Delivering Secure Healthcare Applications with OSS

Robert Wood - CMS
Gedd Johnson - Defense Unicorns

WHAT IS CENTERS FOR MEDICARE AND MEDICAID

CMS's mission is to serve Medicare & Medicaid beneficiaries

- We provide medicare and medicaid benefits to 133 Million People Nationwide
- Primary recipients are over 62 years old, or those with low/no income and are most at risk.

The CMS vision is to become the most energized, efficient, customer friendly Agency in the government. CMS will strengthen the health care services & information available to Medicare & Medicaid beneficiaries & the health care providers who serve them.

What is Centers for Medicare & Medicaid

CMS's mission is to serve Medicare & Medicaid beneficiaries

- We provide medicare and medicaid benefits to 133 Million People Nationwide
- Primary recipients are over 62 years old, or those with low/no income and are most at risk.

The CMS vision is to become the most energized, efficient, customer friendly Agency in the government. CMS will strengthen the health care services & information available to Medicare & Medicaid beneficiaries & the health care providers who serve them.

Challenges

- Security, Governance, Risk, and Compliance have become large resource drains on the software development cycle
- Cloud technology and cloud native applications are numerous and difficult to stay up to date on
- Waterfall and water-scrum-fall software development processes used in the government are still slow
- Greater than 6,500 contracted engineers support our systems in comparison to 46 ISPG staff and 423 OIT staff members that manage the services delivery.
- Due to this, there is a lack of integrations and automation with numerous data silos that make managing and keeping CMS secure difficult.

Solution

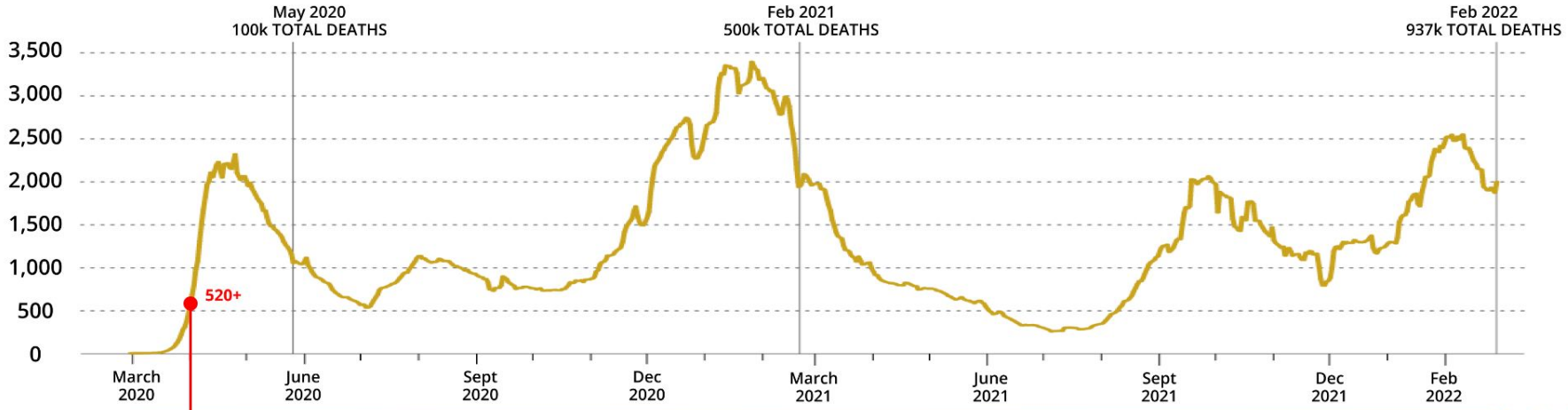
The batCAVE aims to be CMS's devsecops platform as a service (PaaS) that accelerates the time to value for mission owners by automating away a significant portion of the security, infrastructure, and project startup workloads.

