Objectifying Your Incident Management

Robert Floodeen (New Anderton, USA/UK)

Robert Floodeen

Partner, New Anderton

About

- Focused on driving incident response consulting activities
- Over 20 years of experience in cybersecurity
  - Team Lead, Pentagon IDS Team
  - Manager of a US DoD CERT
  - CSIRT Capacity Development team at CMU's CERT/CC
  - XO at CMU's Software Engineering Institute
  - US market manager at PWC for cyber security readiness consulting
  - Director of IR Consulting, Dell SecureWorks, EMEA
  - VP of Global Cybersecurity Services
- BS and MS in Computer Science, and an MBA
- Exec Ed. Certificates, Wharton and Oxford Saïd

Previous Focus Areas

- Network Forensics
- Large Scale Crisis Response
- CSIRT Research and Development

History of Passion for Security

- Chaired 3 Committees for the Forum of Incident Response and Security Teams (FIRST)
  - Conference Program Committee Chair
  - Education Committee Chair
  - Membership Committee Chair
- Editor *ISO 27035:2016 Incident Management*
- Co-Author: *Managing a National CSIRT with Critical Success Factors*, U.N. International Telecommunication Union. ITU-D RGQ22-1/1
- Adjunct Instructor at Carnegie Mellon University in Digital Forensics, Event Reconstruction

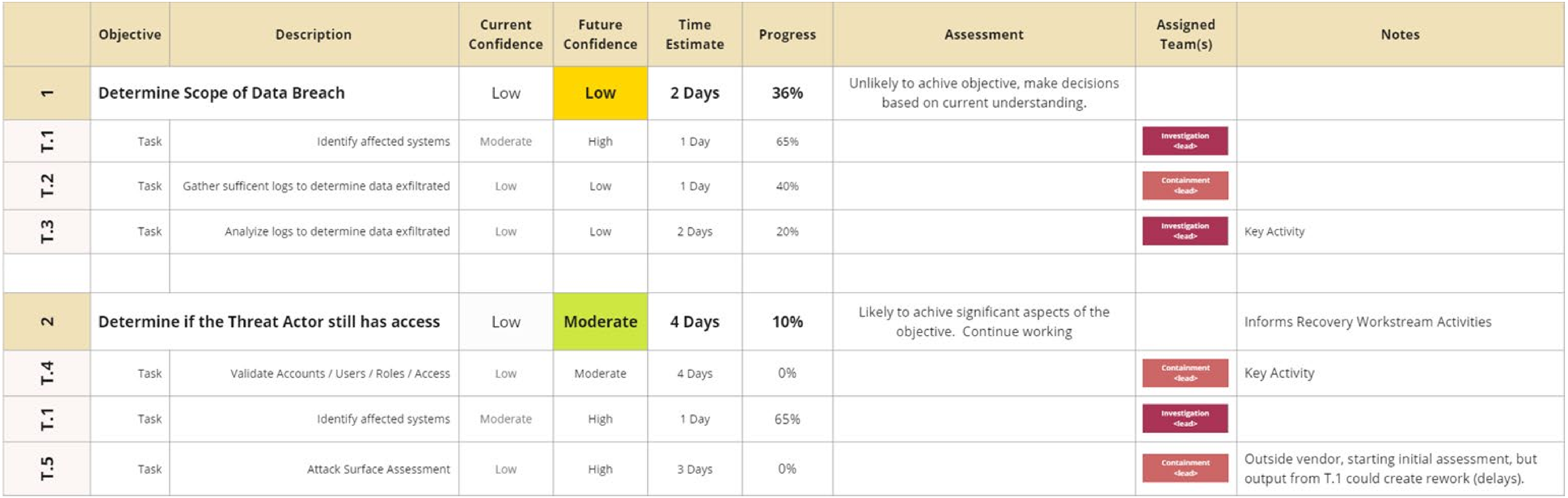
Objectifying your incident management

Agenda

- Introduce the concept
- Review decision making
- Discuss incident communication
- Review the building blocks
- Put it all together
- Q&A

Objective:

