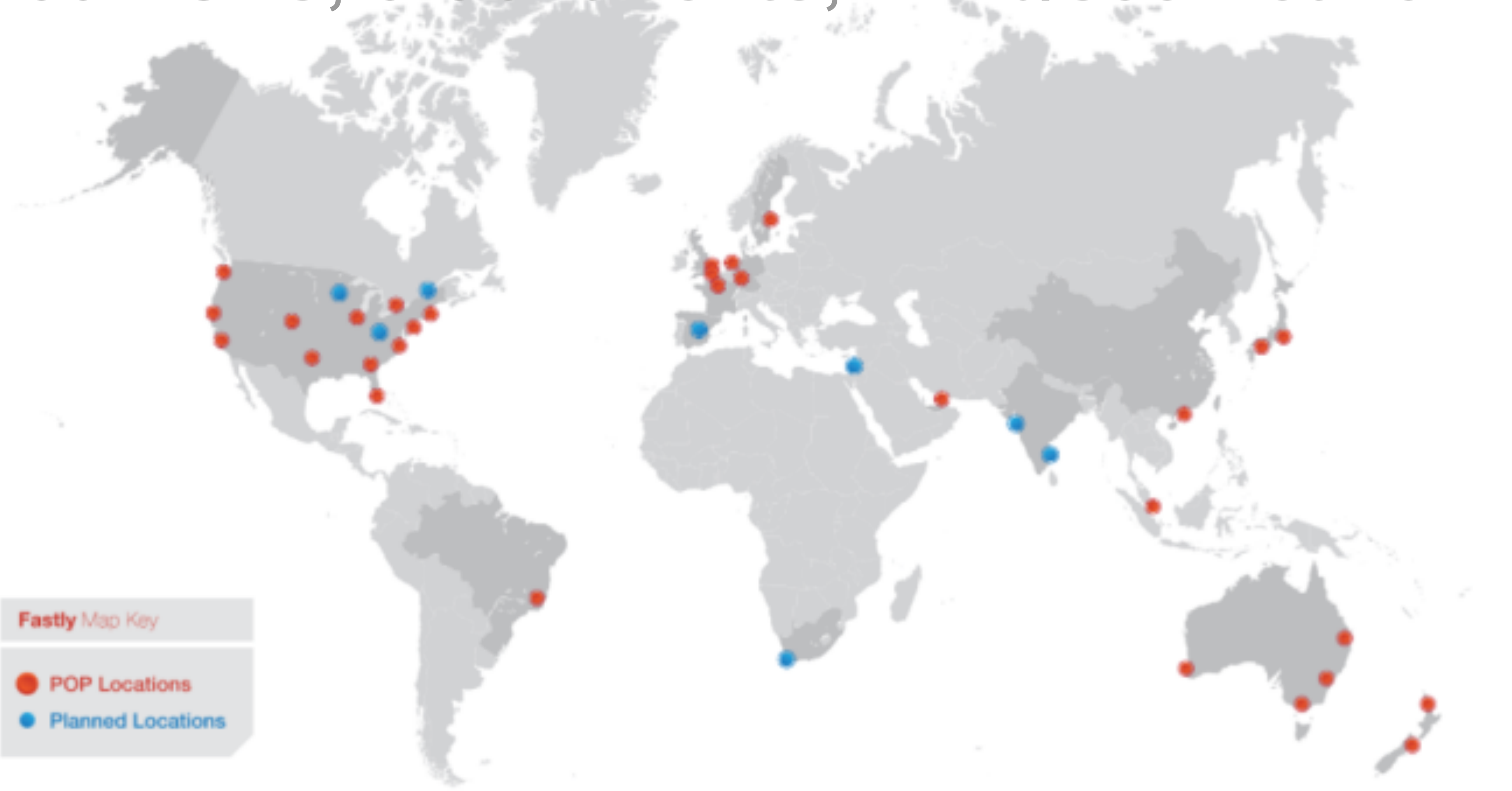
Incident Command:

The far side of the edge

Lisa Phillips
Tom Daly
Maarten Van Horenbeeck

30 POPs; 5 Continents; ~7Tb/sec Network



INCIDENT
COMMAND

Program Goals

Decision Making

Reduce MTTR

Provide Comms

Understand Impact

Structured Involvement

Improve for Next Time

- FEMA National Incident Management
- Fire Department and Police
- Business Crisis Management
- Technology Peers who came before us

Incidents

- Fastly sees a variety of events that could classify as an incident
  - Distributed Denial of Service attacks
  - Critical security vulnerabilities
  - Software bugs
  - Upstream network outages
  - Datacenter failures
  - Third Party service provider events
  - “Operator Error”

