Bootstrap Your Startup's Security

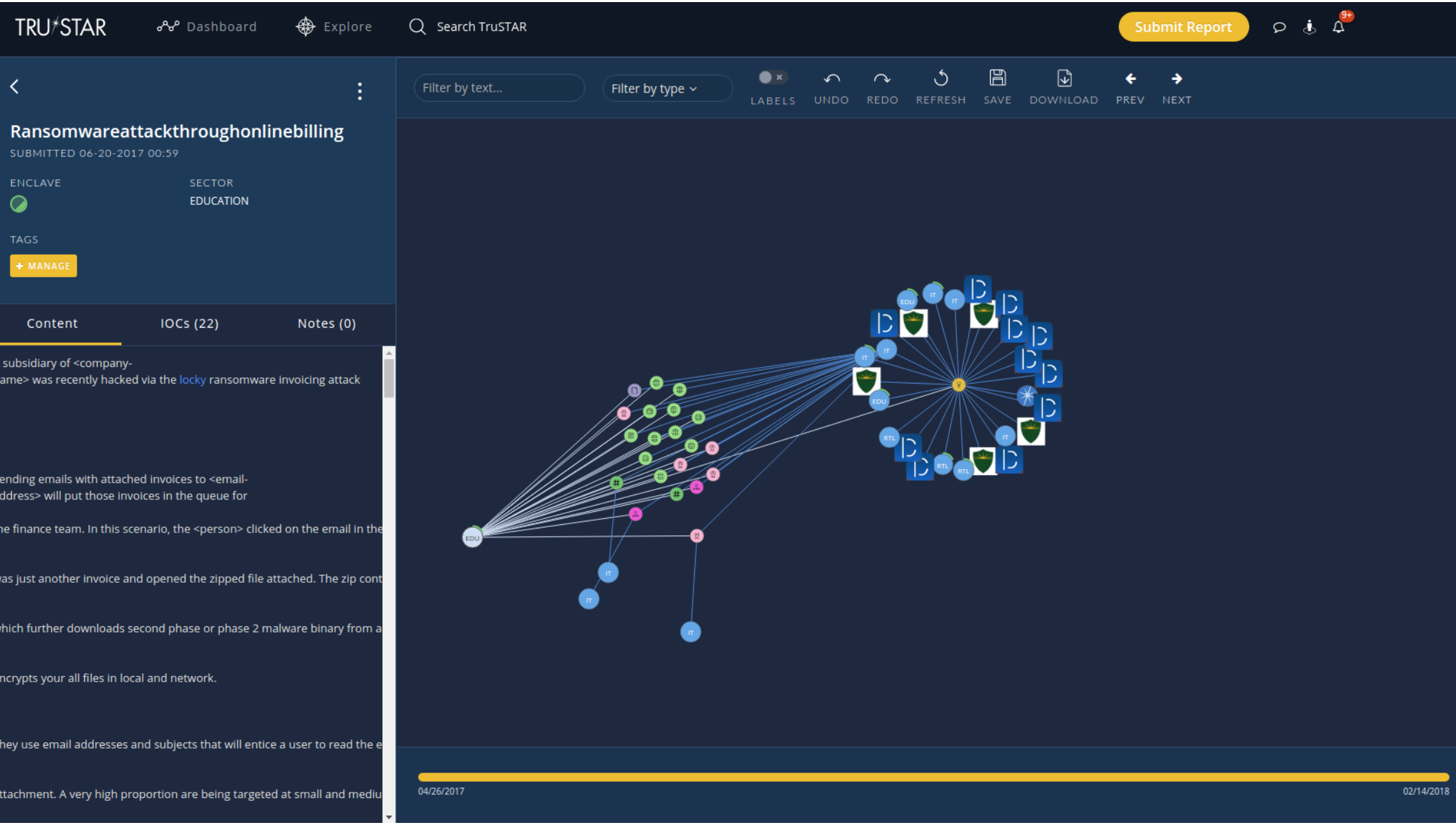
Patrick Coughlin - patrick@trustar.co
George Chamales - george@criticalsec.com

Add security to everyone's job.

Make security enhance operations.

Use security as a competitive advantage.

30 min presentation + 30 min discussion


TRUSTAR
Dashboard
Explore
Search TruSTAR
Submit Report
Ransomwareattackthroughonlinebilling
SUBMITTED 06-20-2017 00:59
ENCLAVE
SECTOR
EDUCATION
TAGS
+ MANAGE
Content
IOCs (22)
Notes (0)
subsidiary of <company-
ame> was recently hacked via the locky ransomware invoicing attack
ending emails with attached invoices to <email-
ddress> will put those invoices in the queue for
he finance team. In this scenario, the <person> clicked on the email in the
as just another invoice and opened the zipped file attached. The zip cont
hich further downloads second phase or phase 2 malware binary from a
ncrypts your all files in local and network.
hey use email addresses and subjects that will entice a user to read the e
ttachment. A very high proportion are being targeted at small and mediu
Filter by text...
Filter by type
LABELS
UNDO
REDO
REFRESH
SAVE
DOWNLOAD
PREV
NEXT
04/26/2017
02/14/2018

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 date 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 steramline 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**.