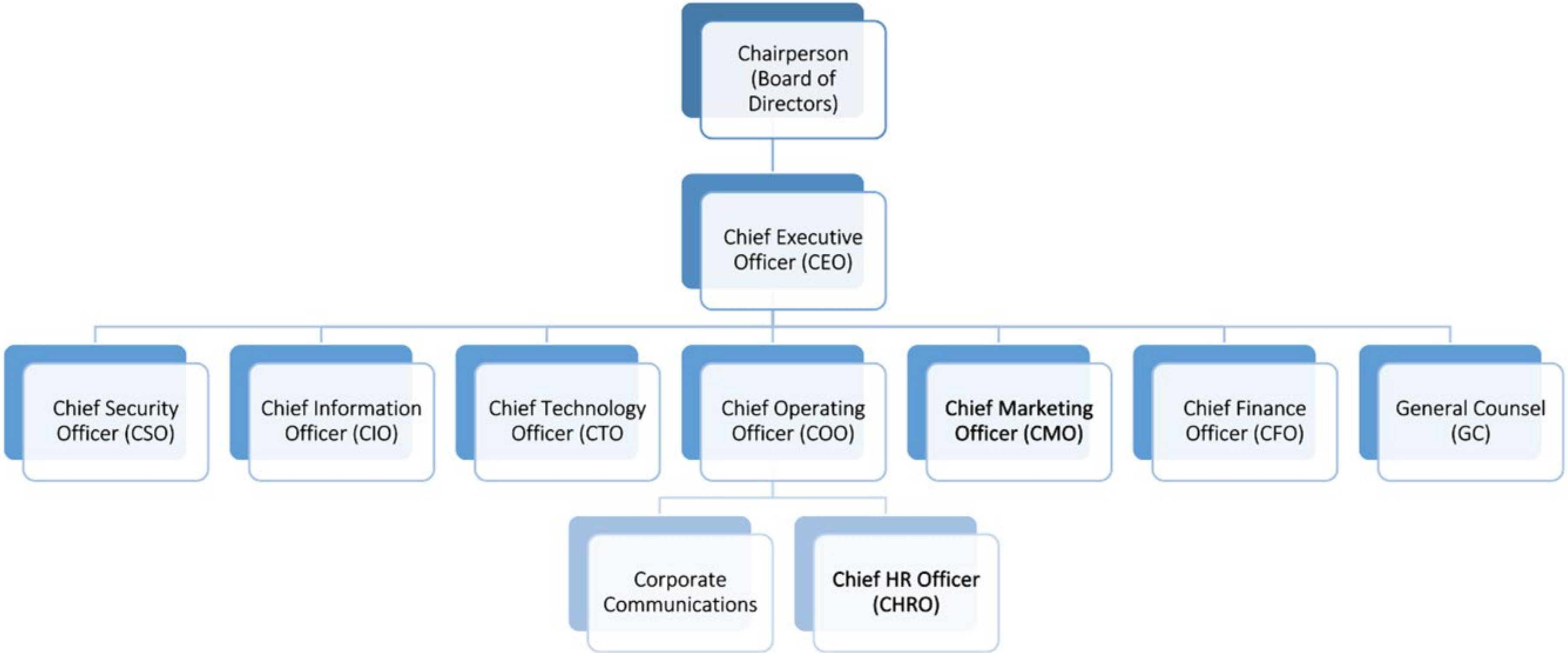
Understand an approach to managing your incidents



	Objective	Description	Current Confidence	Future Confidence	Time Estimate	Progress	Assessment	Assigned Team(s)	Notes
1	**Determine Scope of Data Breach**		Low	**Low**	**2 Days**	**36%**	Unlikely to achive objective, make decisions based on current understanding.		
T.1	Task	Identify affected systems	Moderate	High	1 Day	65%		Investigation <lead>	
T.2	Task	Gather sufficent logs to determine data exfiltrated	Low	Low	1 Day	40%		Containment <lead>	
T.3	Task	Analyize logs to determine data exfiltrated	Low	Low	2 Days	20%		Investigation <lead>	Key Activity
2	**Determine if the Threat Actor still has access**		Low	**Moderate**	**4 Days**	**10%**	Likely to achive significant aspects of the objective. Continue working		Informs Recovery Workstream Activities
T.4	Task	Validate Accounts / Users / Roles / Access	Low	Moderate	4 Days	0%		Containment <lead>	Key Activity
T.1	Task	Identify affected systems	Moderate	High	1 Day	65%		Investigation <lead>	
T.5	Task	Attack Surface Assessment	Low	High	3 Days	0%		Containment <lead>	Outside vendor, starting initial assessment, but output from T.1 could create rework (delays).

