simple-windows-notifications": "2.0.7",
    "@indutny/sneequals": "4.0.0",
    "@popperjs/core": "2.11.8",
    "@react-aria/utils": "3.25.3",
    "@react-spring/web": "9.7.5",
    "@signalapp/better-sqlite3": "9.0.10",
    "@signalapp/libsignal-client": "0.65.4",
    "@signalapp/quill-cjs": "2.1.2",
     ... 81 more ...
 },
 “devDependencies”: {
    "@babel/core": "7.26.0",
    "@babel/plugin-proposal-class-properties": "7.18.6",
    "@babel/plugin-proposal-nullish-coalescing-operator": "7.18.6",
    ... 134 more ...
 },
 ...
}
```

SBOMs and VEX

Sources: CycloneDX spec, CycloneDX bom-examples


```
{
 "bomFormat": "CycloneDX",
 ...
 "metadata" : {
  "timestamp" : "2022-03-03T00:00:00Z",
  "component" : {
   "version": "1.0",
   "bom-ref" : "product-example-app”,
   ...
  }
 },
 “components”: [  ...1000s of dependencies with version, hash, license info... ],
 "vulnerabilities": [
  {
   "id": "CVE-2021-44228",
   "source": {
    "name": "NVD",
    "url": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228"
   },
   "analysis": {
    "state": "exploitable",
    "response": ["will_not_fix", "update"],
    "detail": "This version is affected. Customers are advised to upgrade to the latest
release."
   },
   "affects": [ { "ref": ”product-example-app” } ]
  }
 ] }
```

Case Study 1: SUNBURST (2021)

POLITICO

The attack on governmental organizations and businesses using the SolarWinds software is the largest and “most sophisticated” attack ever, the president of U.S. software giant Microsoft said.

