

Bootstrap Your Startup's Security

Add security to everyone's job.
Make security enhance operations.
Use security as a competitive advantage.

Patrick Coughlin - patrick@trustar.co
George Chamales - george@criticalsec.com

30 min presentation + 30 min discussion



Filter by text...

Filter by type ▾

LABELS

UNDO

REDO

REFRESH

SAVE

DOWNLOAD

PREV

NEXT

Ransomware attack through online billing

SUBMITTED 06-20-2017 00:59

ENCLAVE



SECTOR

EDUCATION

TAGS

+ MANAGE

Content

IOCs (22)

Notes (0)

A subsidiary of <company-name> was recently hacked via the [locky](#) ransomware invoicing attack

ending emails with attached invoices to <email-address> will put those invoices in the queue for

the finance team. In this scenario, the <person> clicked on the email in the

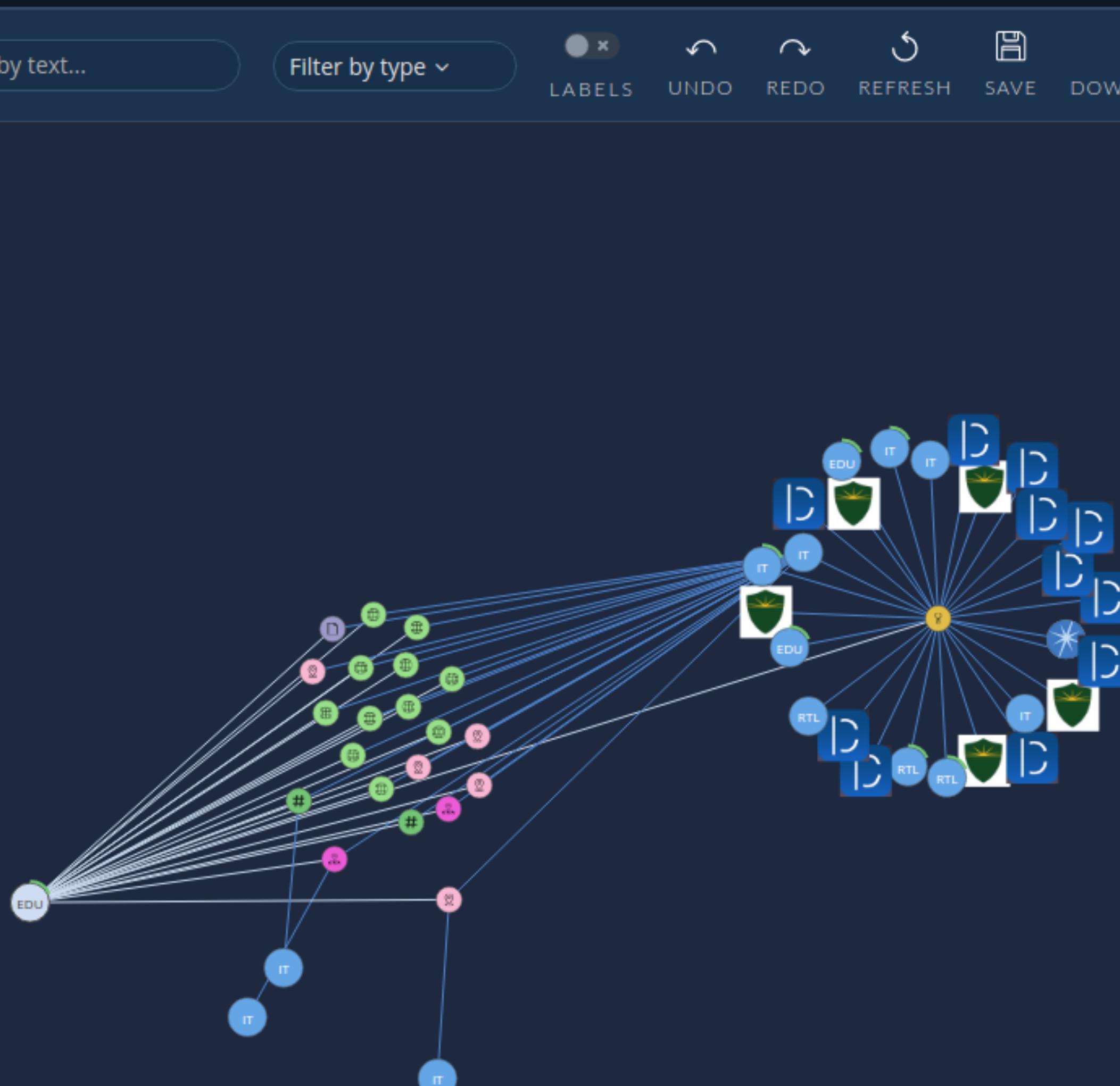
was just another invoice and opened the zipped file attached. The zip con

which further downloads second phase or phase 2 malware binary from a

encrypts your all files in local and network.

They use email addresses and subjects that will entice a user to read the e

attachment. A very high proportion are being targeted at small and medium



Agenda

Add security to everyone's job.

Make security enhance operations.

Use security as a competitive advantage.

Add ...and its security to everyone's job description.

Chief Executive Officer

- Develop high-quality business strategies ensuring their alignment with short & long-term objectives
- Lead and motivate subordinates to advance employee engagement develop a high performing managerial team
- Maintain a deep knowledge of the markets and industry of the company.
- Oversee all operations and business activities to ensure they produce the desired results and are consistent with the overall strategy and mission
- Make high-quality investing decisions to advance the business and increase profits
- Enforce adherence to legal guidelines and in-house policies to maintain the company's legality, business ethics, **and its security**.
- Review financial and non-financial reports to devise solutions or improvements
- Build trust relations with key partners and stakeholders and act as a point of contact for important shareholders
- Analyze problematic situations and occurrences and provide solutions to ensure company survival, growth, **and its security**.
- Maintain a deep knowledge of the markets and industry of the company.

Director of Customer Success

- Manage relationships with key customer accounts at the technical and executive level across growing Fortune 500 customer companies (~25% travel).
- Architect and quarterback customer success at strategic accounts, driving intelligence exchange into security operations.
- Evangelize the TruSTAR product and lead strategic business development initiatives that align with your unique network and professional experience, namely in the technology sector and in the federal agency space.
- Recruit, train, and lead other members of the customer success team as we grow.
- Customer lifecycle management experience from inception through all lifecycle stages **and its security**

Technical Account Manager

- Manage relationships with key customer accounts at the technical and executive level across growing Fortune 500 customer companies (~30% travel).
- Assist customers in architecting TruSTAR and intelligence exchange into their security operations and quarterback implementation and expansion across security teams.
- Collect qualitative feedback from customers through regular touch-points with their technical teams to get an in-depth understanding of their needs.
- Measure and report on quantitative metrics to help develop deeper understanding of engagement levers and leading indicators of customer success.
- Advocate for customer needs **and its security** inside company and assist in translating feedback into product requirements.
- Evangelize the TruSTAR product and lead strategic business development initiatives that align with your unique network and professional experience, namely in the technology sector and federal agency space.

Junior Account Manager

- Assist with management of key customer accounts across growing Fortune 500 customer companies.
- Ensure that customers have platform access, manage targeted customer communications, and resolve minor technical challenges.
- Collect qualitative feedback from customers through regular touch-points with their technical teams to get an in-depth understanding of their needs.
- Measure and report on quantitative metrics to help develop deeper understanding of engagement levers and leading indicators of customer success.
- Advocate for customer needs **and its security** inside company and assist in translating feedback into product requirements.

Account Executive, Sales

- Demonstrate product and new features to help drive engagement with new and existing customers.
- Manage engagement with new target customer accounts
- Collect qualitative feedback from users and quantitatively track engagement across new feature sets.
- Translate customer feedback into engineering requirements and product feature specifications.
- Research market trends and competition and develop competitive analyses to deliver differentiated product features and capabilities.
- Represent TruSTAR at external venues, conferences, and forums to promote the TruSTAR product **and its security**.
- Manage specific product development and analytics prototyping tasks **and its security**.
- Provide insightful strategic analysis to the community of TruSTAR users on security trends.

Chief Operating Officer

- Design and implement business strategies, plans, procedures **and its security**.
- Set comprehensive goals for performance and growth.
- Establish policies that promote company culture and vision
- Oversee daily operations of the company and the work of executives (IT, Marketing, Sales, Finance etc.)
- Lead employees to encourage maximum performance and dedication
- Evaluate performance by analyzing and interpreting data and metrics
- Write and submit reports to the CEO in all matters of importance
- Assist CEO in fundraising ventures
- Participate in expansion activities (investments, acquisitions, corporate alliances etc.)
- Manage relationships with partners/vendors

Communications & Content Marketing Lead

- Work with the leadership team to develop and manage an editorial calendar for content, social media and events **and its security**.
- Quickly draft content and synthesize feedback from others to develop polished content to promote across earned and owned channels.
- Analyze, track, and measure success against clear targets and KPIs and provide routine reporting to leadership for use in strategic planning sessions and investor/board meetings.
- Coordinate TruSTAR speaking and event strategies-developing content and supporting materials.
- Manage outreach to industry influencers and journalists to push TruSTAR messaging, content, and leadership vision.
- Own the website and external facing social channels to ensure we are staying edgy, while maintaining consistency of concept and messaging.
- Collaborate with the product team to stay abreast of product challenges, opportunities **and its security** as we grow.

Fraud Intelligence Lead

- Manage TruSTAR's initial fraud-oriented customers (eg. Fraud Team @ Fortune 50 company) liaising between customer success and product development to architect TruSTAR into their workflow - balancing automation and human investigative cycles
- Expand the Cloud Fraud Intelligence Exchange (Google, AWS, MSFT, Rackspace, IBM, Swisscom, 1&1, and more) to additional members, **and its security**, sharing real data in real-time.
- Develop and manage a fraud go-to-market strategy working closely with leads from business operations, product, and customer success.
- Manage execution of the fraud go-to-market strategy **and its security**, coordinating across business operations, marketing, sales, and product.
- Measure and report on success of fraud business **and its security** across executive team with board-level visibility.