Decision Making & Our Audience

Our Audience



Chairperson (Board of Directors)

Chief Executive Officer (CEO)

Chief Security Officer (CSO)

Chief Information Officer (CIO)

Chief Technology Officer (CTO

Chief Operating Officer (COO)

Chief Marketing Officer (CMO)

Chief Finance Officer (CFO)

General Counsel (GC)

Corporate Communications

Chief HR Officer (CHRO)

External Counsel

Public Relations Firm

Customer's customers

Expert Decision Making

6 or 7 items

Different weights

Consumed in a Non-Linear order

Terminates at a threshold

Experts have similar criteria

Matching expectation to criteria is deemed expert

Missing criteria is assumed negative

Metrics and Tests are positive

Addressed criteria is viewed as an expert

Easy Example

1. Set an Objective
2. List out possible questions
3. Prioritize

Improve decision making with

- Tests/Validation
- Metrics

Purchase a New Car

- Car Price
- Car Safety (Metrics/Tests)
- Number of Seats
- Vehicle Mileage (Metrics/Tests)
- Maintenance Costs
- Insurance Costs

IM Example

1. Set an Objective
2. List out possible questions
3. Prioritize

Improve decision making with

- Tests/Validation
- Metrics

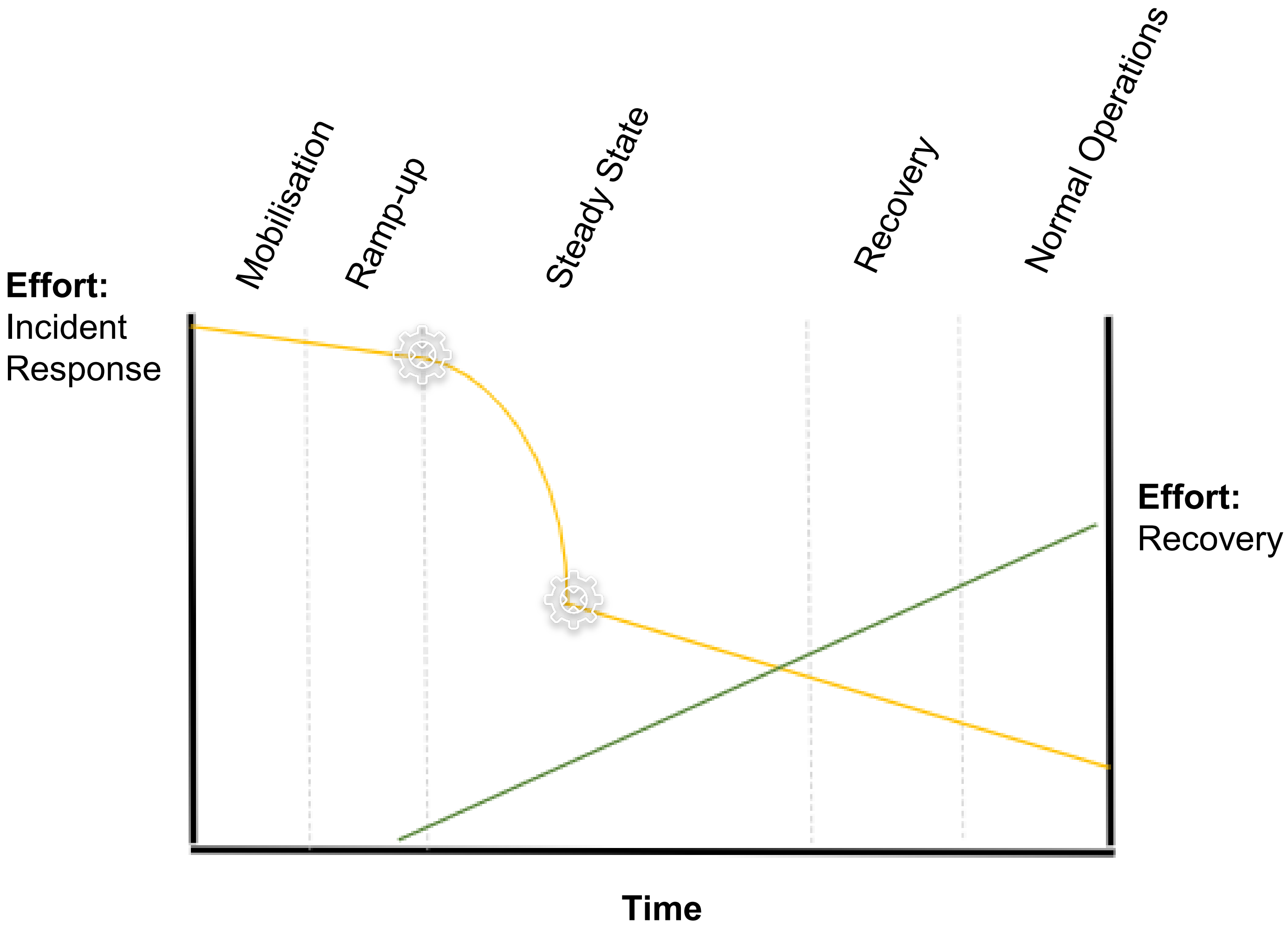
Determine Data Exposure

- Type of data accessed
- Was data accessed
