TEAM 1

CAPSTONE

Project Plan Proposal

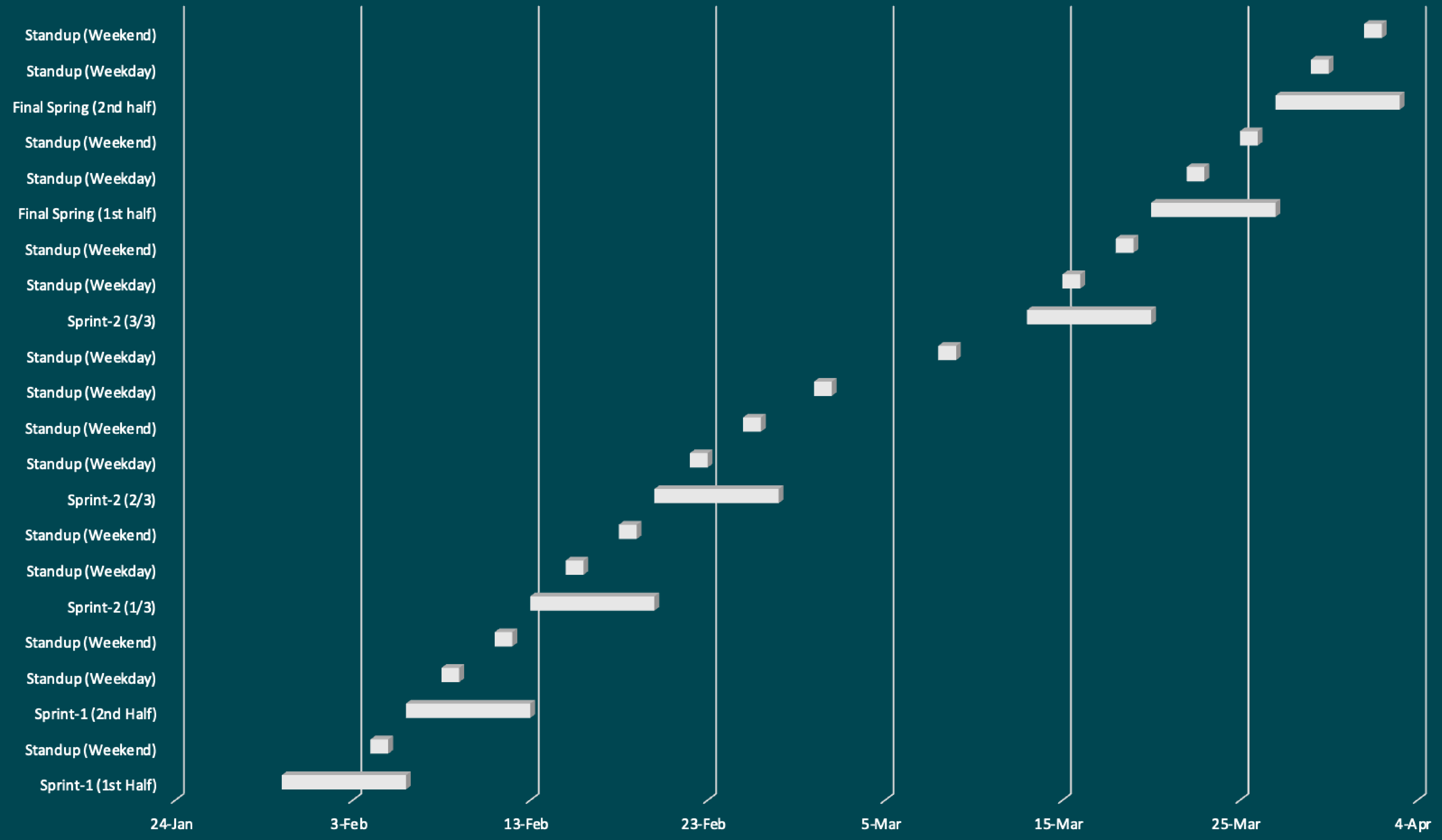
Agenda

- Introduction
- Capstone Timeline
- MITRE Adversary Emulation Plan
- Security Logs Monitoring System
- PostQuantum Cryptography