Operations & Administration

- Coordinate with hiring managers to ensure new hires are welcomed and their 1st day experience is maximized.
- Manage interview schedule coordination across key leadership as the team grows.
- Coordinate special events and team activities at TruSTAR HQ and elsewhere ensuring they are delivered on budget and they promote a fun and connected culture.
- Assist in managing the day-to-day calendars of the co-founders to ensure their time is maximized and deconflicted.
- Apply a critical eye to our brand new space and help design and organize layout in a way that drives collaborative culture.
- Manage budget and vendors for all office supplies, snacks, food, special events, and team activities.
- Hire and manage all 3rd party office services staff with a focus on accountability and professionalism of our work environment **and its security**.
- Ensure cross-functional feedback on the work environment we've created, and deliver recommendations to the executive team on how to continue adapting TruSTAR's home.

Lead Data Scientist

- Work closely with a product engineering team to identify and answer important product questions.
- Work closely with software engineers to extend the functionality of the Extract Transform and Load (ETL) process **and its security**.
- Answer product questions by using appropriate statistical techniques on available data.
- Communicate findings to product managers and engineers.
- Drive the collection of new data and the refinement of existing data sources **and its security**
- Analyze and interpret the results of product experiments.
- Develop best practices for instrumentation, experimentation, **and its security** and communicate those to product engineering teams.

Director of Engineering

- Manages the entire engineering department overseeing resources, staffing, and the enhancement and maintenance of a first-class team.
- In charge of the management and execution of site/software project plans and delivery commitments.
- Leads the development teams with a focus on technologies inclusive of HTML, JavaScript, CSS, and Java.
- Manages the technical integrations and relationships with internal and external stakeholders.
- Drives the strategy, architecture, and development of the business's site/software solutions **and its security**.
- Organizes activities for the development, implementation, release, and maintenance of projects necessary for site/software development and sustenance
- Takes initiative to explore, evangelize, and implement innovative technologies within the business in order to improve the business's internal platforms, **and its security**, as well as customer experience.

Head of Product

- Work closely with a product engineering team to identify and answer important product questions
- Work closely with software engineers to extend the functionality of the Extract Transform and Load (ETL) process **and its security**.
- Answer product questions by using appropriate statistical techniques on available data.
- Communicate findings to product managers and engineers
- Drive the collection of new data and the refinement of existing data sources **and its security**.
- Analyze and interpret the results of product experiments
- Develop best practices for instrumentation, experimentation, and its security and communicate those to product engineering teams.

Frontend Software Engineer

- Architect, build, and maintain critical software components **and its security** across the entire TruSTAR product stack within a highly-secure data processing environment.
- Own major product development initiatives **and its security**, such as security data analytics, correlation, third-party integrations, and anonymous collaboration.
- Develop REST APIs **and its security** for customers to securely share and ingest semi-structured cyber threat intelligence.
- Work closely with TruSTAR co-founders, the Director of Engineering, and the rest of the product development team to advance the product roadmap.
- Provide DevOps support for production services **and its security** in cloud infrastructure using modern tools and frameworks.
- Mentor junior engineers and help grow the technical team **and its security**.

Backend Software Engineer

- Architect, build, and maintain critical software components **and its security** across the entire TruSTAR product stack within a highly-secure data processing environment.
- Own major product development initiatives **and its security**, such as security data analytics, correlation, third-party integrations, and anonymous collaboration.
- Develop REST APIs **and its security** for customers to securely share and ingest semi-structured cyber threat intelligence.
- Work closely with TruSTAR co-founders, the Director of Engineering, and the rest of the product development team to advance the product roadmap.
- Provide DevOps support for production services **and its security** in cloud infrastructure using modern tools and frameworks.
- Mentor junior engineers and help grow the technical team **and its security**.

Infrastructure Engineer

- Manage the online infrastructure **and its security**.
- Support engineering team system provisioning, management, updates **and its security**.
- Develop infrastructure automation systems **and its security** to streamline day-to-day operations
- Manage centralized logging and monitoring systems **and its security**
- Establish and maintain the infrastructure's secret service **and its security**.
- Stay on top of new advances in infrastructure systems, automation, **and its security**.

Junior Data Science

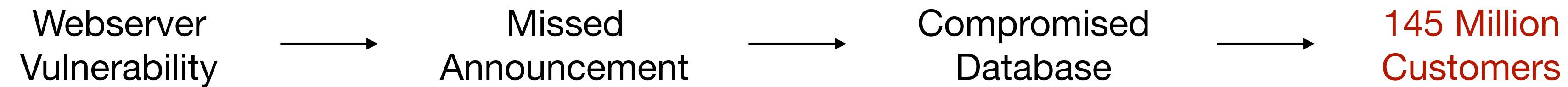
- Apply Machine Learning to Indicator Extraction
- Machine Learning models for white listing of indicators.
- Present results of different machine model evaluations and provide recommendations.
- Natural Language Processing (NLP)
- Increase the accuracy of current Named-Entity Recognizer, by training, validating and testing new models.
- Investigate new algorithms and techniques
- Research and develop graph clustering and path finding algorithms.
- Assist in building out graph analytics playbooks **and its security**.

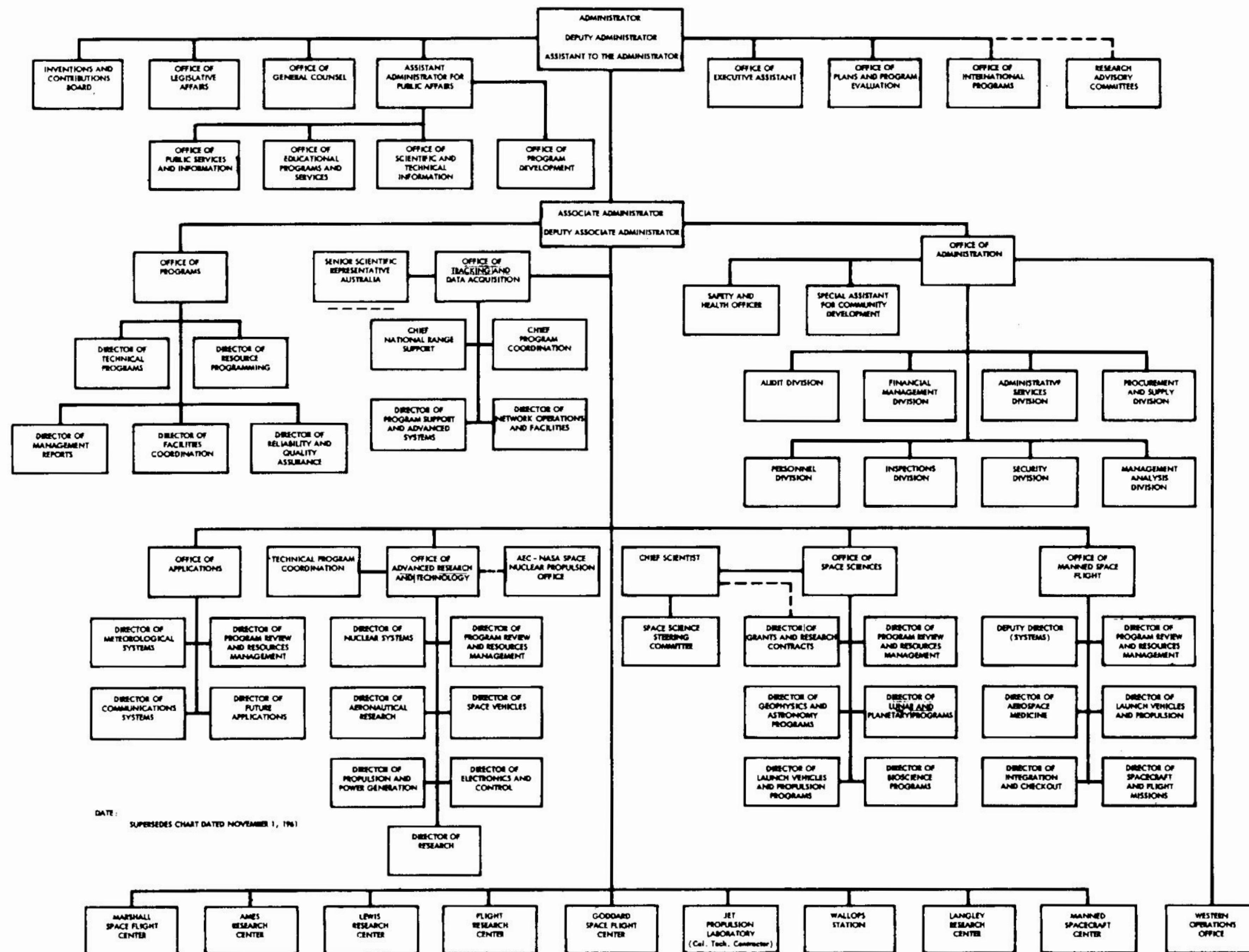


Subsidiarity

Delegate decision making authority
to the smallest competent group.

EQUIFAX







Ryan McGeehan

Jan 16, 2017 · 5 min read

This guy
bootstrapped
Facebook's security.

You don't need a Chief Security Officer.

When hiring security leadership is a bad thing for a startup.

I helped many young technology startups last year (2016) build security programs from scratch, or at least start approaching the subject. Many of them ask if they should hire a CSO or a “security lead”.

My observations are that it can be *harmful* to introduce dedicated security employees *too early* at a startup. This introduction of a specialized role to solve a horizontal problem will often cause early fragmentation and organizational debts.

Instead, startups do better off getting short term guidance from external expertise and tasking existing engineering talent with security projects.