- How much data was accessed
- How much time to inventory data
- Time to inform regulator
- Time to inform customers

Incident Communication

Driving towards an operational cycle that is sustainable and low effort

Balancing an Operational Cycle



NIST

During incident handling, the team may need to provide status updates to certain parties, even in some cases the entire organization. **The team should plan and prepare several communication methods**, including out-of-band methods (e.g., in person, paper), and select the methods that are appropriate for a particular incident. Key aspects that are planned for in these briefings include:

Target Audience: Executive Leadership

Timing: Daily

Information Reported: Status update since the last briefing

Next Steps: What actions are being taken next

FEMA

According to the US Federal Emergency Management Agency, **establishing an operational reporting tempo will help ease reporting and synchronize the lines of effort**. The reporting tempo should identify a timeline for submission of information. Key aspects that are planned for in these briefings include:

Target Audience: Supervisors of Tactical Resources

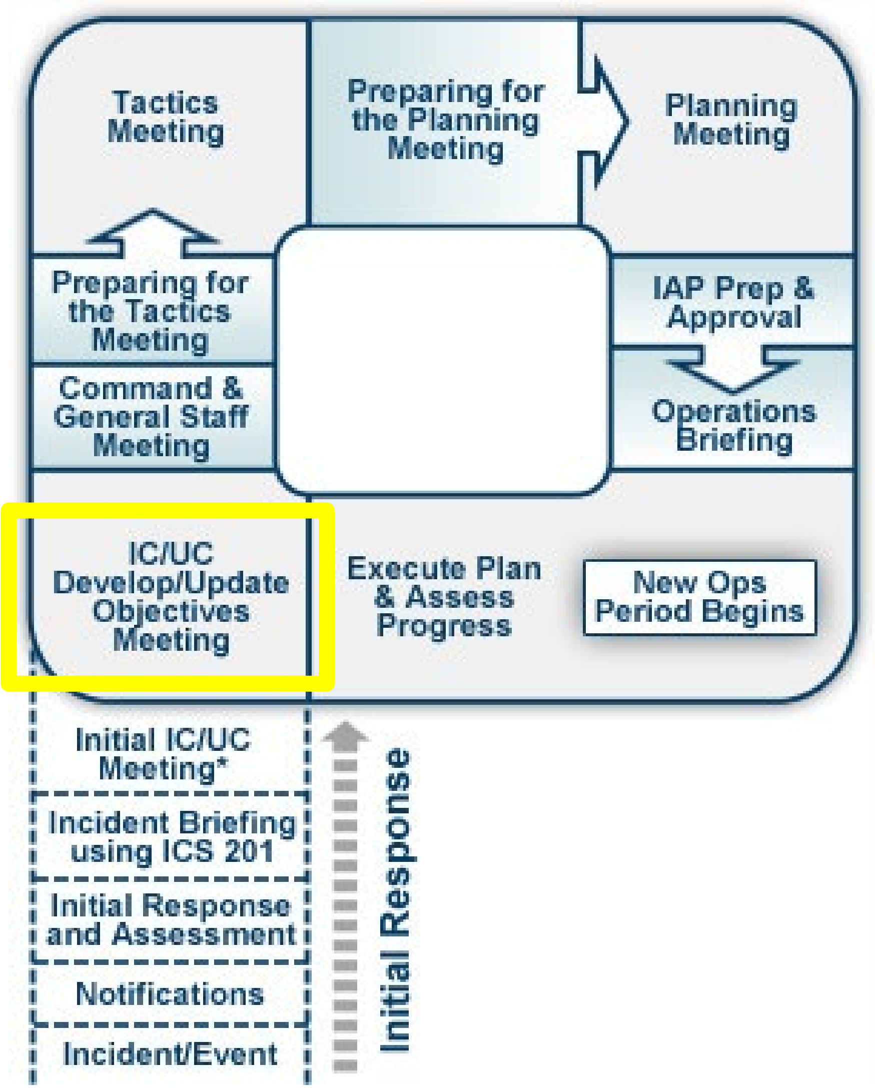
Timing: Every 4-24 hours depending on the nature/complexity of the incident and working conditions