What you defend against

- It’s helpful to categorize:
  - Issues that affect **reliability** of the CDN
  - Issues that affect **security** of customer data and traffic or the business
- Both require very different handling, and addressing them requires a different approach (“**minimize harm**”)
- Events happen at **various levels of customer impact and business risk**.
  - While teams can deal with some events autonomously, others require more high level engagement and coordination

Identifying the issue

- **Fastly does not have a NOC**
- We have **several team-monitored systems**, in addition to some **critical cross-business monitoring**
  - Ganglia / Icinga
  - ELK Stack
  - Graylog
  - Third party service providers (e.g. Datadog, Catchpoint)
- **Immediate escalation to engineers** is needed
- Engineering teams must **own their own destiny** and have control over their alert stream. When they don’t respond, they are **empowered to improve**

People

- It’s all about having the **right people at the right time engaged**
- Engineers have **human needs**
  - Private space and time is a necessity
  - Randomization costs more than just the time spent on an interruption
  - Minimize thrash by being specific about inclusion
- Teams have **individual pager rotations**
- Company maintains a **company wide pager rotation** (Incident Commander)
- Global **Customer Service Focused** Engineers

Incident Commander

- **Deep systems understanding of Fastly**
- Well versed in each team's role and its leaders
- Organizational Trust
- Focuses on:
  - Coordinating actions across multiple responders;
  - Alerting and updating stakeholders— or during major events;
  - designating a specific person to do so;
  - Evaluate the high-level issue and understand its impact;
  - Consult with team experts on necessary actions;
  - Call off or delay other activities that may impact resolution.

Communicating status

- **Identify audiences**
  - Customers
  - Our Customers’ Customers
  - Executives
  - Investors and other interested parties
  - The rest of the company

- **Identify quickly the questions that need answering**, and communicate effectively to address them
- **Think through “rude Q&A”**: it helps you respond to the incident better!
- Ensure **communication channels are highly available**

Continuous improvement

- **Every incident is logged and tracked** in JIRA
- Incident Commander or executive leader owns **generating an Incident Report** and if necessary, a **service/security advisory**

- **Five why's!**
  - Intermediate answers help identify mitigation strategies
  - Final answer tells us the root cause we need to address

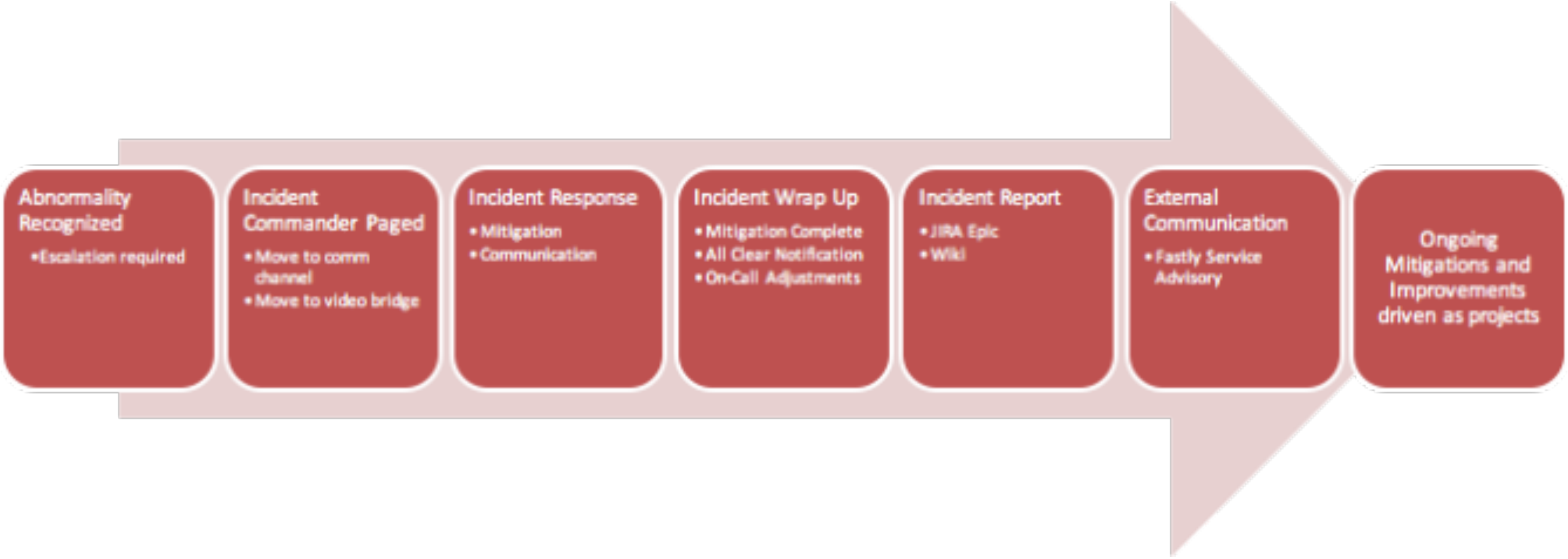
- Some mitigations are no longer part of the incident. **Be clear where you cut off into new projects**, and who owns them

How we put it together!