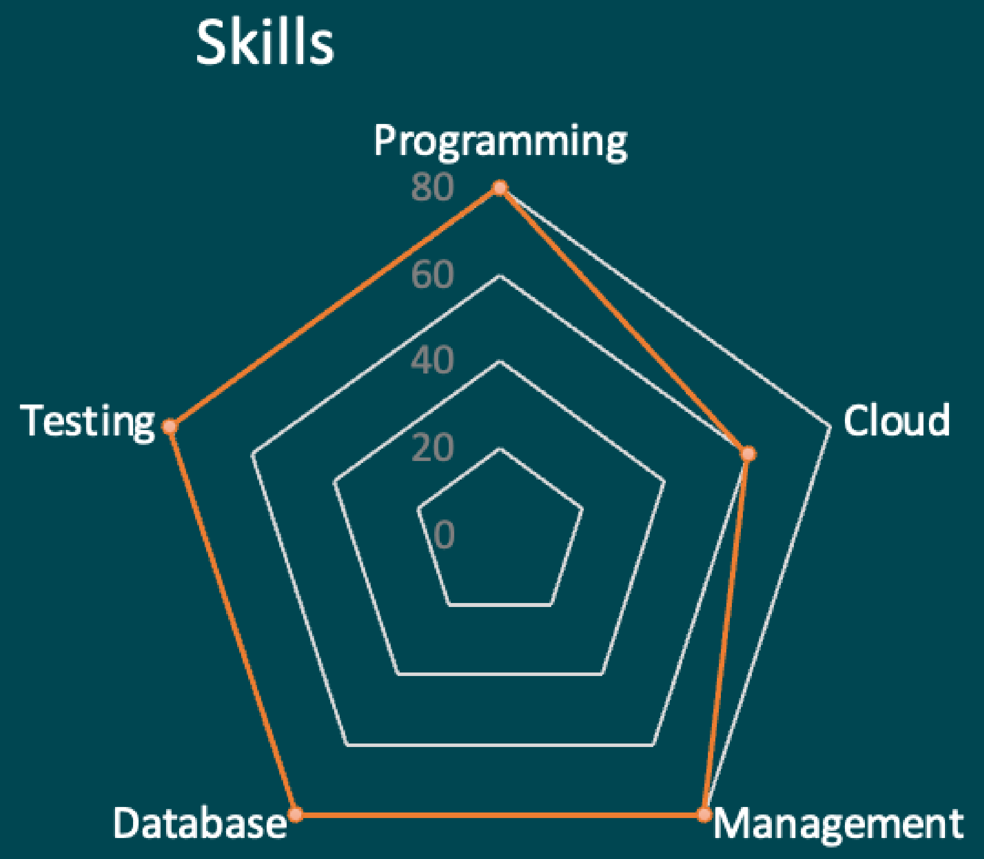
- What is the problem?
- Why are we solving this?
- Execution Timeline
- Methodology

- Questions and Feedback

Calendar


Standup (Weekend)
Standup (Weekday)
Final Spring (2nd half)
Standup (Weekend)
Standup (Weekday)
Final Spring (1st half)
Standup (Weekend)
Standup (Weekday)
Sprint-2 (3/3)
Standup (Weekday)
Standup (Weekday)
Standup (Weekend)
Standup (Weekday)
Sprint-2 (2/3)
Standup (Weekend)
Standup (Weekday)
Sprint-2 (1/3)
Standup (Weekend)
Standup (Weekday)
Sprint-1 (2nd Half)
Standup (Weekend)
Sprint-1 (1st Half)
24-Jan
3-Feb
13-Feb
23-Feb
5-Mar
15-Mar
25-Mar
4-Apr

Who are we?


Skills

Parth Shukla

- CEH Certified
- Python, Bash
- AWS
- VAPT, Bug-Bounties

Peter Psyllos

- Python, C/C++, Matlab, R
- AWS
- Risk Management

Shreyas Nair

- PKI, SecOps, IAM
- Python, JS, Bash
- AWS, Azure DevOps, Terraform, K8s
- AppSec / Prod Sec

Nishant Jain

- AppSec, Bug-Bounties & Pentest
- Python, Go, JS
- AWS
- Web Dev

Yiduo Gu

- Python, C/C++, Matlab
- AWS

MITRE

Adversary Emulation Plan

CALDERA

Overview

Apply MITRE ATT&CK framework and tools to map a real-world cyber incident.

Use the Caldera tool to complete an emulation plan

Deploy a mock scenario in Cloud to represent a compromised system

Key Takeaways

Enhance the team's knowledge and understanding of MITRE ATT&CK framework and tools

Improve the team's incident response and emulation planning capabilities

Purpose

Provide a Comprehensive, Structured, and actionable view of TTPs used by adversaries in cyber attacks

Understand the potential attack scenarios and develop effective defense strategies

Simulating certain scenarios provide vital intel for companies to have a tangible plan

transition from reactive to proactive defense methedologies

Timeline

Sprint 1 | Feb 6 - 12

- Study and familiarize with the MITRE ATT&CK framework and tools.
- Identify a real-world cyber incident to map using the MITRE ATT&CK framework and tools.