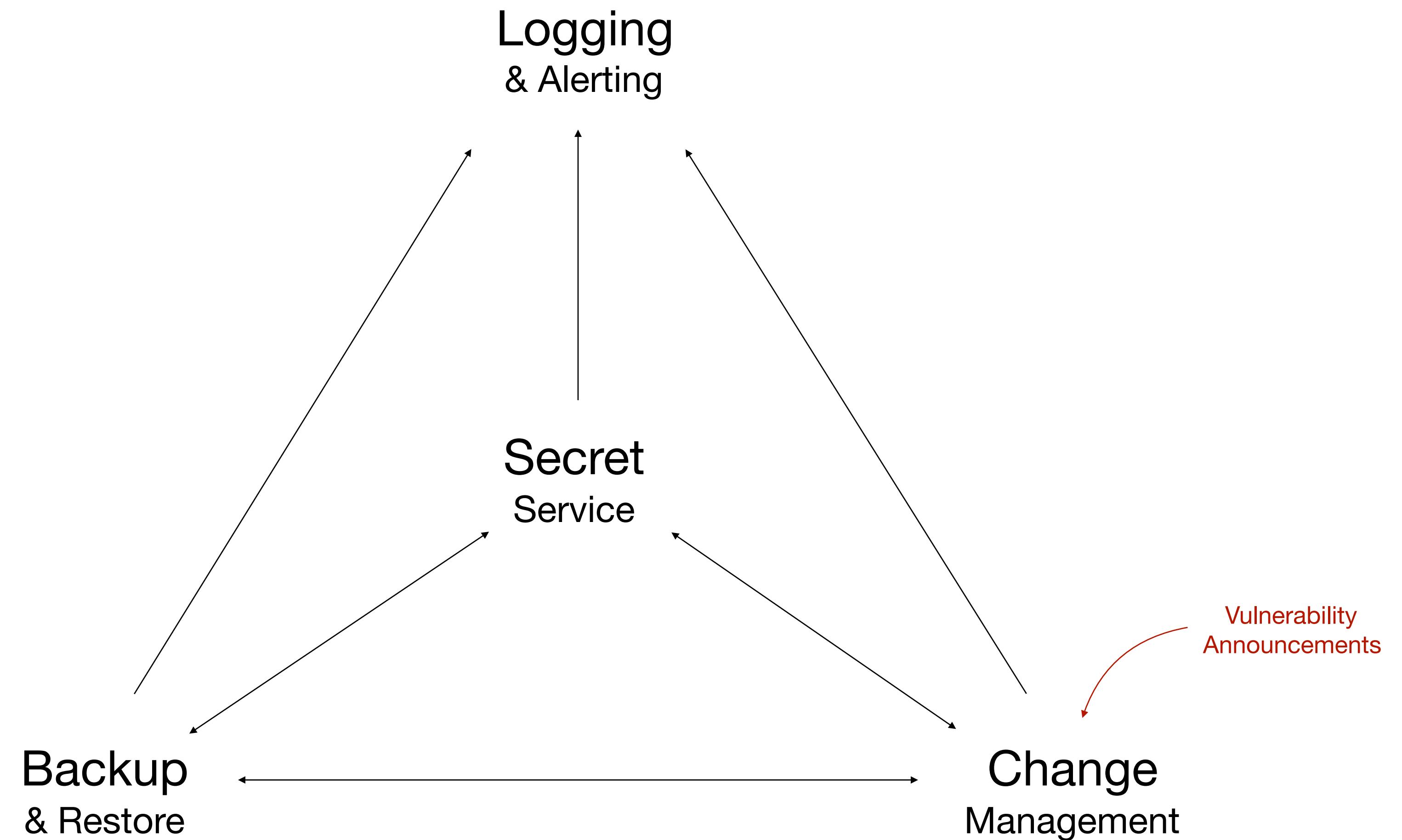
Make security enhance operations.

Principles

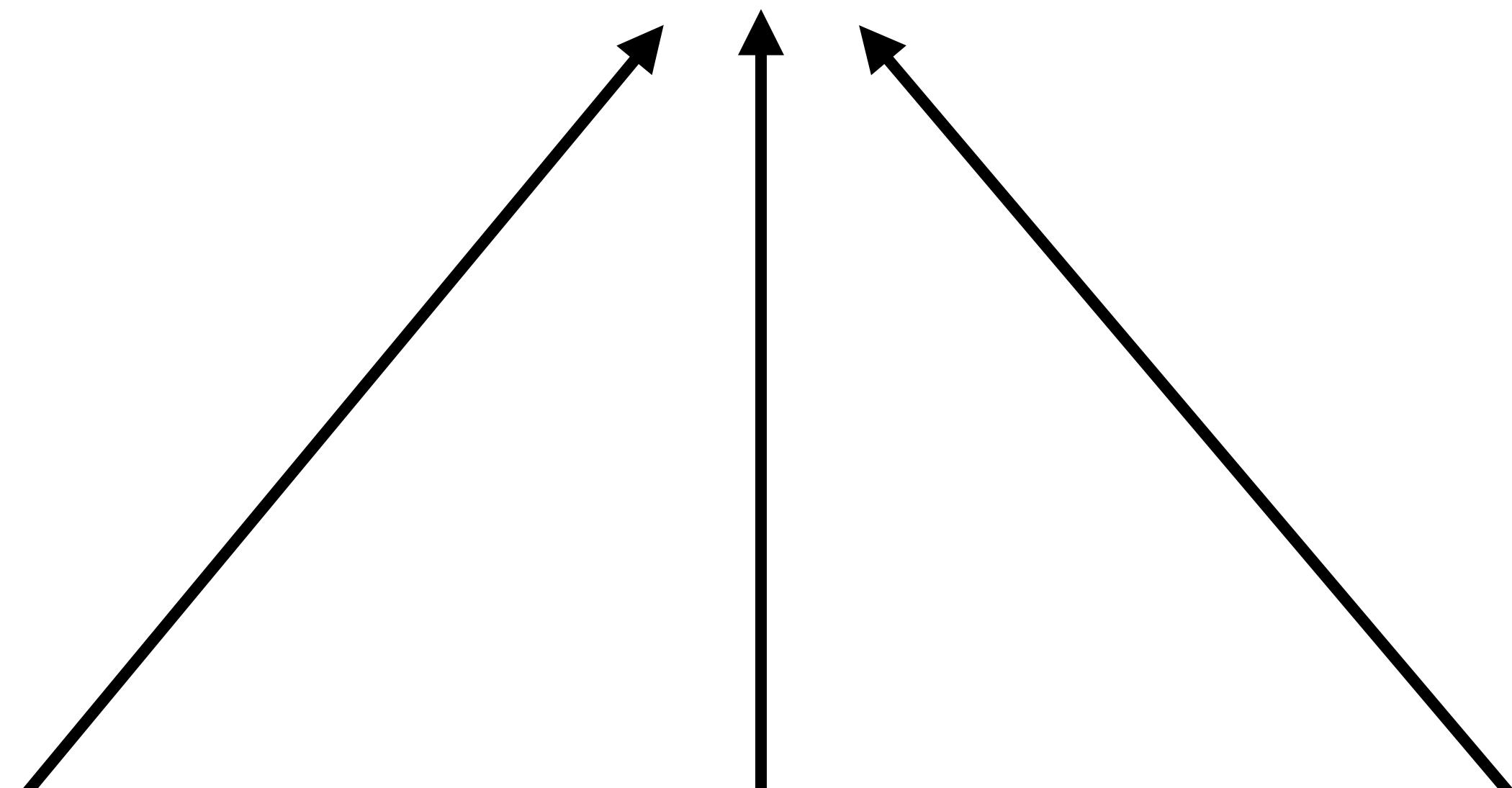
Simplify: Less is more.

The system should do *exactly*
what it needs to do and *nothing* else.

Infrastructure Services



Logging & Alerting



New Search

```
sourcetype=linux_secure "Failed password"
```

✓ 74 events (10/5/14 9:01:00.000 PM to 10/5/14 10:01:52.000 PM)

Events (74)