Incident Response Framework

- Develop definitions of **impact**
- Define **severity** levels
- Define **response and communication** requirements
- Define **post-incident** activities

Incident Response Process



Abnormality Recognized
- Escalation required

Incident Commander Paged
- Move to comm channel
- Move to video bridge

Incident Response
- Mitigation
- Communication

Incident Wrap Up
- Mitigation Complete
- All Clear Notification
- On-Call Adjustments

Incident Report
- JIRA Epic
- Wiki

External Communication
- Fastly Service Advisory

Ongoing Mitigations and Improvements driven as projects

Exercises

- **Regular incident reviews**
  - Review with all commanders past incidents, ensure documentation is up-to-date, and there's an open forum to review interaction
- **Regular training**
  - Onboarding of new Incident Commanders
  - Walkthrough of the process
- **Table top exercises**
  - Scenario written by an incident commander, with input from a small group of partner teams, focusing on worst cases
  - Group walkthrough
  - Document inefficiencies and mitigation plans

Security Incident Response Plan

- Employees trained to **always invoke IC**
- Anyone can invoke the **Security Incident Response Plan (SIRP)** by paging the security team
- Split responsibilities but close coordination:
  - **IC** focuses on restoring business operations and reducing customer impact
  - **SIRP** focuses on investigating the security incident, and ensuring security impact is directly communicated to executive levels
  - **IC** typically has priority on restoring operations. When IC action has security implications SIRP guarantees appropriate escalation

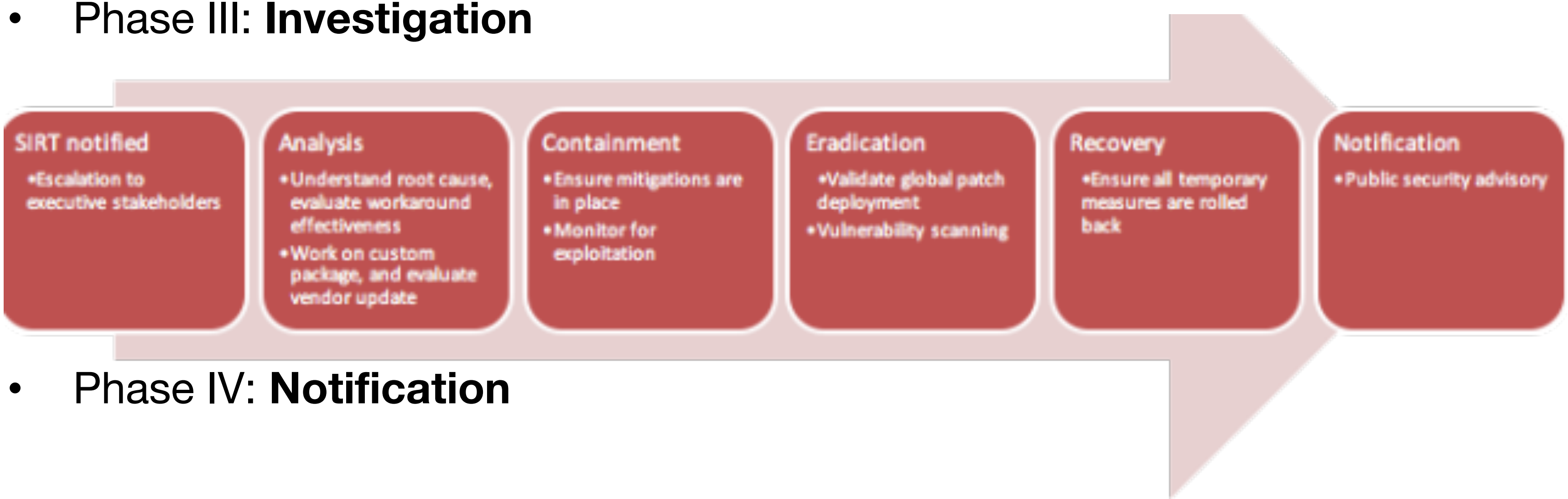
Security Incident Response Plan

- Security Incident Response Plan **convenes a group of executives**:
  - Marketing
  - IT
  - Business Operations
  - Engineering
  - Security
  - HR
  - Legal

- **Process is owned by the Chief Security Officer**, who reports to CEO

Security Incident Response Plan

- Phase I: **Incident Reporting**
- Phase II: **SIRT notification**
- Phase III: **Investigation**