Our Goals

- Reduce the time spent on CMS's ATO and SIA processes
- Reduce the security and infrastructure burden on teams allowing them to focus on the software.
- Ensure true continuous monitoring and security compliance all while providing continuous updates of the software
- Reduce the cost of an end to end application development and from idea to deployment at CMS
- Provide the ability to capture user feedback in a timely manner in order to improve and add features
- Reduce the cost of hosting apps on CMS cloud by enabling dynamic scaling of apps through the power of Kubernetes.
- Provide a simple onboarding process for ADO's that want DevSecOps and don't want to manage their infrastructure and associated security burden.
- **Allow continuous delivery. Get value to the American people faster.**

COVID-19 DEATHS

Average number of daily reported coronavirus deaths in the US



SDLC

1 mo. idea generation of help

SHUTDOWNS 2020

MARCH

03/19
- California

03/21
- Illinois
- New Jersey

03/22
- New York

03/23
- Connecticut
- Louisiana
- Ohio
- Oregon
- Washington

03/24
- Delaware
- Indisana
- Massachusetts
- Michigan
- New Mexico
- West Virginia

03/25
- Hawaii
- Idaho
- Wisconsin
- Vermont

03/26
- Colorado
- Kentucky

03/27
- Minnesota
- New Hampshire

03/28
- Alaska
- Montana
- Rhode Island

03/30
- Kansas
- Maryland
- North Carolina
- Virgina

03/31
- Arizona
- Tennessee

APRIL

04/01
- D.C.
- Nevada
- Pennsylvania

04/02
- Maine
- Texas

04/03
- Georgia
- Florida
- Mississippi

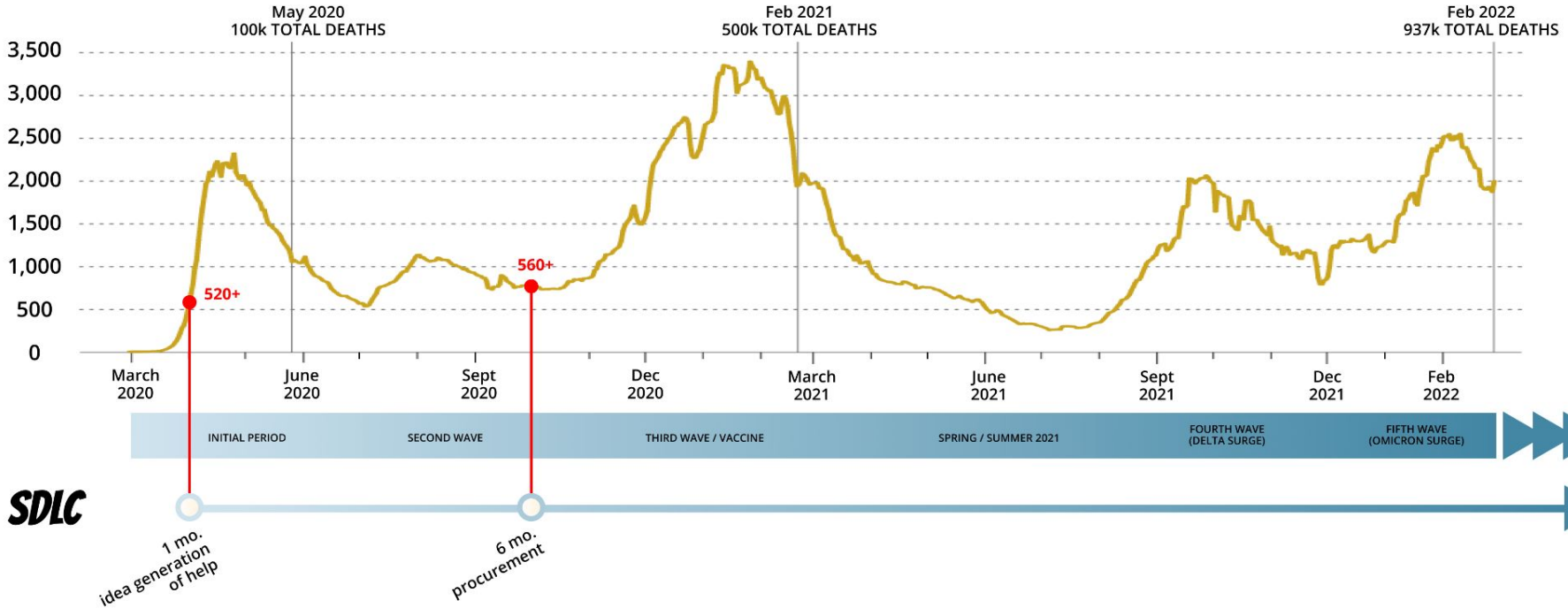
04/04
- Alabama

04/06
- Missouri

04/07
- South Carolina

COVID-19 DEATHS

Average number of daily reported coronavirus deaths in the US



SHUTDOWNS 2020

MARCH

03/19
- California

03/21
- Illinois
- New Jersey

03/22
- New York

03/23
- Connecticut
- Louisiana
- Ohio
- Oregon
- Washington

03/24
- Delaware
- Indisana
- Massachusetts
- Michigan
- New Mexico
- West Virginia