Statistics

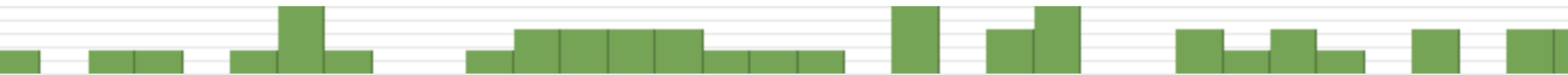
Visualization

Format Timeline ▾

– Zoom Out

+ Zoom to Selection

✗ Deselect



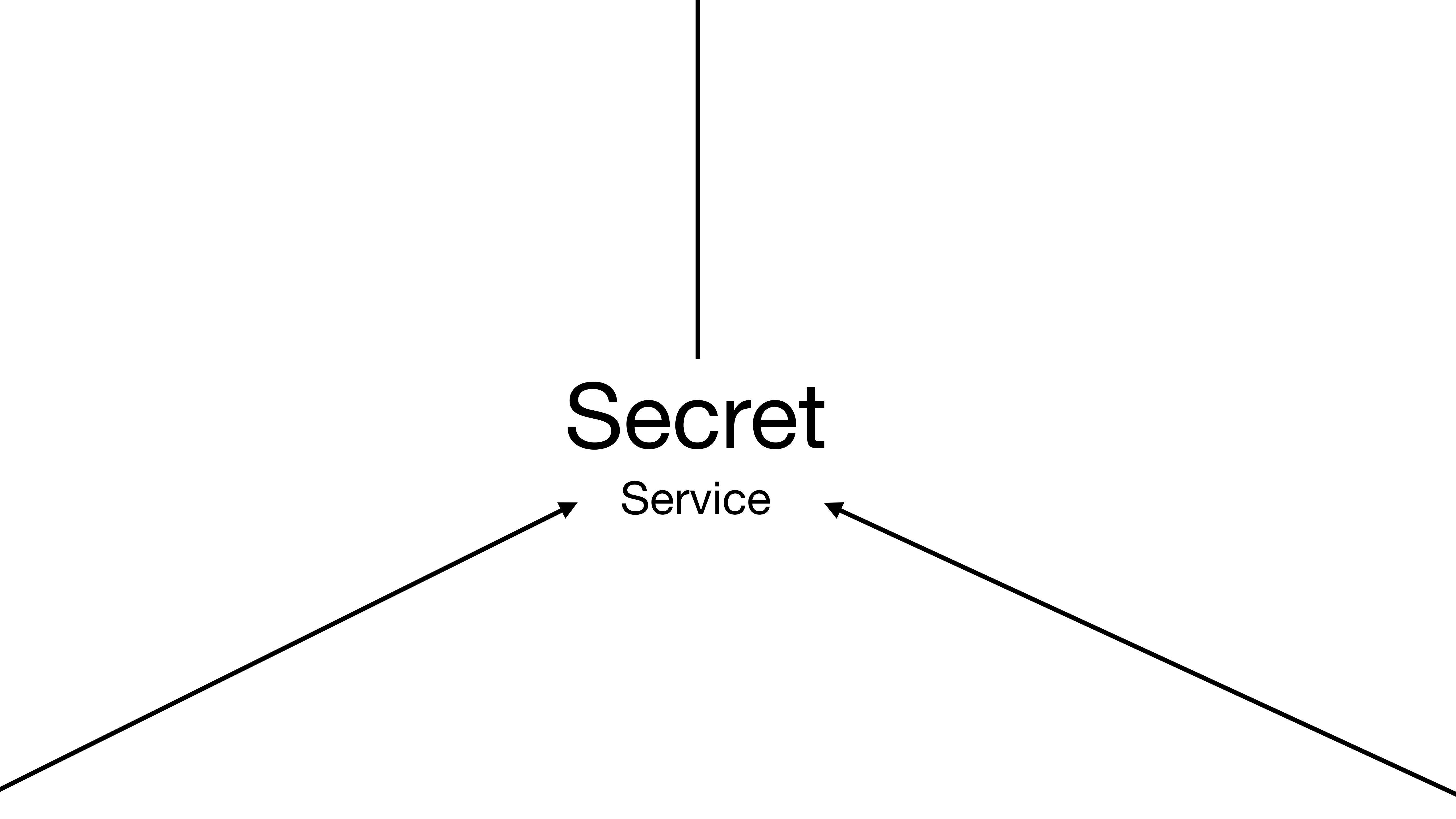
List ▾

Format ▾

20 Per Page ▾

i	Time	Event
>	10/5/14 10:00:47.000 PM	Sun Oct 05 2014 22:00:47 www1 sshd[1812]: Failed password for host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	10/5/14 10:00:16.000 PM	Sun Oct 05 2014 22:00:16 www1 sshd[1755]: Failed password for host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	10/5/14 9:59:37.000 PM	Sun Oct 05 2014 21:59:37 www1 sshd[5453]: Failed password for host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	10/5/14 9:59:28.000 PM	Sun Oct 05 2014 21:59:28 www1 sshd[4472]: Failed password for host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	10/5/14 9:58:39.000 PM	Sun Oct 05 2014 21:58:39 www1 sshd[3610]: Failed password for host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	10/5/14 9:58:28.000 PM	Sun Oct 05 2014 21:58:28 www1 sshd[2586]: Failed password for host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	10/5/14 9:57:26.000 PM	Sun Oct 05 2014 21:57:26 www1 sshd[3661]: Failed password for host = www1 source = /opt/log/www1/secure.log sourcetype = linux_secure
>	10/5/14	Sun Oct 05 2014 21:56:47 www1 sshd[4772]: Failed password for

Critical data hides
in the logs you
don't collect.

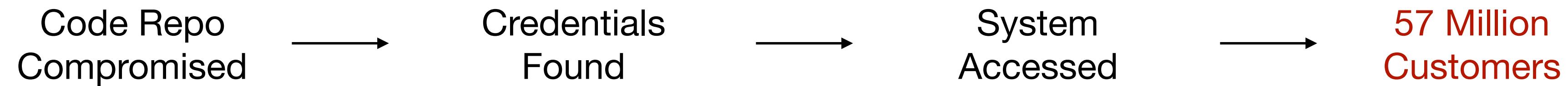


Secret

Service



U B E R



All of Oculus's Rift headsets have stopped working due to an expired certificate

X

Lucas Matney Mar 7, 2018

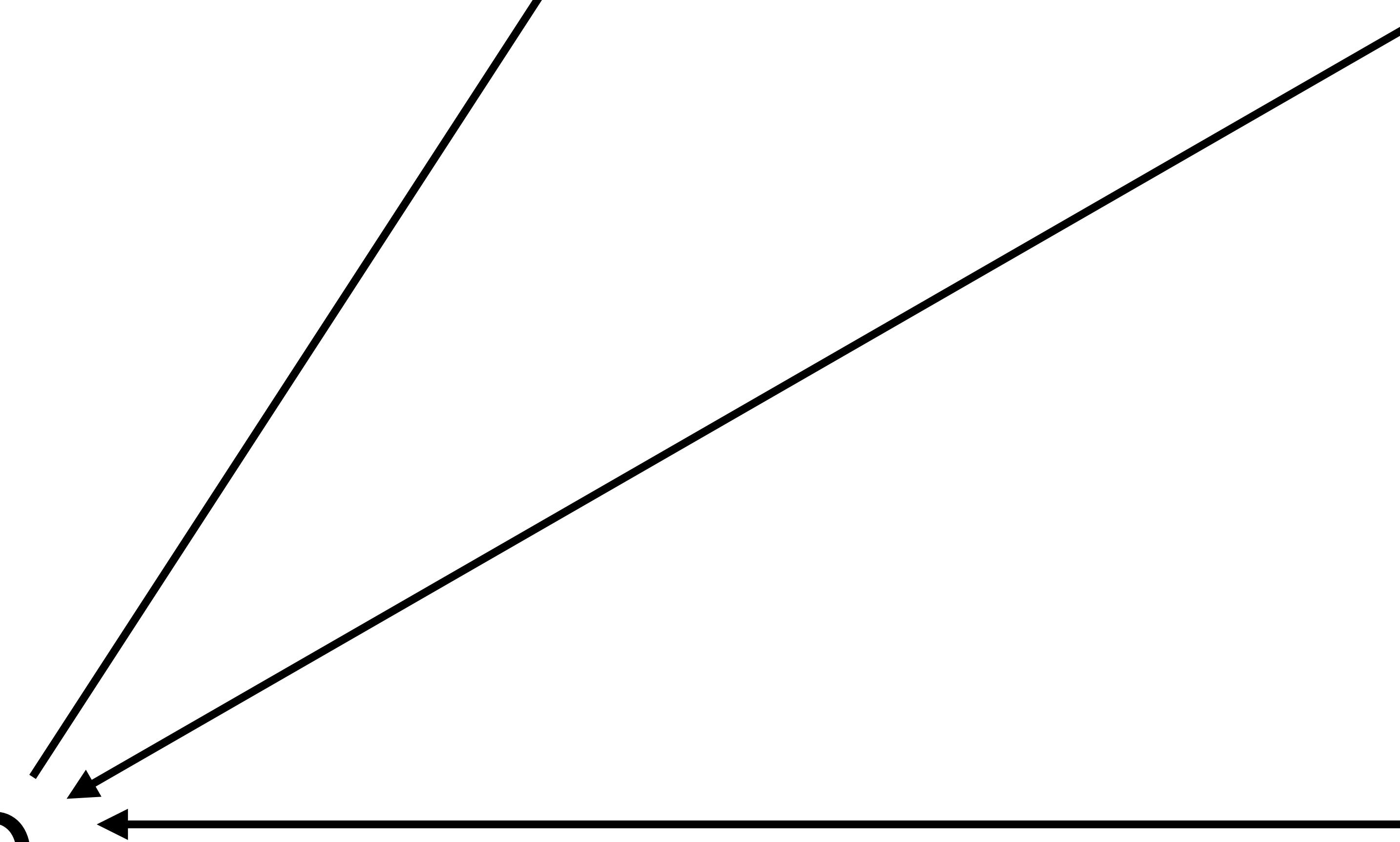
 Comment



Update: After nearly a full day of downtime, the company has issued an official patch [here](#). More details on how to get your Rift up-and-running [here](#).

Someone at **Oculus**  screwed up pretty badly today: An expired certificate appears to have soft-bricked all of the company's Rift VR headsets, with users still unable to fire up software on the devices and no word of an incoming fix from the company yet.