“From a software engineering perspective, it’s probably fair to say that this is the largest and most sophisticated attack the world has ever seen,” Microsoft President Brad Smith told U.S. broadcaster CBS' "60 Minutes" program on Sunday.

Smith said “certainly more than a thousand” engineers must have worked on creating and exploiting the vulnerability in the SolarWinds software.

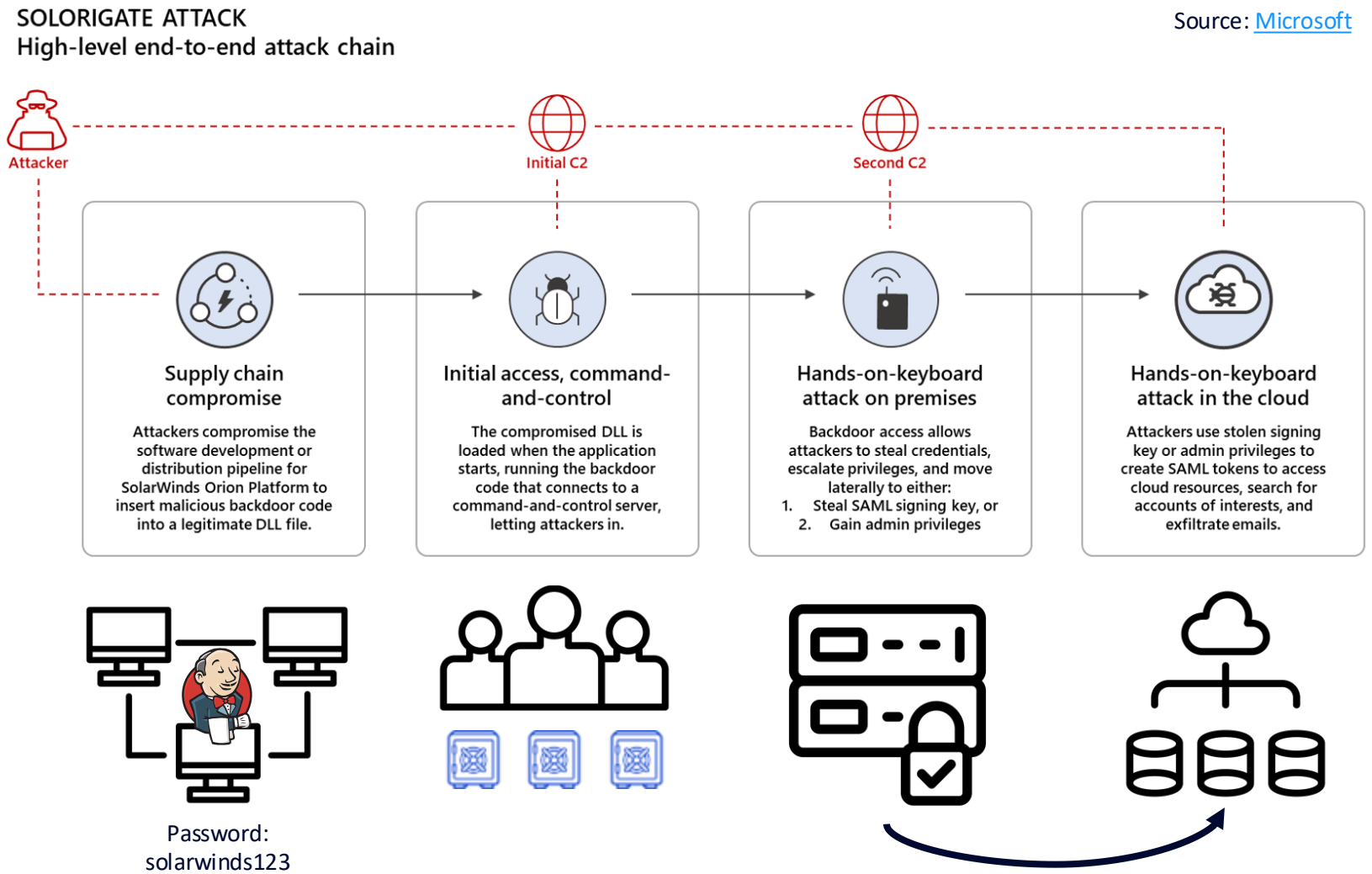
Case Study 1: SUNBURST (2021)

Compromised:

- Microsoft (product source code, compromised resellers)
- FireEye (stole red teaming tools)
- US Department of Homeland Security (6-9 months' persistent access), Treasury, other US agencies
- Many others *may* have been compromised, incl. UK government, NATO, EU Parliament
- "Fewer than 18,000 of 33,000 SolarWinds Orion customers affected"

30% of victims did not use SolarWinds –> access obtained in initial compromises used to target other organizations

Case Study 1: SUNBURST (2021)



Case Study 1: Golden SAML Vulnerability

1. Compromise the on-prem network (in this case, via malicious code embedded in Orion) to compromise the ADFS server
2. Steal signing key and certificate
3. Forge credentials to access federated cloud accounts (AWS, Azure, …)

- Reported by employees in 2016 and 2018, made public in 2017 and 2019
- Microsoft Security Response Center took no action because it didn't cross a security boundary

Source: ProPublica

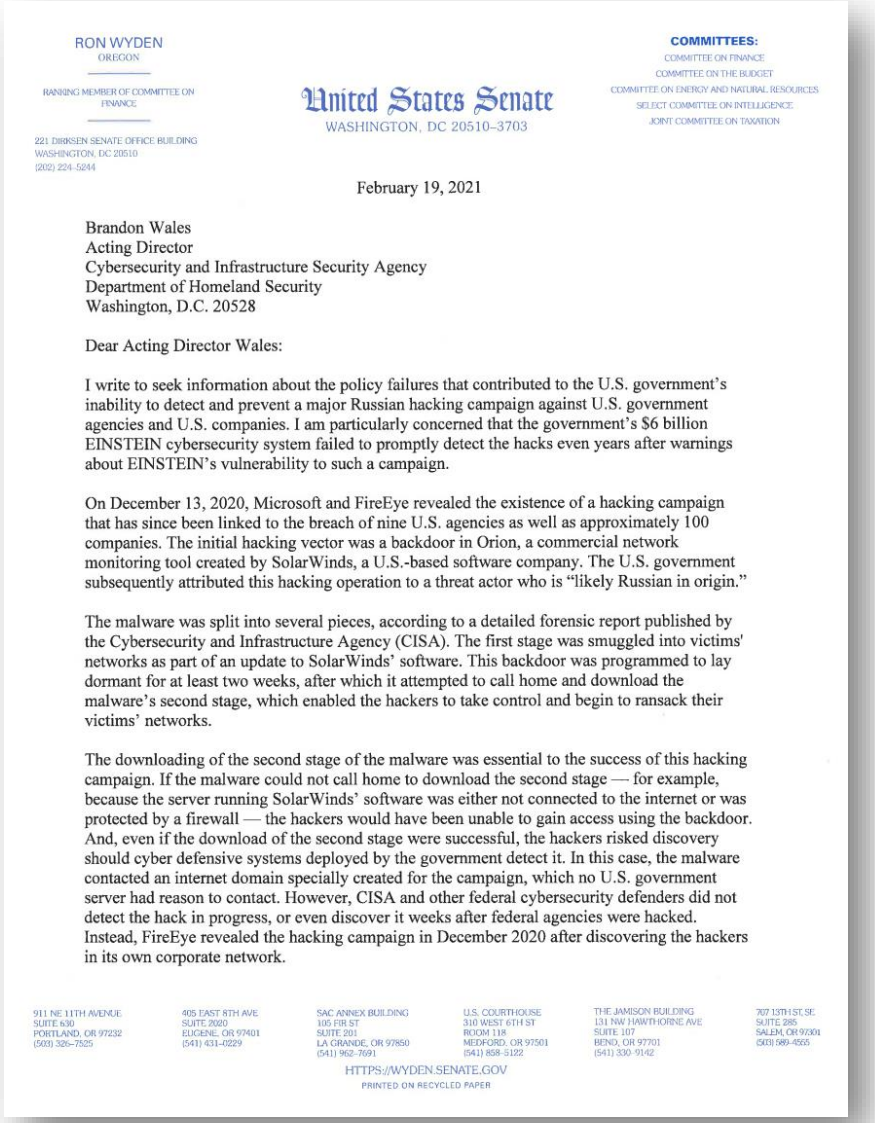
Case Study 1: Control Coverage Gaps (Microsoft)

- **Invalid assumptions in threat modeling**
  - *On-prem -> cloud -> customer -> customer's cloud -> customer's customer* does cross security boundaries!
- **Business pressures and security culture**