03/25
- Hawaii
- Idaho
- Wisconsin
- Vermont

03/26
- Colorado
- Kentucky

03/27
- Minnesota
- New Hampshire

03/28
- Alaska
- Montana
- Rhode Island

03/30
- Kansas
- Maryland
- North Carolina
- Virgina

03/31
- Arizona
- Tennessee

APRIL

04/01
- D.C.
- Nevada
- Pennsylvania

04/02
- Maine
- Texas

04/03
- Georgia
- Florida
- Mississippi

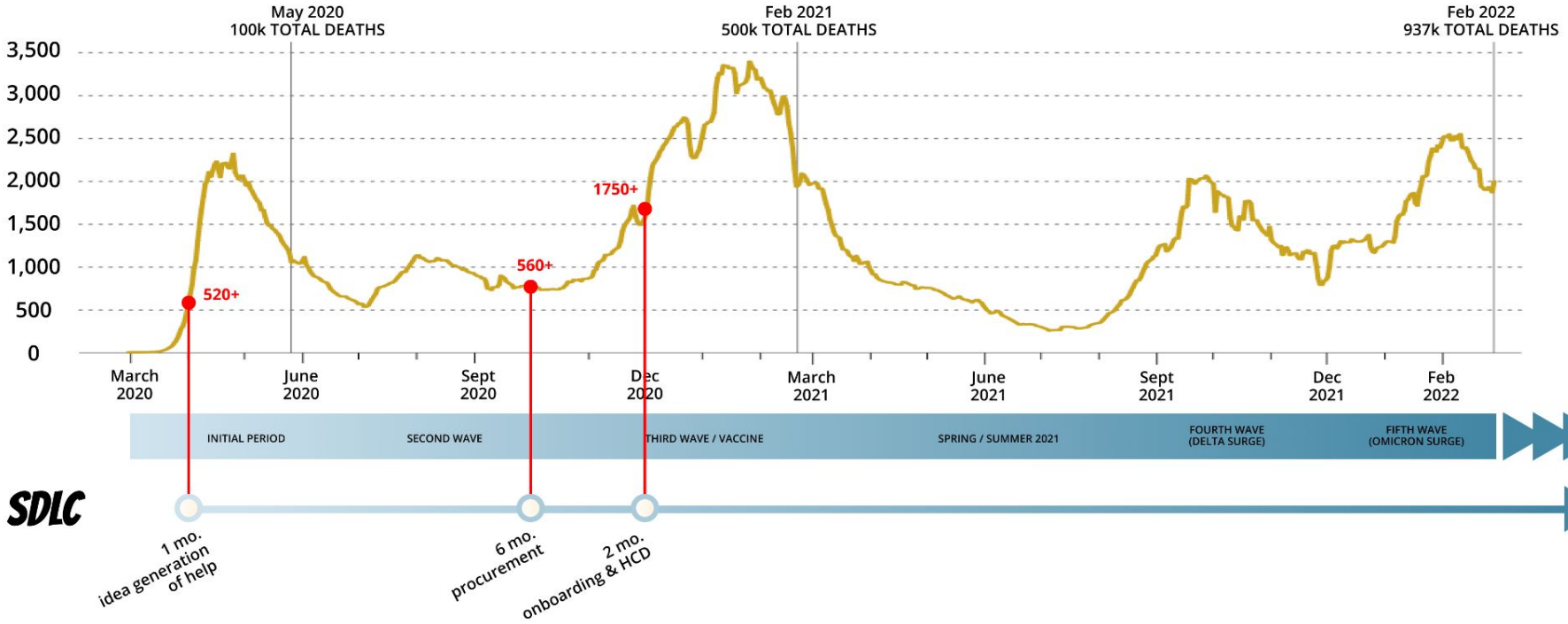
04/04
- Alabama

04/06
- Missouri

04/07
- South Carolina

COVID-19 DEATHS

Average number of daily reported coronavirus deaths in the US



SDLC

1 mo. idea generation of help

6 mo. procurement

2 mo. onboarding & HCD

SHUTDOWNS 2020

MARCH

03/19
- California

03/21
- Illinois
- New Jersey

03/22
- New York

03/23
- Connecticut
- Louisiana
- Ohio
- Oregon
- Washington

03/24
- Delaware
- Indisana
- Massachusetts
- Michigan
- New Mexico
- West Virginia