**Backup
& Restore**





6 million customers



Security keys & software



112,000 files



12,000 social media influencers



198 million voters



3 million fans



TigerSwan

9,400 resumes



123 million households



You take the test, we'll take it from there

150,000 patients



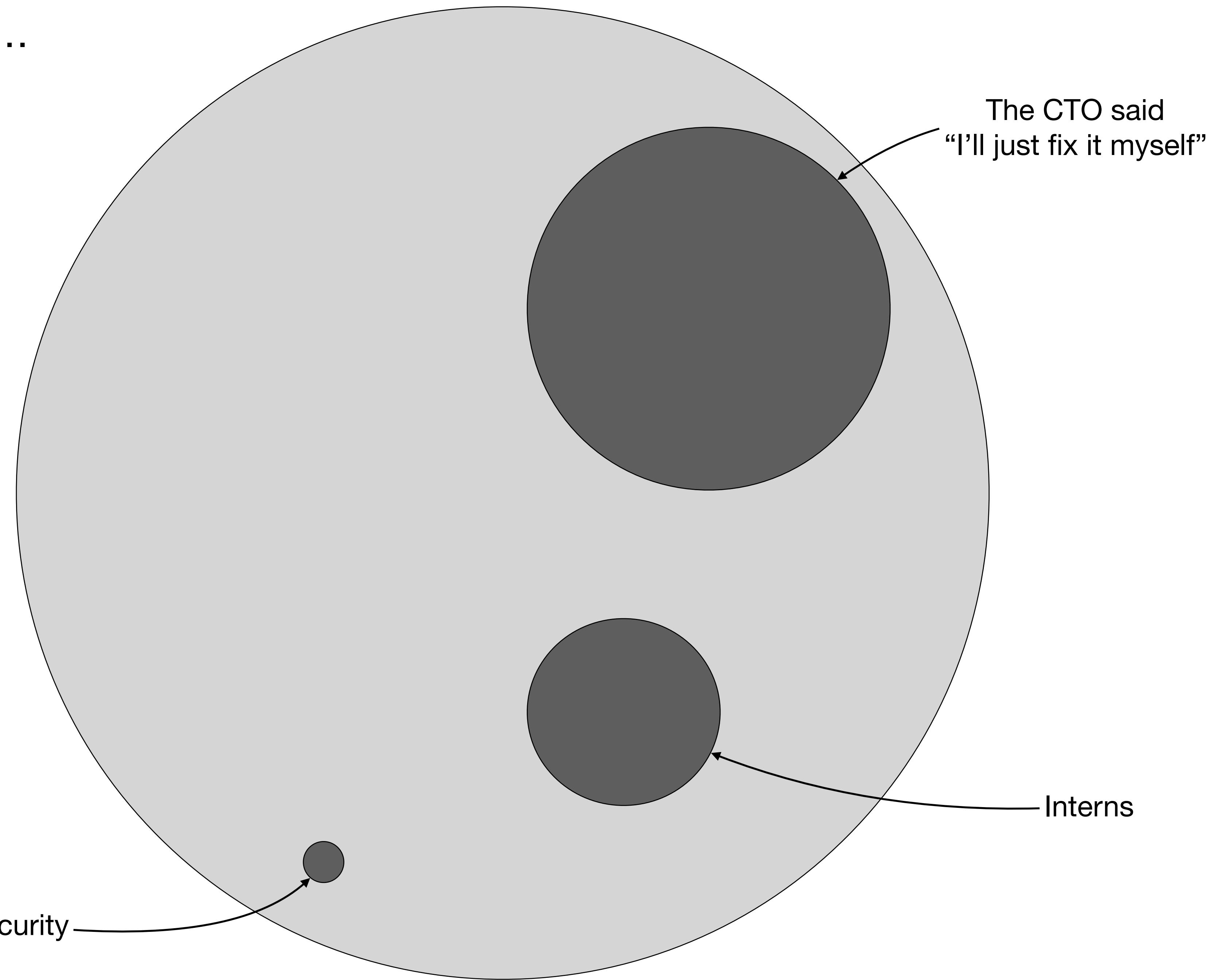
Verizon - <https://www.upguard.com/breaches/verizon-cloud-leak>
Octoly - <https://www.upguard.com/breaches/cloud-leak-octoly>
TigerSwan - <https://www.upguard.com/breaches/cloud-leak-tigerswan>

Accenture - <https://www.upguard.com/breaches/cloud-leak-accenture>
Deep Root Analytics - <https://www.upguard.com/breaches/the-rnc-files>
Alteryx - <https://www.upguard.com/breaches/cloud-leak-alteryx>

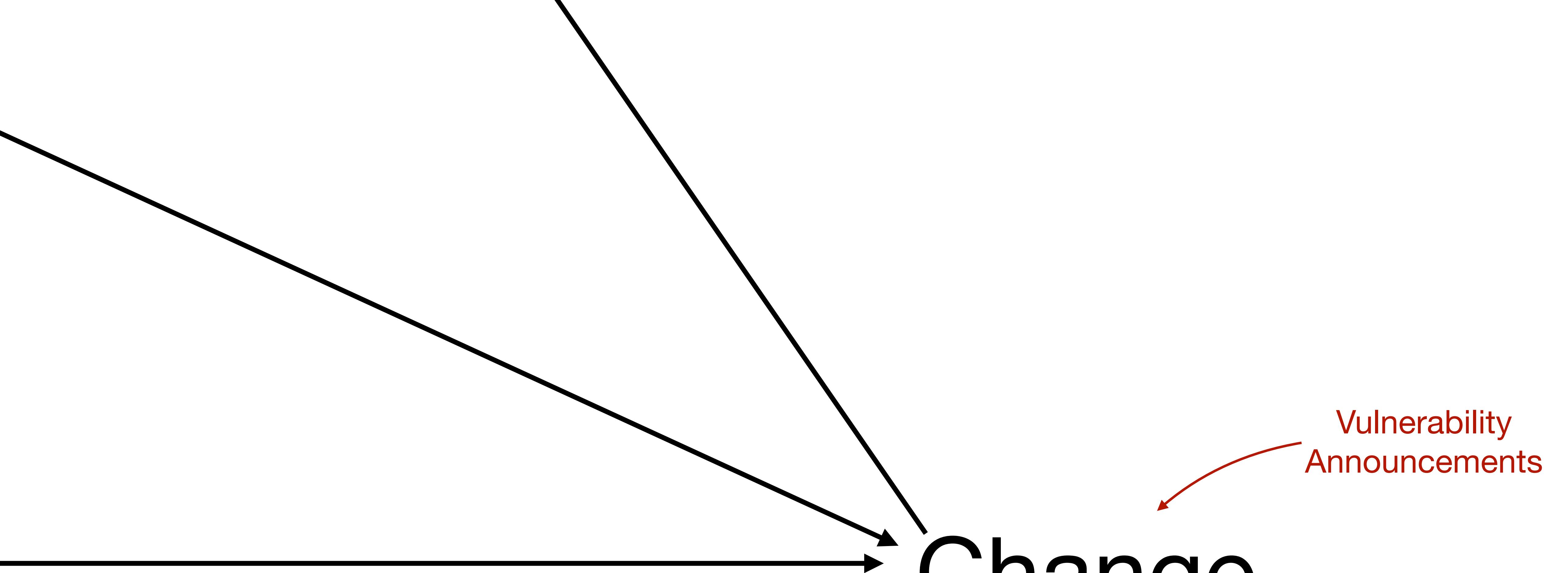
FedEx - <https://mackerpersecurity.com/post/fedex-customer-records-exposed>
WWE - <https://mackerpersecurity.com/post/world-wrestling-entertainment-leaks-3-million-emails>
PHM - <https://mackerpersecurity.com/post/patient-home-monitoring-service-leaks-private-medical-data-online>



Reasons for backups...



Change Management



Vulnerability
Announcements



TESLA

Found Cloud
Credentials



Started Cloud
Server



Mined Crypto
Currency

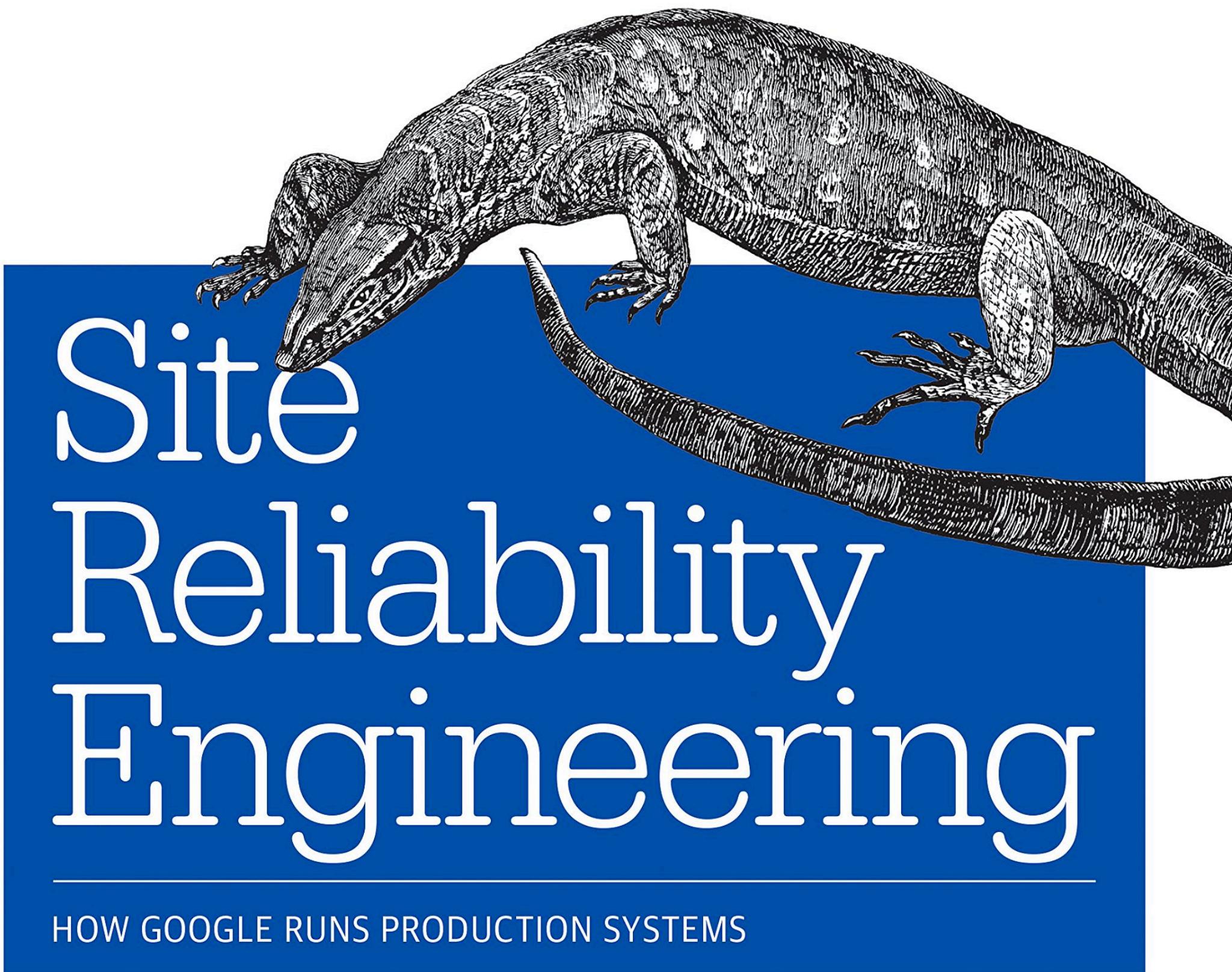


Realized they
weren't the first

Roughly 70% of outages
are due to changes in a live system.