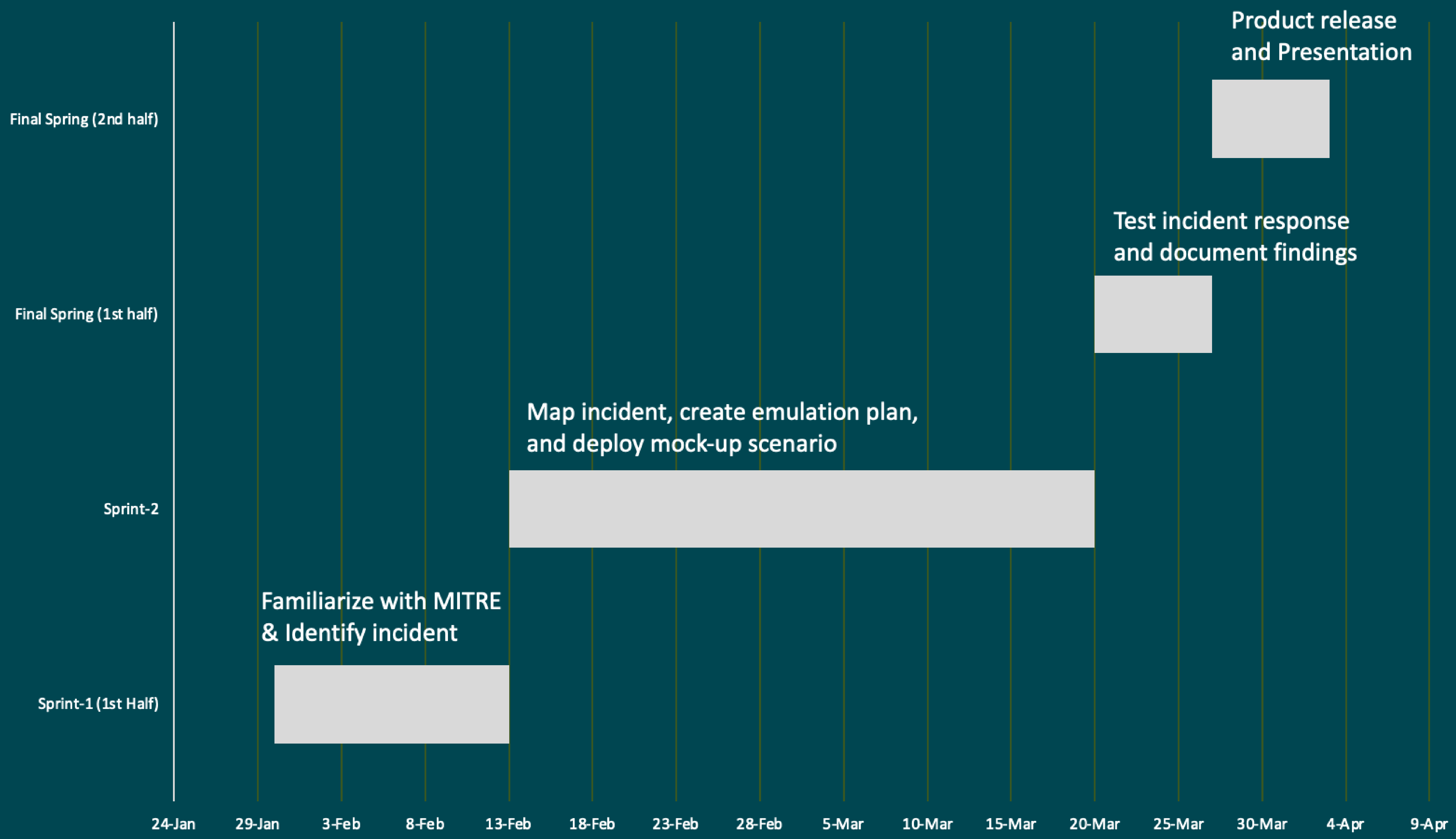
Sprint 2 | Feb 13 - Mar 20

- Map the real-world cyber incident using the MITRE ATT&CK framework and tools.
- Create an emulation plan using the Caldera tool.
- Deploy a mock-up scenario in the cloud that represents the system that was compromised in the studied cyber incident.