03/25
- Hawaii
- Idaho
- Wisconsin
- Vermont

03/26
- Colorado
- Kentucky

03/27
- Minnesota
- New Hampshire

03/28
- Alaska
- Montana
- Rhode Island

03/30
- Kansas
- Maryland
- North Carolina
- Virgina

03/31
- Arizona
- Tennessee

APRIL

04/01
- D.C.
- Nevada
- Pennsylvania

04/02
- Maine
- Texas

04/03
- Georgia
- Florida
- Mississippi

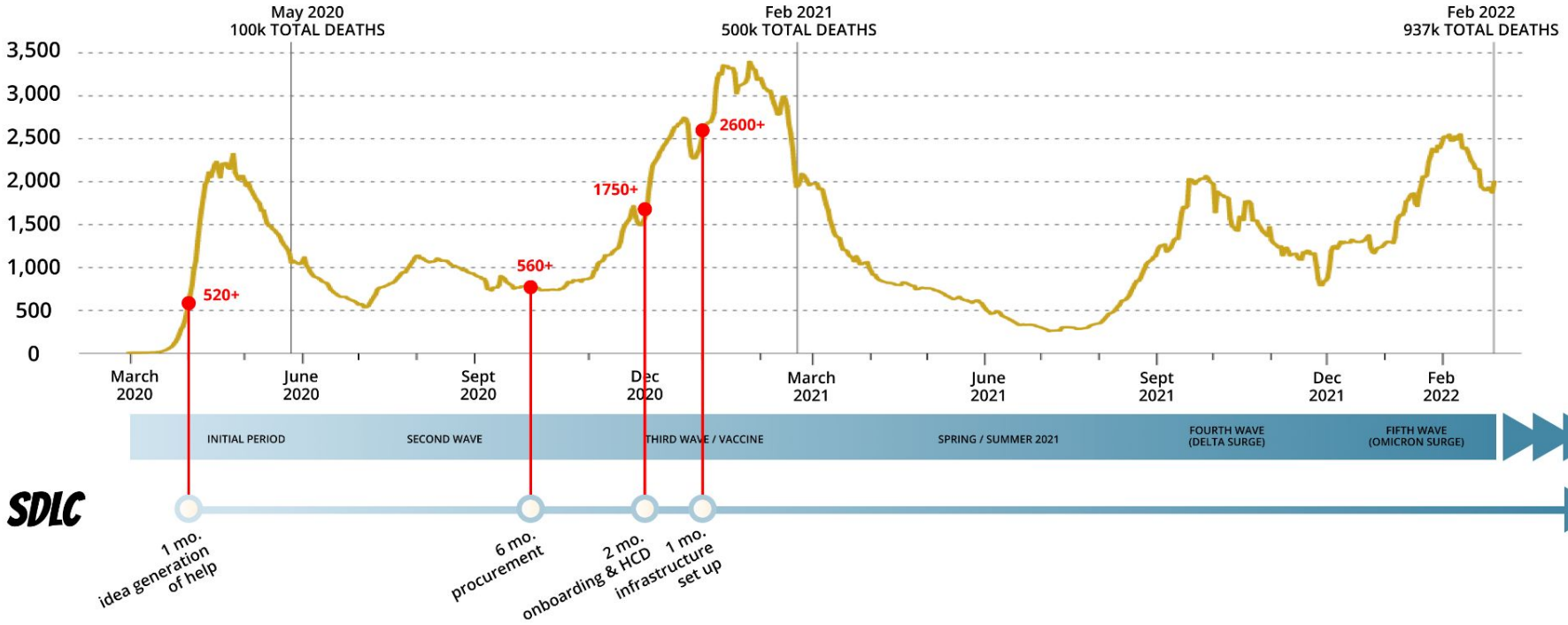
04/04
- Alabama

04/06
- Missouri

04/07
- South Carolina

COVID-19 DEATHS

Average number of daily reported coronavirus deaths in the US



SHUTDOWNS 2020

MARCH

03/19
- California

03/21
- Illinois
- New Jersey

03/22
- New York

03/23
- Connecticut
- Louisiana
- Ohio
- Oregon
- Washington

03/24
- Delaware
- Indisana
- Massachusetts
- Michigan
- New Mexico
- West Virginia