SIRT notified
- Escalation to executive stakeholders

Analysis
- Understand root cause, evaluate workaround effectiveness
- Work on custom package, and evaluate vendor update

Containment
- Ensure mitigations are in place
- Monitor for exploitation

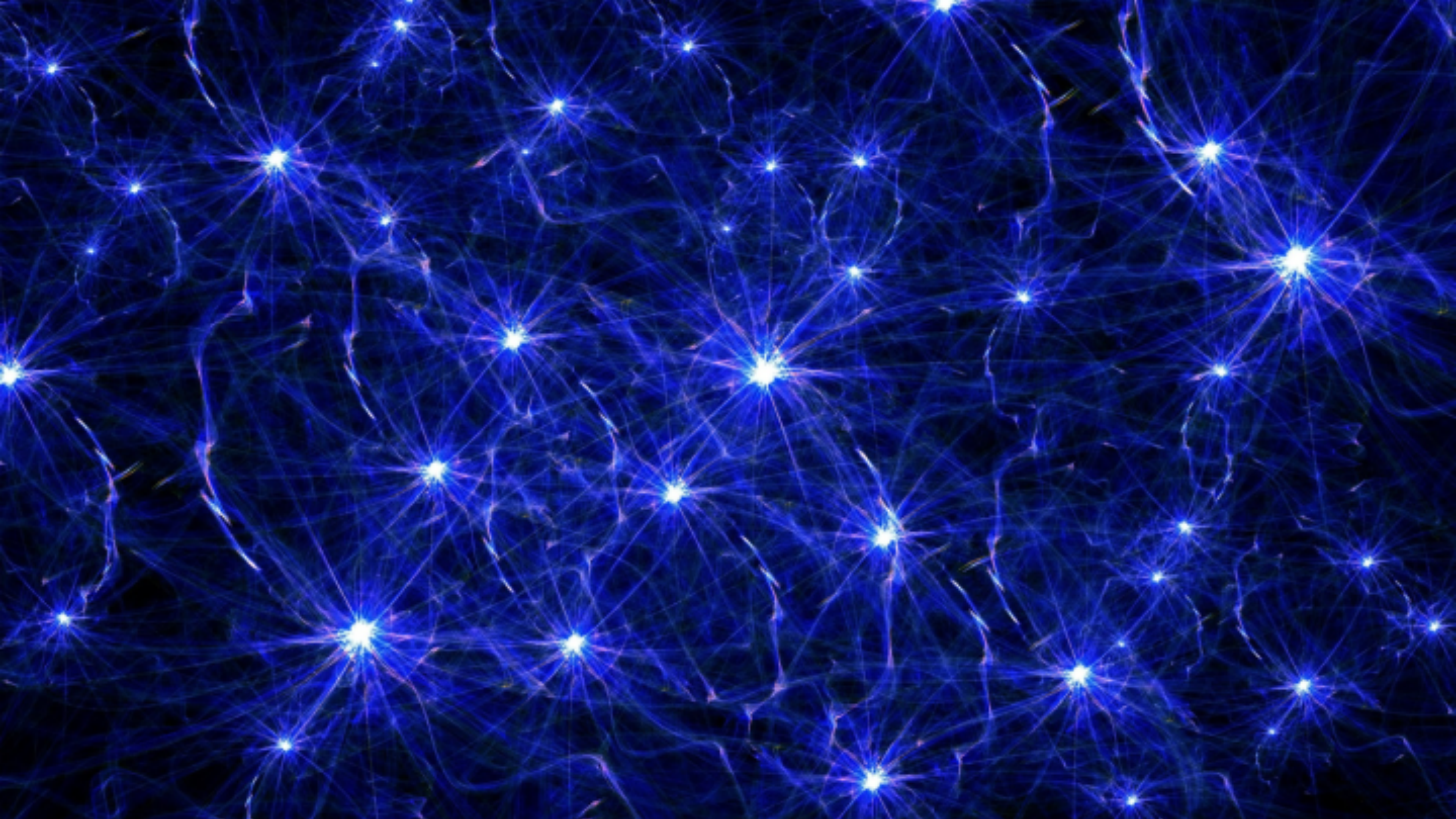
Eradication
- Validate global patch deployment
- Vulnerability scanning