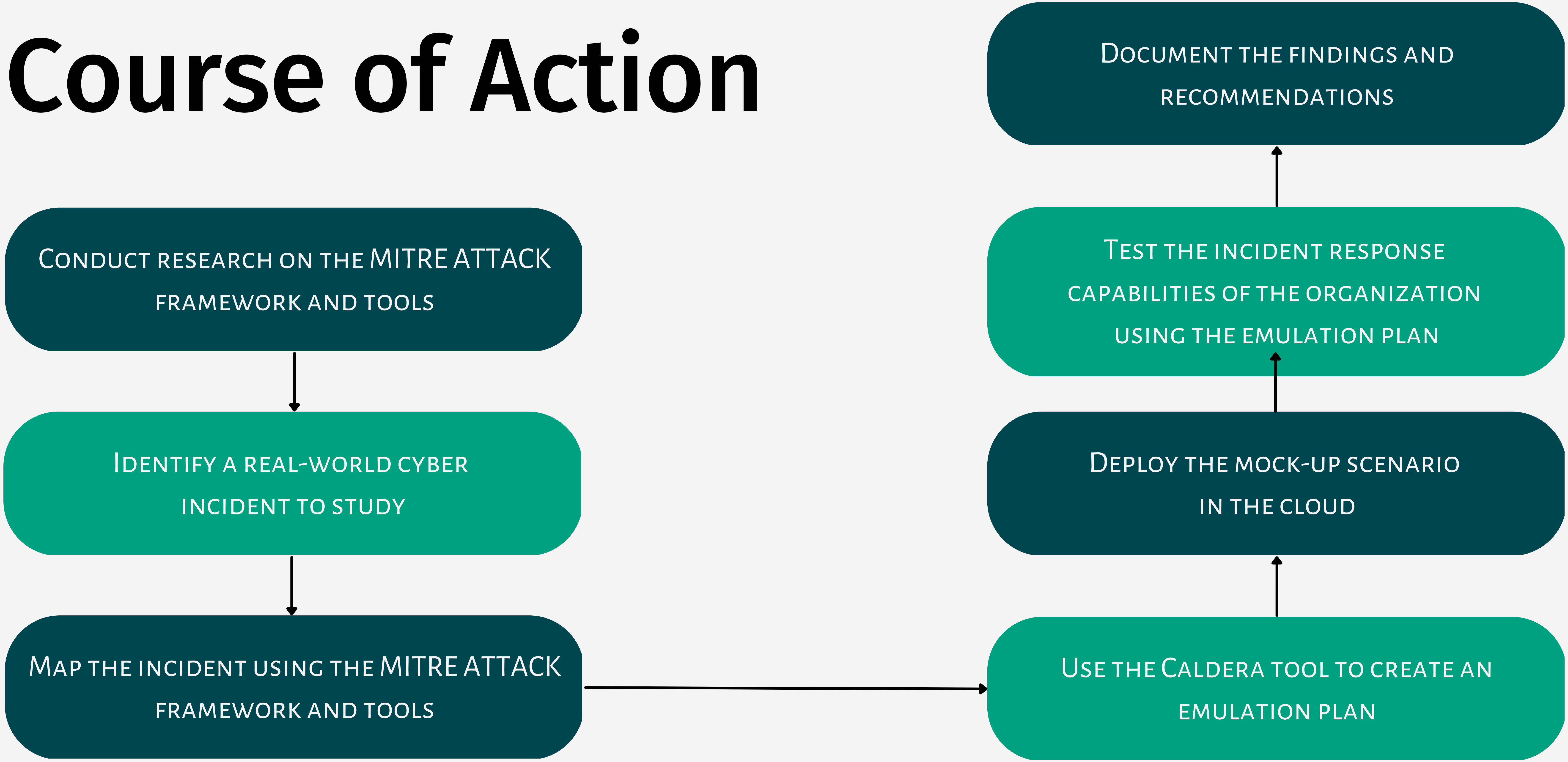
Sprint 3 | Mar 20 - Apr 3

- Test the incident response capabilities of the organization using the emulation plan.
- Document the findings and recommendations.

Calendar


Product release
and Presentation
Test incident response
and document findings
Map incident, create emulation plan,
and deploy mock-up scenario
Familiarize with MITRE
& Identify incident
Final Spring (2nd half)
Final Spring (1st half)
Sprint-2
Sprint-1 (1st Half)
24-Jan
29-Jan
3-Feb
8-Feb
13-Feb
18-Feb
23-Feb
28-Feb
5-Mar
10-Mar
15-Mar
20-Mar
25-Mar
30-Mar
4-Apr
9-Apr

Course of Action



Conduct research on the MITRE ATTACK framework and tools

Identify a real-world cyber incident to study

Map the incident using the MITRE ATTACK framework and tools

Use the Caldera tool to create an emulation plan

Deploy the mock-up scenario in the cloud

Test the incident response capabilities of the organization using the emulation plan