03/25
- Hawaii
- Idaho
- Wisconsin
- Vermont

03/26
- Colorado
- Kentucky

03/27
- Minnesota
- New Hampshire

03/28
- Alaska
- Montana
- Rhode Island

03/30
- Kansas
- Maryland
- North Carolina
- Virgina

03/31
- Arizona
- Tennessee

APRIL

04/01
- D.C.
- Nevada
- Pennsylvania

04/02
- Maine
- Texas

04/03
- Georgia
- Florida
- Mississippi

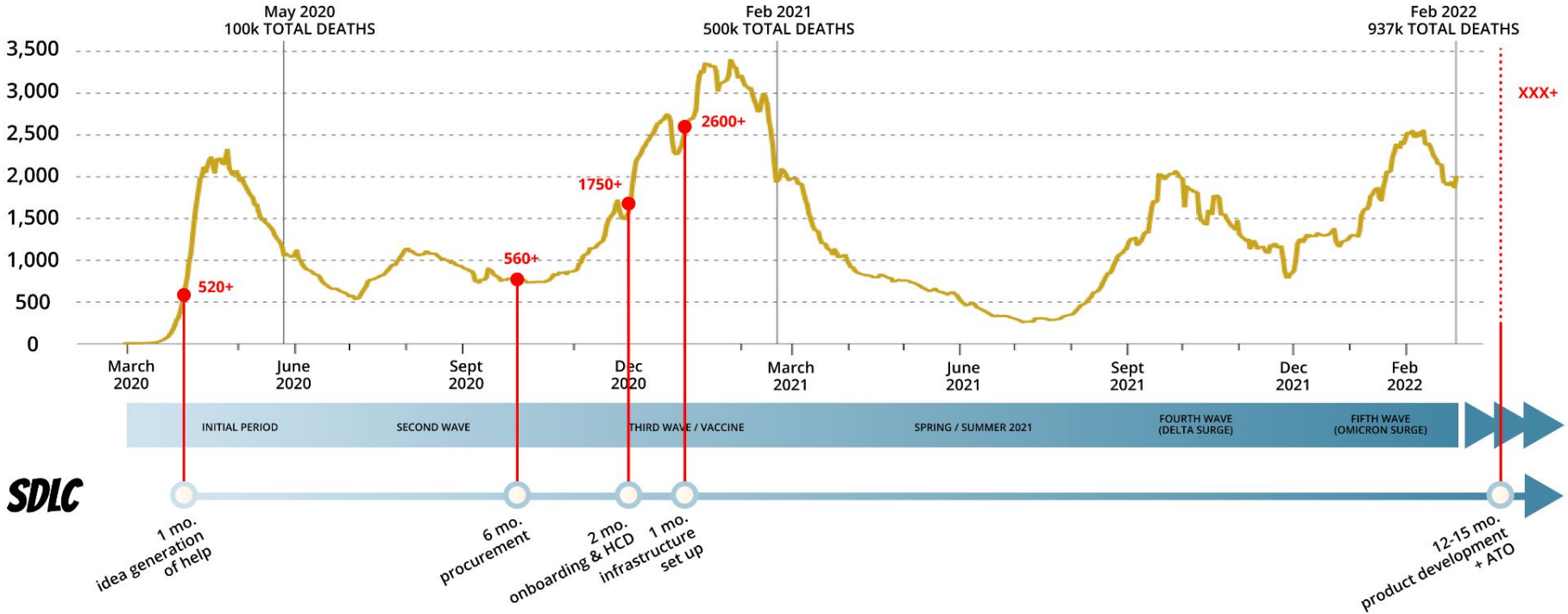
04/04
- Alabama

04/06
- Missouri

04/07
- South Carolina

COVID-19 DEATHS

Average number of daily reported coronavirus deaths in the US



SHUTDOWNS 2020

MARCH

03/19
- California

03/21
- Illinois
- New Jersey

03/22
- New York

03/23
- Connecticut
- Louisiana
- Ohio
- Oregon
- Washington

03/24
- Delaware
- Indisana
- Massachusetts
- Michigan
- New Mexico
- West Virginia