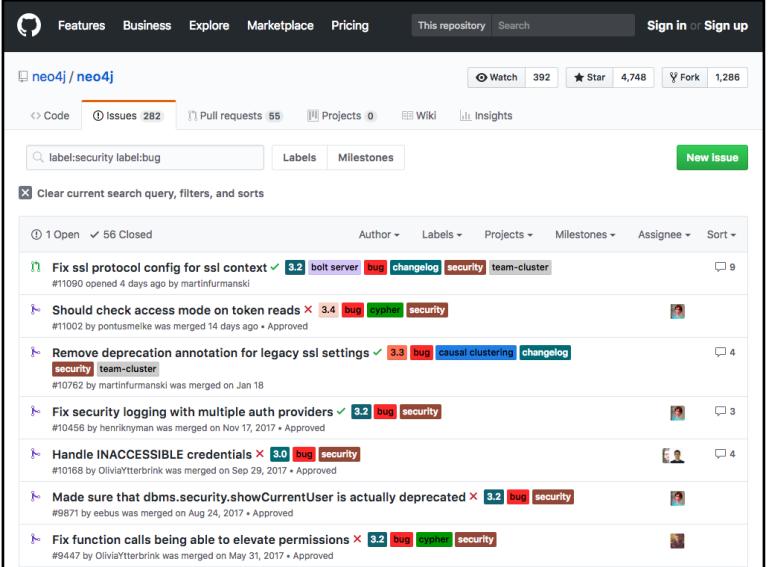
Benjamin Treynor Sloss
Vice President, Google Engineering, founder of Google SRE

<https://landing.google.com/sre/book/index.html>



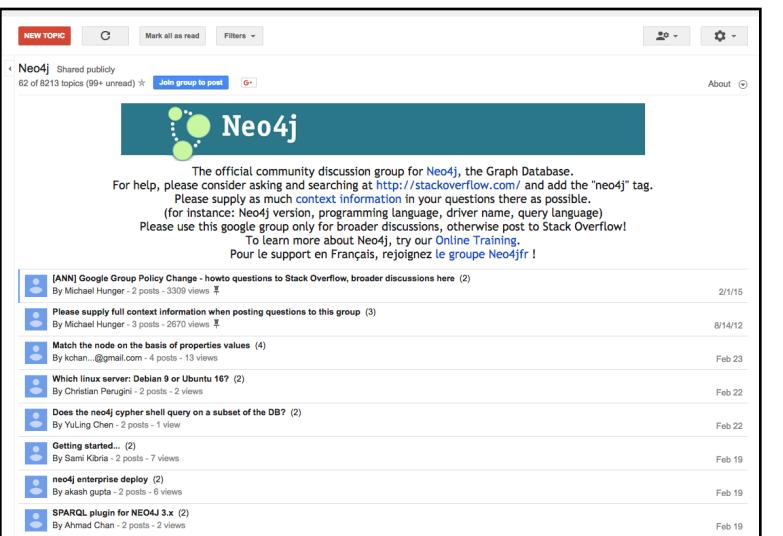
Edited by Betsy Beyer, Chris Jones,
Jennifer Petoff & Niall Richard Murphy

Bugs & Release Notes



CVE Details

National Vulnerability DB

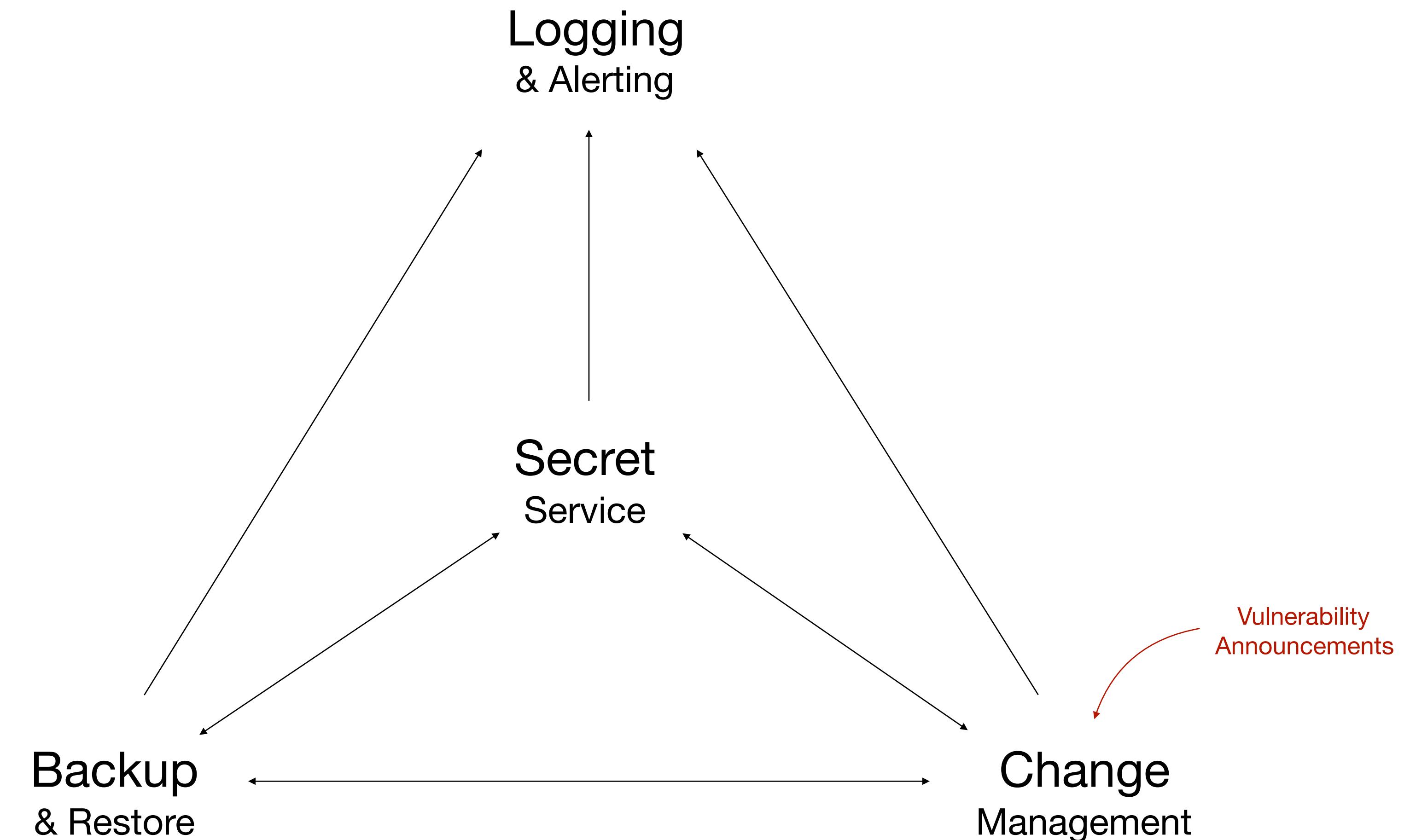


Mailing Lists



Vulnerability Alert Pipeline

**Infrastructure
Services** = Stability



Use security as a competitive advantage.

Customer. Security. Requirements.

SIG_Full_2016_PVH (updated).xlsm

V. Cloud Security
96% Percent Complete
Tab Automation: Enable

Questionnaire Instructions:
 - For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the Additional Information Field in column F to provide.
 - To display the entire contents of the tab and disable the transfer of responses from the Lite tab, select the word "Disable" in the Tab Automation field at the top of the page.
 - Use the Maturity column to identify the maturity of the question. See the How To Guide for instructions on filling out this field.

Ques Num	Question/Request	Response	Maturity	Additional Information	Service Model	Deployment Model	AUP Reference	ISO 27002:2013 Relevant
5 V.1	Are Cloud Services provided? If yes, what service model is provided (select all that apply):	Yes					V.1 Service and Deployment Models	Determining the scope information management
6 V.1.1	Software as a Service (SaaS)?	Yes					V.1 Service and Deployment Models	NA
7 V.1.2	Platform as a Service (PaaS)?	No					V.1 Service and Deployment Models	NA
8 V.1.3	Infrastructure as a Service (IaaS)?	No					V.1 Service and Deployment Models	NA
9 V.1.4	What deployment models are provided (select all that apply):						V.1 Service and Deployment Models	Determining the scope information management
10 V.1.4.1	Private cloud?	Yes					V.1 Service and Deployment Models	NA
11 V.1.4.2	Public cloud?	No					V.1 Service and Deployment Models	NA
12 V.1.4.3	Community cloud?	No					V.1 Service and Deployment Models	NA
13 V.1.4.4	Hybrid cloud?	No					V.1 Service and Deployment Models	NA
14 V.1.5	Where is the cloud infrastructure hosted:							Determining the scope information management
15 V.1.5.1	Data center: single tenancy?	No						NA
16 V.1.5.2	Co-location: dedicated server?	No						NA
17 V.1.5.3	Co-location: shared server?	No						NA
18 V.1.5.4	Co-location: dedicated cabinet?	No						NA
19 V.1.5.5	Co-location: shared cabinet?	No						NA
20 V.1.5.6	Co-location: dedicated cage?	No						NA
21 V.1.5.7	Co-location: shared cage?	No						NA
22 V.1.5.8	Cloud provider: (e.g., AWS)?	Yes						NA
23 V.1.6	What legal jurisdiction does data reside (select all that apply):						P.1 Scoped Privacy Data Inventory and Flows	Identification of applicable legislation and contractual requirements
24 V.1.6.1	USA?	Yes					P.1 Scoped Privacy Data Inventory and Flows	NA
25 V.1.6.2	Canada?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
26 V.1.6.3	Asia?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
27 V.1.6.4	South America?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
28 V.1.6.5	Australia?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
29 V.1.6.6	Asia-Pacific?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
30 V.1.6.7	Africa?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
31 V.1.6.8	Europe (EU)?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
32 V.1.6.9	Europe (non-EU)?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
33 V.1.6.10	Other (please specify)?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
34 V.1.7	Can clients define the legal jurisdictions of their data? If yes, can they define where the data is:	No		Data stored in US only.			P.1 Scoped Privacy Data Inventory and Flows	Identification of applicable legislation and contractual requirements
35 V.1.7.1	Stored?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
36 V.1.7.2	Processed?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
37 V.1.7.3	Transmitted?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
38 V.1.7.4	Accessed?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
39 V.1.8	Are application instances part of the services provided?	No					P.1 Scoped Privacy Data Inventory and Flows	9.4.1
40 V.1.8.1	Are these instances shared with other clients?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
41 V.1.9	Are database instances part of the services provided?	No					P.1 Scoped Privacy Data Inventory and Flows	9.4.1
42 V.1.9.1	Are these instances shared with other clients?	No					P.1 Scoped Privacy Data Inventory and Flows	NA
43 V.1.10	Is data segmentation and separation capability between clients provided? If yes, is it:	Yes					V.1 Service and Deployment Models	9.4.1
44 V.1.10.1	Physical segmentation (private cloud)?	No						Information access requirements
45 V.1.10.2	Network segmentation?	No						9.4.1
46 V.1.10.3	System segmentation (unique system instances (e.g., virtualization))?	No						Information access requirements
47 V.1.10.4	Application segmentation (unique application instances)?	No						9.4.1
48 V.1.10.5	Application segmentation (e.g., application ID, metadata tagging)?	Yes						Information access requirements

