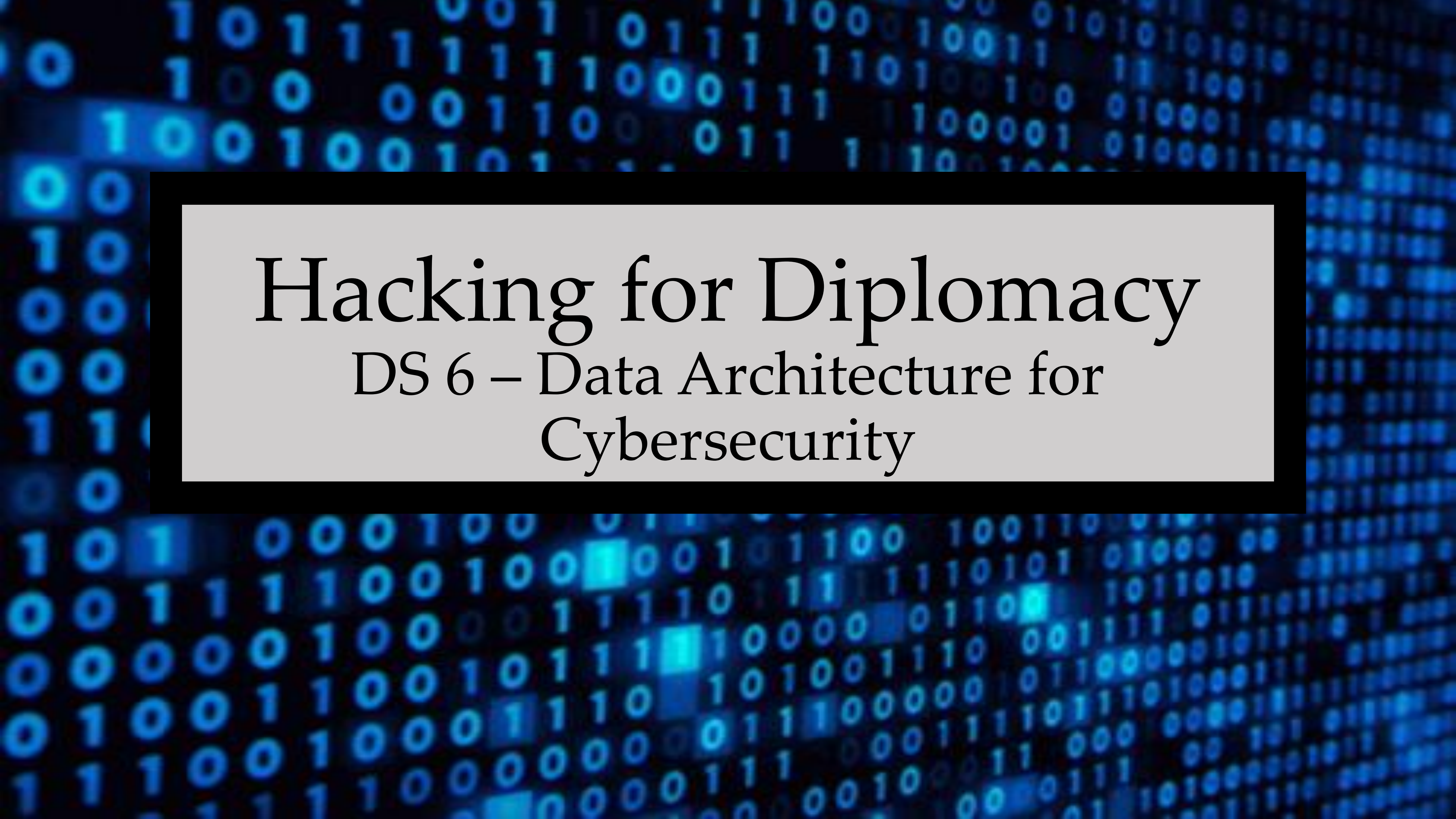


Hacking for Diplomacy

DS 6 – Data Architecture for Cybersecurity

Meet the Team

Jaime Campanelli, A.J. Musacchio, Jenelle Salazar, Randall Weber

E.D.A.C Consulting

Enhanced

Data

Architecture

for

Cybersecurity

Initial Problem Statement

Network defenders in the Office of Cyber Monitoring and Operations need a better way to query and correlate data in a hybrid and multi-cloud data ecosystem in order to develop analytics capability at the network defender level and inform insight-driven decisions on cybersecurity incident response at the senior leadership level.

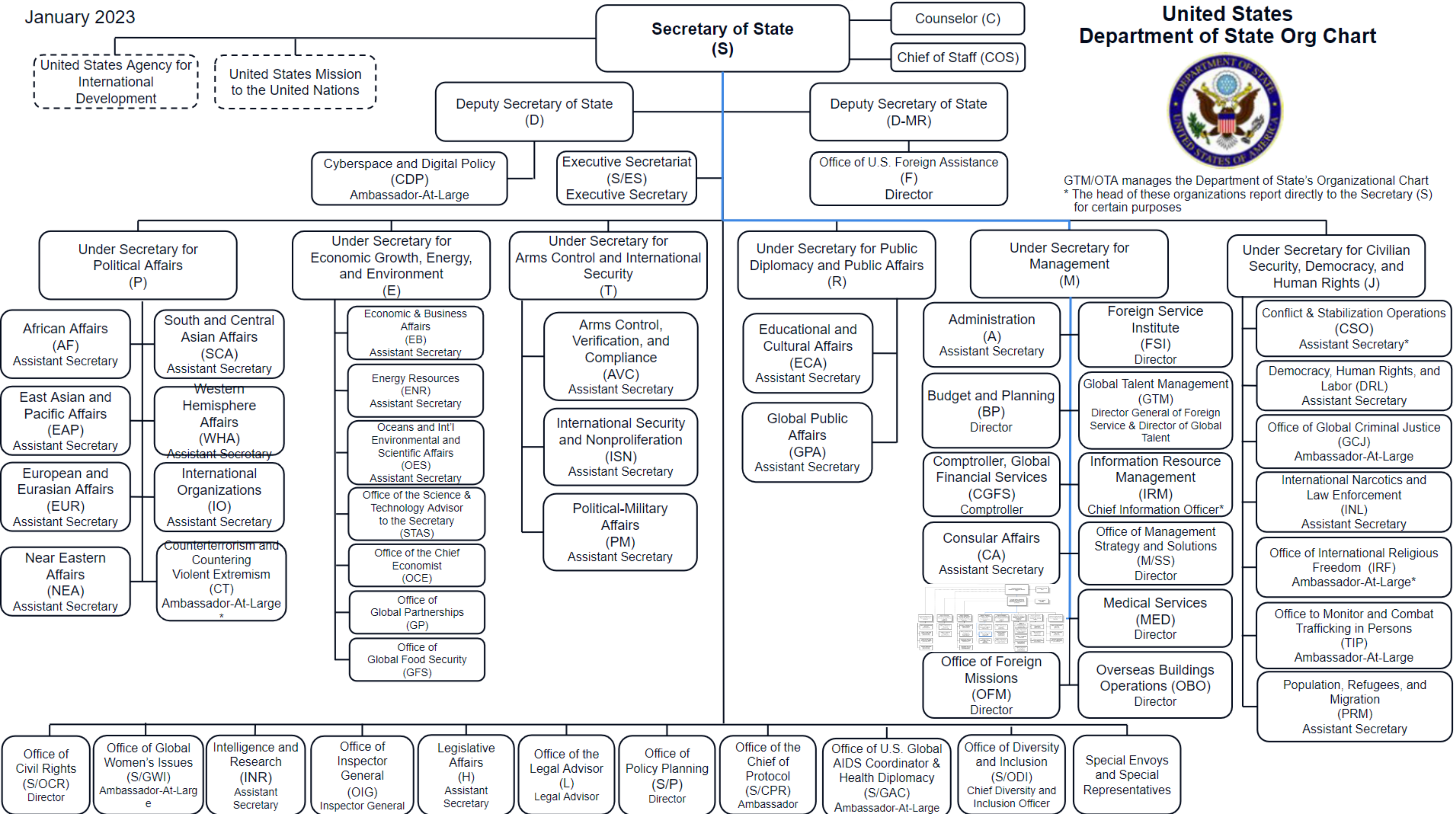
Revised Problem Statement

Network defenders in the Office of Cyber Monitoring and Operations need a better **agnostic way to collect, store, and analyze logs**. **This system will be used to inform cybersecurity related decisions** on the network defender and incident response level. **To pair with this, policy will be required to help Network Defenders implement new changes and become more aware.**

January 2023

United States Department of State Org Chart

GTM/OTA manages the Department of State's Organizational Chart
* The head of these organizations report directly to the Secretary (S) for certain purposes



Secretary of State (S)

- Counselor (C)
- Chief of Staff (COS)
- United States Agency for International Development
- United States Mission to the United Nations

Deputy Secretary of State (D)

- Cyberspace and Digital Policy (CDP) Ambassador-At-Large

Executive Secretariat (S/ES) Executive Secretary

Deputy Secretary of State (D-MR)

- Office of U.S. Foreign Assistance (F) Director

Under Secretary for Political Affairs (P)

- African Affairs (AF) Assistant Secretary
- East Asian and Pacific Affairs (EAP) Assistant Secretary
- European and Eurasian Affairs (EUR) Assistant Secretary
- Near Eastern Affairs (NEA) Assistant Secretary
- South and Central Asian Affairs (SCA) Assistant Secretary
- Western Hemisphere Affairs (WHA) Assistant Secretary
- International Organizations (IO) Assistant Secretary
- Counterterrorism and Countering Violent Extremism (CT) Ambassador-At-Large *

Under Secretary for Economic Growth, Energy, and Environment (E)

- Economic & Business Affairs (EB) Assistant Secretary
- Energy Resources (ENR) Assistant Secretary
- Oceans and Int'l Environmental and Scientific Affairs (OES) Assistant Secretary
- Office of the Science & Technology Advisor to the Secretary (STAS)
- Office of the Chief Economist (OCE)
- Office of Global Partnerships (GP)
- Office of Global Food Security (GFS)

Under Secretary for Arms Control and International Security (T)

- Arms Control, Verification, and Compliance (AVC) Assistant Secretary
- International Security and Nonproliferation (ISN) Assistant Secretary
- Political-Military Affairs (PM) Assistant Secretary

Under Secretary for Public Diplomacy and Public Affairs (R)

- Educational and Cultural Affairs (ECA) Assistant Secretary
- Global Public Affairs (GPA) Assistant Secretary

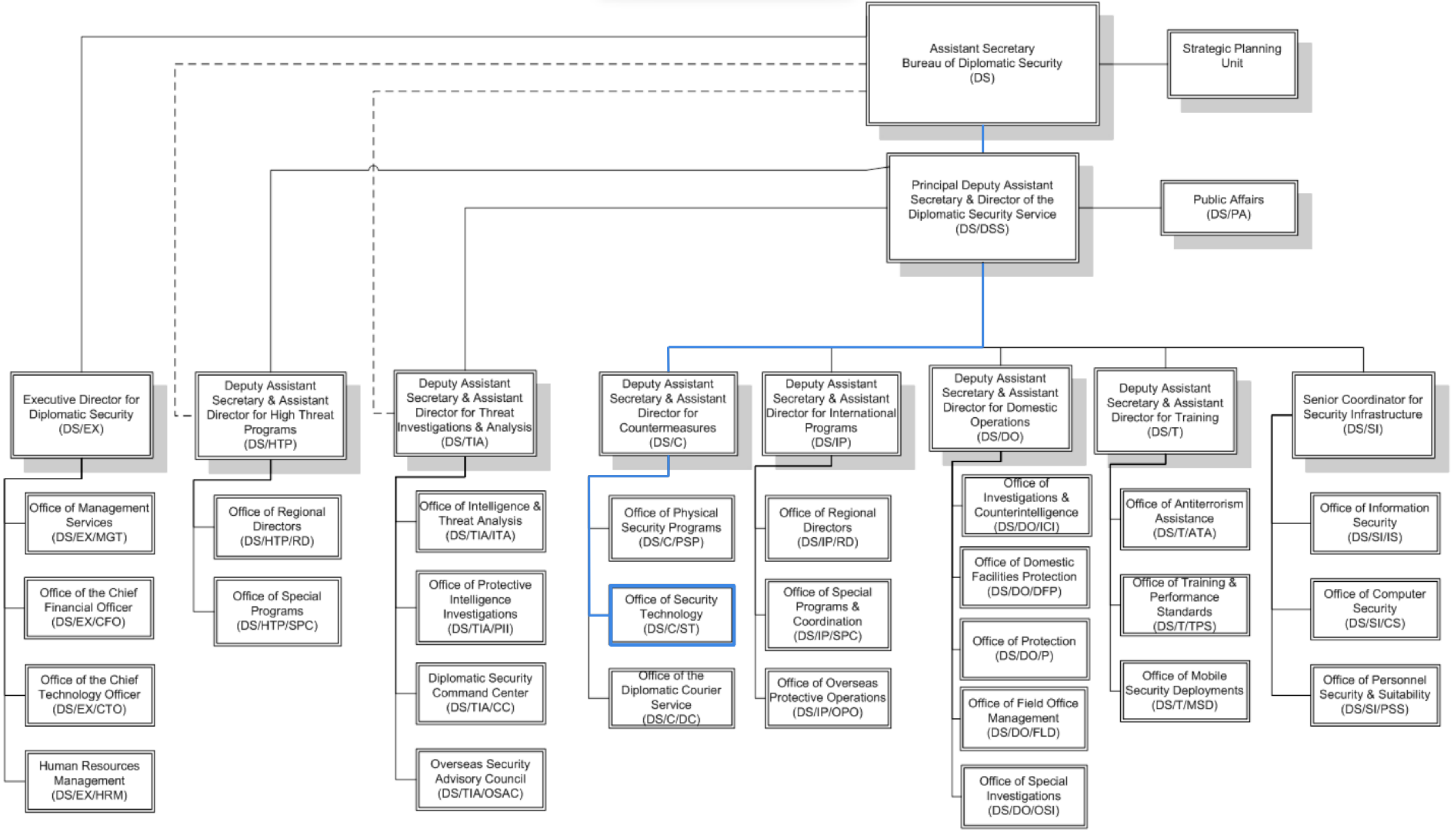
Under Secretary for Management (M)

- Administration (A) Assistant Secretary
- Budget and Planning (BP) Director
- Comptroller, Global Financial Services (CGFS) Comptroller
- Consular Affairs (CA) Assistant Secretary
- Office of Foreign Missions (OFM) Director
- Foreign Service Institute (FSI) Director
- Global Talent Management (GTM) Director General of Foreign Service & Director of Global Talent
- Information Resource Management (IRM) Chief Information Officer*
- Office of Management Strategy and Solutions (M/SS) Director
- Medical Services (MED) Director
- Overseas Buildings Operations (OBO) Director

Under Secretary for Civilian Security, Democracy, and Human Rights (J)

- Conflict & Stabilization Operations (CSO) Assistant Secretary*
- Democracy, Human Rights, and Labor (DRL) Assistant Secretary
- Office of Global Criminal Justice (GCJ) Ambassador-At-Large
- International Narcotics and Law Enforcement (INL) Assistant Secretary
- Office of International Religious Freedom (IRF) Ambassador-At-Large*
- Office to Monitor and Combat Trafficking in Persons (TIP) Ambassador-At-Large
- Population, Refugees, and Migration (PRM) Assistant Secretary

- Office of Civil Rights (S/OCR) Director
- Office of Global Women's Issues (S/GWI) Ambassador-At-Large
- Intelligence and Research (INR) Assistant Secretary
- Office of Inspector General (OIG) Inspector General
- Legislative Affairs (H) Assistant Secretary
- Office of the Legal Advisor (L) Legal Advisor
- Office of Policy Planning (S/P) Director
- Office of the Chief of Protocol (S/CPR) Ambassador
- Office of U.S. Global AIDS Coordinator & Health Diplomacy (S/GAC) Ambassador-At-Large
- Office of Diversity and Inclusion (S/ODI) Chief Diversity and Inclusion Officer
- Special Envoys and Special Representatives



Assistant Secretary Bureau of Diplomatic Security (DS)

Strategic Planning Unit

Principal Deputy Assistant Secretary & Director of the Diplomatic Security Service (DS/DSS)

Public Affairs (DS/PA)

Executive Director for Diplomatic Security (DS/EX)

- Office of Management Services (DS/EX/MGT)
- Office of the Chief Financial Officer (DS/EX/CFO)
- Office of the Chief Technology Officer (DS/EX/CTO)
- Human Resources Management (DS/EX/HRM)

Deputy Assistant Secretary & Assistant Director for High Threat Programs (DS/HTP)

- Office of Regional Directors (DS/HTP/RD)
- Office of Special Programs (DS/HTP/SPC)

Deputy Assistant Secretary & Assistant Director for Threat Investigations & Analysis (DS/TIA)

- Office of Intelligence & Threat Analysis (DS/TIA/ITA)
- Office of Protective Intelligence Investigations (DS/TIA/PII)
- Diplomatic Security Command Center (DS/TIA/CC)
- Overseas Security Advisory Council (DS/TIA/OSAC)

Deputy Assistant Secretary & Assistant Director for Countermeasures (DS/C)

- Office of Physical Security Programs (DS/C/PSP)
- Office of Security Technology (DS/C/ST)
- Office of the Diplomatic Courier Service (DS/C/DC)

Deputy Assistant Secretary & Assistant Director for International Programs (DS/IP)

- Office of Regional Directors (DS/IP/RD)
- Office of Special Programs & Coordination (DS/IP/SPC)
- Office of Overseas Protective Operations (DS/IP/OPO)

Deputy Assistant Secretary & Assistant Director for Domestic Operations (DS/DO)

- Office of Investigations & Counterintelligence (DS/DO/ICI)
- Office of Domestic Facilities Protection (DS/DO/DFP)
- Office of Protection (DS/DO/P)
- Office of Field Office Management (DS/DO/FLD)
- Office of Special Investigations (DS/DO/OSI)