03/25
- Hawaii
- Idaho
- Wisconsin
- Vermont

03/26
- Colorado
- Kentucky

03/27
- Minnesota
- New Hampshire

03/28
- Alaska
- Montana
- Rhode Island

03/30
- Kansas
- Maryland
- North Carolina
- Virgina

03/31
- Arizona
- Tennessee

APRIL

04/01
- D.C.
- Nevada
- Pennsylvania

04/02
- Maine
- Texas

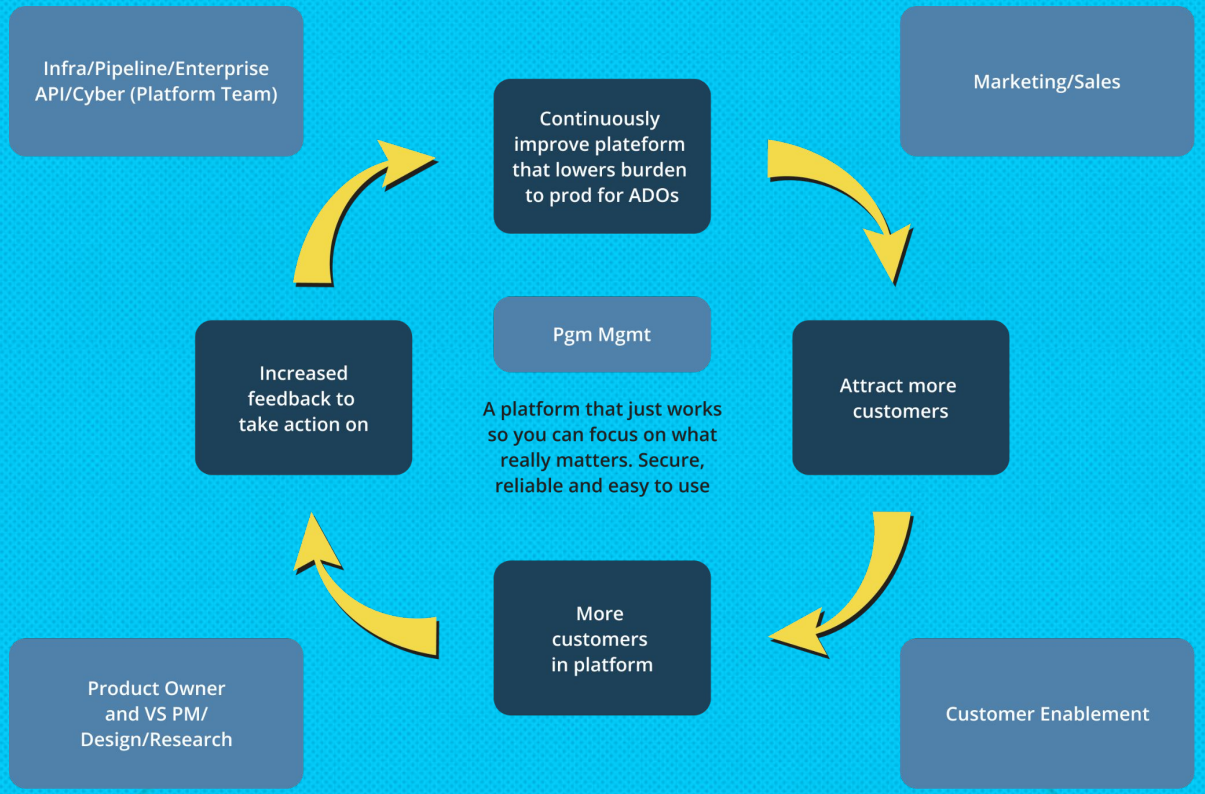
04/03
- Georgia
- Florida
- Mississippi

04/04
- Alabama

04/06
- Missouri

04/07
- South Carolina

THE FLYWHEEL



batCAVE

Built On Open Source

- Batcave is built on exclusively open-source software and partnerships in the open-source community
- Accelerated development by leveraging Big Bang by Platform One
- “Contribute-First” Culture