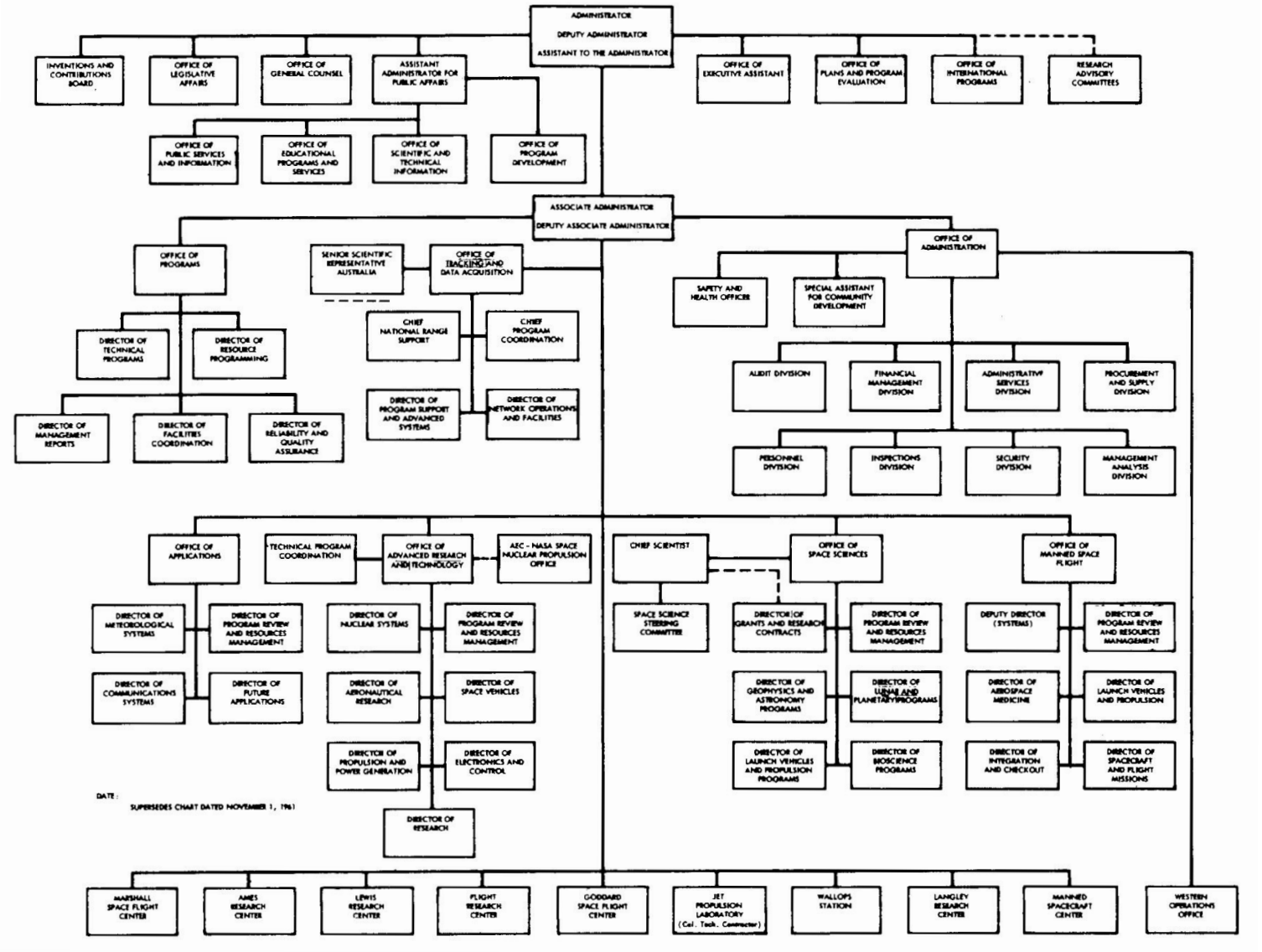
Junior Data Science

- 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**.

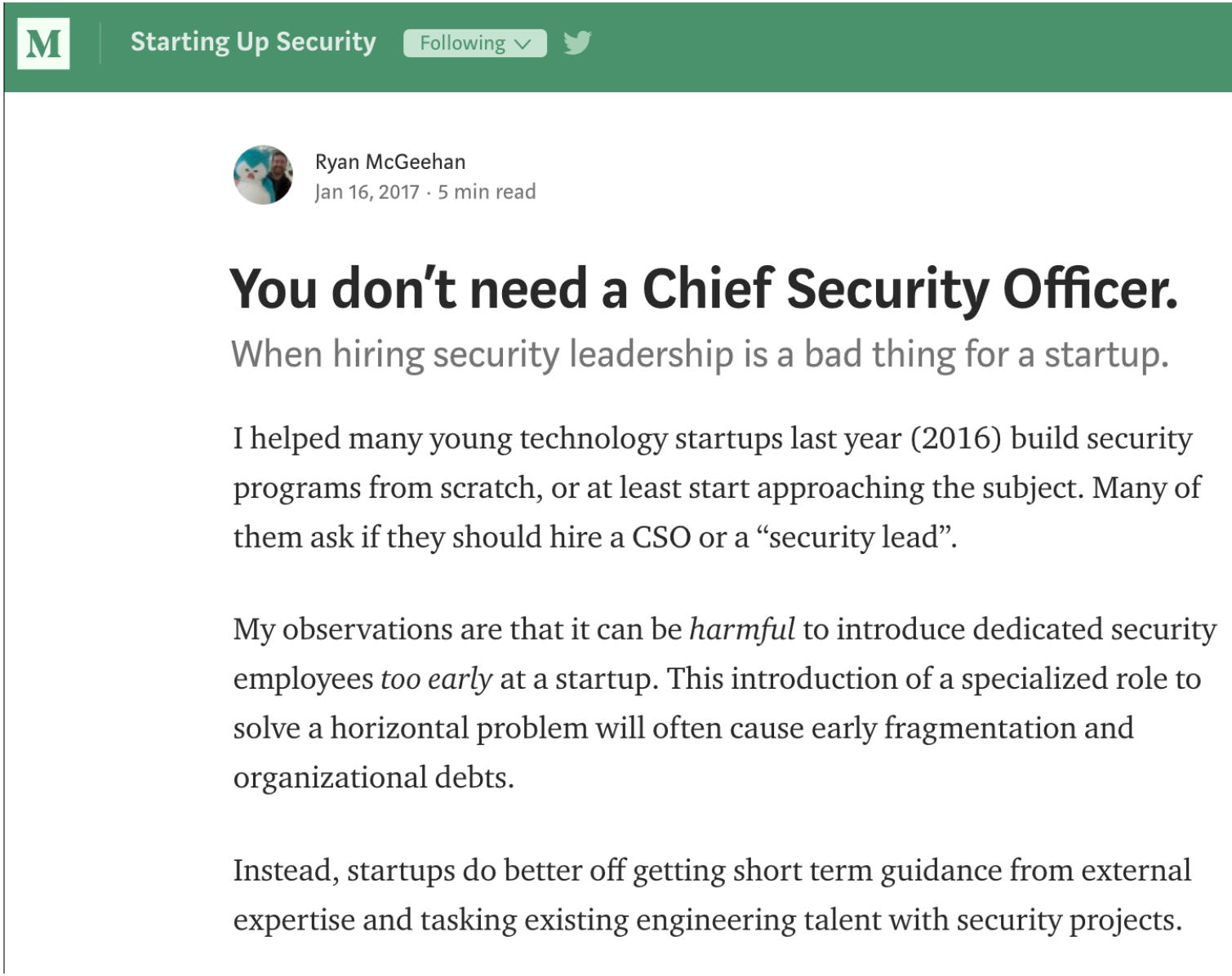
Subsidiarity

Delegate decision making authority to the smallest competent group.

Webserver Vulnerability → Missed Announcement → Compromised Database → 145 Million Customers