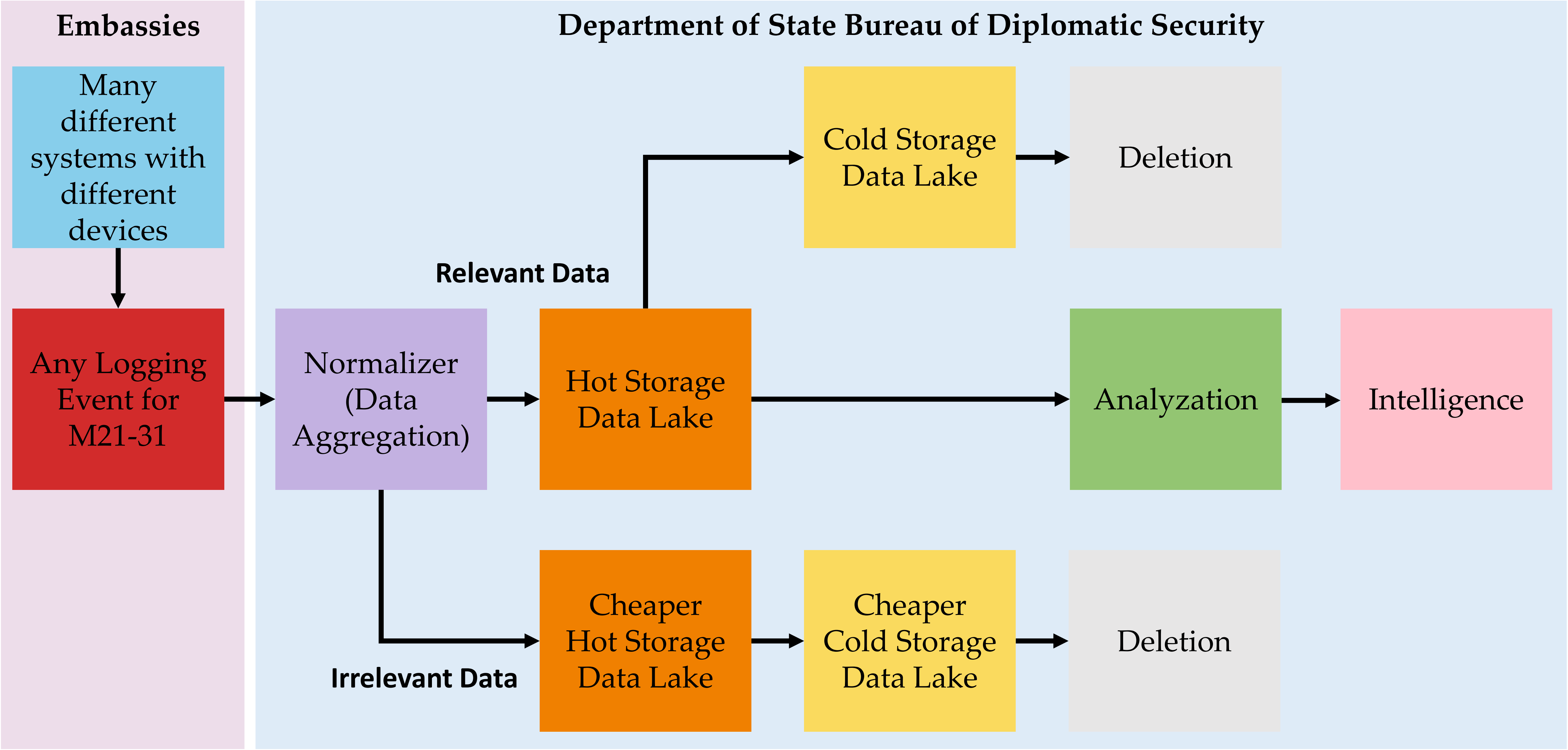
Deputy Assistant Secretary & Assistant Director for Training (DS/T)

- Office of Antiterrorism Assistance (DS/T/ATA)
- Office of Training & Performance Standards (DS/T/TPS)
- Office of Mobile Security Deployments (DS/T/MSD)

Senior Coordinator for Security Infrastructure (DS/SI)

- Office of Information Security (DS/SI/IS)
- Office of Computer Security (DS/SI/CS)
- Office of Personnel Security & Suitability (DS/SI/PSS)

Final MVP



Embassies

Department of State Bureau of Diplomatic Security

Many different systems with different devices

Any Logging Event for M21-31

Normalizer (Data Aggregation)

Relevant Data

Hot Storage Data Lake

Cold Storage Data Lake

Deletion

Analyzation

Intelligence

Irrelevant Data

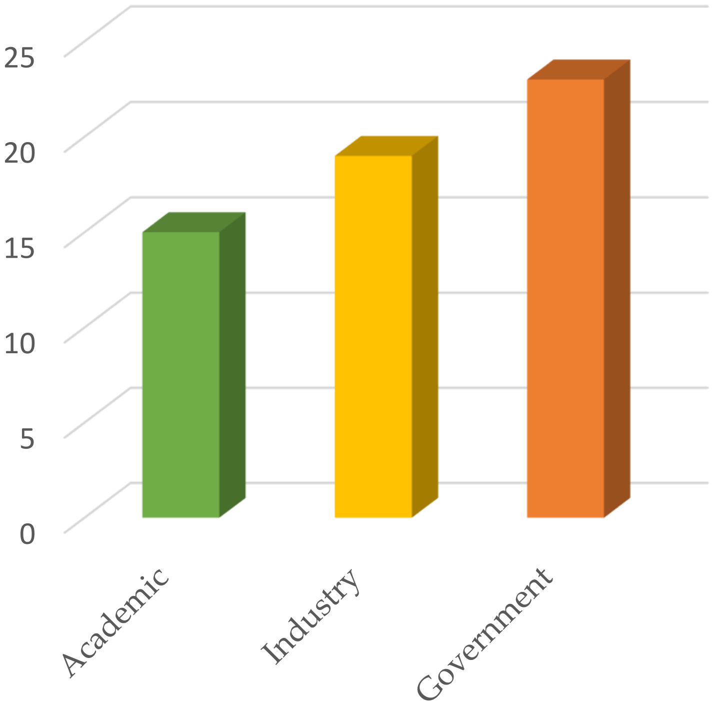
Cheaper Hot Storage Data Lake

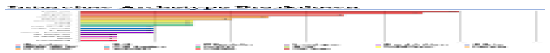
Cheaper Cold Storage Data Lake

Deletion

Interview Breakdown By Sector

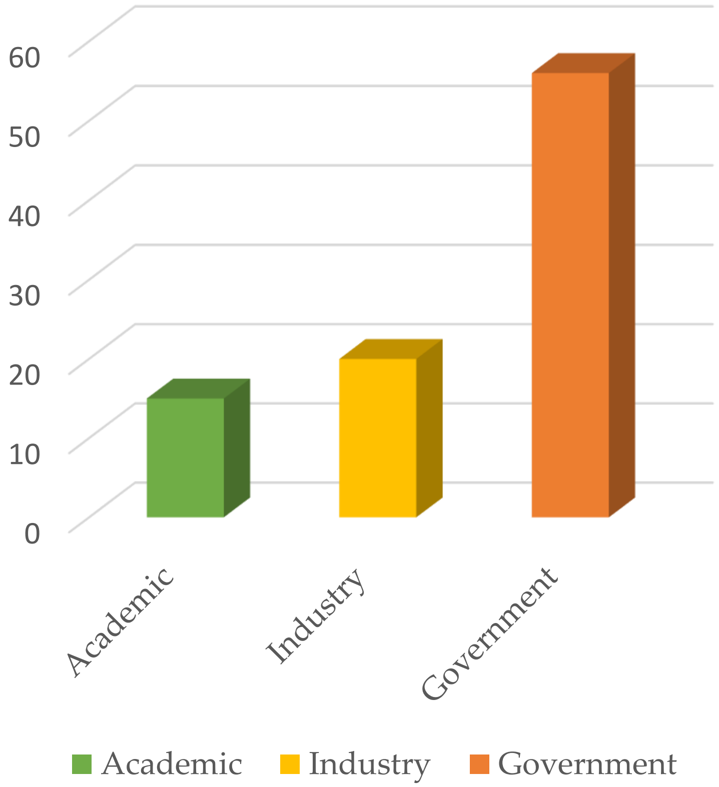
- Across all 15 weeks we had a total of **59 <u>unique</u> interviews** across 3 sectors:
  - **Academic** – 15
  - **Industry** – 19
  - **Government** – 23





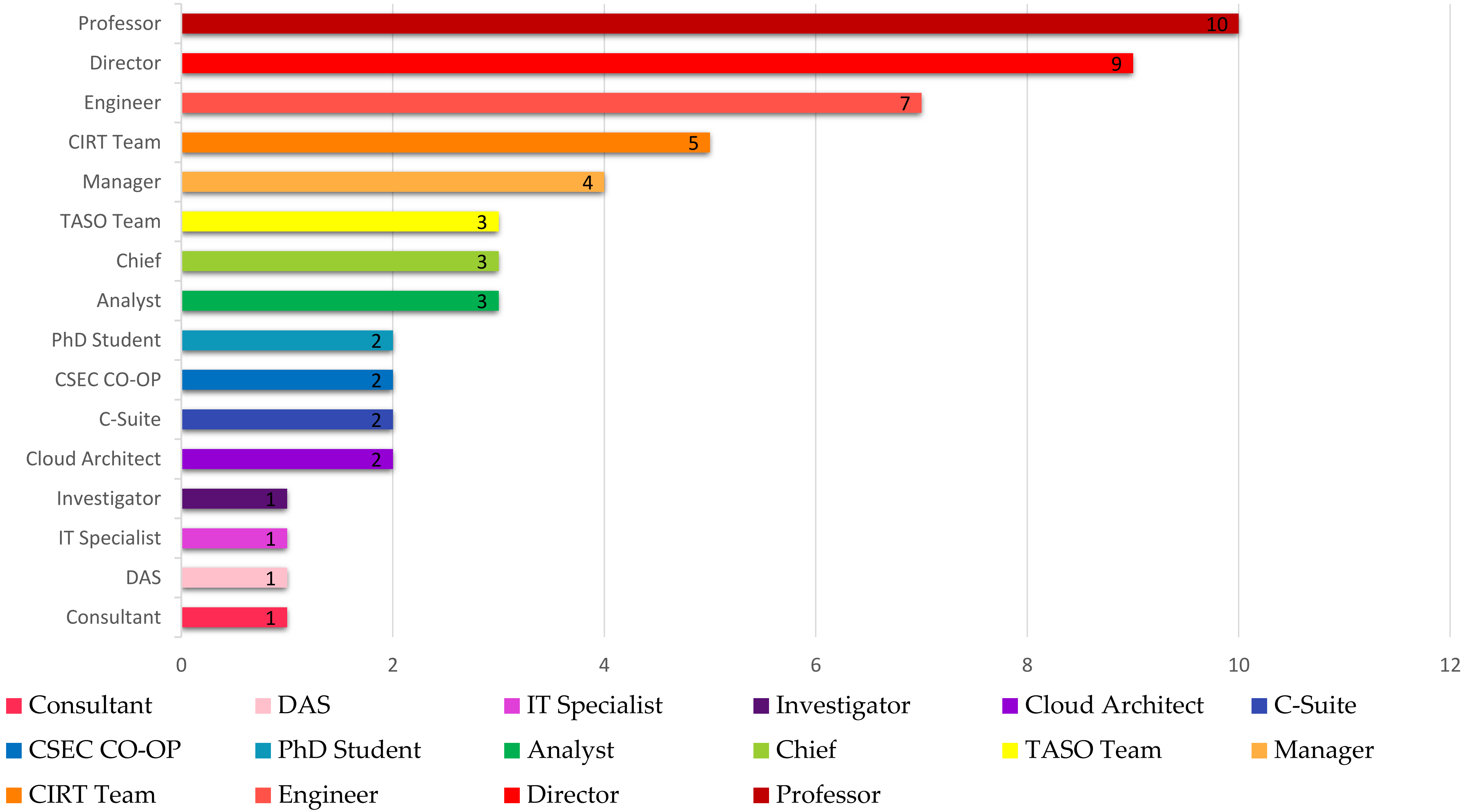
Unique

- Across all 15 weeks we had a total of **91 <u>total</u> interviews** across 3 sectors:
  - **Academic** – 15
  - **Industry** – 20
  - **Government** – 56



Total

Interview Archetype Breakdown



Project Journey

Weeks 1-5

- Meetings with sponsor to focus on understanding the problem
- Discovery Interviews
  - Interviews with consultants, security engineers, and [illegible]
  - Understanding technologies involved in the [illegible] and their capabilities

Total Interviews: **17**
Research Papers: **20**
Days Left: **70**

Weeks 1-5

- ❖ Meetings with sponsors to focus on understanding the problem
- ❖ Discovery Interviews
  - ❖ Interviews with consultants, security engineers, and educators
  - ❖ Understanding technologies involved in the Problem Statement and their capabilities

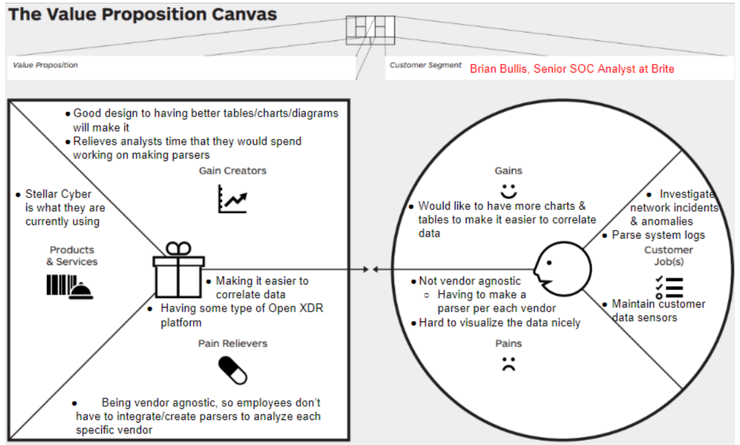
Weeks 1-5: Interviews

David Hagan – Cloud Data Architect, Office of Cyber Monitoring and Operations

- ❖ Data storage and log aggregation
- ❖ Big takeaway: Data Lakes for storage
  - ❖ Aggregate events and then place in cloud storage

Other Important VPCs

Brian Bullis



Brian Bullis, Senior SOC Analyst at Brite

Gain Creators:
- Good design to having better tables/charts/diagrams will make it
- Relieves analysts time that they would spend working on making parsers

Products & Services:
- Stellar Cyber is what they are currently using

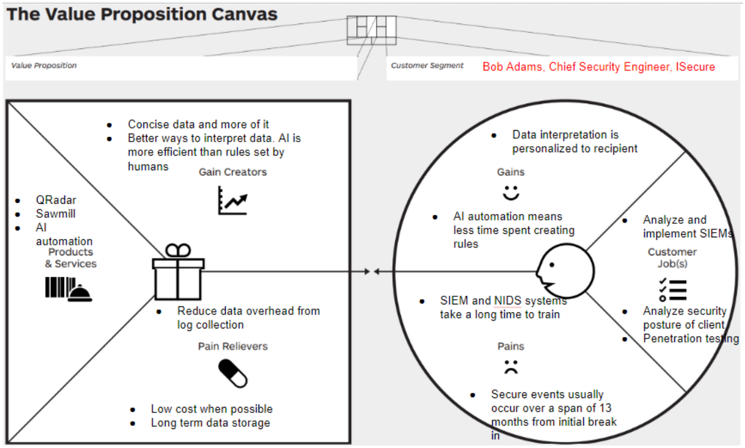
Pain Relievers:
- Making it easier to correlate data
- Having some type of Open XDR platform
- Being vendor agnostic, so employees don't have to integrate/create parsers to analyze each specific vendor

Gains:
- Would like to have more charts & tables to make it easier to correlate data

Customer Job(s):
- Investigate network incidents & anomalies
- Parse system logs
- Maintain customer data sensors

Pains:
- Not vendor agnostic
  - Having to make a parser per each vendor
- Hard to visualize the data nicely

Bob Adams



Bob Adams, Chief Security Engineer, ISecure

Gain Creators:
- Concise data and more of it
- Better ways to interpret data. AI is more efficient than rules set by humans

Products & Services:
- QRadar
- Sawmill
- AI automation

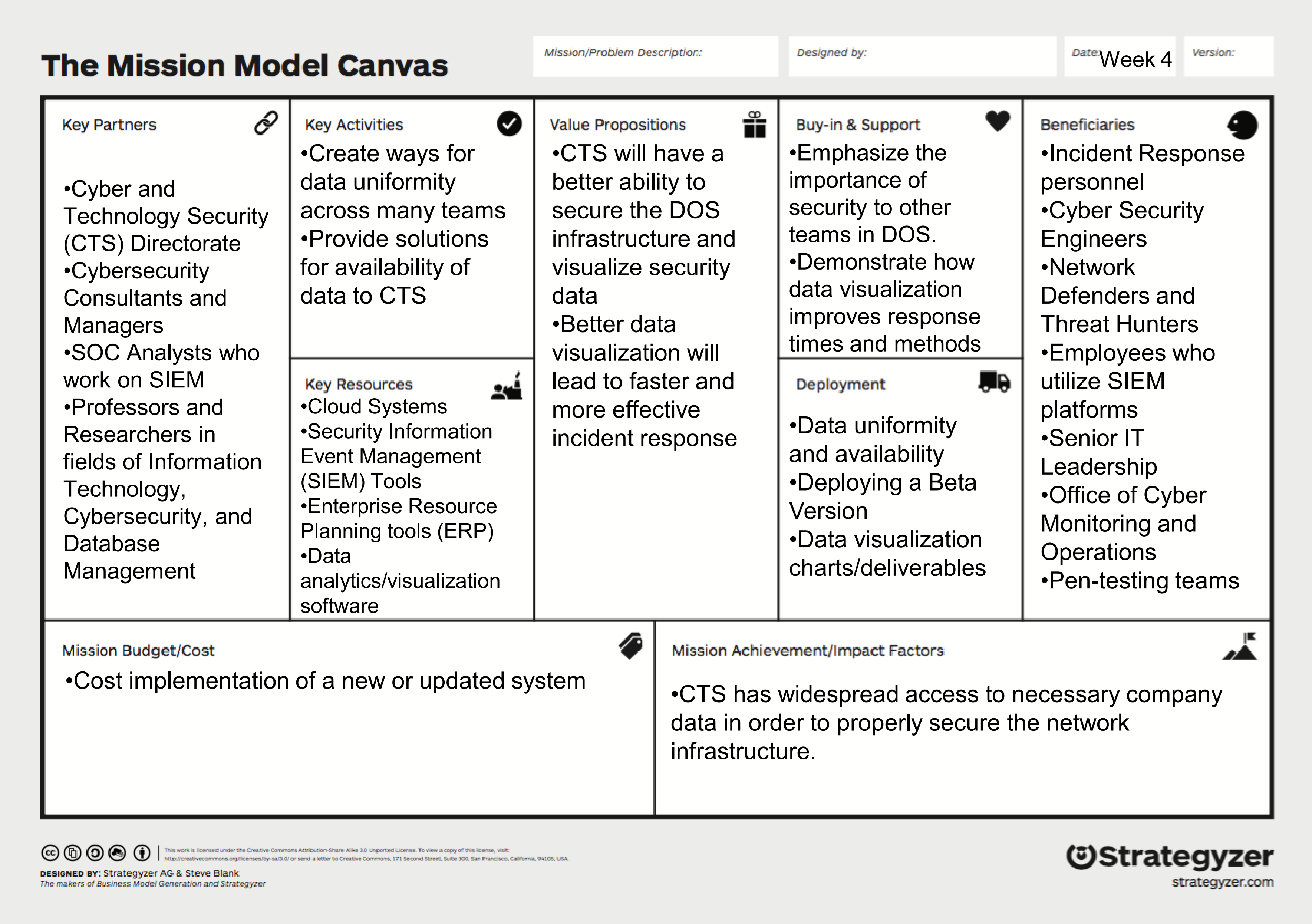
Pain Relievers:
- Reduce data overhead from log collection
- Low cost when possible
- Long term data storage

Gains:
- Data interpretation is personalized to recipient
- AI automation means less time spent creating rules

Customer Job(s):
- Analyze and implement SIEMs
- Analyze security posture of client
- Penetration testing

Pains:
- SIEM and NIDS systems take a long time to train
- Secure events usually occur over a span of 13 months from initial break in

Weeks 1-5: Mission Model Canvas



The Mission Model Canvas

Mission/Problem Description:

Designed by:

Date: Week 4

Version:

Key Partners

- Cyber and Technology Security (CTS) Directorate
- Cybersecurity Consultants and Managers
- SOC Analysts who work on SIEM
- Professors and Researchers in fields of Information Technology, Cybersecurity, and Database Management

Key Activities

- Create ways for data uniformity across many teams
- Provide solutions for availability of data to CTS

Key Resources

- Cloud Systems
- Security Information Event Management (SIEM) Tools
- Enterprise Resource Planning tools (ERP)
- Data analytics/visualization software

Value Propositions

- CTS will have a better ability to secure the DOS infrastructure and visualize security data
- Better data visualization will lead to faster and more effective incident response

Buy-in & Support

- Emphasize the importance of security to other teams in DOS.
- Demonstrate how data visualization improves response times and methods