Information Reported: Status update since the last briefing

Next Steps: What actions are being taken next

- Objectives Development/Update
- Strategy Meeting/Command and General Staff Meeting
- Tactics Meeting
- Planning Meeting
- Period Briefing

FEMA’s Planning “P”


Tactics Meeting
Preparing for the Planning Meeting
Planning Meeting
Preparing for the Tactics Meeting
IAP Prep & Approval
Command & General Staff Meeting
Operations Briefing
IC/UC Develop/Update Objectives Meeting
Execute Plan & Assess Progress
New Ops Period Begins
Initial IC/UC Meeting*
Incident Briefing using ICS 201
Initial Response and Assessment
Notifications
Incident/Event
Initial Response

The Building Blocks

Blocks

- Objectives
- Tasks
- Workstreams
- Confidence Levels
- Time Estimations

Objective

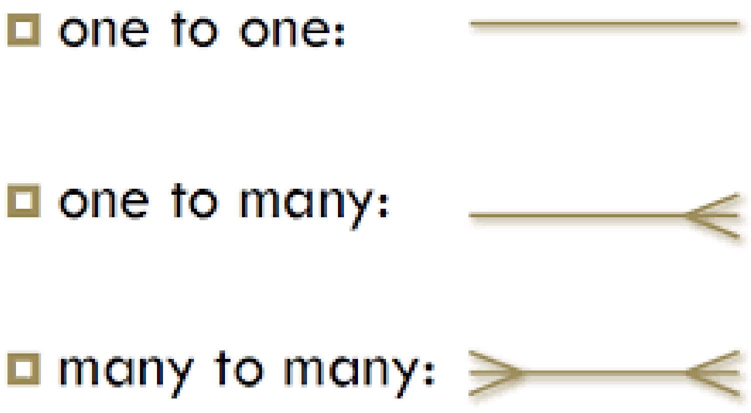
Answer the big picture questions, ‘What are we trying to do?’

- limit the number of ‘active’ objectives to 3, maybe 4

- be SMART about creating them
  - Specific
  - Measurable
  - Action-Oriented
  - Realistic
  - Time-frame

Example: **Before Monday, identify what data was exfiltrated from the MongoDB server**

Task



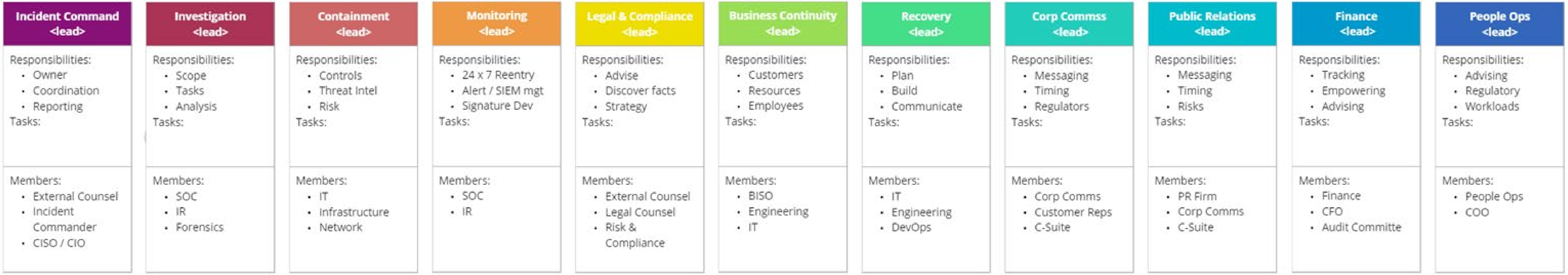
The activities that make up an objective