ADMINISTRATOR
DEPUTY ADMINISTRATOR
ASSISTANT TO THE ADMINISTRATOR
INVENTIONS AND CONTRIBUTIONS BOARD
OFFICE OF LEGISLATIVE AFFAIRS
OFFICE OF GENERAL COUNSEL
ASSISTANT ADMINISTRATOR FOR PUBLIC AFFAIRS
OFFICE OF EXECUTIVE ASSISTANT
OFFICE OF PLANS AND PROGRAM EVALUATION
OFFICE OF INTERNATIONAL PROGRAMS
RESEARCH ADVISORY COMMITTEES
OFFICE OF PUBLIC SERVICES AND INFORMATION
OFFICE OF EDUCATIONAL PROGRAMS AND SERVICES
OFFICE OF SCIENTIFIC AND TECHNICAL INFORMATION
OFFICE OF PROGRAM DEVELOPMENT
ASSOCIATE ADMINISTRATOR
DEPUTY ASSOCIATE ADMINISTRATOR
OFFICE OF PROGRAMS
SENIOR SCIENTIFIC REPRESENTATIVE AUSTRALIA
OFFICE OF TRACKING AND DATA ACQUISITION
OFFICE OF ADMINISTRATION
SAFETY AND HEALTH OFFICER
SPECIAL ASSISTANT FOR COMMUNITY DEVELOPMENT
DIRECTOR OF TECHNICAL PROGRAMS
DIRECTOR OF RESOURCE PROGRAMMING
CHIEF NATIONAL RANGE SUPPORT
CHIEF PROGRAM COORDINATION
AUDIT DIVISION
FINANCIAL MANAGEMENT DIVISION
ADMINISTRATIVE SERVICES DIVISION
PROCUREMENT AND SUPPLY DIVISION
DIRECTOR OF MANAGEMENT REPORTS
DIRECTOR OF FACILITIES COORDINATION
DIRECTOR OF RELIABILITY AND QUALITY ASSURANCE
DIRECTOR OF PROGRAM SUPPORT AND ADVANCED SYSTEMS
DIRECTOR OF NETWORK OPERATIONS AND FACILITIES
PERSONNEL DIVISION
INSPECTIONS DIVISION
SECURITY DIVISION
MANAGEMENT ANALYSIS DIVISION
OFFICE OF APPLICATIONS
TECHNICAL PROGRAM COORDINATION
OFFICE OF ADVANCED RESEARCH AND TECHNOLOGY
AEC - NASA SPACE NUCLEAR PROPULSION OFFICE
CHIEF SCIENTIST
OFFICE OF SPACE SCIENCES
OFFICE OF MANNED SPACE FLIGHT
DIRECTOR OF METEOROLOGICAL SYSTEMS
DIRECTOR OF PROGRAM REVIEW AND RESOURCES MANAGEMENT
DIRECTOR OF NUCLEAR SYSTEMS
DIRECTOR OF PROGRAM REVIEW AND RESOURCES MANAGEMENT
SPACE SCIENCE STEERING COMMITTEE
DIRECTOR OF GRANTS AND RESEARCH CONTRACTS
DIRECTOR OF PROGRAM REVIEW AND RESOURCES MANAGEMENT
DEPUTY DIRECTOR (SYSTEMS)
DIRECTOR OF PROGRAM REVIEW AND RESOURCES MANAGEMENT
DIRECTOR OF COMMUNICATIONS SYSTEMS
DIRECTOR OF FUTURE APPLICATIONS
DIRECTOR OF AERONAUTICAL RESEARCH
DIRECTOR OF SPACE VEHICLES
DIRECTOR OF GEOPHYSICS AND ASTRONOMY PROGRAMS
DIRECTOR OF LUNAR AND PLANETARY PROGRAMS
DIRECTOR OF AEROSPACE MEDICINE
DIRECTOR OF LAUNCH VEHICLES AND PROPULSION
DIRECTOR OF PROPULSION AND POWER GENERATION
DIRECTOR OF ELECTRONICS AND CONTROL
DIRECTOR OF LAUNCH VEHICLES AND PROPULSION PROGRAMS
DIRECTOR OF BIOSCIENCE PROGRAMS
DIRECTOR OF INTEGRATION AND CHECKOUT
DIRECTOR OF SPACECRAFT AND FLIGHT MISSIONS
DIRECTOR OF RESEARCH
DATE :
SUPERSEDES CHART DATED NOVEMBER 1, 1961
MARSHALL SPACE FLIGHT CENTER
AMES RESEARCH CENTER
LEWIS RESEARCH CENTER
FLIGHT RESEARCH CENTER
GODDARD SPACE FLIGHT CENTER
JET PROPULSION LABORATORY
(Cal. Tech. Contractor)
WALLOPS STATION
LANGLEY RESEARCH CENTER
MANNED SPACECRAFT CENTER
WESTERN OPERATIONS OFFICE

This guy bootstrapped Facebook's security.



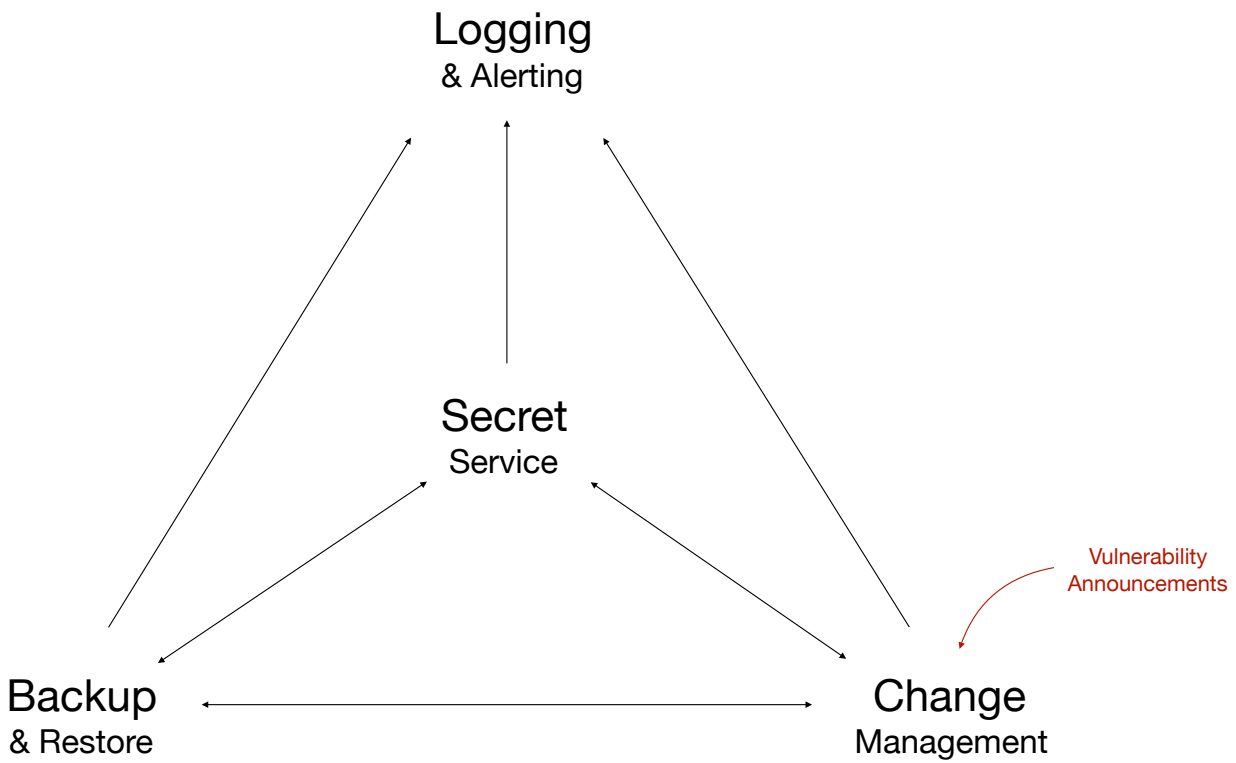
Make security enhance operations.