Deployment

- Data uniformity and availability
- Deploying a Beta Version
- Data visualization charts/deliverables

Beneficiaries

- Incident Response personnel
- Cyber Security Engineers
- Network Defenders and Threat Hunters
- Employees who utilize SIEM platforms
- Senior IT Leadership
- Office of Cyber Monitoring and Operations
- Pen-testing teams

Mission Budget/Cost

- Cost implementation of a new or updated system

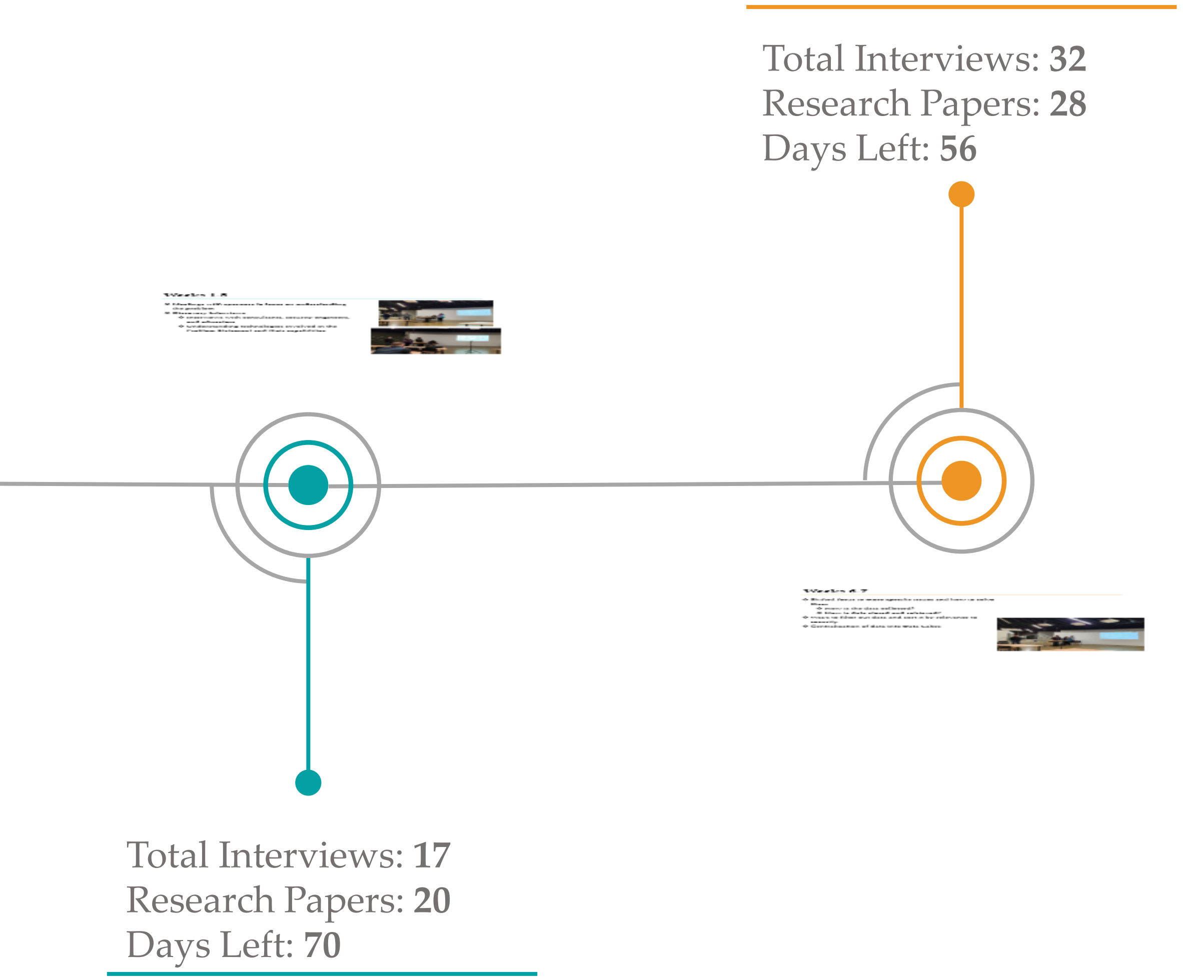
Mission Achievement/Impact Factors

- CTS has widespread access to necessary company data in order to properly secure the network infrastructure.

DESIGNED BY: Strategyzer AG & Steve Blank
The makers of Business Model Generation and Strategyzer

Strategyzer
strategyzer.com

Project Timeline



Weeks 1-5

[illegible]

Total Interviews: **17**
Research Papers: **20**
Days Left: **70**

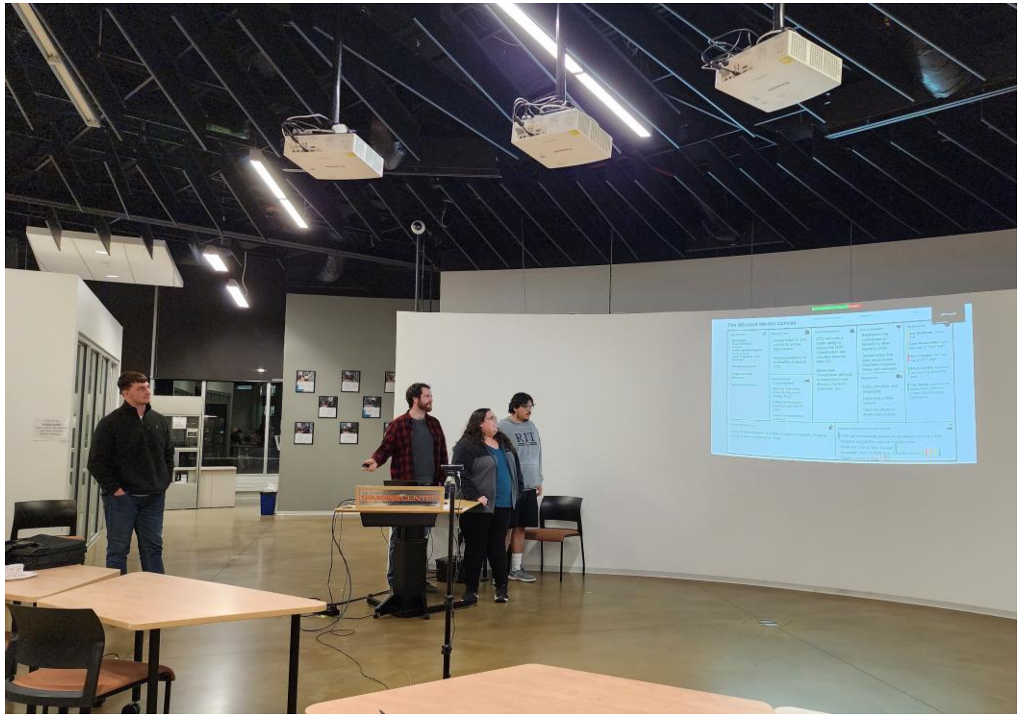
Total Interviews: **32**
Research Papers: **28**
Days Left: **56**

Weeks 6-7

[illegible]

Weeks 6-7

- Shifted focus to more specific issues and how to solve them
    - How is the data collected?
    - How is data stored and retrieved?
- Ways to filter out data and sort it by relevance to security
- Centralization of data into Data Lakes



Weeks 6-7: Interviews

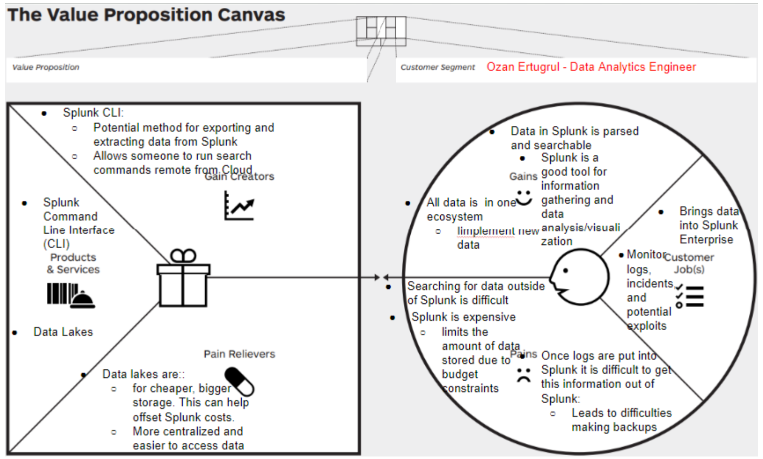
Mike Pinch – Director, Security Risk Advisors

- ❖ Presented the idea of a data pipeline and fusion center
- ❖ Cribl allowed easy traversal of unsorted logs within a data lake
- ❖ Importance of filtering incoming information as "useful" or less-useful.

> **“The problem with SOCs across the industry view and use SIEM as the center of their data universe… which it shouldn’t be”**
> **– Mike Pinch**

Other Important VPCs

Ozan Ertugrul



The Value Proposition Canvas

Value Proposition

Customer Segment Ozan Ertugrul - Data Analytics Engineer

- Splunk CLI:
  - Potential method for exporting and extracting data from Splunk
  - Allows someone to run search commands remote from Cloud

Gain Creators

- Splunk Command Line Interface (CLI)

Products & Services

- Data Lakes

Pain Relievers

- Data lakes are::
  - for cheaper, bigger storage. This can help offset Splunk costs.
  - More centralized and easier to access data

- Data in Splunk is parsed and searchable
  - Splunk is a good tool for information gathering and data analysis/visualization
- All data is in one ecosystem
  - Iimplement new data

Gains

- Brings data into Splunk Enterprise
- Monitor logs, incidents, and potential exploits

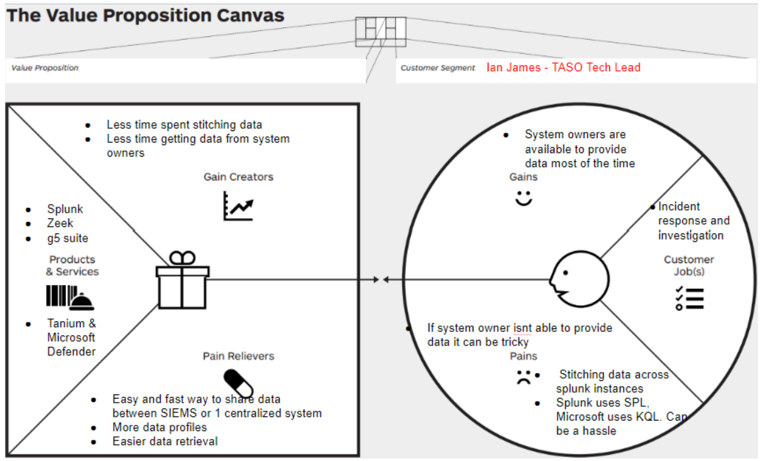
Customer Job(s)

- Searching for data outside of Splunk is difficult
- Splunk is expensive
  - limits the amount of data stored due to budget constraints

Pains

- Once logs are put into Splunk it is difficult to get this information out of Splunk:
  - Leads to difficulties making backups

Ian James



The Value Proposition Canvas

Value Proposition

Customer Segment Ian James - TASO Tech Lead

- Less time spent stitching data
- Less time getting data from system owners

Gain Creators

- Splunk
- Zeek
- g5 suite

Products & Services

- Tanium & Microsoft Defender

Pain Relievers

- Easy and fast way to share data between SIEMS or 1 centralized system
- More data profiles
- Easier data retrieval

- System owners are available to provide data most of the time

Gains

- Incident response and investigation

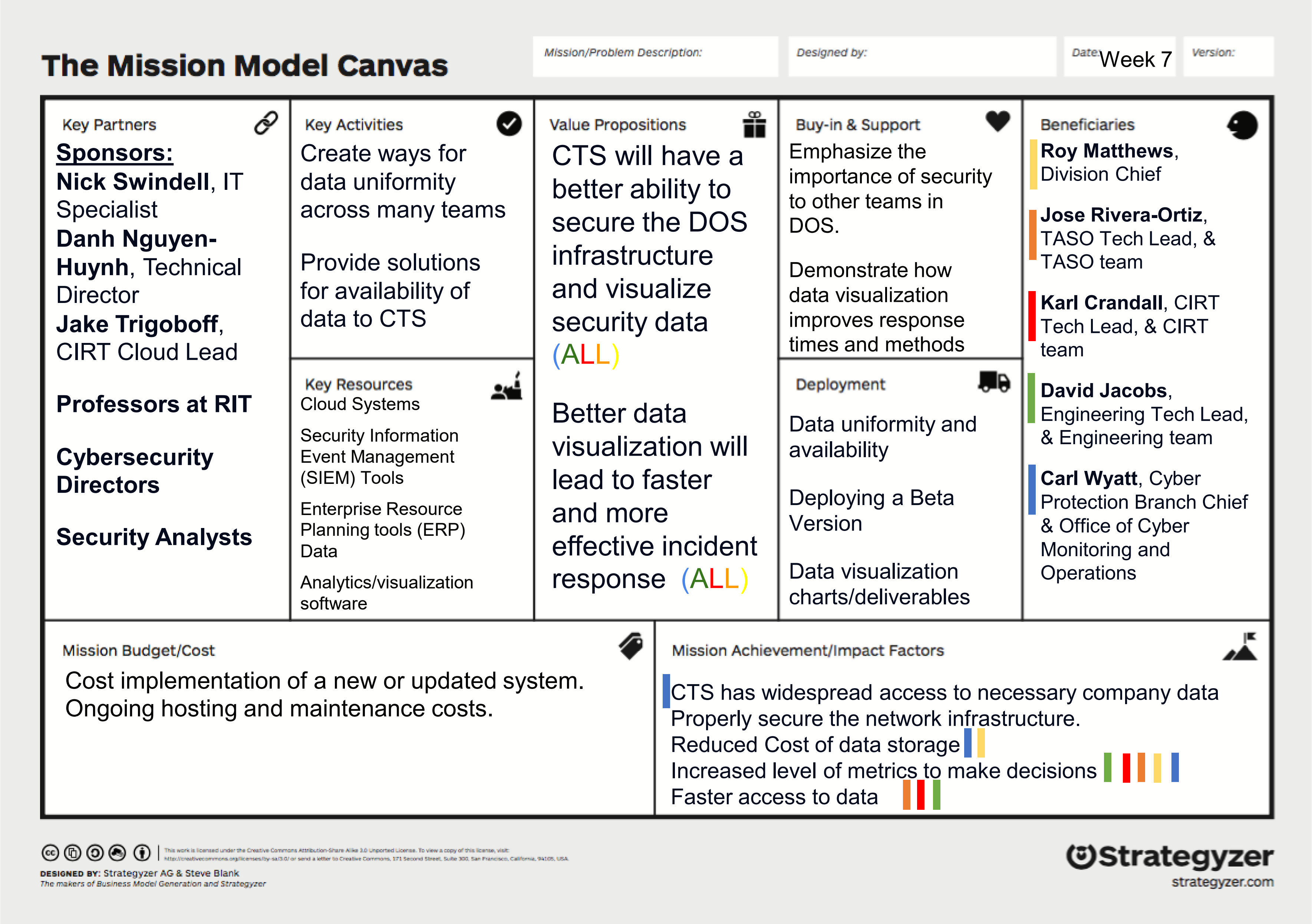
Customer Job(s)

- If system owner isnt able to provide data it can be tricky

Pains

- Stitching data across splunk instances
- Splunk uses SPL, Microsoft uses KQL. Can be a hassle

Weeks 6-7: Mission Model Canvas



The Mission Model Canvas

Mission/Problem Description:

Designed by:

Date: Week 7

Version:

Key Partners

Sponsors:
Nick Swindell, IT Specialist
Danh Nguyen-Huynh, Technical Director
Jake Trigoboff, CIRT Cloud Lead

Professors at RIT

Cybersecurity Directors

Security Analysts

Key Activities

Create ways for data uniformity across many teams

Provide solutions for availability of data to CTS

Key Resources

Cloud Systems

Security Information Event Management (SIEM) Tools

Enterprise Resource Planning tools (ERP) Data

Analytics/visualization software

Value Propositions

CTS will have a better ability to secure the DOS infrastructure and visualize security data (ALL)

Better data visualization will lead to faster and more effective incident response (ALL)

Buy-in & Support

Emphasize the importance of security to other teams in DOS.

Demonstrate how data visualization improves response times and methods

Deployment

Data uniformity and availability

Deploying a Beta Version

Data visualization charts/deliverables

Beneficiaries

🟨 **Roy Matthews**, Division Chief

🟧 **Jose Rivera-Ortiz**, TASO Tech Lead, & TASO team

🟥 **Karl Crandall**, CIRT Tech Lead, & CIRT team

🟩 **David Jacobs**, Engineering Tech Lead, & Engineering team

🟦 **Carl Wyatt**, Cyber Protection Branch Chief & Office of Cyber Monitoring and Operations

Mission Budget/Cost

Cost implementation of a new or updated system.
Ongoing hosting and maintenance costs.