Recovery
- Ensure all temporary measures are rolled back

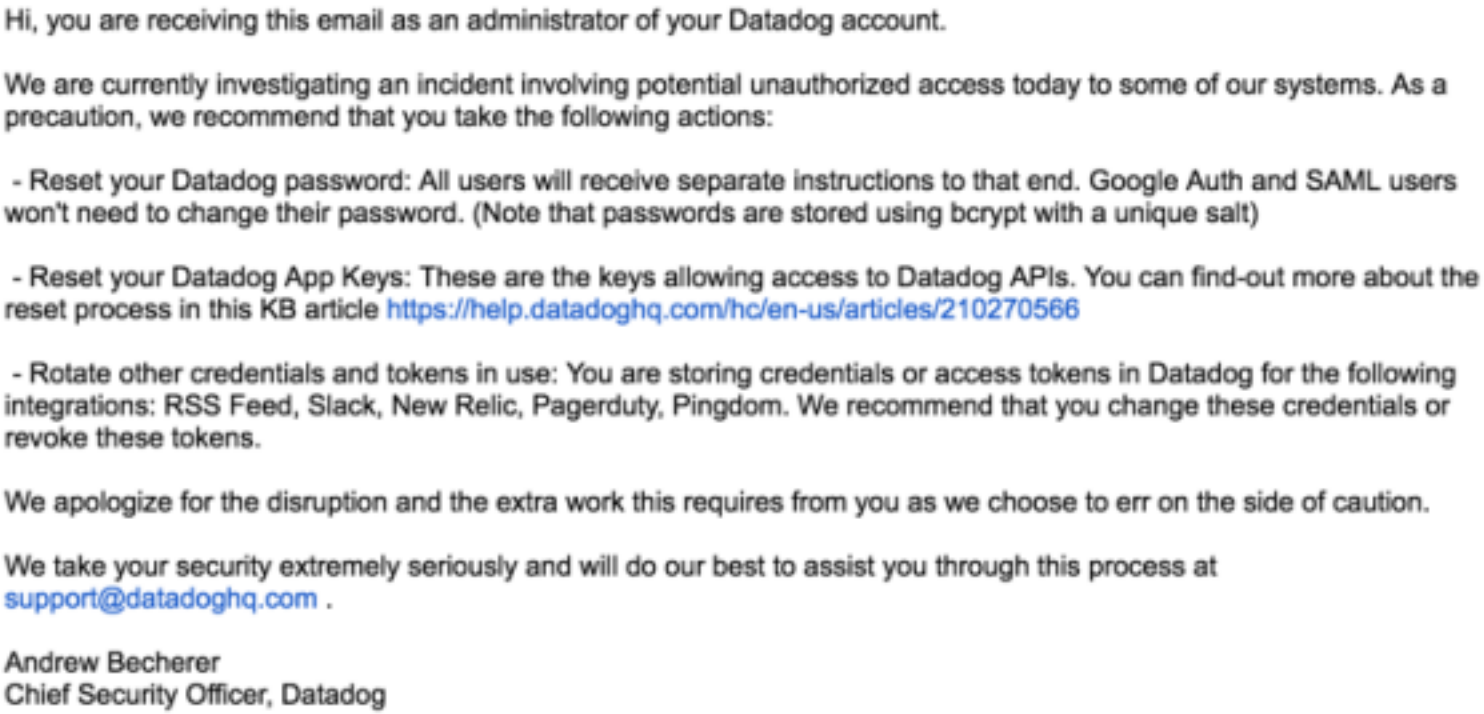
Notification
- Public security advisory

- Phase IV: **Notification**

Case study:
Breach at a supplier



Saturday morning e-mail



Hi, you are receiving this email as an administrator of your Datadog account.

We are currently investigating an incident involving potential unauthorized access today to some of our systems. As a precaution, we recommend that you take the following actions:

- Reset your Datadog password: All users will receive separate instructions to that end. Google Auth and SAML users won't need to change their password. (Note that passwords are stored using bcrypt with a unique salt)

- Reset your Datadog App Keys: These are the keys allowing access to Datadog APIs. You can find-out more about the reset process in this KB article https://help.datadoghq.com/hc/en-us/articles/210270566

- Rotate other credentials and tokens in use: You are storing credentials or access tokens in Datadog for the following integrations: RSS Feed, Slack, New Relic, Pagerduty, Pingdom. We recommend that you change these credentials or revoke these tokens.

We apologize for the disruption and the extra work this requires from you as we choose to err on the side of caution.

We take your security extremely seriously and will do our best to assist you through this process at support@datadoghq.com .