Document the findings and recommendations

PostQuantum Cryptography

Challenges and Adoption

Overview

As Quantum computing revolutionizes compute, it poses a significant threat to current crypto methods

Post-quantum cryptography aims to address this threat by developing new cryptographic algorithms that are resistant to quantum attacks

Assess challenges of Implementing PQC

Key Takeaways

Enhance the team's knowledge of cryptography, Public Key Infrastructure, Quantum cryptography and Post Quantum Cryptography

Understand and Address challenges of implementing Post Quantum Cryptography

Purpose

Security: Understand traditional cryptographic standards and how Post Quantum Cryptography can secure org' from quantum computing threats

Compliance: Many organizations are required to comply with regulations and standards that mandate the use of secure encryption

Interoperability: Standardization and compatibility are crucial for secure communication and data exchange between different systems and organizations.

Addressing the challenges in the adoption of post-quantum cryptography for compliance and interoperability

Timeline

Sprint 1 | Feb 6 - 12

- Study the challenges associated with the adoption of post-quantum cryptography

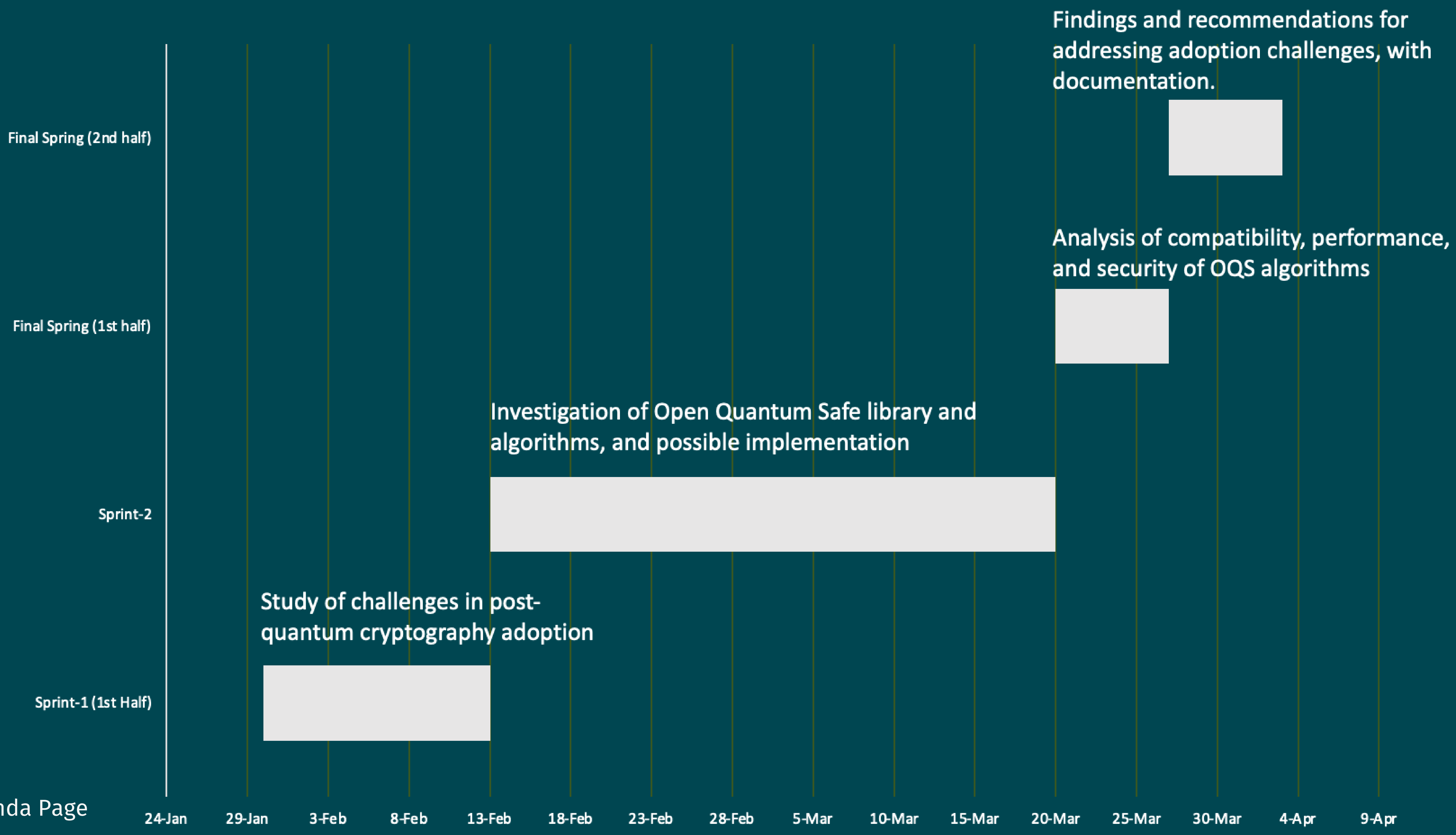
Sprint 2 | Feb 13 - Mar 20

- Investigate the use of the Open Quantum Safe library and its post-quantum algorithms
- Analyze the compatibility, performance, and security of the post-quantum algorithms included in OQS