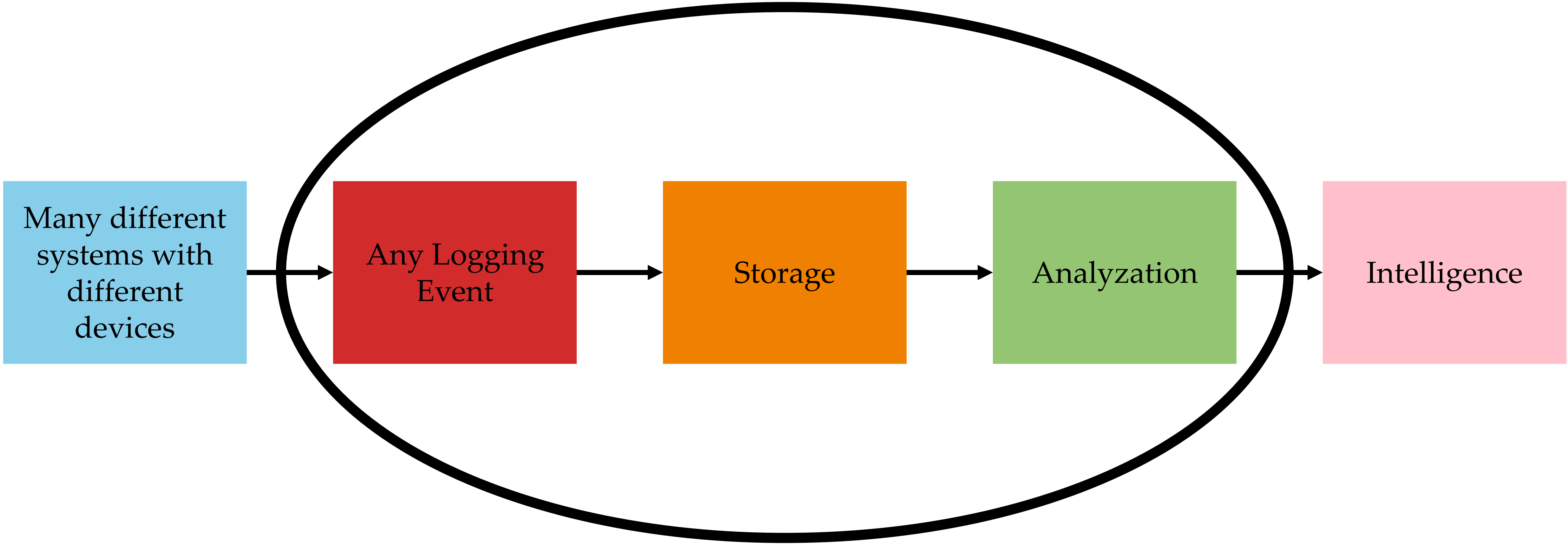
Mission Achievement/Impact Factors

🟦 CTS has widespread access to necessary company data
Properly secure the network infrastructure.
Reduced Cost of data storage 🟦 🟨
Increased level of metrics to make decisions 🟩 🟥 🟧 🟨 🟦
Faster access to data 🟧 🟥 🟩

DESIGNED BY: Strategyzer AG & Steve Blank
The makers of Business Model Generation and Strategyzer

Strategyzer
strategyzer.com

Week 6 – First Problem Flowchart



Many different systems with different devices

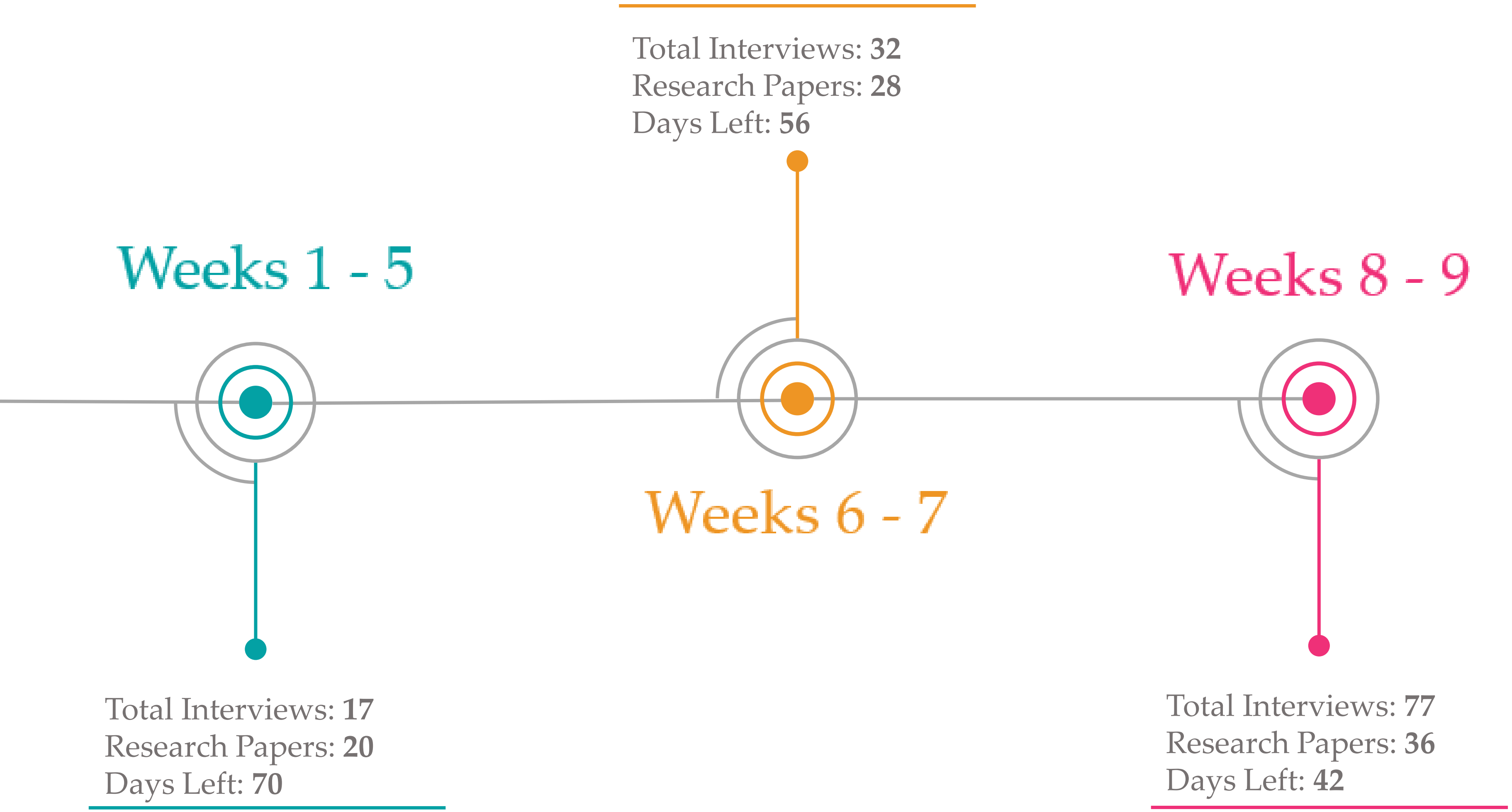
Any Logging Event

Storage

Analyzation

Intelligence

Project Timeline



Weeks 1 - 5

Total Interviews: **17**
Research Papers: **20**
Days Left: **70**

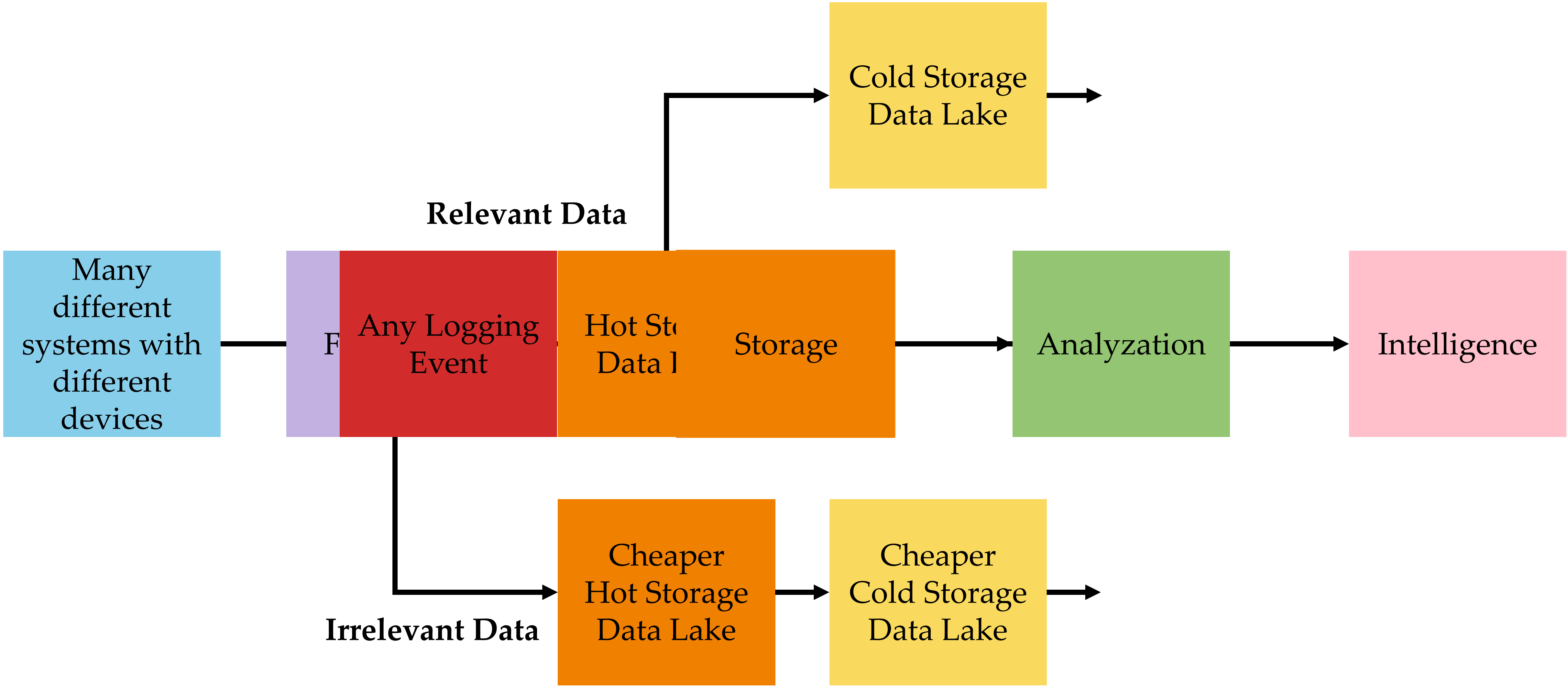
Weeks 6 - 7

Total Interviews: **32**
Research Papers: **28**
Days Left: **56**

Weeks 8 - 9

Total Interviews: **77**
Research Papers: **36**
Days Left: **42**

Week 8 – Second MVP



Weeks 8-9

- During Weeks 8 & 9 we visited our sponsors in Washington D.C., Maryland & Virginia
  - Toured DoS SA-20 location & off-site data center
  - Met with 15+ people including, but not limited to:
    - Senior management
    - Incident response personnel

Weeks 8-9: Interviews

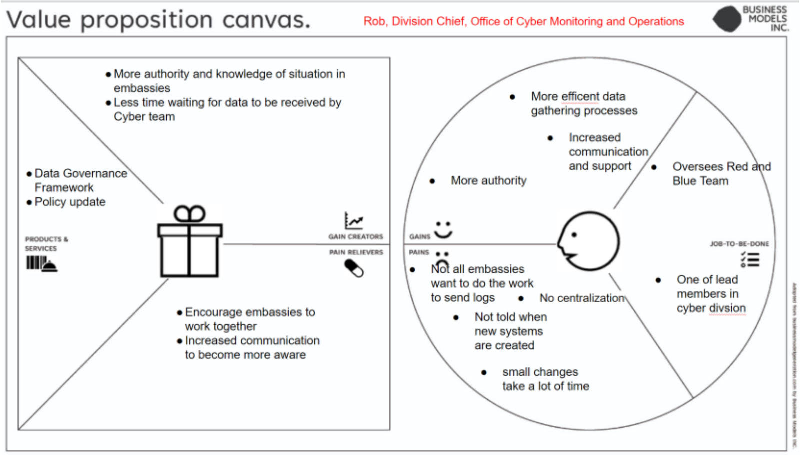
Roy Matthews - Division Chief, Office of Cyber Monitoring and Operations

- ❖ Discussed change management and onboarding processes
- ❖ New software goes through engineering management process to ensure it complies with standards/"meets baseline"

> **"Walk through the critical path with milestones."**
> **- Roy Matthews**

Other Important VPCs

Rob



Value proposition canvas.

Rob, Division Chief, Office of Cyber Monitoring and Operations

- More authority and knowledge of situation in embassies
- Less time waiting for data to be received by Cyber team

- Data Governance Framework
- Policy update

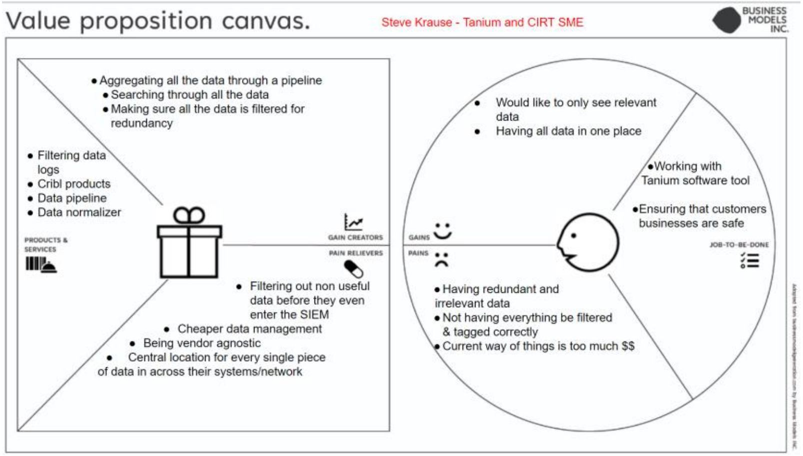
- Encourage embassies to work together
- Increased communication to become more aware

- More efficent data gathering processes
- Increased communication and support
- More authority

- Oversees Red and Blue Team
- One of lead members in cyber divsion

- Not all embassies want to do the work to send logs
- No centralization
- Not told when new systems are created
- small changes take a lot of time

Steve Krause



Value proposition canvas.

Steve Krause - Tanium and CIRT SME

- Aggregating all the data through a pipeline
- Searching through all the data
- Making sure all the data is filtered for redundancy

- Filtering data logs
- Cribl products
- Data pipeline
- Data normalizer

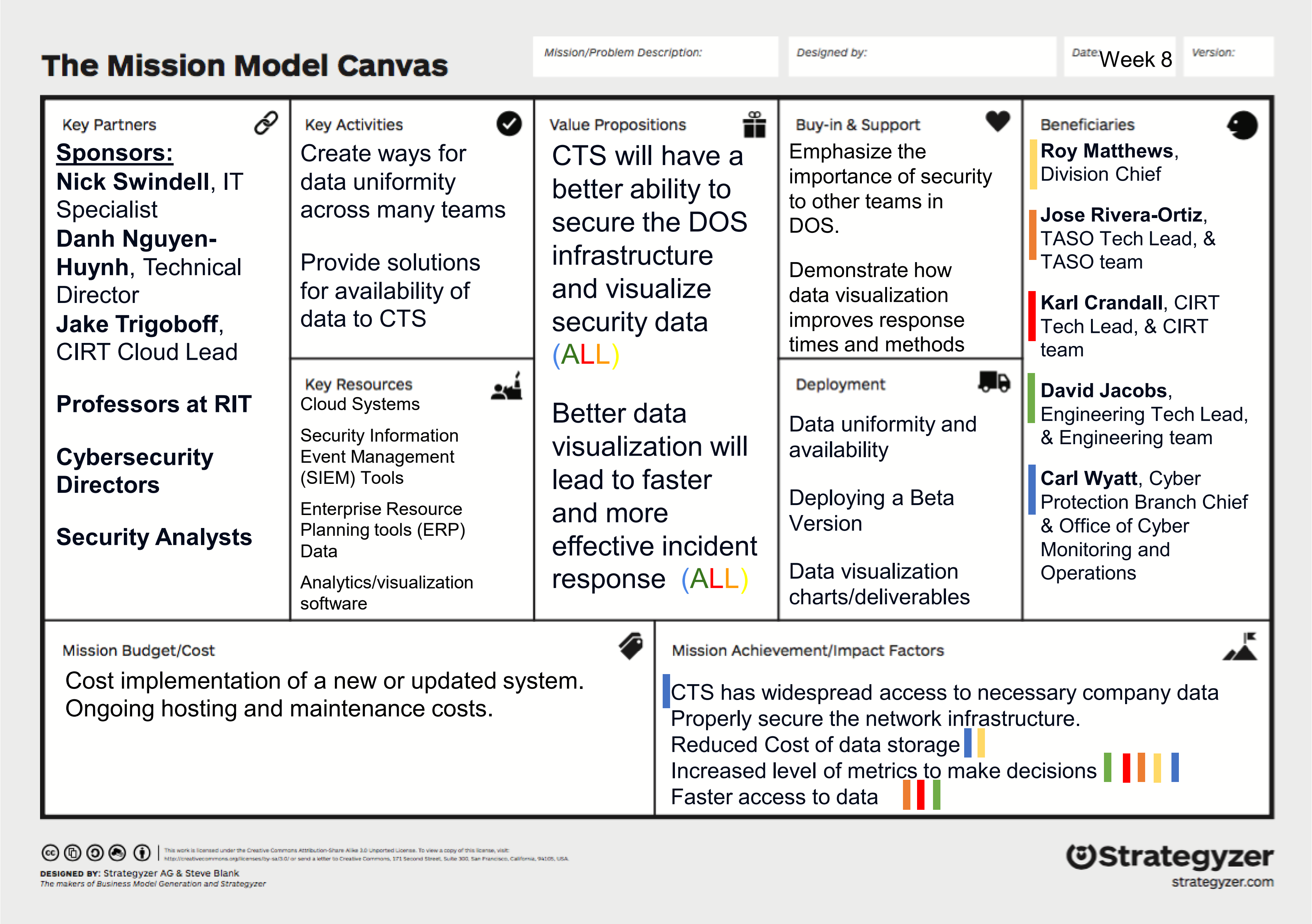
- Filtering out non useful data before they even enter the SIEM
- Cheaper data management
- Being vendor agnostic
- Central location for every single piece of data in across their systems/network

- Would like to only see relevant data
- Having all data in one place

- Working with Tanium software tool
- Ensuring that customers businesses are safe

- Having redundant and irrelevant data
- Not having everything be filtered & tagged correctly
- Current way of things is too much $$

Weeks 8-9: Mission Model Canvas



The Mission Model Canvas

Mission/Problem Description:

Designed by:

Date: Week 8

Version:

Key Partners

Sponsors:

Nick Swindell, IT Specialist

Danh Nguyen-Huynh, Technical Director

Jake Trigoboff, CIRT Cloud Lead

Professors at RIT

Cybersecurity Directors

Security Analysts

Key Activities

Create ways for data uniformity across many teams

Provide solutions for availability of data to CTS

Key Resources

Cloud Systems

Security Information Event Management (SIEM) Tools

Enterprise Resource Planning tools (ERP) Data

Analytics/visualization software

Value Propositions

CTS will have a better ability to secure the DOS infrastructure and visualize security data (ALL)

Better data visualization will lead to faster and more effective incident response (ALL)

Buy-in & Support

Emphasize the importance of security to other teams in DOS.

Demonstrate how data visualization improves response times and methods

Deployment

Data uniformity and availability

Deploying a Beta Version

Data visualization charts/deliverables

Beneficiaries

🟨 **Roy Matthews**, Division Chief

🟧 **Jose Rivera-Ortiz**, TASO Tech Lead, & TASO team

🟥 **Karl Crandall**, CIRT Tech Lead, & CIRT team

🟩 **David Jacobs**, Engineering Tech Lead, & Engineering team

🟦 **Carl Wyatt**, Cyber Protection Branch Chief & Office of Cyber Monitoring and Operations

Mission Budget/Cost

Cost implementation of a new or updated system.
Ongoing hosting and maintenance costs.