Principles

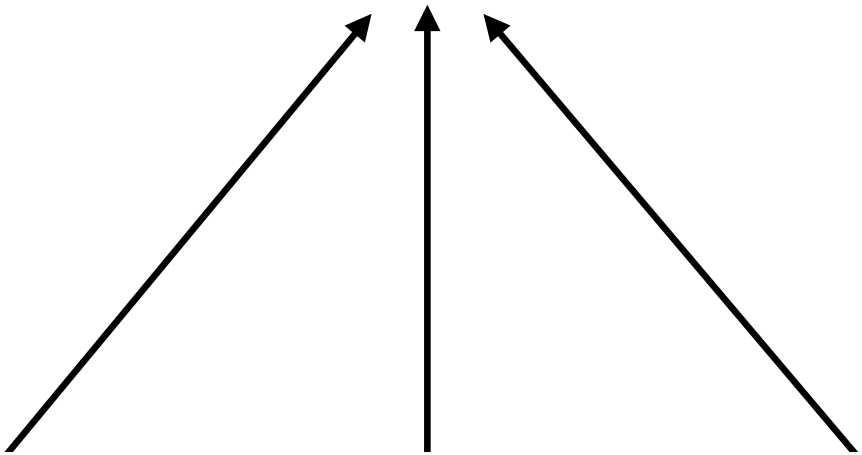
Simplify: Less is more.