  - Disclosing the vulnerability could have cost Microsoft massive investment from US government in cloud services
  - And the proposed solution would stop federal smart cards working for login
  - People get promoted for $$ cloud deals, not for fixing vulnerabilities
- **MSRC under-resourced**

Case Study 1: Control Coverage Gaps (SolarWinds)

- **Software supply chain security**
- **Security culture**
  - It’s never solely the intern’s fault
- **Under-resourced**
  - “…the volume of security issues being identified over the last month have [sic] outstripped the capacity of Engineering teams to resolve.”
  - “…a 2018 presentation prepared by a company engineer and shared internally, including with Brown, that SolarWinds’ remote access set-up was ‘not very secure’ and that someone exploiting the vulnerability ‘can basically do whatever without us detecting it until it’s too late…’”

Case Study 1: Policymakers' Responses



RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510–3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

February 19, 2021

Brandon Wales
Acting Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Washington, D.C. 20528

Dear Acting Director Wales:

I write to seek information about the policy failures that contributed to the U.S. government's inability to detect and prevent a major Russian hacking campaign against U.S. government agencies and U.S. companies. I am particularly concerned that the government's $6 billion EINSTEIN cybersecurity system failed to promptly detect the hacks even years after warnings about EINSTEIN's vulnerability to such a campaign.