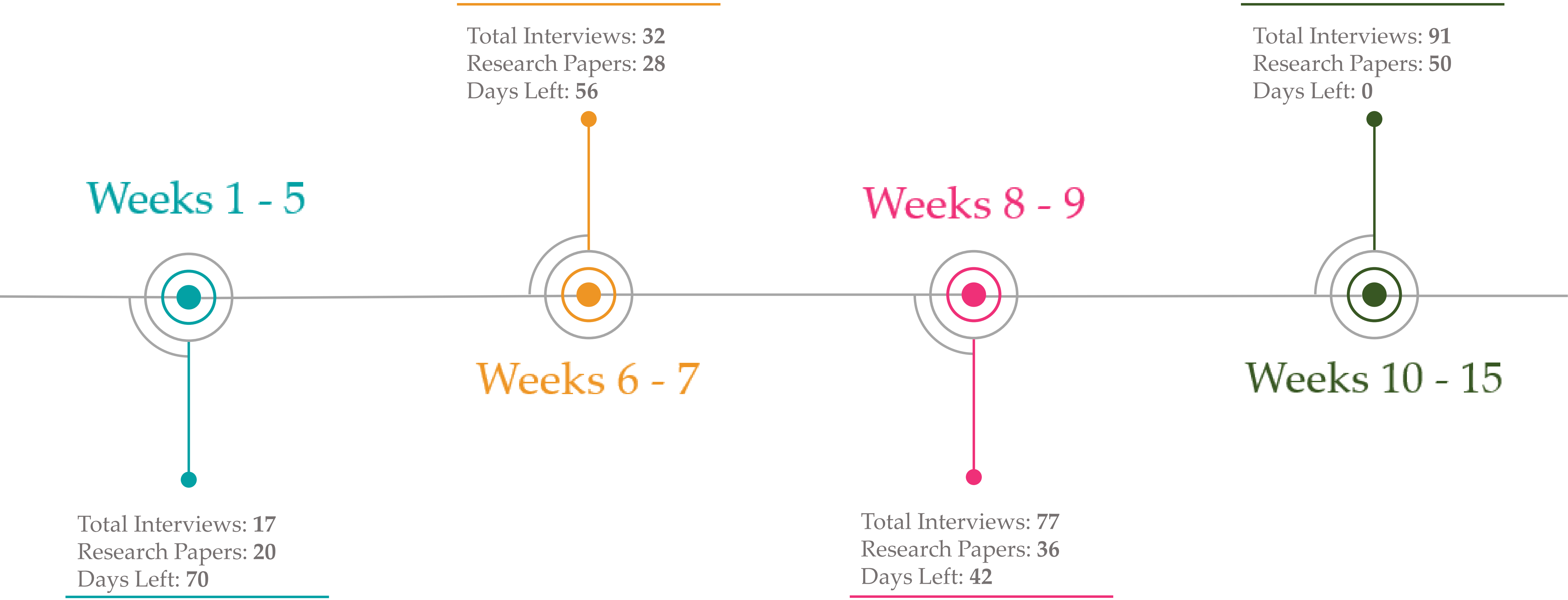
Mission Achievement/Impact Factors

🟦 CTS has widespread access to necessary company data
Properly secure the network infrastructure.
Reduced Cost of data storage 🟦🟨
Increased level of metrics to make decisions 🟩🟥🟧🟨🟦
Faster access to data 🟧🟥🟩

DESIGNED BY: Strategyzer AG & Steve Blank
The makers of Business Model Generation and Strategyzer

Strategyzer
strategyzer.com

Project Timeline



Weeks 1 - 5

Total Interviews: **17**
Research Papers: **20**
Days Left: **70**

Weeks 6 - 7

Total Interviews: **32**
Research Papers: **28**
Days Left: **56**

Weeks 8 - 9

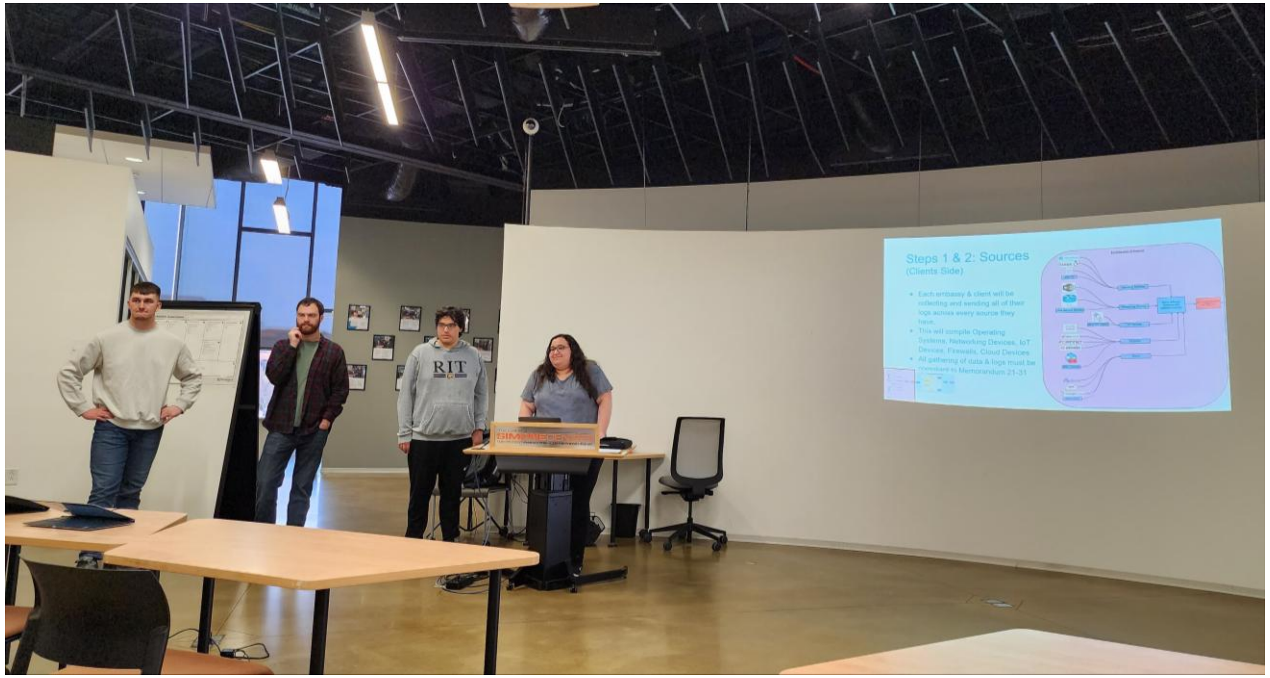
Total Interviews: **77**
Research Papers: **36**
Days Left: **42**

Weeks 10 - 15

Total Interviews: **91**
Research Papers: **50**
Days Left: **0**

Weeks 10-15

- Created proper Gantt Deployment Chart
- Finalized our MVP with sponsors
- Interviews focused on following areas:
  - Disaster Recovery & Business Continuity
  - Onboarding Procedures
  - Risk Management



Weeks 10-15: Interviews

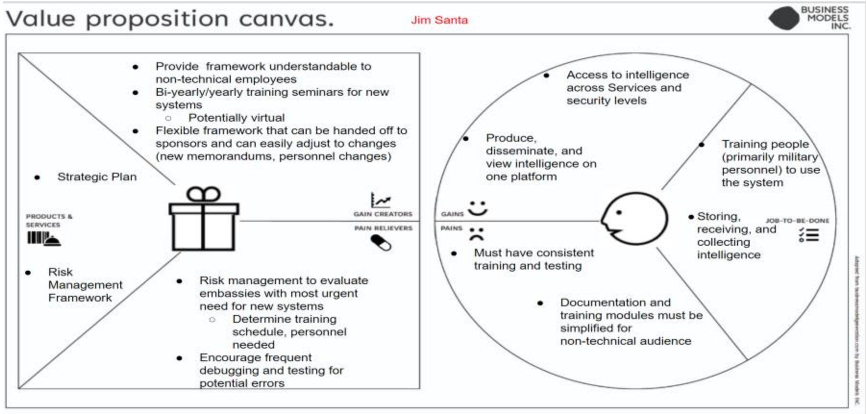
Jake Trigoboff - CIRT Cloud Lead, Office of Cyber Monitoring and Operations

- ❖ Onboarding and introduction phases
- ❖ Collaboration with Technical and Management
- ❖ KPIs are focused on incident statistics (types, frequency, logging requirements)

> "Once we figure out flow of change management having some integrations between management and technical side will be important."
> - Jake Trigoboff

Other Important VPCs

Dr. Jim Santa



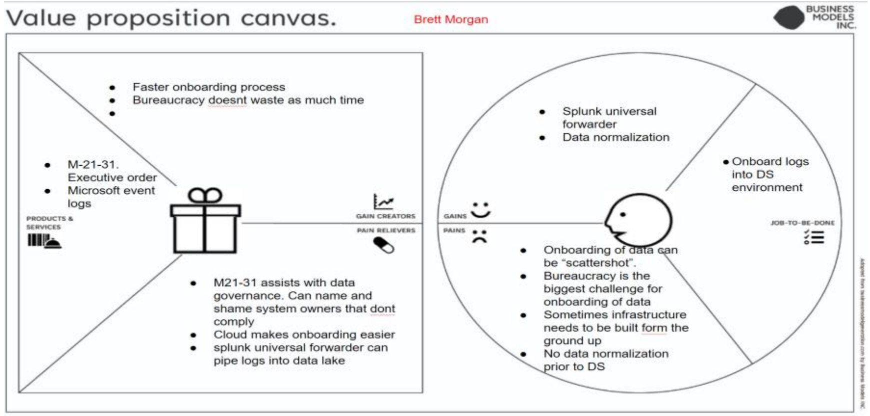
- Provide framework understandable to non-technical employees
- Bi-yearly/yearly training seminars for new systems
  - Potentially virtual
- Flexible framework that can be handed off to sponsors and can easily adjust to changes (new memorandums, personnel changes)

- Strategic Plan
- Risk Management Framework

- Risk management to evaluate embassies with most urgent need for new systems
  - Determine training schedule, personnel needed
- Encourage frequent debugging and testing for potential errors

- Access to intelligence across Services and security levels
- Produce, disseminate, and view intelligence on one platform
- Training people (primarily military personnel) to use the system
- Storing, receiving, and collecting intelligence
- Must have consistent training and testing
- Documentation and training modules must be simplified for non-technical audience

Brett Morgan



- Faster onboarding process
- Bureaucracy doesnt waste as much time
-

- M-21-31. Executive order
- Microsoft event logs

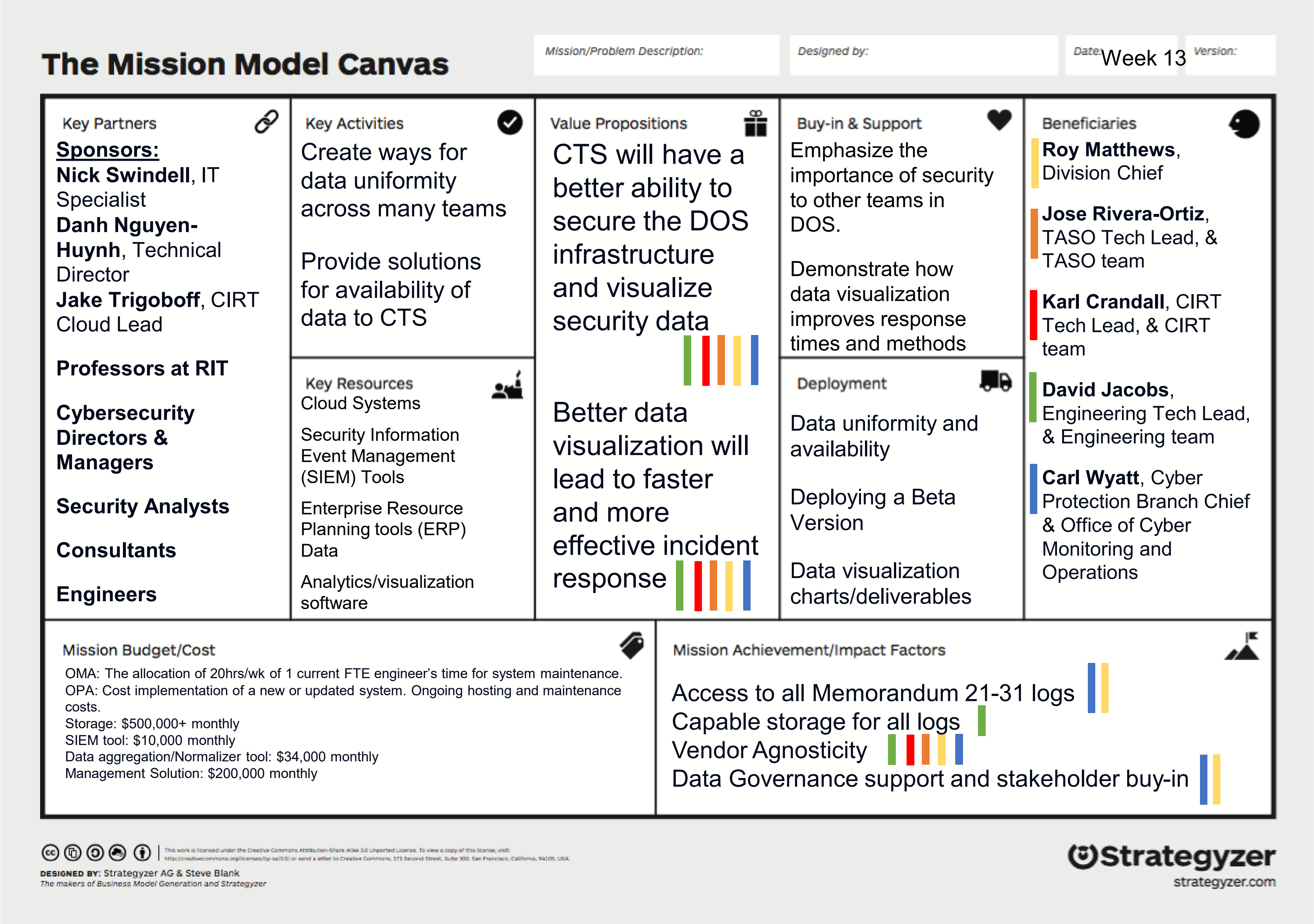
- M21-31 assists with data governance. Can name and shame system owners that dont comply
- Cloud makes onboarding easier
- splunk universal forwarder can pipe logs into data lake

- Splunk universal forwarder
- Data normalization

- Onboard logs into DS environment

- Onboarding of data can be "scattershot".
- Bureaucracy is the biggest challenge for onboarding of data
- Sometimes infrastructure needs to be built form the ground up
- No data normalization prior to DS

Weeks 10-15: Mission Model Canvas



The Mission Model Canvas

Mission/Problem Description:

Designed by:

Date: Week 13

Version:

Key Partners

Sponsors:

Nick Swindell, IT Specialist

Danh Nguyen-Huynh, Technical Director

Jake Trigoboff, CIRT Cloud Lead

Professors at RIT

Cybersecurity Directors & Managers

Security Analysts

Consultants

Engineers

Key Activities

Create ways for data uniformity across many teams

Provide solutions for availability of data to CTS

Key Resources

Cloud Systems

Security Information Event Management (SIEM) Tools

Enterprise Resource Planning tools (ERP) Data

Analytics/visualization software

Value Propositions

CTS will have a better ability to secure the DOS infrastructure and visualize security data 🟩🟥🟧🟨🟦

Better data visualization will lead to faster and more effective incident response 🟩🟥🟧🟨🟦

Buy-in & Support

Emphasize the importance of security to other teams in DOS.

Demonstrate how data visualization improves response times and methods

Deployment

Data uniformity and availability

Deploying a Beta Version

Data visualization charts/deliverables

Beneficiaries

🟨 **Roy Matthews**, Division Chief

🟧 **Jose Rivera-Ortiz**, TASO Tech Lead, & TASO team

🟥 **Karl Crandall**, CIRT Tech Lead, & CIRT team

🟩 **David Jacobs**, Engineering Tech Lead, & Engineering team

🟦 **Carl Wyatt**, Cyber Protection Branch Chief & Office of Cyber Monitoring and Operations

Mission Budget/Cost

OMA: The allocation of 20hrs/wk of 1 current FTE engineer's time for system maintenance.
OPA: Cost implementation of a new or updated system. Ongoing hosting and maintenance costs.
Storage: $500,000+ monthly
SIEM tool: $10,000 monthly
Data aggregation/Normalizer tool: $34,000 monthly
Management Solution: $200,000 monthly

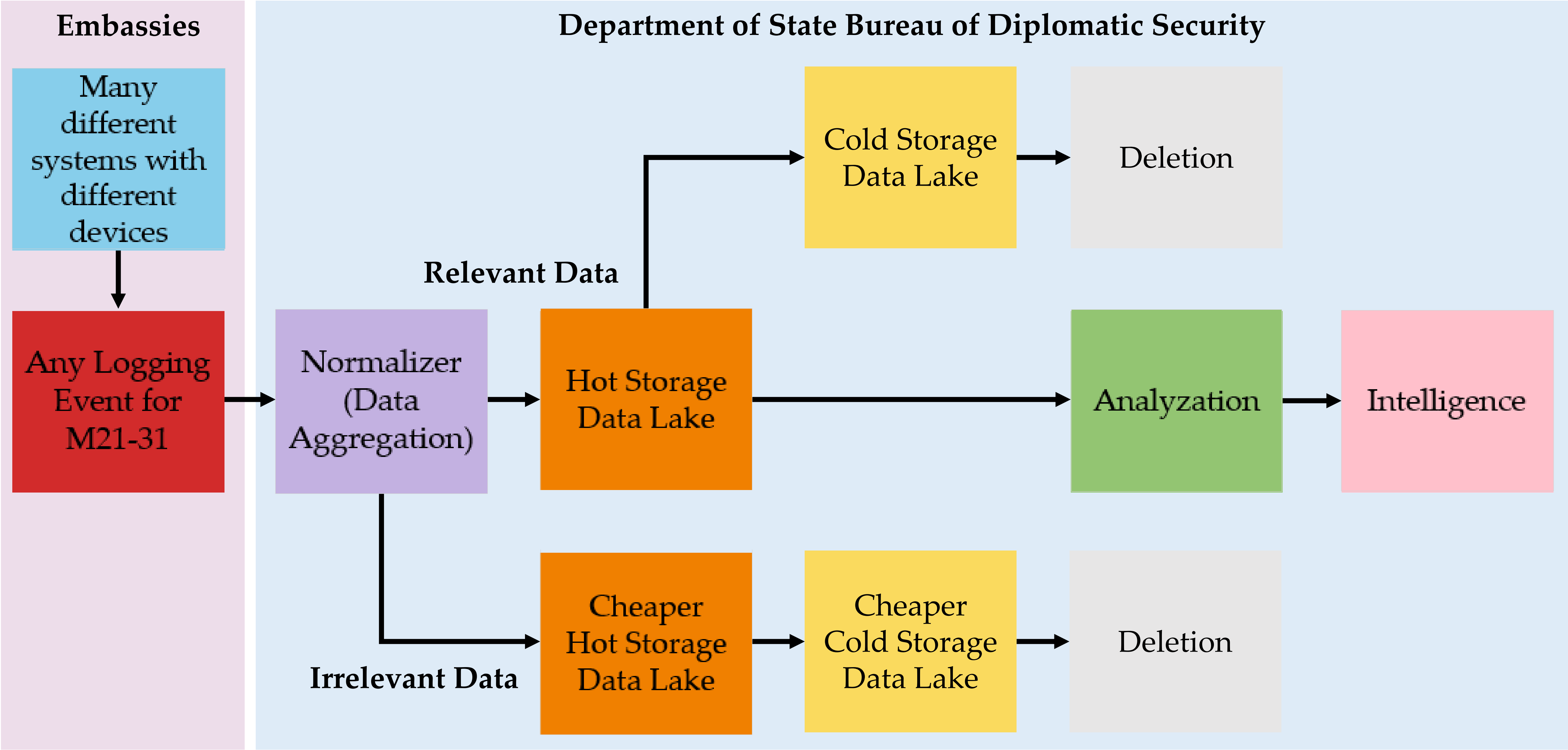
Mission Achievement/Impact Factors

Access to all Memorandum 21-31 logs 🟦🟨
Capable storage for all logs 🟩
Vendor Agnosticity 🟩🟥🟧🟨🟦
Data Governance support and stakeholder buy-in 🟦🟨

DESIGNED BY: Strategyzer AG & Steve Blank
The makers of Business Model Generation and Strategyzer

Strategyzer
strategyzer.com

Week 10 - Final MVP


Embassies

Department of State Bureau of Diplomatic Security

Many different systems with different devices

Any Logging Event for M21-31

Normalizer (Data Aggregation)