Andrew Becherer
Chief Security Officer, Datadog

Vendor security breach

- DataDog notification received via e-mail
- **13:24 GMT:** Escalation to the security team
- **13:38 GMT:** IC is engaged
  - **Initial assessment and questions**
    - Partner has suffered a security incident
    - Potential disclosure of metrics data
    - Rotation of credentials is required
  - **Initial action items**
    - Engage appropriate teams: SRE and Observability
    - Implement Incident Command bridge and meetings
    - Plan for rotation of keys, as advised by vendor
    - Identify all locations where keys are in use

Vendor security breach

- **13:46 GMT:** SIRT is engaged
  - **Initial assessment and questions**
    - Vendor has suffered a security incident
    - Has the vendor contained the incident?
    - What data do we store with the vendor?
    - How are customers affected?
  - **Initial action items**
    - Outreach to vendor to understand scope
    - Identify data stored at vendor
    - Investigate customer use of vendor product

Vendor security breach

- Addressing Fastly’s **internal use of the vendor**
  - **14:10 GMT:** All use of API keys across Fastly is identified
  - **14:30 GMT:** Plan of action is defined to rotate keys
  - **15:45 GMT:** Production keys have been revoked
  - **16:05 GMT:** All other integrations have been disconnected.
  - **17:05 GMT:** IC is shut down as imminent risk has been addressed.
- Identify and **mitigate customer exposure** and **security exposure**
  - **14:30 GMT:** Scope of customer API exposure is identified.
  - **15:05 GMT:** SIRT is virtually convened.

Vendor security breach

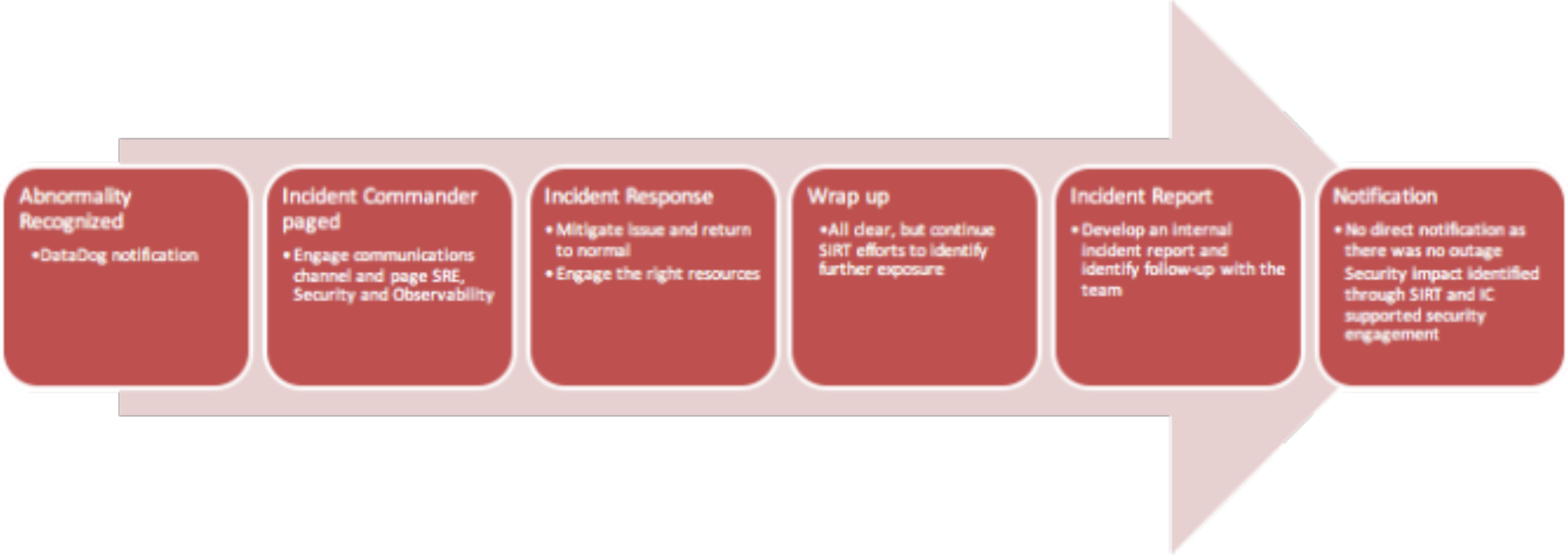
- Identify and **mitigate customer exposure** and **security exposure**
  - **15:10 GMT:** Plan in place to identify and contact all affected customers, and notify them of potential API key exposure.
  - **00:07 GMT:** Customers have been warned and made aware of new product features that limit key exposure.

- Regular check-ins to measure compliance with the customer notification.

- Based on information available, deep dive into Fastly's network assets to review whether a similar attack could have affected us.