Sprint 3 | Mar 20 - Apr 3

- Provide recommendations for addressing the challenges in the adoption of post-quantum cryptography
- Document the findings and recommendations

Calendar



Findings and recommendations for addressing adoption challenges, with documentation.

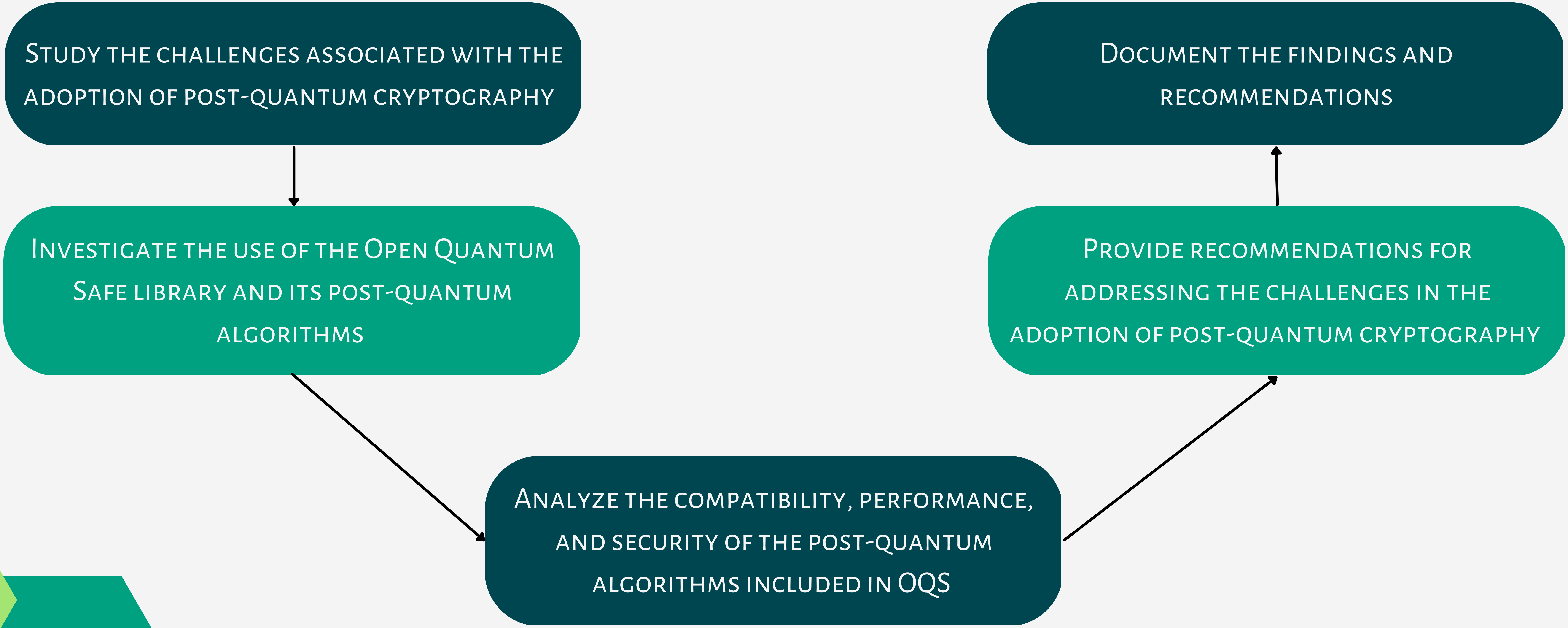
Analysis of compatibility, performance, and security of OQS algorithms

Investigation of Open Quantum Safe library and algorithms, and possible implementation

Study of challenges in post-quantum cryptography adoption

Back to Agenda Page

Course of Action



Study the challenges associated with the adoption of post-quantum cryptography

Investigate the use of the Open Quantum Safe library and its post-quantum algorithms

Analyze the compatibility, performance, and security of the post-quantum algorithms included in OQS

Provide recommendations for addressing the challenges in the adoption of post-quantum cryptography

Document the findings and recommendations

Security Logs Monitoring System

Overview

Deploy an enterprise architecture in the cloud that includes a variety of endpoints

Centralized log collector to forward local logs from all systems

Test and improve the system's security and incident response capabilities

Key Takeaways

Enhance the team's knowledge of designing and implementing a complex architecture to simulate DNS/SQL/Web Servers, Linux/Windows Machines and External Laptop and mobile devices.