Relevant Data

Hot Storage Data Lake

Cold Storage Data Lake

Deletion

Analyzation

Intelligence

Irrelevant Data

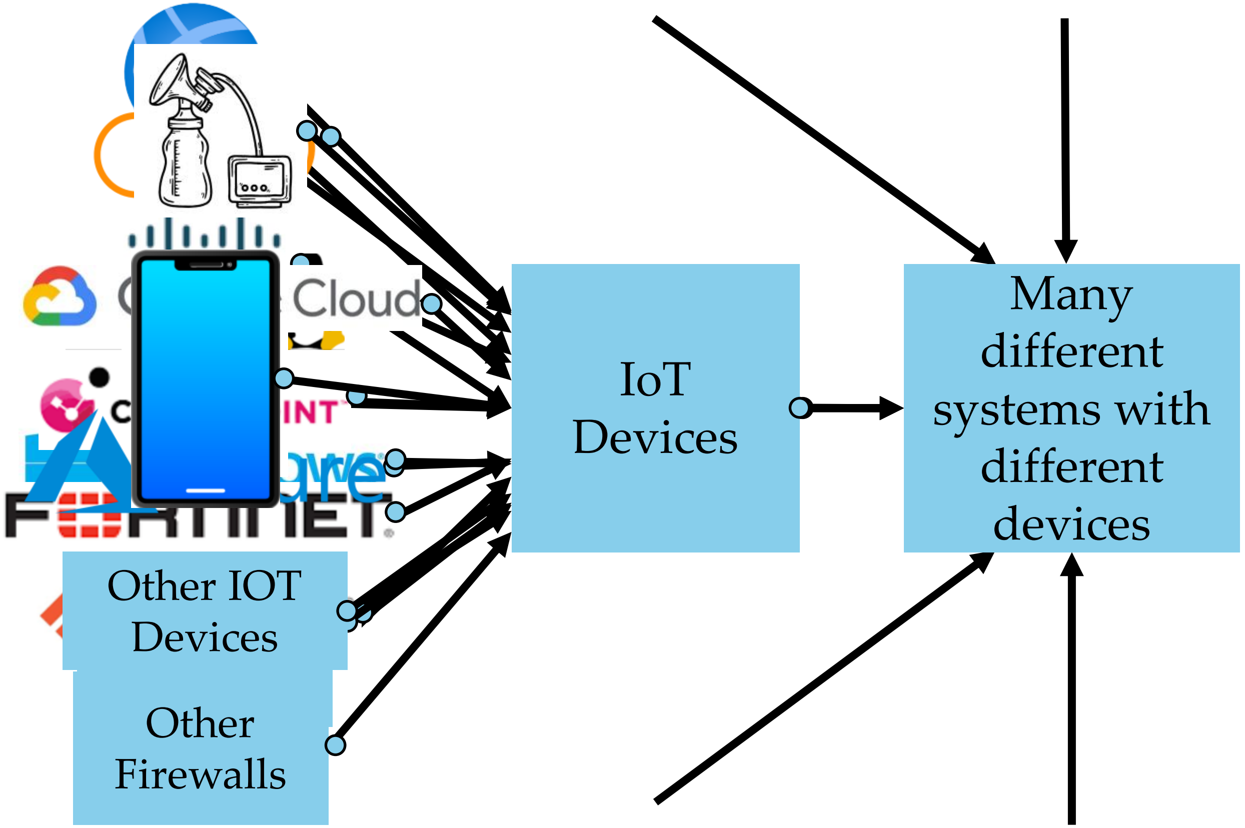
Cheaper Hot Storage Data Lake

Cheaper Cold Storage Data Lake

Deletion

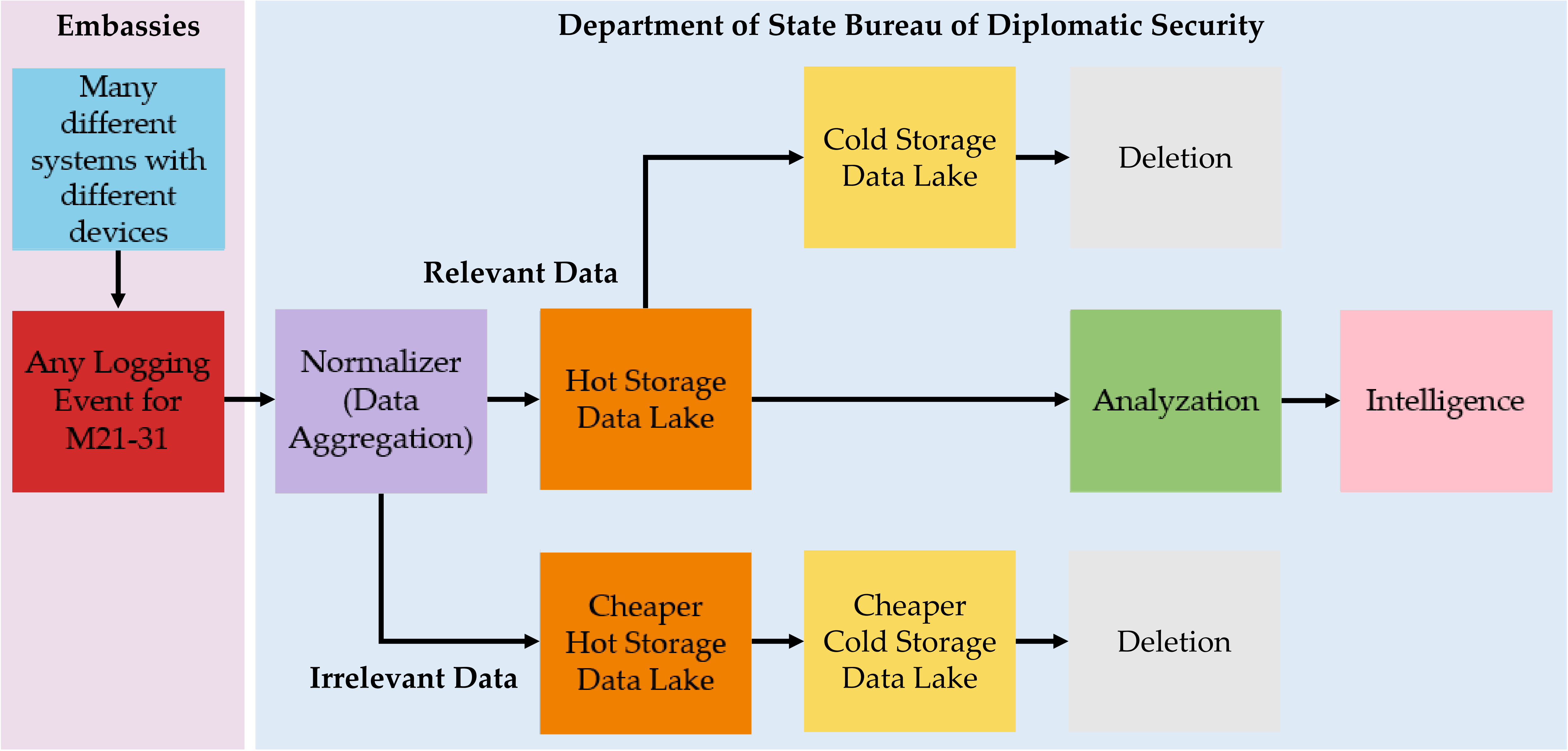
Step 1 - Sources

Embassies Side



- ❖ Each embassy will collect all of their source logs
- ❖ Every data source will be categorized by its type
- ❖ Including all
  - ❖ Operating Systems
  - ❖ Networking Devices
  - ❖ Firewalls
  - ❖ Cloud Devices
  - ❖ IoT Devices

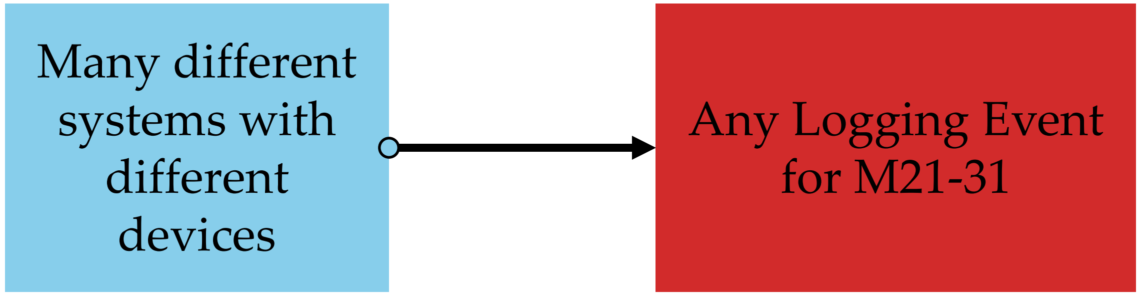
Week 10 - Final MVP



Embassies
Department of State Bureau of Diplomatic Security
Many different systems with different devices
Any Logging Event for M21-31
Normalizer (Data Aggregation)
Relevant Data
Hot Storage Data Lake
Cold Storage Data Lake
Deletion
Analyzation
Intelligence
Irrelevant Data
Cheaper Hot Storage Data Lake
Cheaper Cold Storage Data Lake
Deletion

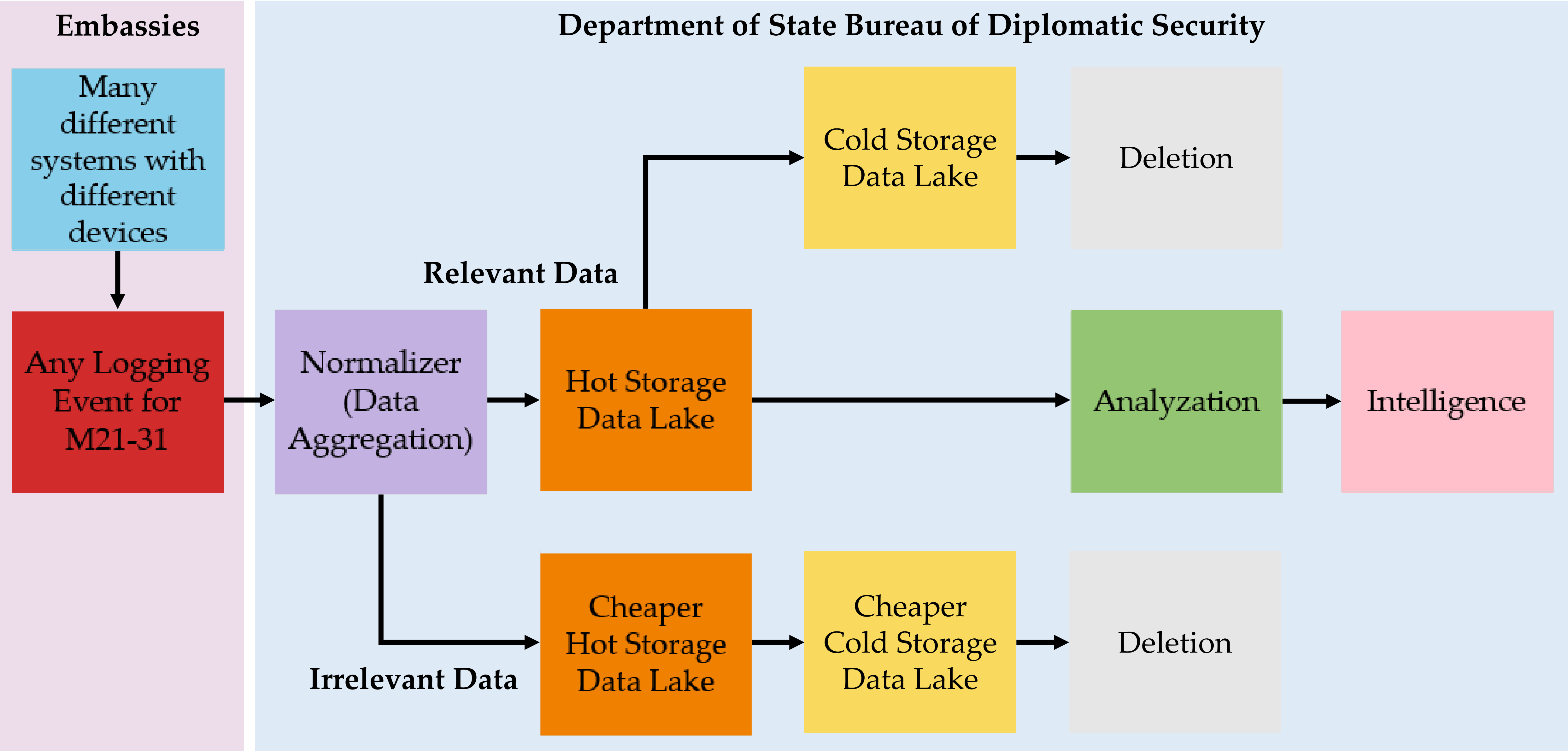
Step 2 - M21-31 Logging Event

Embassies Side


Many different systems with different devices
Any Logging Event for M21-31

- All gathering of data & logs must be compliant to Memorandum 21-31
- Developed to ensure centralized visibility for Security Operations Center (SOC) of federal agencies.
- It addresses:
  - Logging
  - Log retention
  - Log management

Week 10 - Final MVP



Embassies

Department of State Bureau of Diplomatic Security

Many different systems with different devices

Any Logging Event for M21-31

Normalizer (Data Aggregation)

Relevant Data

Hot Storage Data Lake

Cold Storage Data Lake

Deletion

Analyzation

Intelligence

Irrelevant Data

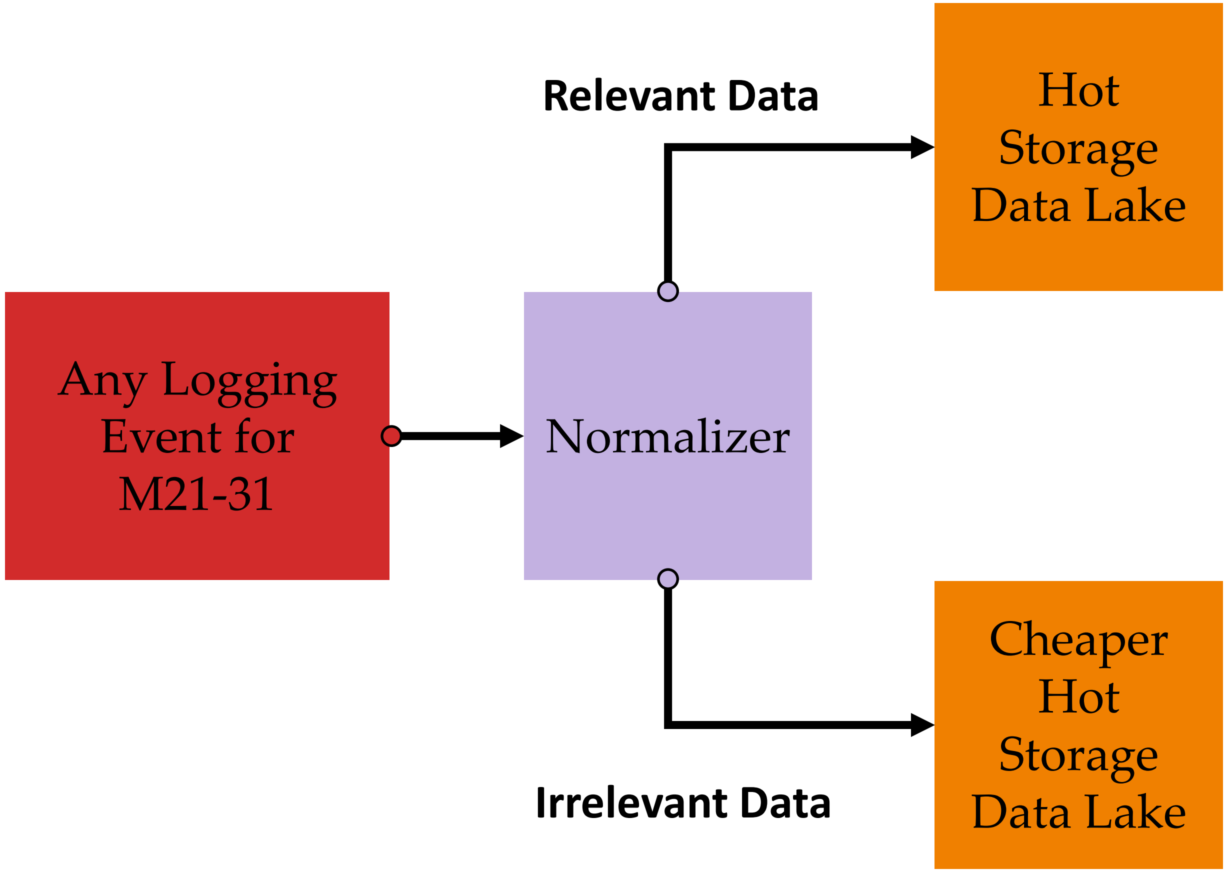
Cheaper Hot Storage Data Lake

Cheaper Cold Storage Data Lake

Deletion

Step 3 - Normalizer

DoS Side



- Categorized logs are sent to the normalizer
- Makes sure logs will be tagged with its source
- Normalizer aggregates all the data and logs
- Analyze and classify each log as relevant or irrelevant
  - **Relevant:** This log will help in investigation and is useful
  - **Irrelevant:** This log may not help, not have useful info and potentially wastes space

Recommend Software Solutions – Normalizer

Cribl®

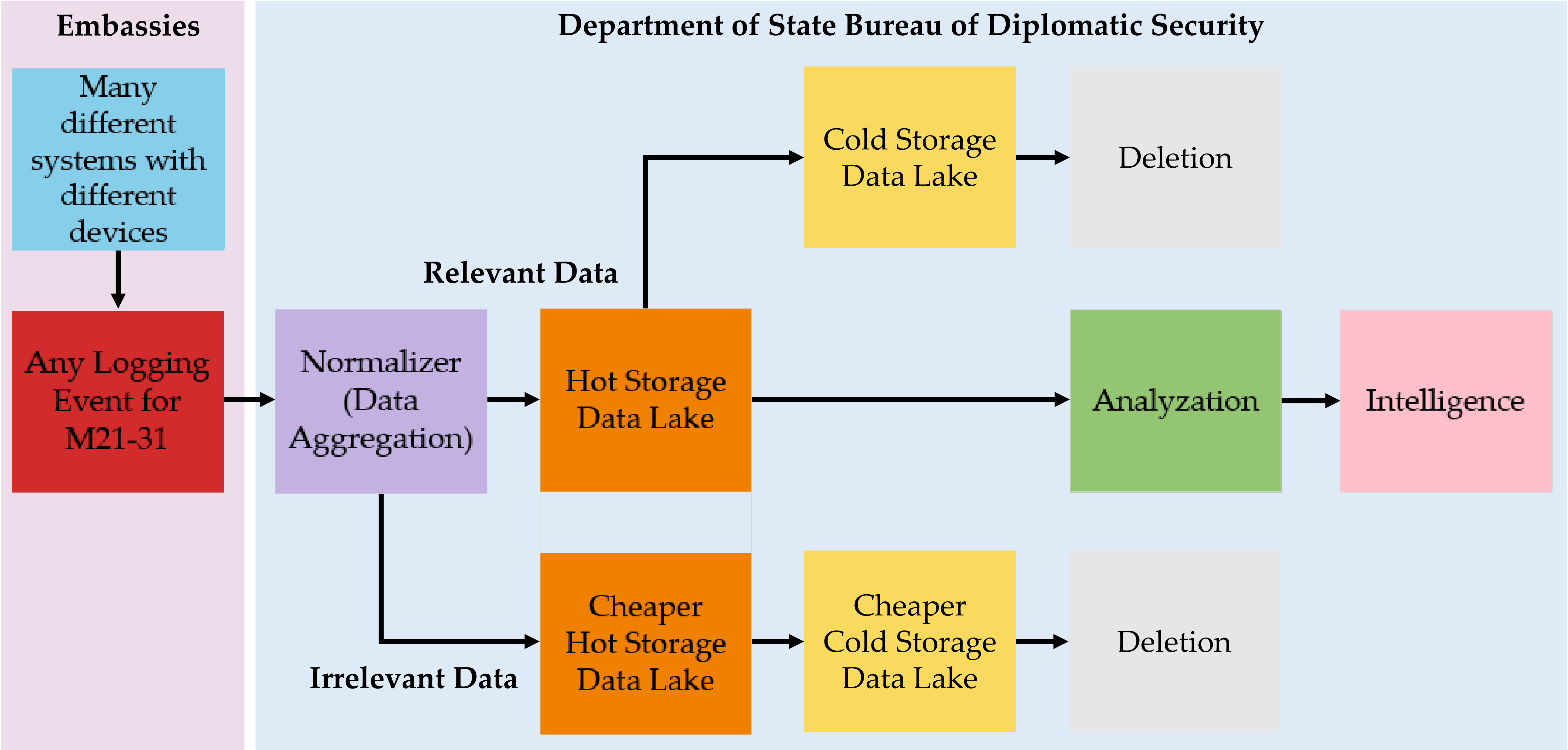
Pros:

- Universal Receiver
- Dashboard – Easy to understand/use, can click and drag sources to destinations
- Integration with other software including other recommended software.