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

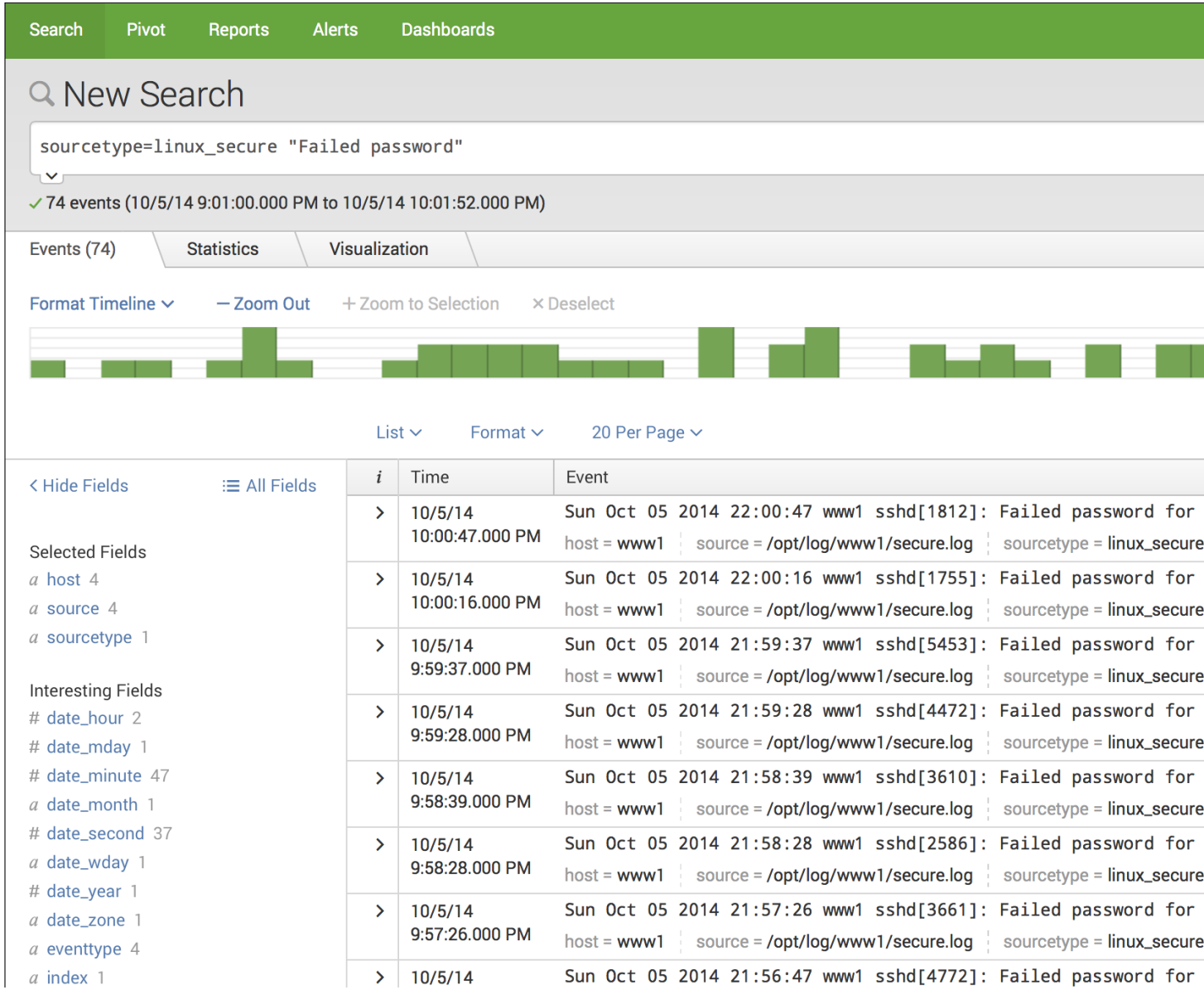
Infrastructure Services

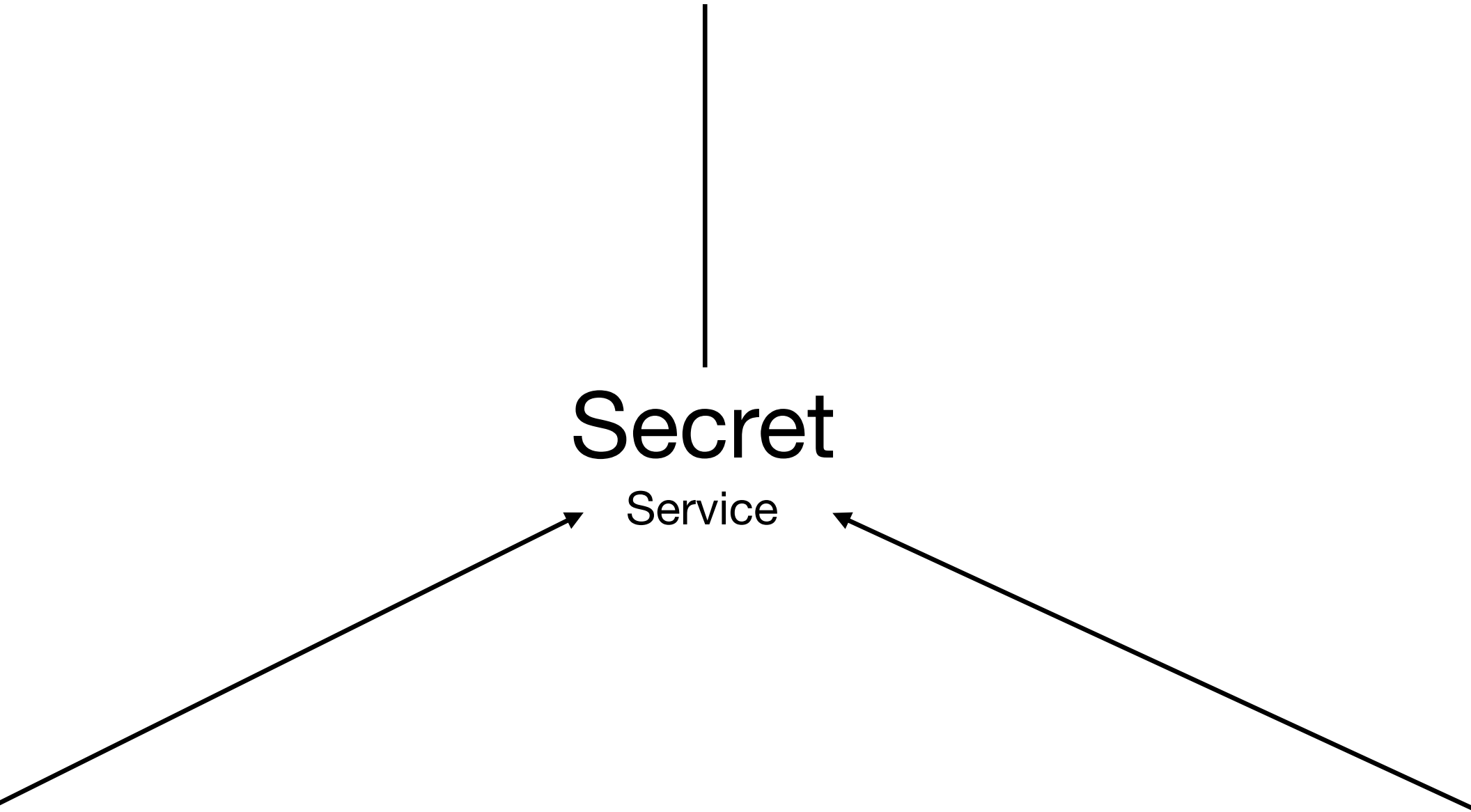


Logging
& Alerting



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



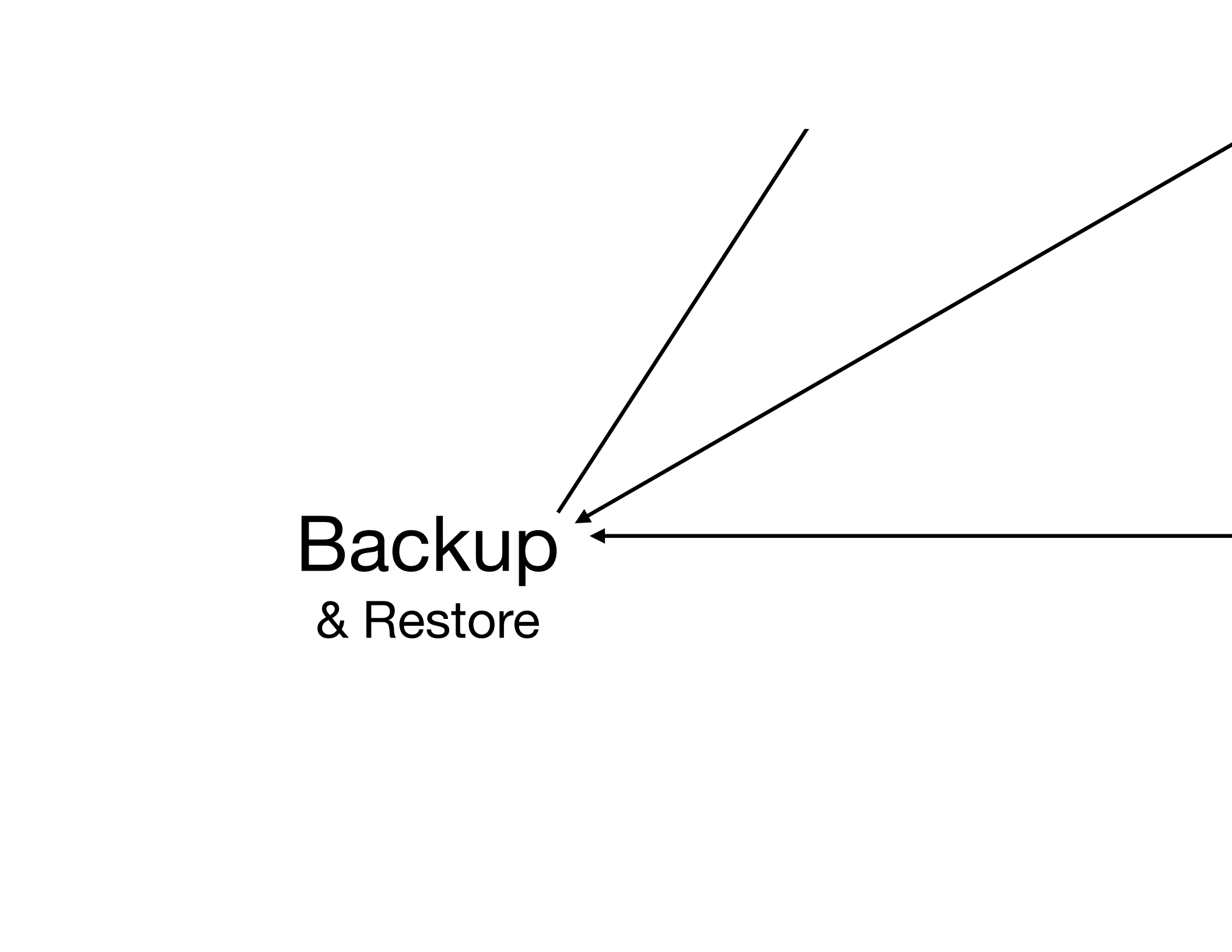

Secret
Service

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

Lucas Matney Mar 7, 2018

> ***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

verizon

6 million customers

accenture

Security keys & software

FedEx

112,000 files