Upstream Application ⟺ Big Bang ⟺ Batcave

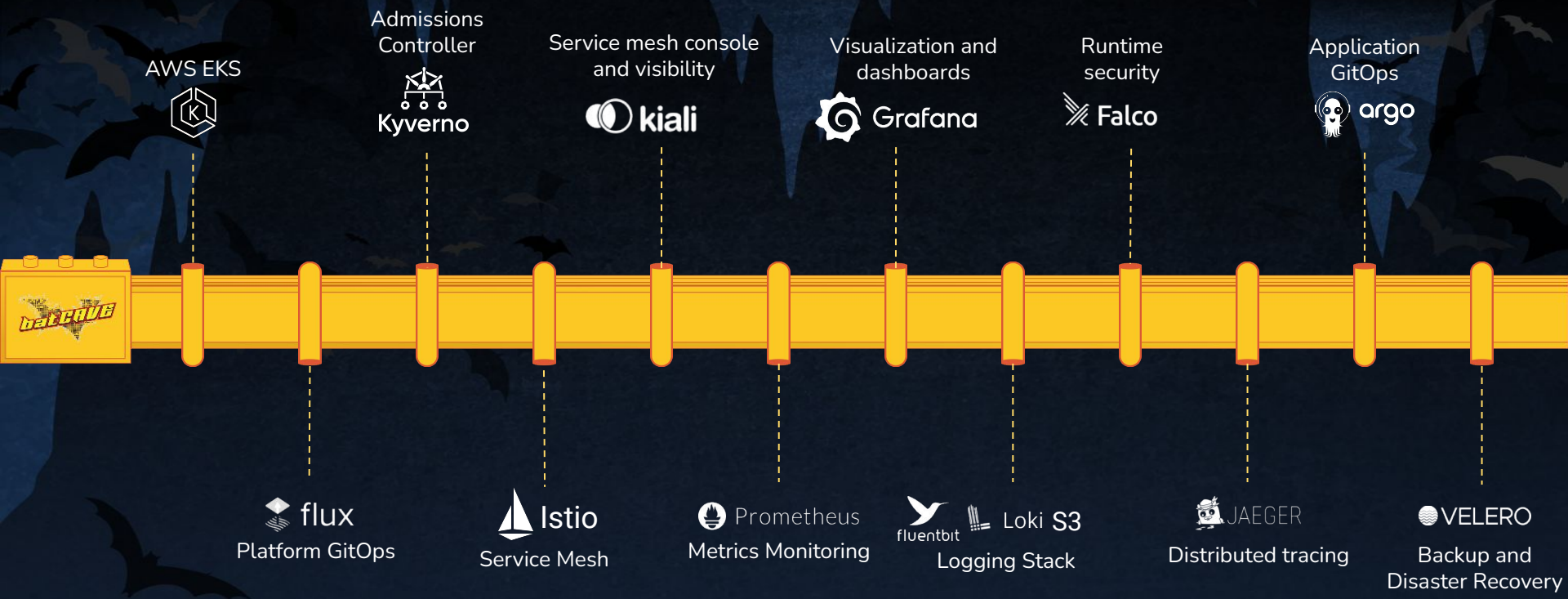
BIG BANG

- Secure, declarative baseline configuration for a K8s-based platform
- “Marketplace” of secure, cloud-native apps and services
- Provides OSCAL control mappings to NIST 800-53
- Open source!

PLATFORM ONE
BIG BANG

Utility Belt

Deployed in all batCAVE environments for security control inheritance



Delivery Models

SINGLE-TENANT PAAS

- Single ADO per cluster
- Fully managed by Batcave team

MULTI-TENANT PAAS

- Multiple ADOs running on the same cluster
- Apps separated by namespace and node
- Fully managed by Batcave team

ADO OWNED / OPERATED

- ADO deploys and operates a Batcave cluster
- Managed by ADO, Batcave team provides code

Primary Concerns

- Balancing developer freedom and platform opinionation
- Maximizing security control inheritance

Major Milestones

Q4 -'22

Full & Independent ATO

Q4 - '22

Production-level Multi-tenancy

Q1 - '23

Enterprise Services Deployment (Secrets, ZT, GRC)

Q2 - '23

Security Data Lake Integration

Q2 - '23

CMS Cloud Automation

batCAVE

Major Accomplishments

1. 80% control mapping of CMS's NIST 800-53 implementation

2. Codification of key strategic policy moves into the batCAVE (SBOM, zero trust, etc.) that shift past checkbox compliance work