Cons:

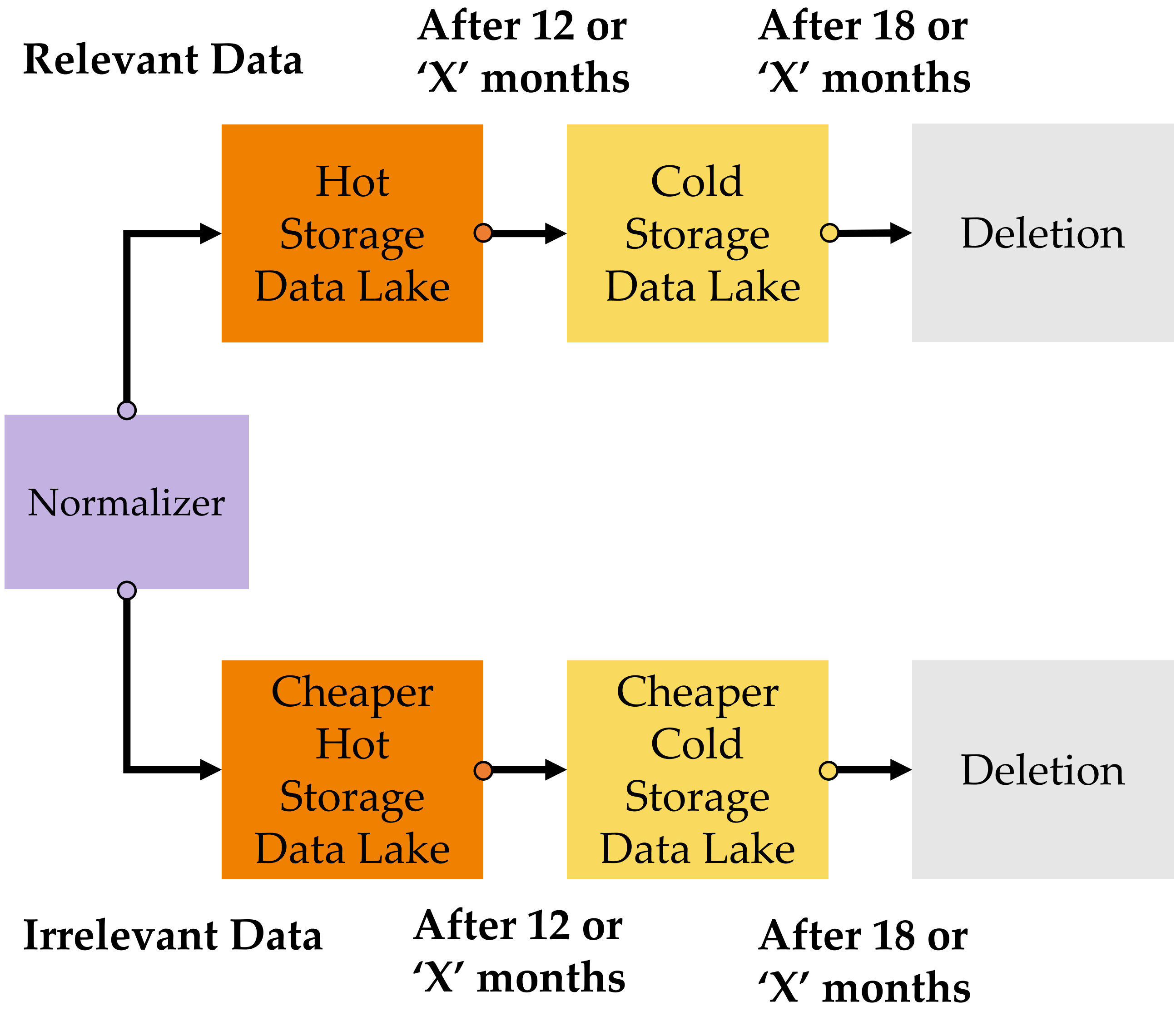
- No Artificial Intelligence or Machine Learning functionality

Week 10 - Final MVP


Embassies
Department of State Bureau of Diplomatic Security
Many different systems with different devices
Any Logging Event for M21-31
Normalizer (Data Aggregation)
Relevant Data
Hot Storage Data Lake
Cold Storage Data Lake
Deletion
Analyzation
Intelligence
Irrelevant Data
Cheaper Hot Storage Data Lake
Cheaper Cold Storage Data Lake
Deletion

Steps 4, 5, & 6 - Data Storage

DoS Side



- Data will be stored in a Data Warehouse in the Department of State
- Relevant data and irrelevant data will be split up into different data lakes for cost and relevance
- Mandated in M21-31:
  - After 12-'X' months in hot storage, data will be moved to cold storage
  - After 18-'X' months in cold storage, data will be deleted

Recommend Software Solutions – Data Storage

databricks

Pros:

- Pricing based on computing usage
- Auto-scaling
- Real-time data lineage

Cons:

- Only at-rest encryption on data

snowflake

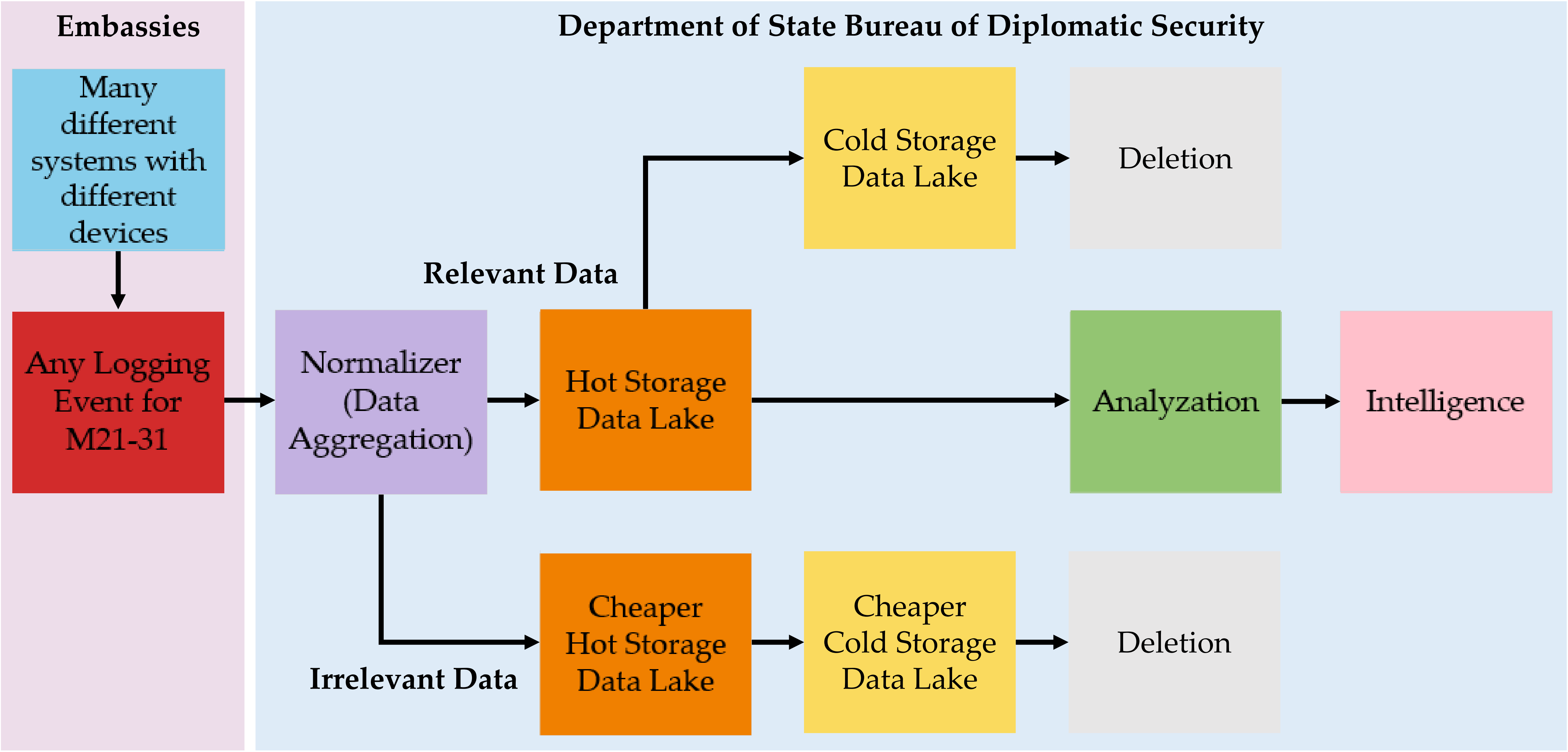
Pros:

- At-rest and in-transit encryption on data
- Good scaling capabilities
    - Easy to increase and decrease size of data warehouse based on needs

Cons:

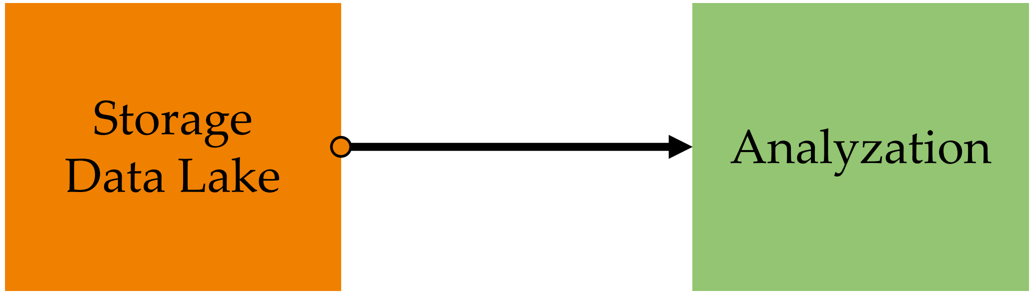
- Pricing based on storage volume
- No auto-scaling – not as fast

Week 10 - Final MVP


Embassies
Department of State Bureau of Diplomatic Security
Many different systems with different devices
Any Logging Event for M21-31
Normalizer (Data Aggregation)
Relevant Data
Hot Storage Data Lake
Cold Storage Data Lake
Deletion
Analyzation
Intelligence
Irrelevant Data
Cheaper Hot Storage Data Lake
Cheaper Cold Storage Data Lake
Deletion

Step 7 - Analyze

DoS Side



- ❖ The SIEM tool will pull the data from the data lakes
- ❖ The SIEM tool will display all the data to showcase what is happening on the network & sources

Recommend Software Solutions – Analysis

splunk>

Pros:

- Current SIEM tool
- Well integrated data collection and analysis

Cons:

- Current contract is expensive
- Not easy to get data out of Splunk once it is put in (indexed)

Azure

Sentinel

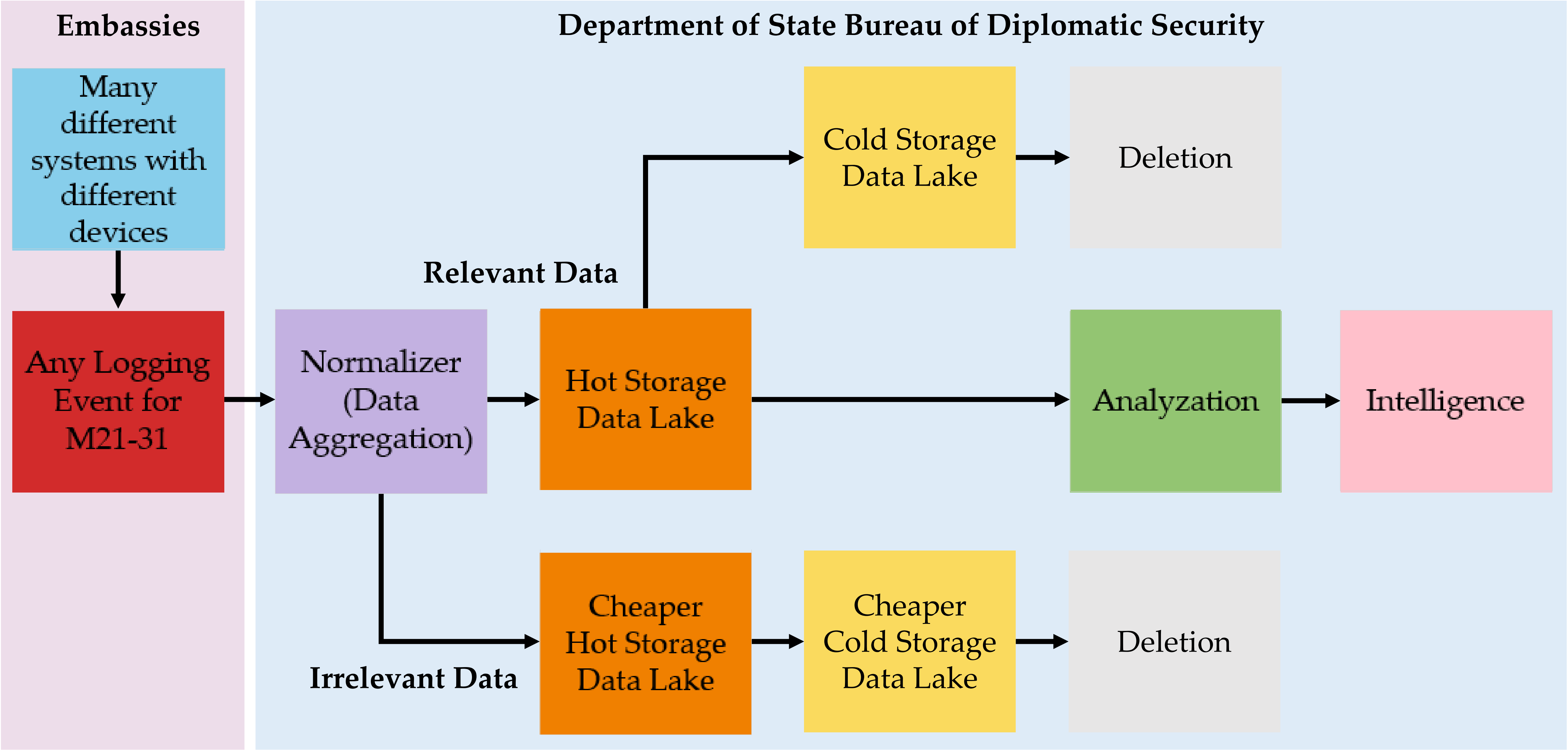
Pros:

- Use of historical data (can bring from cold to hot)
- Artificial Intelligence and Machine Learning
  - Includes behavioral analysis data and task automation

Cons:

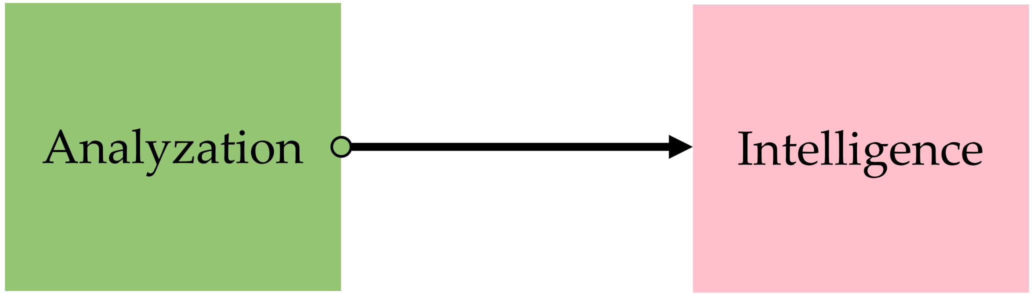
- Complex pricing system

Week 10 - Final MVP


Embassies
Department of State Bureau of Diplomatic Security
Many different systems with different devices
Any Logging Event for M21-31
Normalizer (Data Aggregation)
Relevant Data
Hot Storage Data Lake
Cold Storage Data Lake
Deletion
Analyzation
Intelligence
Irrelevant Data
Cheaper Hot Storage Data Lake
Cheaper Cold Storage Data Lake
Deletion

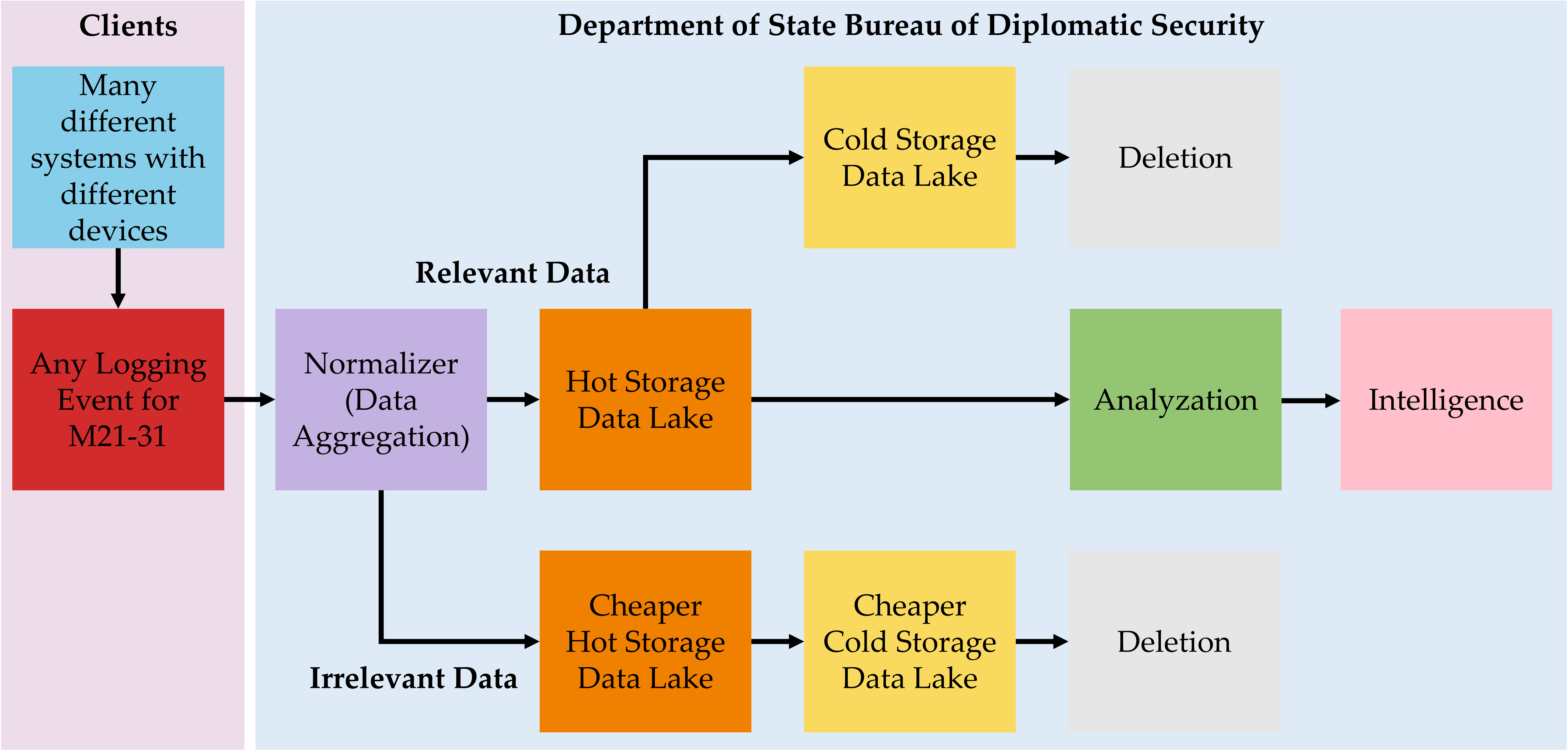
Step 8 - Intelligence

DoS Side



- Analysts at DoS will analyze & examine the data for any malicious incidents.
- DoS Analysts will work with the embassies to remediate the issue.
- Once the issue is resolved, embassies and the DoS Analysts will make sure to prevent similar events from happening in the future