Improve the teams knowledge on collecting security event logs and deriving valuable insights that assist during incident detection and mitigation

Purpose

CENTRALIZED LOG COLLECTION AND ATTACK SIMULATION IN THE CLOUD TO IMPROVE THE SECURITY AND MONITORING OF THE ARCHITECTURE

ANALYSIS OF LOG DATA FROM VARIOUS SOURCES, WHICH CAN HELP IDENTIFY POTENTIAL SECURITY THREATS AND VULNERABILITIES

SIMULATE ATTACKS TO TEST THE EFFECTIVENESS OF SECURITY MEASURES AND MAKE IMPROVEMENTS IN DEFENSE AGAINST COMMON ATTACK VECTORS

IDENTIFY AND MITIGATE POTENTIAL THREATS, AND ENSURE COMPLIANCE WITH REGULATORY REQUIREMENTS

Timeline

Sprint 1 | Feb 6 - 12

- Cloud deployment of enterprise architecture with a variety of endpoints

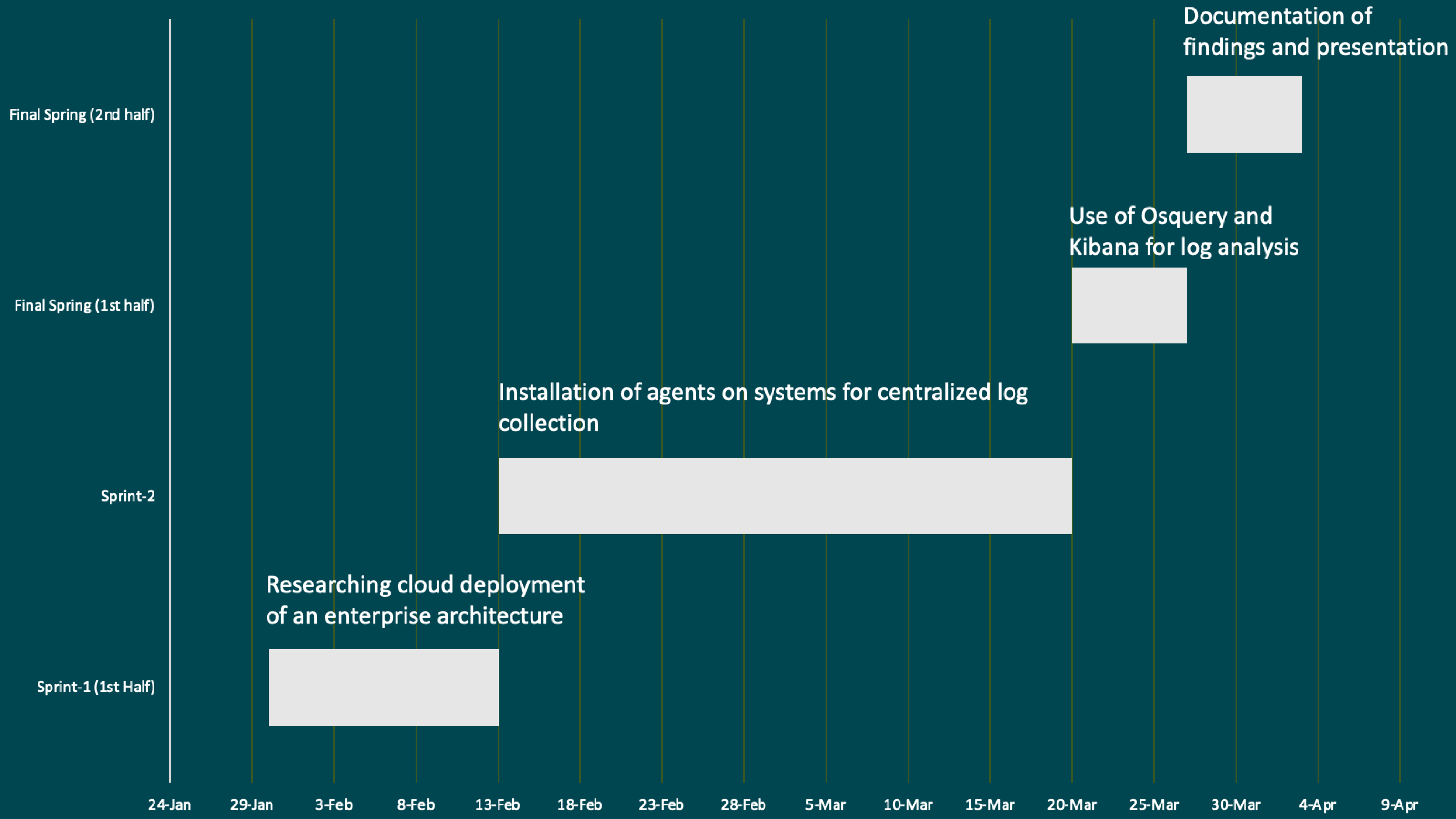
Sprint 2 | Feb 13 - Mar 20

- Installation of agents on all systems to forward local logs to a centralized log collector