Vendor security breach

Incident Command: mitigate immediate business impact



Abnormality Recognized

- DataDog notification

Incident Commander paged

- Engage communications channel and page SRE, Security and Observability

Incident Response

- Mitigate issue and return to normal
- Engage the right resources

Wrap up

- All clear, but continue SIRT efforts to identify further exposure

Incident Report

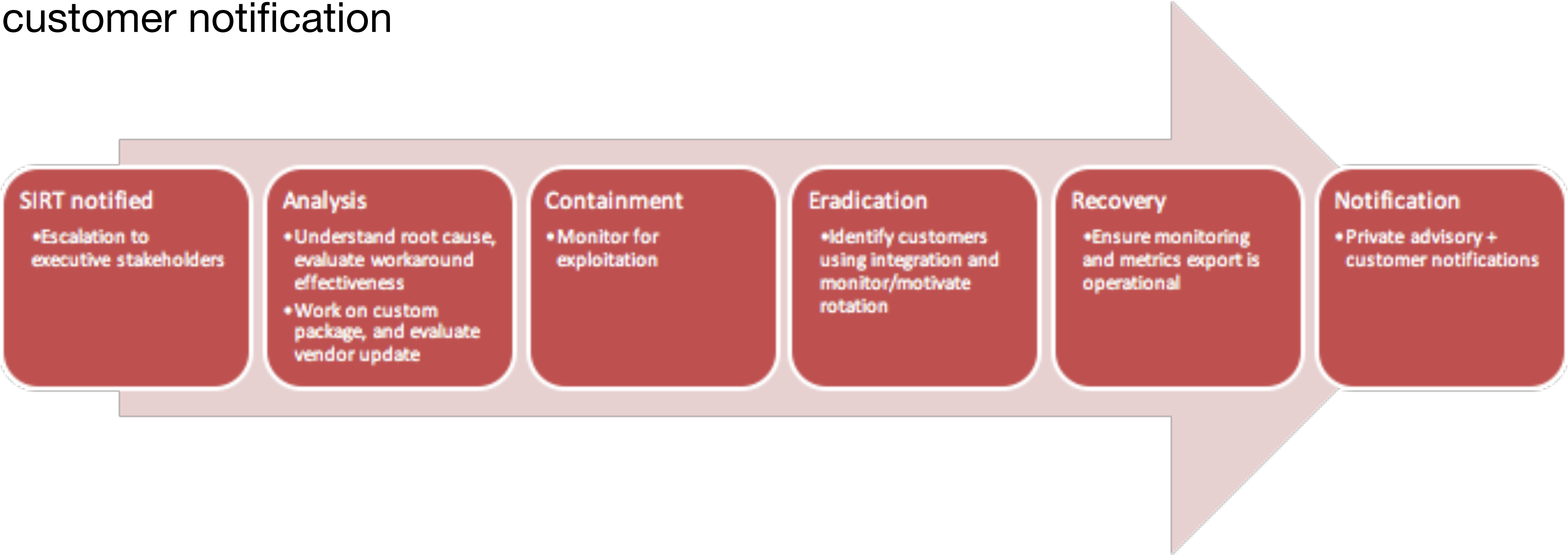
- Develop an internal incident report and identify follow-up with the team

Notification

- No direct notification as there was no outage
  Security impact identified through SIRT and IC supported security engagement

Vendor security breach

Security Incident Response Plan:
Identify exposure of customer information, coordinate containment, mitigation and customer notification



SIRT notified

- Escalation to executive stakeholders

Analysis

- Understand root cause, evaluate workaround effectiveness
- Work on custom package, and evaluate vendor update