Security Policy

TruSTAR Security Policy



George Chamales
Last modified Jan 29, 2018

Dealing With A Security Incident?

Please store the Security Coordinator's contact info in your phone & computer:

Chris Roblee

crobbee@trustar.co

+1 (248) 248-2488

Reporting a security incident? See section 2.2

Responding to a reported security incident? See section 2

Introduction

Welcome to the TruSTAR Security Policy. Here you'll find all of the different ways we maintain the security of our company. This document is ordered around a set of simple principles that form the foundation of our security philosophy.

All of our security rules, requirements and recommendations flow from these principles, and it's your job as an employee of TruSTAR to burn a few minutes reading through the whole thing. A lot of it will be relevant to your work and the bits that aren't will give you a better understanding of how the company works and why certain decisions are getting made.

Our Security Principles:

0. **Responsibility:** Security is Literally Your Job.
1. **Assets:** If it's Used, it's Tracked
2. **Incident Response:** Over-Share, Overreact
3. **Physical Security:** Locked by Default
4. **Communications Security:** Encrypted by Default
5. **System Security:** Starts Locked Down, Stays Locked Down
6. **Network Access:** Nothing Moves Without Permission
7. **Data Access:** Need to Know
8. **Backup & Recovery:** We Never Lose Data
9. **Account Management:** Minimum Privileges, Maximum Control
10. **Software Dev & Deployment:** Bugs Get Squished
11. **Periodic Reviews & Updates:** There Will Be a Test.

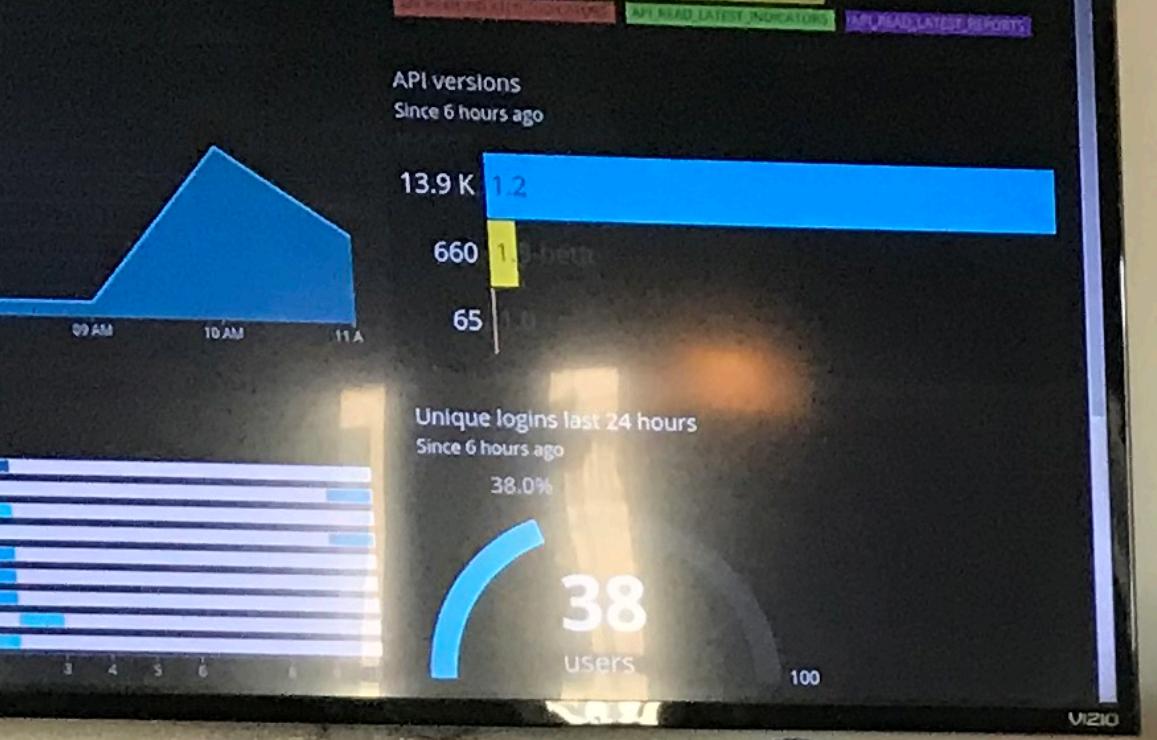
0. Responsibility: Security is Literally Your Job

After giving it a lot of thought, we realized that the most efficient way to ensure that security is built into our products and services is to make building security in a core part of every employee's job. That's not a generic, wishy-washy phrase ala "if you see something, say something". When we say that security is everyone's job, we mean that both specifically and literally.

Everyone's job description includes the phrase "...and its security".

This applies to everyone: If you're a web developer, then you're responsible for writing code...and its security. If you're the CEO, then your job is to oversee the operation of the company...and its security. If you're a part of the sales team with access to our social media accounts,

- [Introduction](#)
- [0. Responsibility: Security is Literally Your Job](#)
- [1. Assets: If it's Used, it's Tracked.](#)
 - [1.1 Hardware Inventory](#)
 - [1.2 Software Inventory](#)
 - [1.3 Account Inventory](#)
 - [1.4 Client Information Inventory](#)
 - [1.5 External Services Inventory](#)
 - [1.6 Subcontractor Inventory](#)
- [2. Incident Response: Over-Share, Overreact](#)
 - [2.1 Spotting Vulnerabilities and Potential Attacks](#)
 - [2.2 Reporting Incidents](#)
 - [2.3 Tracking Incidents](#)
 - [2.4 Customer Notification](#)
 - [2.5 Incident Response & Recovery](#)
 - [2.5.1 Employee Computers](#)
 - [2.5.2 Application Servers](#)
 - [2.5.3 External Services](#)
 - [2.6 Debriefing & Applying Lessons Learned](#)
- [3. Physical Security: Locked By Default](#)
- [4. Communications Security: Encrypted By Default](#)
- [5. System Security: Starts Locked Down, Stays Locked Down.](#)
 - [5.1 Employee Computers](#)
 - [5.2 Company Mobile Phones](#)
 - [5.3 Application Servers](#)
 - [5.4 External Services](#)
- [6. Network Access: Nothing Moves Without Permission.](#)
- [7. Data Access: Need to Know](#)
- [8. Backup and Recovery: We Never Lose Data.](#)
- [9. Account Management: Minimum Privileges, Maximum Control](#)
- [10. Software Development & Deployment: Bugs Get Squished](#)
- [11. Periodic Review & Update: There will be a test.](#)
 - [11.1 Ongoing Checks](#)
 - [11.2 Quarterly Checks](#)
 - [11.3 Biannual Checks](#)
 - [11.4 Yearly Checks](#)
- [12. Congratulations!](#)



Auditor

WOTD

Compliance

Formidad (es)

Mal (Mal)

Paran

Mar

Phone to address

↓



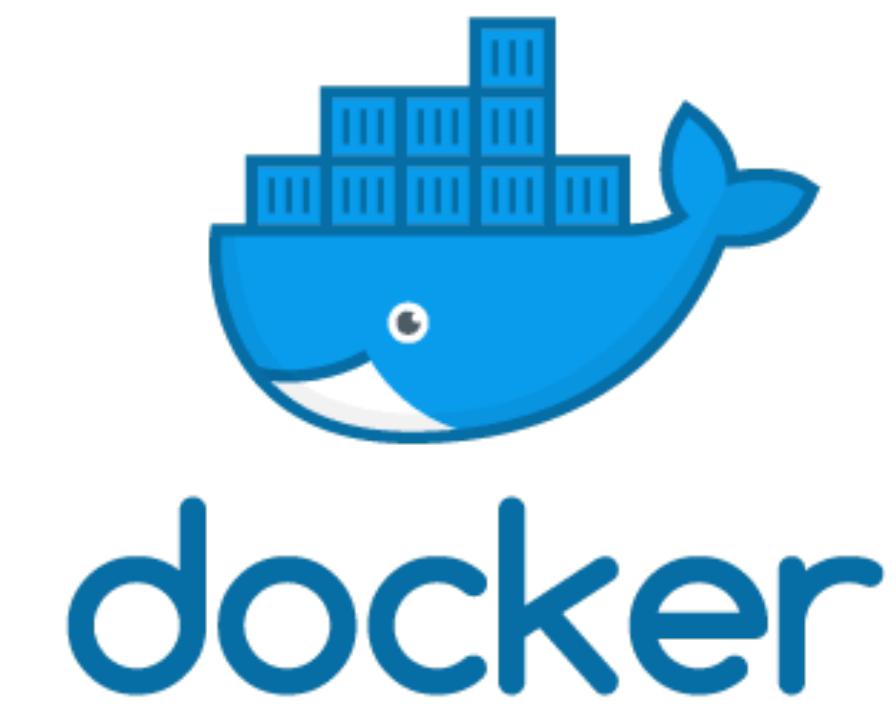


5 people



honeycomb

20 people



+500 people

Bootstrap Your Startup's Security

Patrick Coughlin - patrick@trustar.co

George Chamales - george@criticalsec.com

Add security to everyone's job.