- Use of Osquery and Kibana for centralized log collection and analysis

Sprint 3 | Mar 20 - Apr 3

- Simple simulation of attacks to trigger the logs of every system
- Documentation of findings and recommendations
- Product release

Calendar



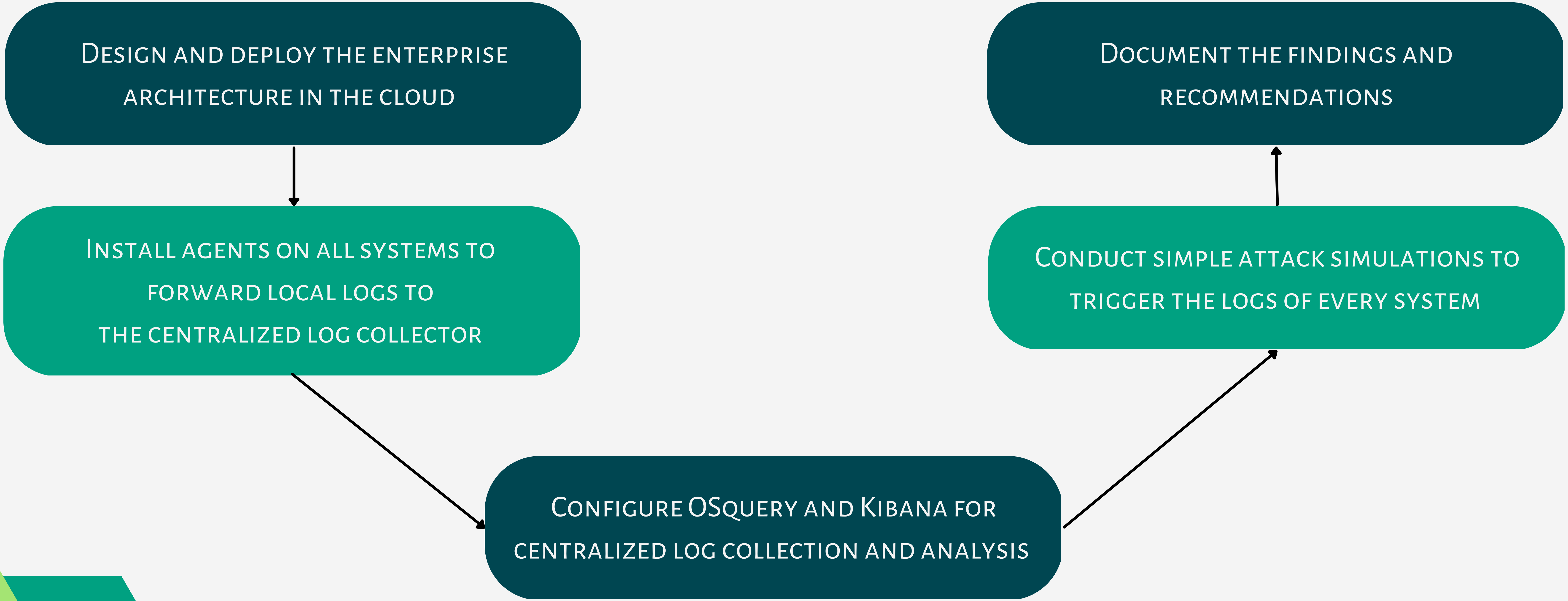
Researching cloud deployment of an enterprise architecture

Installation of agents on systems for centralized log collection

Use of Osquery and Kibana for log analysis

Documentation of findings and presentation

Course of Action



Design and deploy the enterprise architecture in the cloud

Install agents on all systems to forward local logs to the centralized log collector

Configure OSquery and Kibana for centralized log collection and analysis

Conduct simple attack simulations to trigger the logs of every system

Document the findings and recommendations

Thank you

Questions / Feedback?