One to Many

- 1 task could be supporting multiple objectives

Example: **identify users/roles/systems that communicated with the MongoDB server**

Workstream



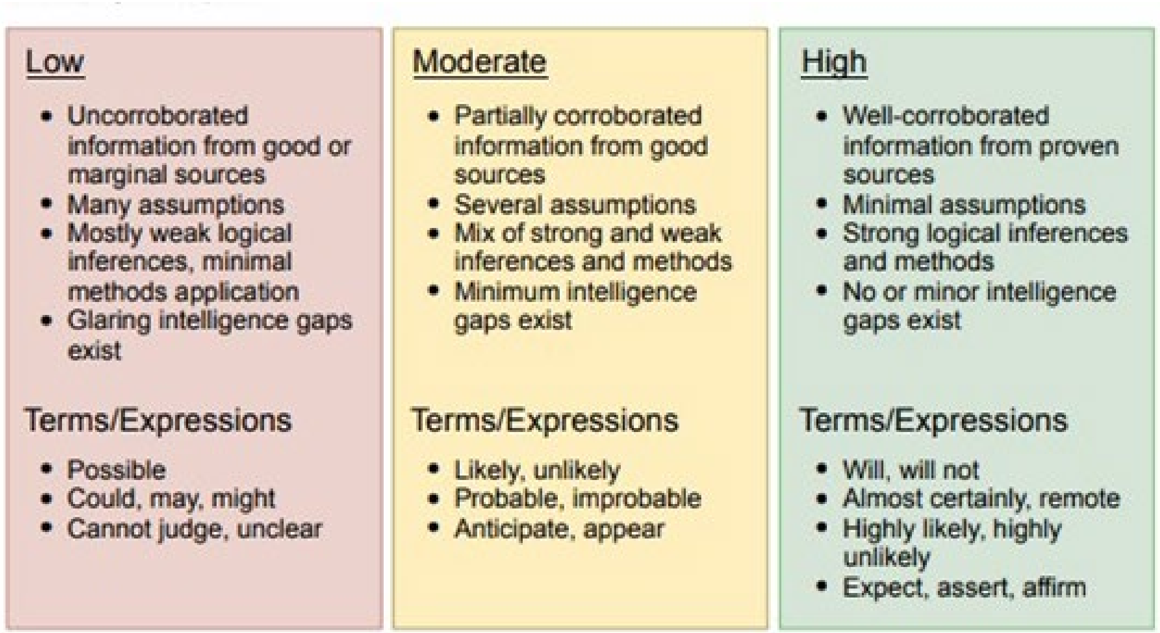
Incident Command <lead>	Investigation <lead>	Containment <lead>	Monitoring <lead>	Legal & Compliance <lead>	Business Continuity <lead>	Recovery <lead>	Corp Commss <lead>	Public Relations <lead>	Finance <lead>	People Ops <lead>
Responsibilities: • Owner • Coordination • Reporting Tasks:	Responsibilities: • Scope • Tasks • Analysis Tasks:	Responsibilities: • Controls • Threat Intel • Risk Tasks:	Responsibilities: • 24 x 7 Reentry • Alert / SIEM mgt • Signature Dev Tasks:	Responsibilities: • Advise • Discover facts • Strategy Tasks:	Responsibilities: • Customers • Resources • Employees Tasks:	Responsibilities: • Plan • Build • Communicate Tasks:	Responsibilities: • Messaging • Timing • Regulators Tasks:	Responsibilities: • Messaging • Timing • Risks Tasks:	Responsibilities: • Tracking • Empowering • Advising Tasks:	Responsibilities: • Advising • Regulatory • Workloads Tasks:
Members: • External Counsel • Incident Commander • CISO / CIO	Members: • SOC • IR • Forensics	Members: • IT • Infrastructure • Network	Members: • SOC • IR	Members: • External Counsel • Legal Counsel • Risk & Compliance	Members: • BISO • Engineering • IT	Members: • IT • Engineering • DevOps	Members: • Corp Comms • Customer Reps • C-Suite	Members: • PR Firm • Corp Comms • C-Suite	Members: • Finance • CFO • Audit Committe	Members: • People Ops • COO

Confidence Level

What is your confidence?