Week 10 - Final MVP


Clients
Department of State Bureau of Diplomatic Security
Many different systems with different devices
Any Logging Event for M21-31
Normalizer (Data Aggregation)
Relevant Data
Hot Storage Data Lake
Cold Storage Data Lake
Deletion
Analyzation
Intelligence
Irrelevant Data
Cheaper Hot Storage Data Lake
Cheaper Cold Storage Data Lake
Deletion

Onboarding Notes

- Annual training highlighting new features, software updates, other changes
- Make sure current equipment can handle project
- Determine implementation on specific embassies with key metrics

> **"Training on software should be a continuous, long-term process."**
> **- Bryan Reinicke, MIS Capstone Professor**

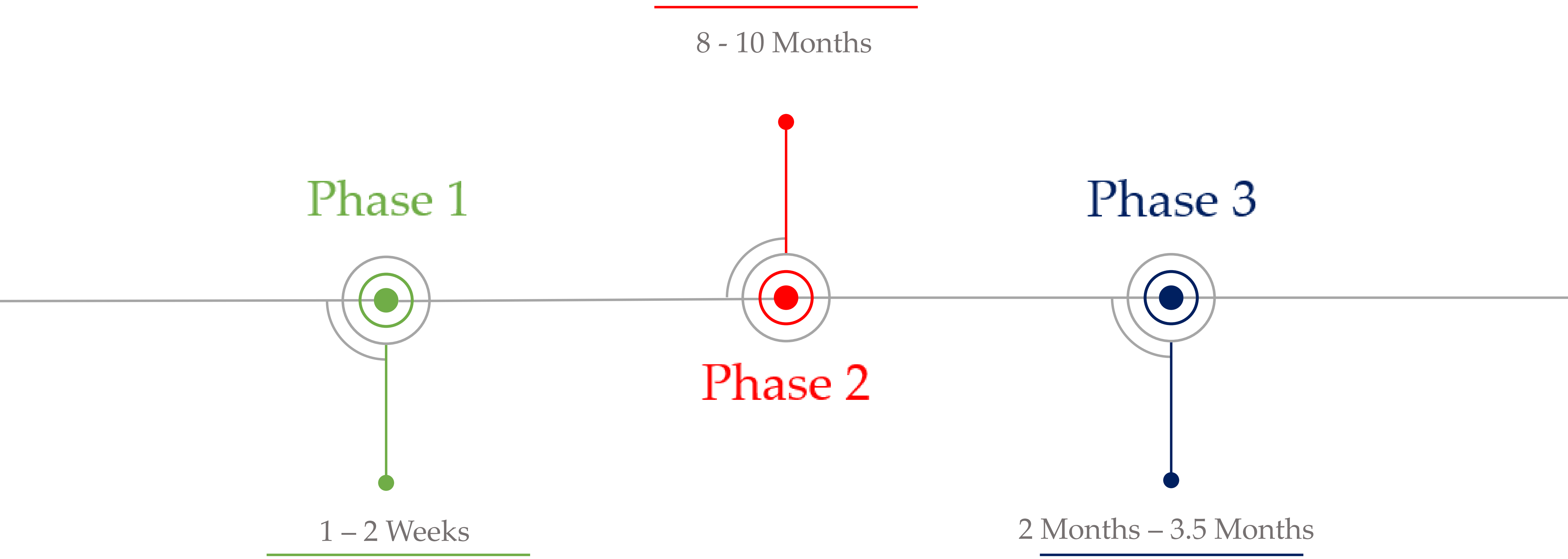
Disaster Recovery Notes

- Ensure any new software additions meet security standards and do not increase vulnerability.
- How long are servers active? 24 hours?
- What is risk tolerance?

> **"Backups, backups, backups!!!"**
> **– Paul Centanni, CISO at Acture Solutions**

Deployment – Overview

Approximate Total Time Length: 10.5 Months – 14 Months



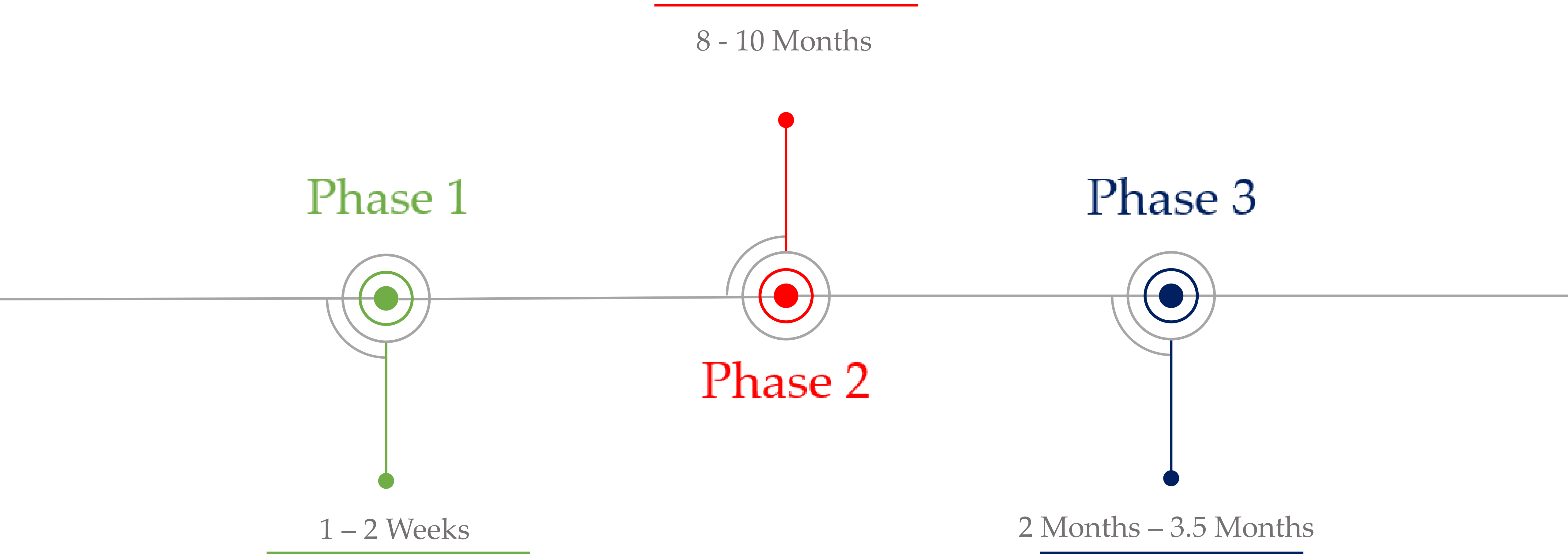
Deployment – Phase 1

		Month 1	
Phase 1		1-2 weeks – Introduce the Solution	

- ❖ The focus of Phase 1 be introducing the solution to sponsors and senior management.
  - ❖ Share research on software
  - ❖ Develop estimates of implementation time
  - ❖ Outlining risk management process, key performance indicators, and goals.

Deployment – Overview

Approximate Total Time Length: 10.5 Months – 14 Months



8 - 10 Months

Phase 1

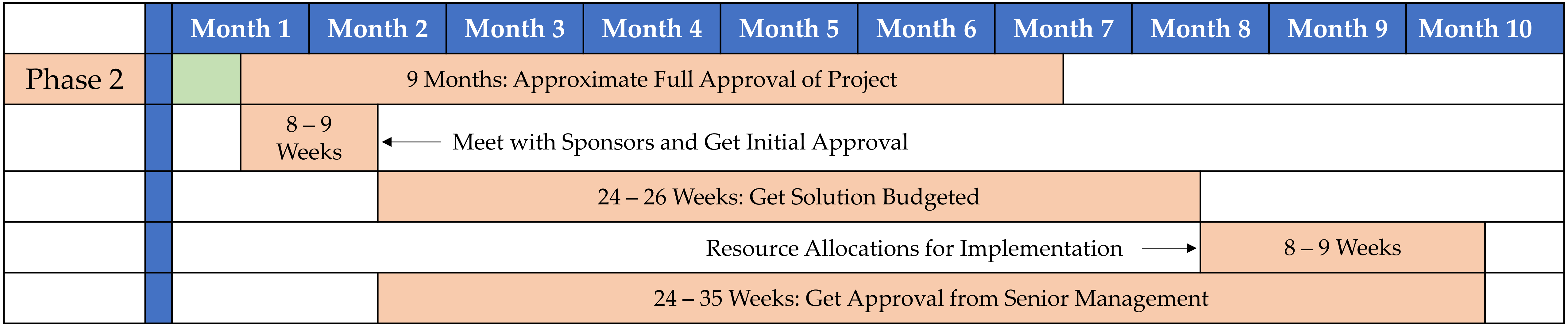
Phase 2

Phase 3

1 – 2 Weeks

2 Months – 3.5 Months

Deployment – Phase 2



Month 1 | Month 2 | Month 3 | Month 4 | Month 5 | Month 6 | Month 7 | Month 8 | Month 9 | Month 10

Phase 2

9 Months: Approximate Full Approval of Project

8 – 9 Weeks

Meet with Sponsors and Get Initial Approval

24 – 26 Weeks: Get Solution Budgeted

Resource Allocations for Implementation

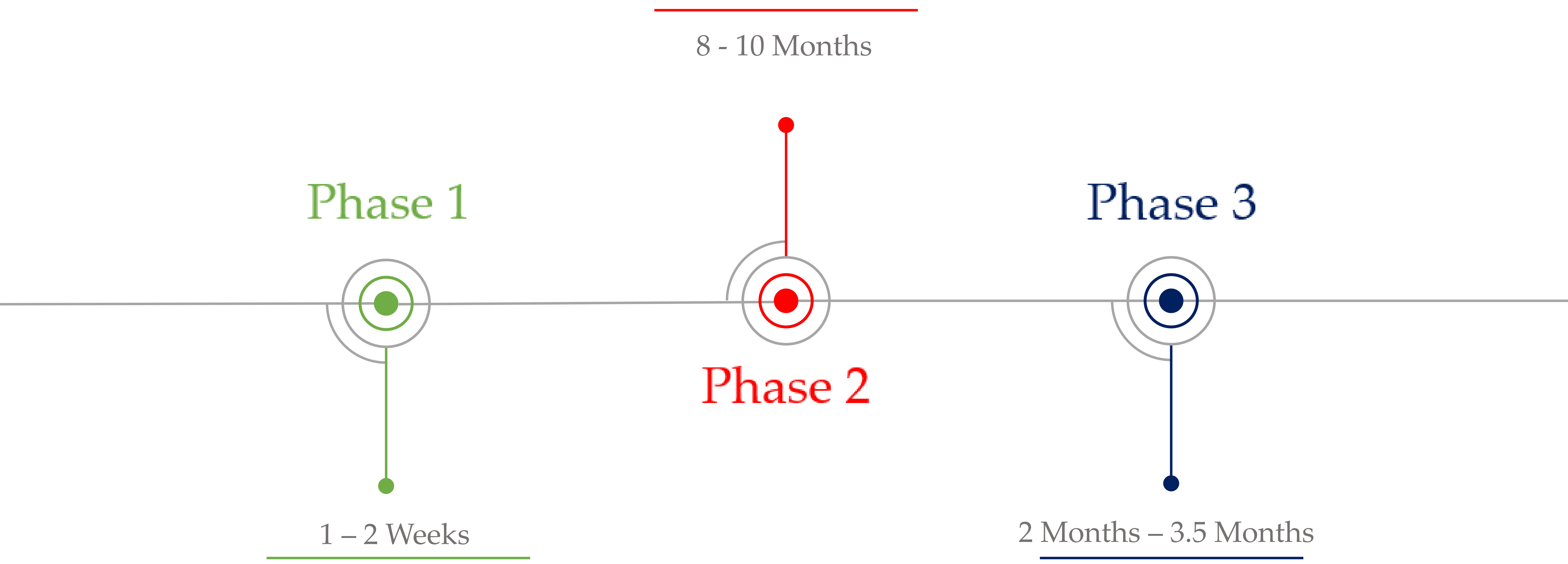
8 – 9 Weeks

24 – 35 Weeks: Get Approval from Senior Management

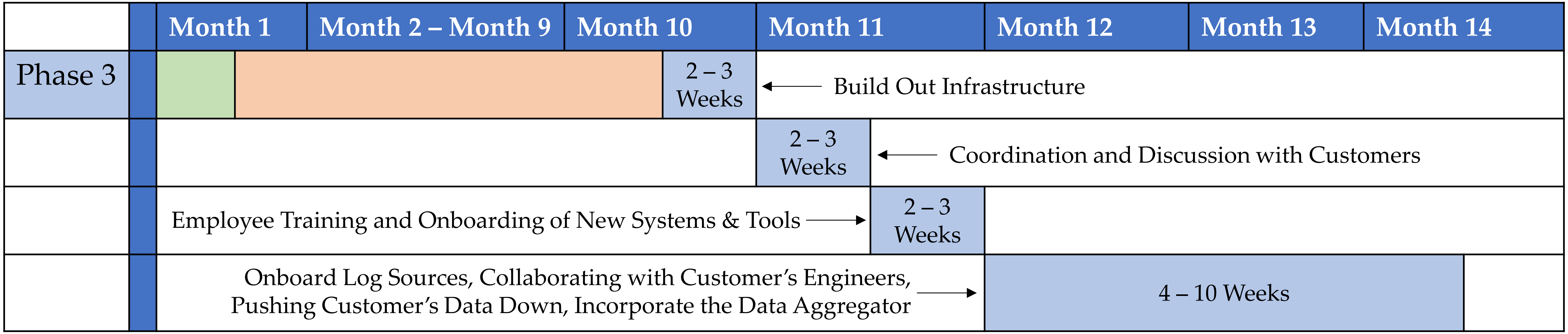
- The focus of Phase 2 will be approval and resource allocation.
    - Official project approval from senior management
    - Budgeting and cost projection
    - Resource allocation
        - Hardware, software, personnel

Deployment – Overview

Approximate Total Time Length: 10.5 Months – 14 Months



Deployment – Phase 3



Month 1

Month 2 – Month 9

Month 10

Month 11

Month 12

Month 13

Month 14

Phase 3

2 – 3 Weeks ← Build Out Infrastructure

2 – 3 Weeks ← Coordination and Discussion with Customers

Employee Training and Onboarding of New Systems & Tools → 2 – 3 Weeks

Onboard Log Sources, Collaborating with Customer's Engineers, Pushing Customer's Data Down, Incorporate the Data Aggregator → 4 – 10 Weeks

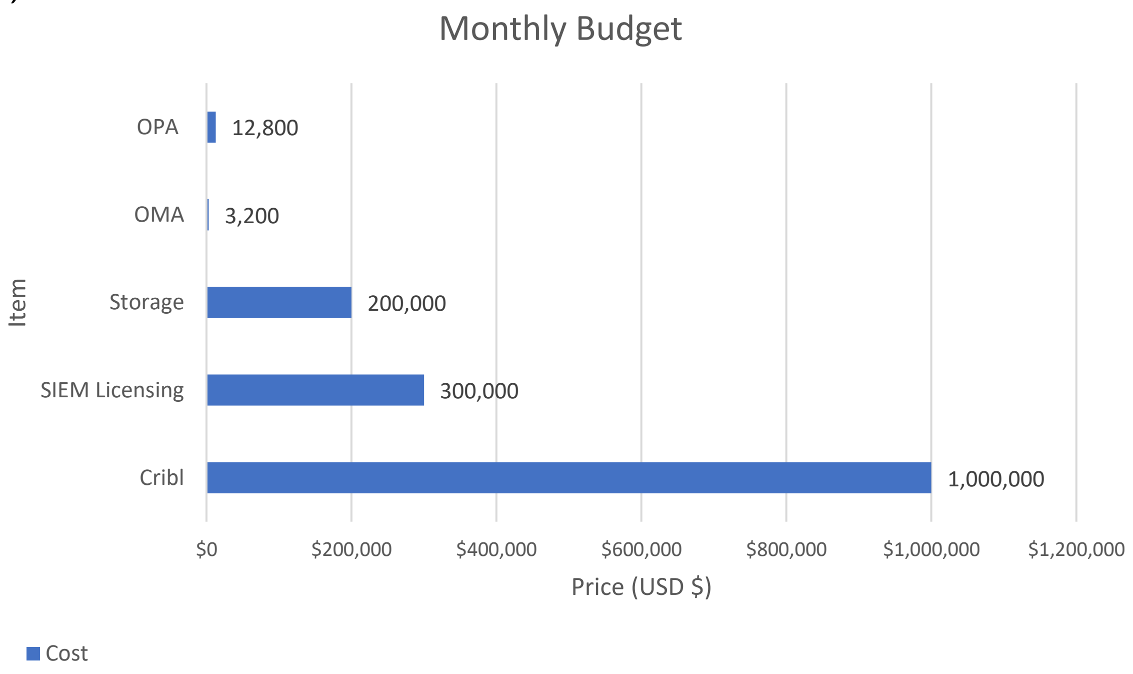
- The focus of Phase 3 will be onboarding and deployment.
  - Onboarding logs and data
  - Implementing new software
  - Training employees

Monthly Budget

Implementation:

- ❖ Data Normalizer software (Cribl): $1,000,000
- ❖ Cost of licensing and use of Data Lake Storage: $200,000
- ❖ SIEM Licensing and use: $250,000
- ❖ OMA cost of system maintenance per month: $3,200
- ❖ OPA cost for system implementation: $12,800

Total: $1,516,000



Special Thanks

Thank you, Nick, Danh, and Jake, and our other Sponsors!

Special Thanks

Thank you to all the people we interviewed!

Manny Medrano

Ozan Ertugrul

Gharun Lacy

David Hagan

Andy Meneely

Alex McPherson

Christine Shely

Carlos R. Rivero

Ken Miller

Tom Kopchak

Brian Bullis

Bob LaBanz

Danh Nguyen-Huynh

Jeremy Brown

Dave Ballard

Bryan Reinicke

Sara Kastner

David Kirk

Roy Matthews

Mohammed Saidur

Ray Romano

David Loshin

Ali Tosyali

Quang Bui

James Bridgen

Justin Balroop

Kyle Smith

Nick Swindell

Steve Krause

Chad Rooney

John Topp

Jim Santa

Michael Wofford

Bill Stackpole

Myra Rowell

Anthony Henry

Rob

Paul Centanni

Sean Doran

Mark Johnson

Carl Randall

Jon-Michael Lacek

Mehdi Mirakhorli

Jose Rivera-Ortiz

Nick Ortiz

Michael Kelly

Rob Naik

Demetrius J Gooden

Jake Trigboff

Mike Pinch

Ian James

Rob Mennell

Saikat Biswas

Nate Matthews

Bob Adams

James H. Moore

Brett Morgan

Maxwell Baron

Special Thanks

Thank you to our mentor Rob!

Special Thanks

Thank you, Jim Santa and Suvam!

Questions?