On December 13, 2020, Microsoft and FireEye revealed the existence of a hacking campaign that has since been linked to the breach of nine U.S. agencies as well as approximately 100 companies. The initial hacking vector was a backdoor in Orion, a commercial network monitoring tool created by SolarWinds, a U.S.-based software company. The U.S. government subsequently attributed this hacking operation to a threat actor who is "likely Russian in origin."

The malware was split into several pieces, according to a detailed forensic report published by the Cybersecurity and Infrastructure Agency (CISA). The first stage was smuggled into victims' networks as part of an update to SolarWinds' software. This backdoor was programmed to lay dormant for at least two weeks, after which it attempted to call home and download the malware's second stage, which enabled the hackers to take control and begin to ransack their victims' networks.

The downloading of the second stage of the malware was essential to the success of this hacking campaign. If the malware could not call home to download the second stage — for example, because the server running SolarWinds' software was either not connected to the internet or was protected by a firewall — the hackers would have been unable to gain access using the backdoor. And, even if the download of the second stage were successful, the hackers risked discovery should cyber defensive systems deployed by the government detect it. In this case, the malware contacted an internet domain specially created for the campaign, which no U.S. government server had reason to contact. However, CISA and other federal cybersecurity defenders did not detect the hack in progress, or even discover it weeks after federal agencies were hacked. Instead, FireEye revealed the hacking campaign in December 2020 after discovering the hackers in its own corporate network.

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

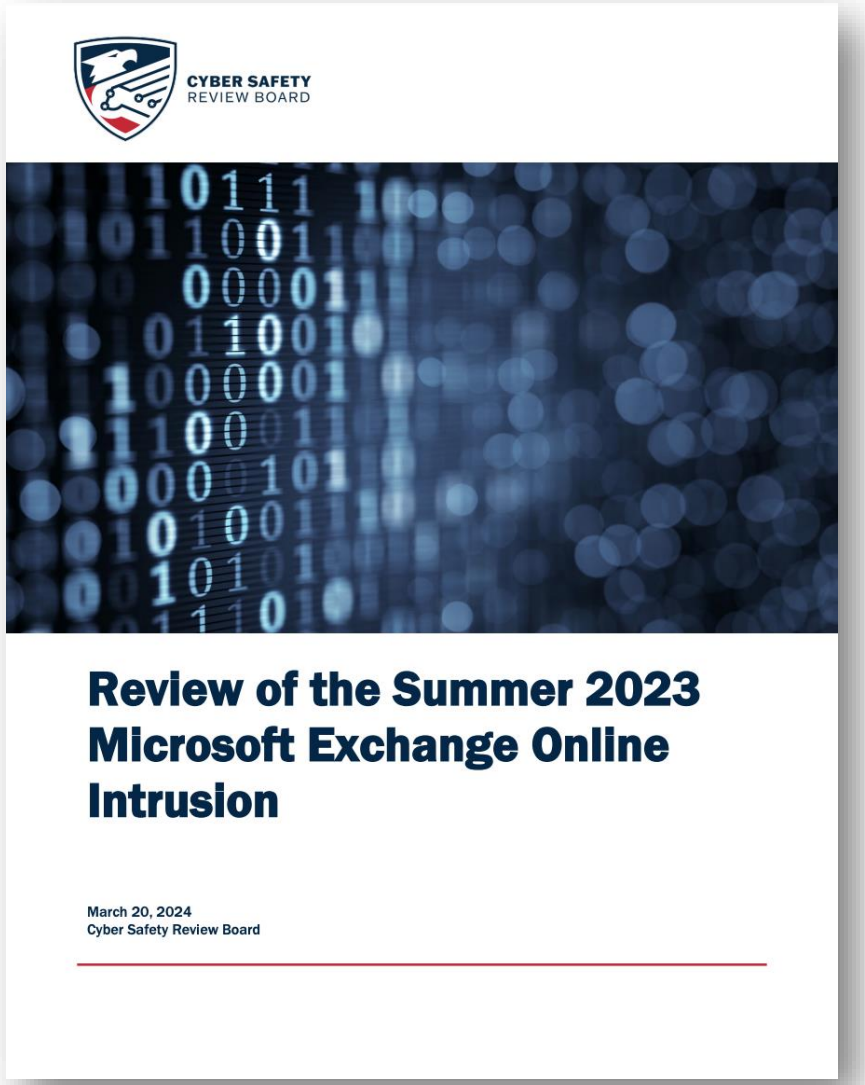
U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

HTTPS://WYDEN.SENATE.GOV
PRINTED ON RECYCLED PAPER

Case Study 2: Microsoft Exchange Online Intrusion (2023)



Storm-0558

- Gained access to an engineer's account in 2021 via a compromised device. *Nobody knows what they did then.* First cases of mailbox exfiltration in 2023
- Targets included senior US government officials involved in Secretary of State Antony Blinken and Commerce Secretary Gina Raimondo's visits to China

Compromised

- US victims: official and personal mailboxes of senior government officials, 22 enterprise orgs, 391 personal email accounts
- Non-US: 63 high-profile individuals in the UK
- Theoretically any data in any Microsoft cloud application and any third-party app using Microsoft's identity provider

Case Study 2: Control Coverage Gaps

- **Threat modeling**