OCTOLY

12,000 social media influencers

DEEP ROOT

198 million voters

3 million fans

TigerSwan

9,400 resumes

alteryx

123 million housholds

phm PATIENT HOME MONITORING

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

150,000 patients

UpGuard

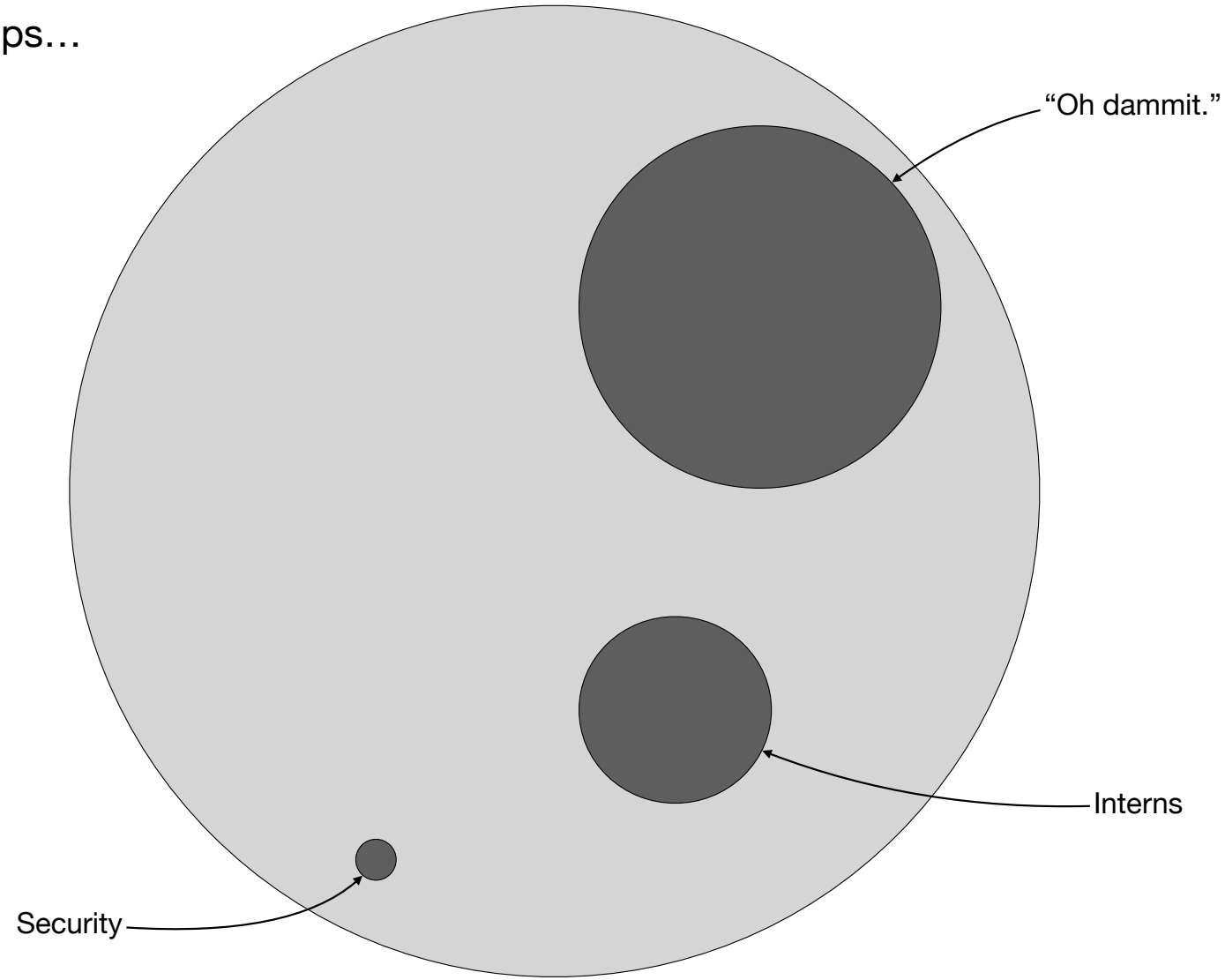
KROMTECH

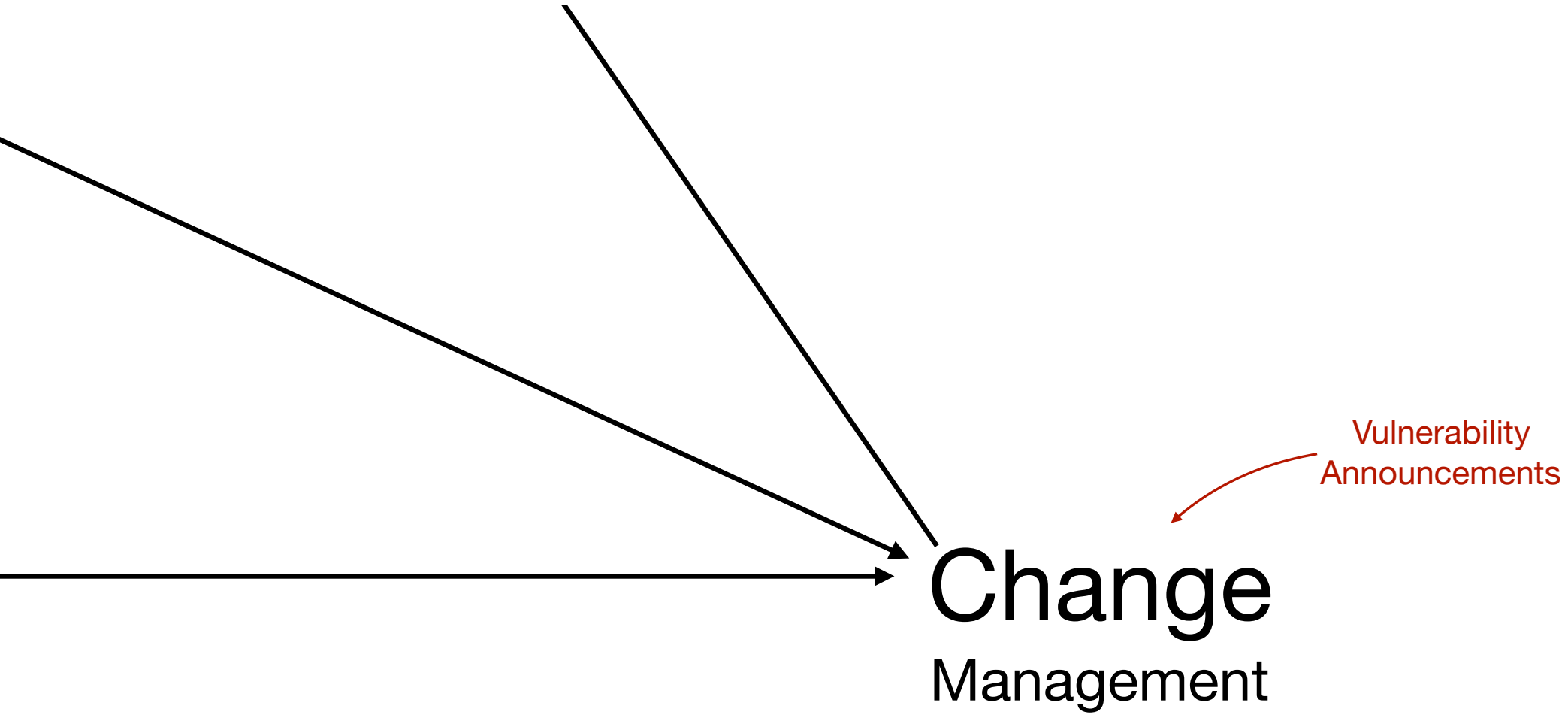
Verizon - https://www.upguard.com/breaches/verizon-cloud-leak
Octoly - https://www.upguard.com/breaches/cloud-leak-octoly
TigerSwan - https://www.upguard.com/breaches/cloud-leak-tigerswan