Containment

- Monitor for exploitation

Eradication

- Identify customers using integration and monitor/motivate rotation

Recovery

- Ensure monitoring and metrics export is operational

Notification

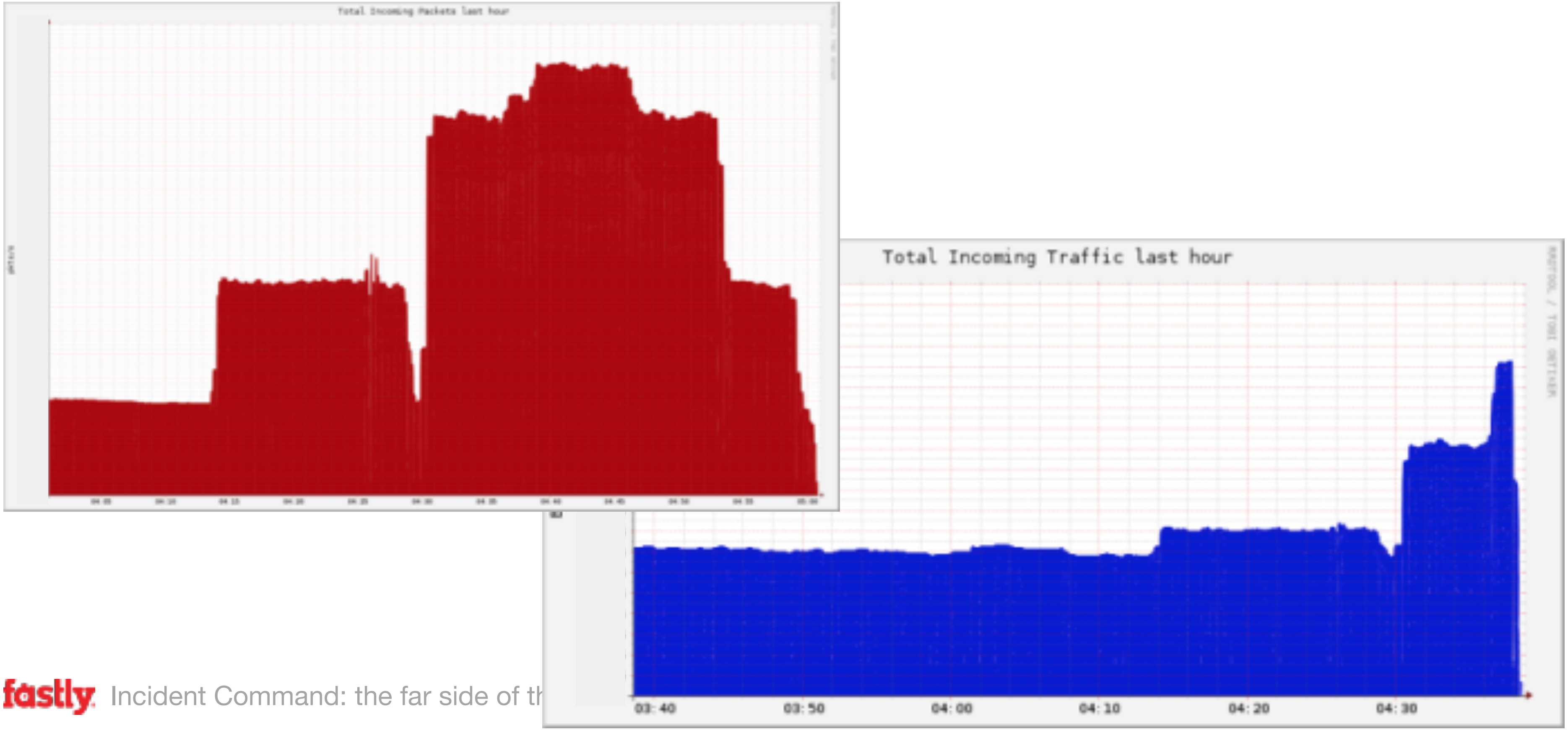
- Private advisory + customer notifications

Vendor security breach: lessons learned

- Identify **automated methods** for core vendors to report incidents;
- Create **partnership models that enable secure integrations**;
- When sharing data with a supplier, **you continue to own making sure the data is secure;**
- **Educate customers** on how to use features securely.

Case study:
Denial of Service

Sunday Morning DDoS (and Coffee)



Sunday Morning DDoS

- March 6, 2016:
  - 16:50 GMT: Monitoring systems detect problems in Frankfurt POP
  - 16:52 GMT: Monitoring systems detect problems in Amsterdam POP
  - 16:53 GMT: Incident Command initiated
  - 16:58 GMT: Status posted reflecting impact to EU performance
  - 17:00 GMT to 04:50 GMT+1d: Bifurcation / isolated based mitigation across POPs
- March 7, 2016
  - Ongoing: DDoS flows move to Asia POPs
  - 04:50 GMT: Mitigations hold; attack subsides
  - 04:55 GMT+1d: Incident Command concluded

DDoS: Characteristics

- **Shape shifting**, with a mix of:
  - UDP floods; notably DNS reflection
  - TCP ACK floods
  - TCP SYN floods
- **Internet Wide Effects:**
  - Backbone congestion
  - Elevated TCP Retransmission
  - We saw a few hundred Gb/ssec, but it was quite likely more than that...

DDoS: Retrospective

- **Incident Command:** ensure ongoing CDN availability and reliability
- **Security Incident Response Plan:** Engage security community to identify flow sources; bad actors; malware; and future capabilities.
- **Lessons learned:**
  - Pre-planned bifurcation techniques proved invaluable in time to mitigate
  - Mitigation options were limited by IP addressing architecture
  - DDoS can often mask other system availability events
- **Improvements:**
  - Separation of Infrastructure and Customer IP addressing; as well a DNS-based dependencies
  - Continued threat intelligence gathering to understand future TTP vectors
  - Emphasis on team health for long running events; rotations and food.

Lessons

- Start with the basics
  - Incident discovery
  - Incident management runbooks
  - Clear communication, both up and down
  - A strong focus on post-mortem
- Empower your engineers to deal effectively with workload
- Continue to let incidents teach you
- Partner closely with all stakeholders

Q&A

lisa@fastly.com
tjd@fastly.com
maarten@fastly.com