3. Multiple layers of value proposition for different stakeholders (cost, speed, security, standardization)

4. Deployment of CMS's first purple team working full-time inside of the batCAVE from day 1

Success Story

Mohan Gowda

Sr. Computer Systems Architect
EPPE

Features of batCAVE that exceeded your expectations

The pipeline and the utility belt that takes the pressure off the ADO

EPPE highlighted the following benefits

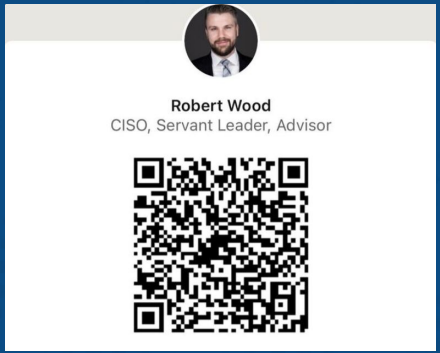
- Integration is better and the timeline to production is a lot shorter
- Ability to focus on our application code requirements
- batCAVE works with us closely to update our work integrations to better suit the pipeline and how we can benefit from our continuous standing and ATO that is part of the pipeline
- The security aspect and compliance is key

Collaboration & Culture

Collaboration and boundary pushing

1. Anchored in human-centered design
    a. Open learning and engaging sessions internally and cross agencies
    b. Design insights fed into broader tech ecosystem at the agency (and HHS)
2. Open code, controls, process, and policy
    a. Open access internally
    b. Lead in to a curated open source ecosystem of security, privacy, and compliance resources

Thank you!



Connect on LinkedIn!

Session Link + Feedback