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

Reasons for backups…




Vulnerability
Announcements
Change
Management

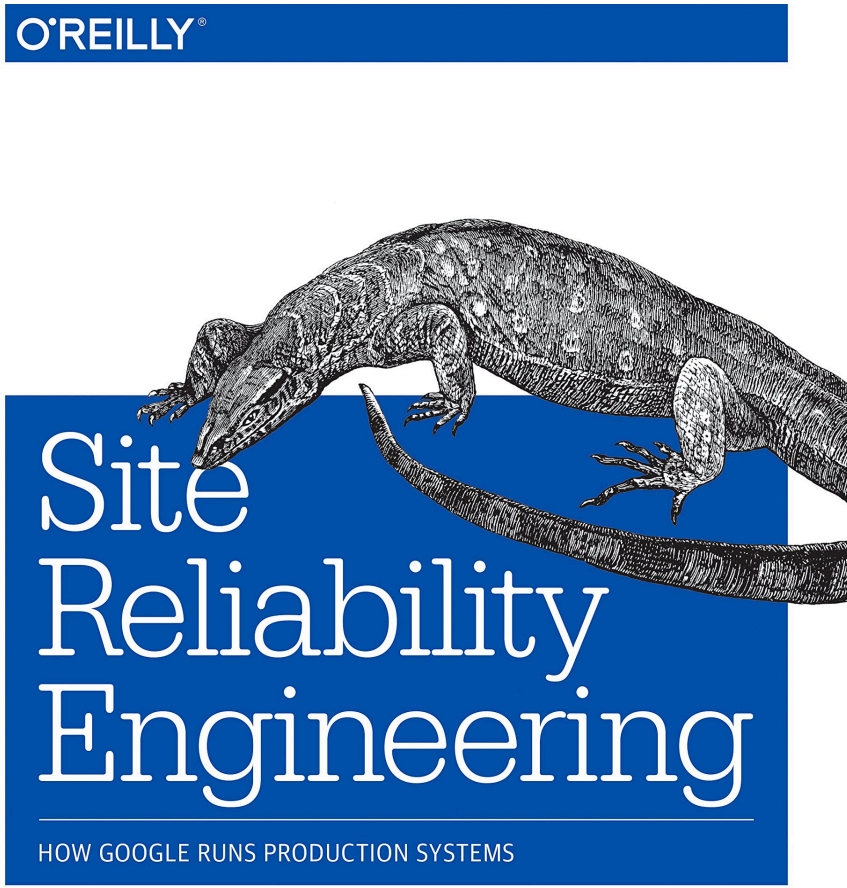
TESLA

Identified Cloud Console → Accessed Cloud Credentials → Collected Data → Found Cryptominers

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

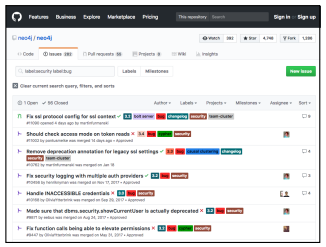
Benjamin Treynor Sloss
Vice President, Google Engineering, founder of Google SRE

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



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

Bugs & Release Notes



Injested by

CVE Details

National Vulnerability DB

Injested by

zapier

Creates Ticket

Assigned to

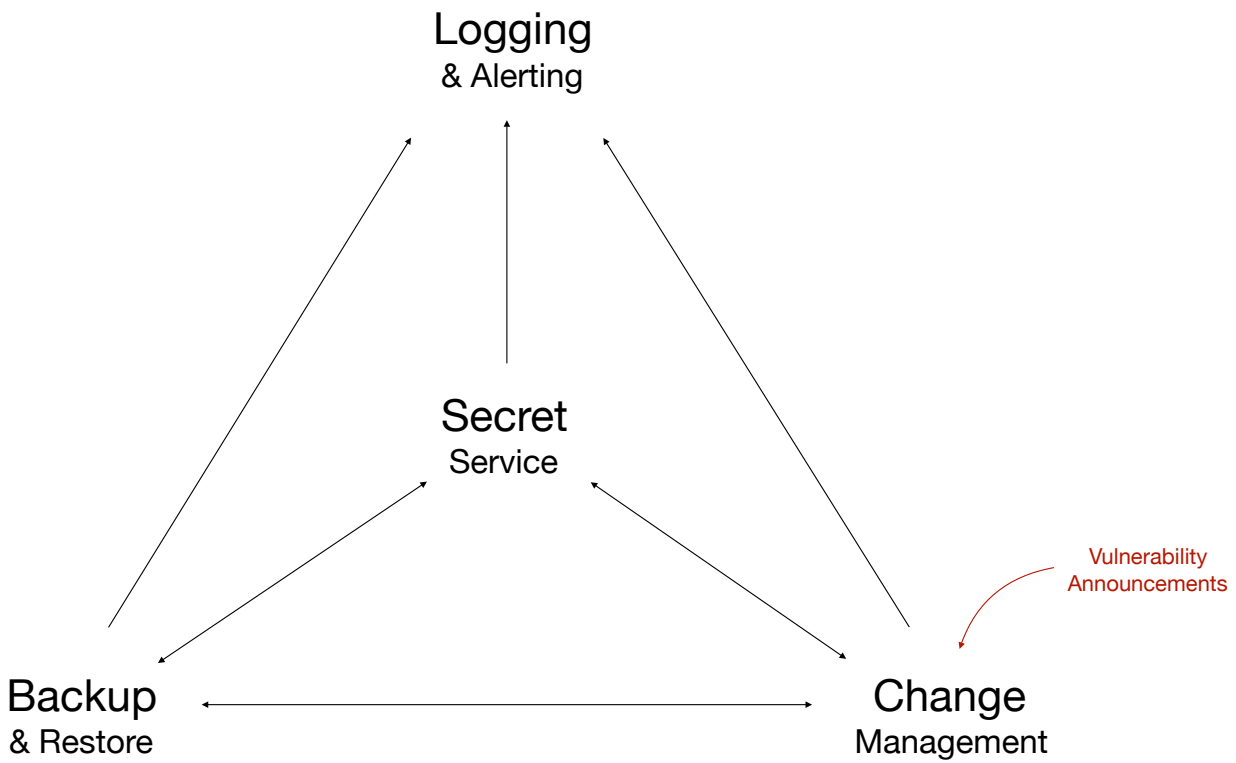
This guy.