  - If consumer account -> enterprise account had been identified as a security boundary, they may have identified the validation vulnerability that enabled consumer keys to be used to authenticate to enterprise customer data
- **Credential management**
  - Paused rotation of their MSA key for consumer auth, decided not to roll out a system for automated rotation, 2016 key usable for 7 years
  - MSA key not securely stored (in HSM)
  - No conformity checks for access tokens (attacker’s tokens were clearly forged)

Case Study 2: Control Coverage Gaps

- **Endpoint monitoring and intrusion detection**
  - Compromised employee laptop not detected in 2021
  - Didn’t detect 2023 incident – informed by US State Dept
  - Insufficient logs and monitoring data to determine how or when the attacker stole the key
- **Plus the gaps from Case Study 1**

Case Study 2: Policymakers' Responses

RECOMMENDATION 1: Microsoft's customers would benefit from its CEO and Board of Directors directly focusing on the company's security culture. The CEO and Board should develop, and share publicly, a plan with specific timelines to make fundamental, security-focused reforms across the company and its full suite of products, and then hold leaders at all levels of the company accountable for its implementation. Given the company's critical importance to its more than one billion customers and the national security of this nation and, indeed, the entire world, progress in this area should be rapid and substantial.

RECOMMENDATION 2: Microsoft leadership should consider directing internal Microsoft teams to deprioritize feature developments across the company's cloud infrastructure and product suite until substantial security improvements have been made. In all instances, security risks should be fully and appropriately assessed and addressed before new features are deployed.

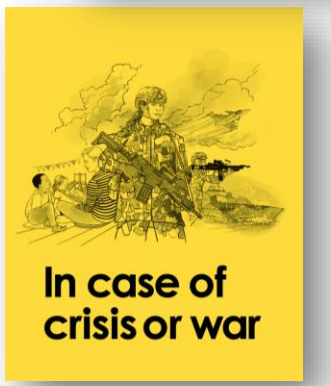
Can we help companies make the business case for security?

A Friedman doctrine-- The Social Responsibility of Business Is to Increase Its Profits

By Milton Friedman

Sept. 13, 1970

For the total defence to be able to manage the consequences of an armed attack, maintaining electronic communications and postal services is very important. Few actors are fully independent within the civil preparedness sector, which makes public-private collaboration essential.



Civil defence

Civil defence involves everyone who lives in Sweden, alongside government agencies, regional authorities, municipalities, private sector and non-profit organisations. One of the most important tasks of the civil defence is to support the military defence. Another core task is to protect the population and ensure that essential public services are uninterrupted as far as possible – even during times of war. Essential public services include energy, healthcare and transport.

Thanks for listening!

Copyright Notice

CLOUD DONE RIGHT