Make security enhance operations.

Use security as a competitive advantage.

bootstrappingsecurity.com

Incident Response

Incident Response / IR-1

Incident Response [Template]

[Edit](#) [Comment](#) [Assign](#) [Start Progress](#) [Done](#) [Admin](#) ▾

Type: Task Status: [TO DO](#) (View workflow)
Priority: Medium Resolution: Unresolved
Labels: None

Description
Template of sub-tasks for responding to an incident.
Each subtask is related to entries in our process for dealing with incidents. When leading an IR activity you can delete / add sub-tasks as necessary.

Attachments
[Drop files to attach, or browse.](#)

Issue links
is cloned by [IR-18 Station Unable to connect to production DB](#) [IN PROG...](#)

Sub-tasks Progress + ...

1. [\[IR-#\] Incident Reported](#) [TO DO](#) Unassigned
2. [\[IR-#\] Response Process Startup](#) [TO DO](#) Unassigned
3. [\[IR-#\] Initial Customer Notification](#) [TO DO](#) Unassigned
4. [\[IR-#\] Lock-Down](#) [TO DO](#) Unassigned
5. [\[IR-#\] Find & Fix](#) [TO DO](#) Unassigned
6. [\[IR-#\] Customer Update](#) [TO DO](#) Unassigned
7. [\[IR-#\] Recovery & Debrief](#) [TO DO](#) Unassigned

Activity

All [Comments](#) History Activity

Tickets

Search [Save as](#) [Import](#) [Export](#) [Help](#) [Basic](#) [Advanced](#)

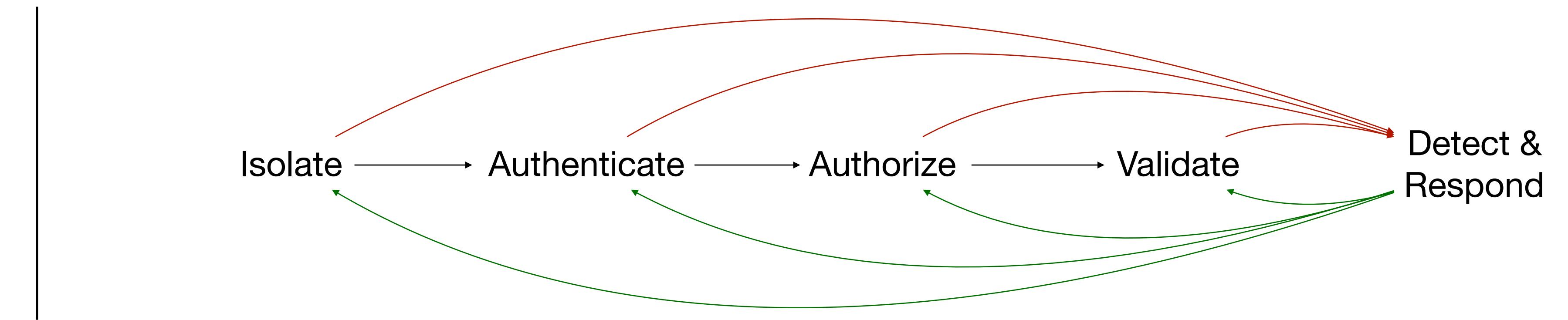
text ~ "TSR-"

151-188 of 188 [View](#)

Columns ▾

T	Key	Summary	Assignee	Reporter	P	Status	Resolution	Created	Updated	Due
EN-37	EN-3 / TSR-DBS-DE-2-RDS: Example alerts that are generated to alert database level administrators of suspicious activity at the database level (if separate from IDS)	Daniel Solmirano	Daniel Solmirano	↑ DONE	Done	11/Dec/17	05/Feb/18			...
EN-36	EN-13 / TSR-APP-AN-1-BE: Application User Listing	Serge Kurenkov	Serge Kurenkov	↑ DONE	Done	11/Dec/17	26/Jan/18			
EN-35	EN-14 / TSR-DBS-AZ-1-Neo4j: Database directory permissions showing access rights associated with each group/role	Unassigned	Manas Choksi	↑ DONE	Done	11/Dec/17	05/Feb/18			
EN-34	EN-3 / TSR-DBS-DE-1-RDS: Example database log extract	Steven Chamales	Daniel Solmirano	↑ DONE	Done	11/Dec/17	26/Jan/18			
EN-33	EN-13 / TSR-APP-IS-3-BE: Fictitious data used in dev activities	Daniel Solmirano	Serge Kurenkov	↑ DONE	Done	11/Dec/17	26/Jan/18			
EN-32	EN-3 / TSR-DBS-VA-2-RDS: Most recent database access log review	Steven Chamales	Daniel Solmirano	↑ DONE	Done	11/Dec/17	05/Feb/18			
EN-31	EN-13 / TSR-APP-IS-2-BE: Encryption policies and procedures with revision history	Serge Kurenkov	Serge Kurenkov	↑ DONE	Unresolved	11/Dec/17	26/Jan/18			
EN-30	EN-14 / TSR-DBS-AN-3-Neo4j: Database authentication configurations	Daniel Solmirano	Manas Choksi	↑ DONE	Done	11/Dec/17	05/Feb/18			
EN-29	EN-14 / TSR-DBS-AN-2-Neo4j: Database administrators/super user listing	Steven Chamales	Manas Choksi	↑ DONE	Done	11/Dec/17	05/Feb/18			
EN-28	EN-3 / TSR-DBS-VA-1-RDS: Most recent database user access review	Steven Chamales	Daniel Solmirano	↑ DONE	Done	11/Dec/17	31/Jan/18			
EN-27	EN-14 / TSR-DBS-AN-1-Neo4j: Database user listing	Steven Chamales	Manas Choksi	↑ DONE	Done	11/Dec/17	05/Feb/18			
EN-26	EN-13 / TSR-APP-IS-1-BE: Encryption methods and configurations for data in transit	Serge Kurenkov	Serge Kurenkov	↑ DONE	Done	11/Dec/17	26/Jan/18			
EN-25	EN-3 / TSR-DBS-AZ-1-RDS: Database directory permissions showing access rights associated with each group/role	Daniel Solmirano	Daniel Solmirano	↑ DONE	Done	11/Dec/17	11/Dec/17			
EN-24	EN-14 / TSR-DBS-IS-3-Neo4j: Encryption methods and configurations for data at rest	Steven Chamales	Manas Choksi	↑ DONE	Done	11/Dec/17	05/Feb/18			
EN-23	EN-13 / TSR-APP-LOG-1-BE: Application audit logging configurations	Serge Kurenkov	Serge Kurenkov	↑ DONE	Unresolved	11/Dec/17	26/Jan/18			
EN-22	EN-3 / TSR-DBS-AN-3-RDS: Database authentication configurations	Daniel Solmirano	Daniel Solmirano	↑ DONE	Done	11/Dec/17	11/Dec/17			

Service Security



Service Security

Elasticsearch (ES) Database Technology



Manas Choksi

Last modified Jan 22, 2018 by Daniel Solmirano

Technology Overview	
Environment	Production
Review Period	3 Months
Review Ticket	<input checked="" type="checkbox"/> EN-58 - TSR-DBS ES Compliance Tasks DONE

TABLE OF CONTENTS

- 1.0 Management
 - 1.2 Description
 - 1.3 Logging
 - 1.3.1 Logging System
 - 1.3.2 Log Directories & Files
- 1.4 Backup, Verification & Restore
 - 1.4.1 Backup Process
 - 1.4.2 Backup Verification
 - 1.4.3 Restore Process
- 1.5 Update Process
- 1.6 Vulnerability Notifications
- 1.7 Periodic Review & Approval
- 2.0 Security Controls
- 2.1 Isolate
 - 2.1.1 Firewall Rules
- 2.2 Authenticate
 - 2.2.1 Secrets Management
 - 2.2.2 Adding Users
 - 2.2.3 Modifying Users
 - 2.2.4 Removing Users
- 2.3 Authorize
 - 2.3.2 Adding Groups
 - 2.3.3 Modifying Groups
 - 2.3.4 Removing Groups
- 2.4 Validate
- 2.5 Detect
 - 2.5.1 Indicators of Compromise
 - 2.5.2 Common Signals
- 2.6 Respond
- 3.0 Future Updates

1.0 Management

1.2 Description

Elasticsearch is a highly scalable open-source full-text search and analytics engine. It allows you to store, search, and analyze big volumes of data quickly and in near real time. It is generally used as the underlying engine/technology that powers applications that have complex search features and requirements.

TruSTAR uses Elasticsearch as a data repository to enable full text search on their incident reports.

The production Elasticsearch cluster is made up of the following hosts:

- Master node (es-master)
- Data node 1 (es-01)
- Data node 2 (es-02)

1.3 Logging

1.3.1 Logging System

Elasticsearch logs different system actions to `$ES_HOME/logs` directory, then logs are forwarded to splunk.

1.3.2 Log Directories & Files

Log Path	Contents
<code>\$ES_HOME/logs/elasticsearch-prod.log</code>	logging queries with errors
<code>\$ES_HOME/logs/elasticsearch-prod_index_search_slowlog.log</code>	logging slow queries
<code>\$ES_HOME/logs/elasticsearch-prod_access.log</code>	Access log