Injested by

Mailing Lists

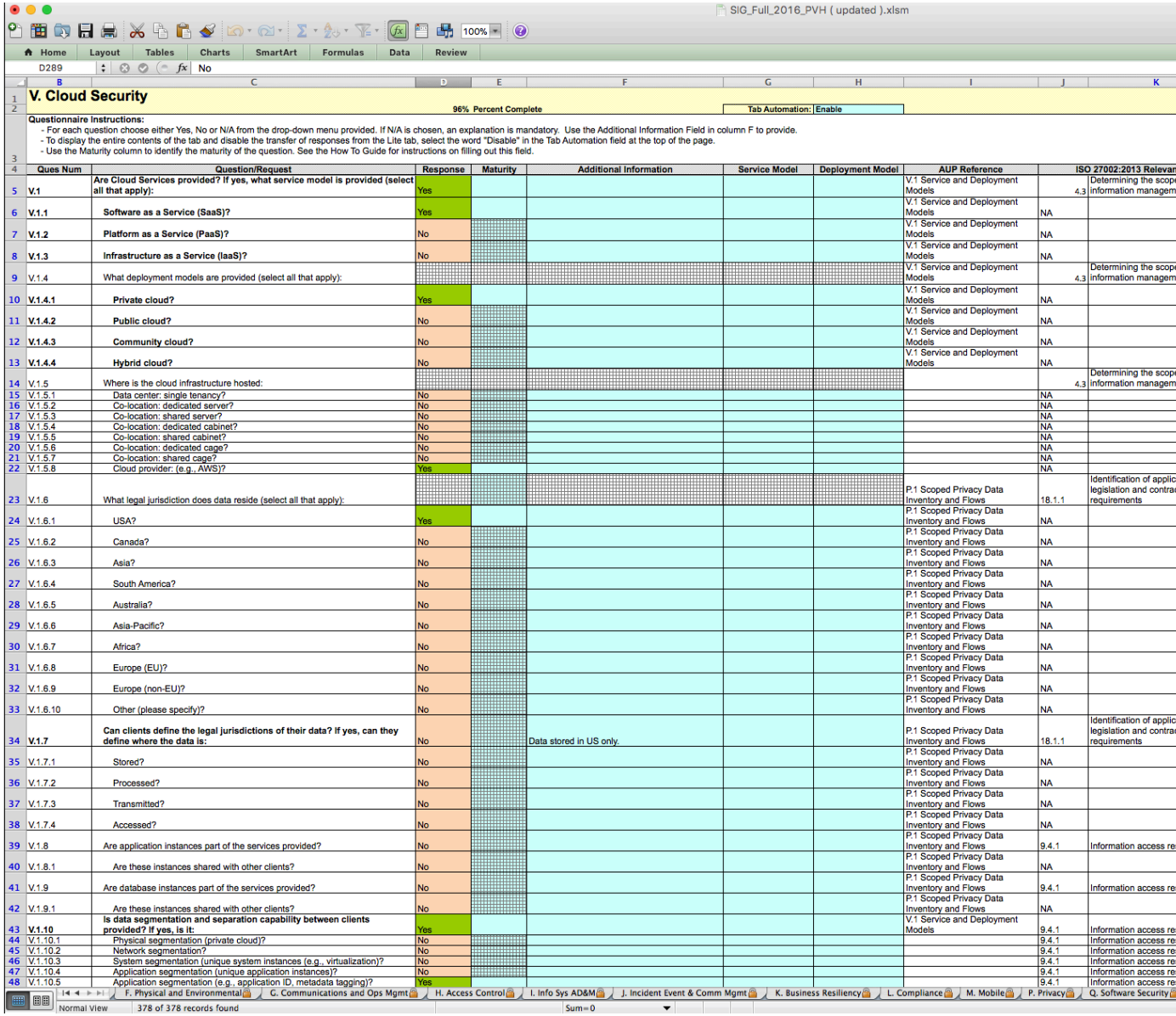
Vulnerability Alert Pipeline

Infrastructure Services = Stability



Use security as a competitive advantage.

Customer.
Security.
Requirements.



SIG_Full_2016_PVH (updated).xlsm

Home | Layout | Tables | Charts | SmartArt | Formulas | Data | Review

D289: No

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 Relevan
V.1	**Are Cloud Services provided? If yes, what service model is provided (select all that apply):**	Yes					V.1 Service and Deployment Models	4.3	Determining the scop information managem
V.1.1	**Software as a Service (SaaS)?**	Yes					V.1 Service and Deployment Models	NA	
V.1.2	**Platform as a Service (PaaS)?**	No					V.1 Service and Deployment Models	NA	
V.1.3	**Infrastructure as a Service (IaaS)?**	No					V.1 Service and Deployment Models	NA	
V.1.4	What deployment models are provided (select all that apply):						V.1 Service and Deployment Models	4.3	Determining the scop information managem
V.1.4.1	**Private cloud?**	Yes					V.1 Service and Deployment Models	NA	
V.1.4.2	**Public cloud?**	No					V.1 Service and Deployment Models	NA	
V.1.4.3	**Community cloud?**	No					V.1 Service and Deployment Models	NA	
V.1.4.4	**Hybrid cloud?**	No					V.1 Service and Deployment Models	NA	
V.1.5	Where is the cloud infrastructure hosted:							4.3	Determining the scop information managem
V.1.5.1	Data center: single tenancy?	No						NA	
V.1.5.2	Co-location: dedicated server?	No						NA	
V.1.5.3	Co-location: shared server?	No						NA	
V.1.5.4	Co-location: dedicated cabinet?	No						NA	
V.1.5.5	Co-location: shared cabinet?	No						NA	
V.1.5.6	Co-location: dedicated cage?	No						NA	
V.1.5.7	Co-location: shared cage?	No						NA	
V.1.5.8	Cloud provider: (e.g., AWS)?	Yes						NA	
V.1.6	What legal jurisdiction does data reside (select all that apply):						P.1 Scoped Privacy Data Inventory and Flows	18.1.1	Identification of applic legislation and contra requirements
V.1.6.1	USA?	Yes					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.6.2	Canada?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.6.3	Asia?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.6.4	South America?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.6.5	Australia?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.6.6	Asia-Pacific?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.6.7	Africa?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.6.8	Europe (EU)?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.6.9	Europe (non-EU)?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.6.10	Other (please specify)?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
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	18.1.1	Identification of applic legislation and contra requirements
V.1.7.1	Stored?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.7.2	Processed?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.7.3	Transmitted?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.7.4	Accessed?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.8	Are application instances part of the services provided?	No					P.1 Scoped Privacy Data Inventory and Flows	9.4.1	Information access re
V.1.8.1	Are these instances shared with other clients?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
V.1.9	Are database instances part of the services provided?	No					P.1 Scoped Privacy Data Inventory and Flows	9.4.1	Information access re
V.1.9.1	Are these instances shared with other clients?	No					P.1 Scoped Privacy Data Inventory and Flows	NA	
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	Information access re
V.1.10.1	Physical segmentation (private cloud)?	No						9.4.1	Information access re
V.1.10.2	Network segmentation?	No						9.4.1	Information access re
V.1.10.3	System segmentation (unique system instances (e.g., virtualization)?	No						9.4.1	Information access re
V.1.10.4	Application segmentation (unique application instances)?	No						9.4.1	Information access re
V.1.10.5	Application segmentation (e.g., application ID, metadata tagging)?	Yes						9.4.1	Information access re

F. Physical and Environmental | G. Communications and Ops Mgmt | H. Access Control | I. Info Sys AD&M | J. Incident Event & Comm Mgmt | K. Business Resiliency | L. Compliance | M. Mobile | P. Privacy | Q. Software Security

Normal View | 378 of 378 records found | Sum=0

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

croblee@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.

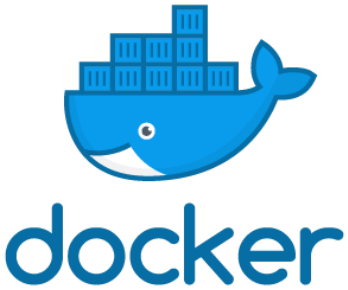
0. Responsibility: Security is Literally Your Job

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,


API versions
Since 6 hours ago
13.9 K
660
65
Unique logins last 24 hours
Since 6 hours ago
38.0%
38
users
100
Auditor
WOTD
Compliance



5 people

20 people

+250 people

Bootstrap Your Startup's Security

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

bootstrappingsecurity.com

Add security to everyone's job.

Make security enhance operations.

Use security as a competitive advantage.