- *US Joint Chiefs of Staff, Joint Intelligence, JP2-0, 2013*

- Based on
  - Assumptions
  - Sourcing
  - Arguments



Low	Moderate	High
• Uncorroborated information from good or marginal sources • Many assumptions • Mostly weak logical inferences, minimal methods application • Glaring intelligence gaps exist	• Partially corroborated information from good sources • Several assumptions • Mix of strong and weak inferences and methods • Minimum intelligence gaps exist	• Well-corroborated information from proven sources • Minimal assumptions • Strong logical inferences and methods • No or minor intelligence gaps exist
Terms/Expressions	Terms/Expressions	Terms/Expressions
• Possible • Could, may, might • Cannot judge, unclear	• Likely, unlikely • Probable, improbable • Anticipate, appear	• Will, will not • Almost certainly, remote • Highly likely, highly unlikely • Expect, assert, affirm

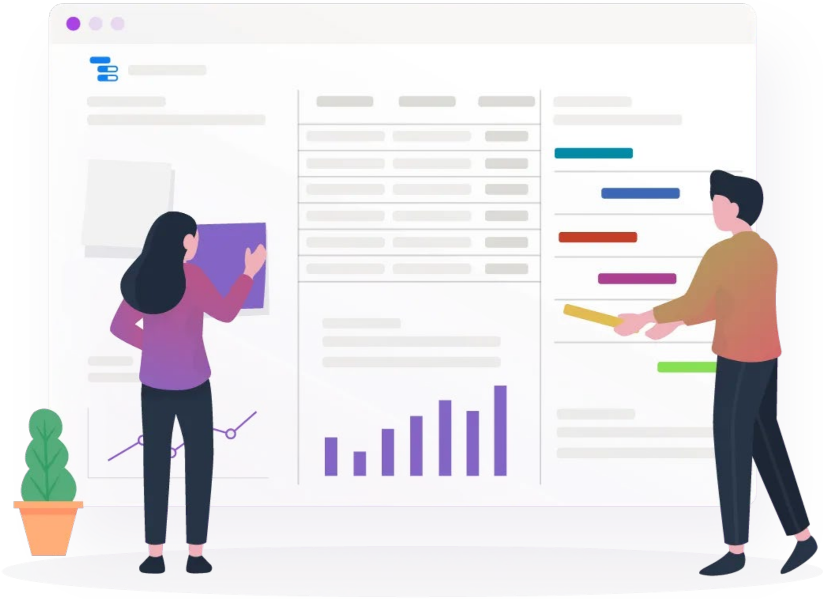
Time Estimation

How long will each task take?

How long will an objective take, based on those tasks?

How do I describe ‘time?’

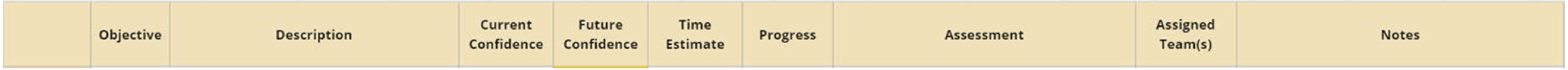
- Common Work Breakdown Structures (WBS)
  - **hour**
  - **Day**
  - Week
  - Month



*Instagannt

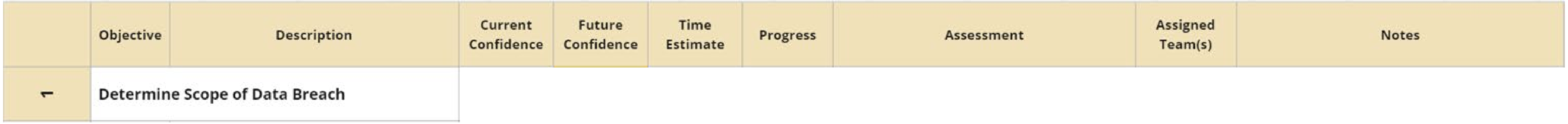
Assembly

Have a framework to display the data



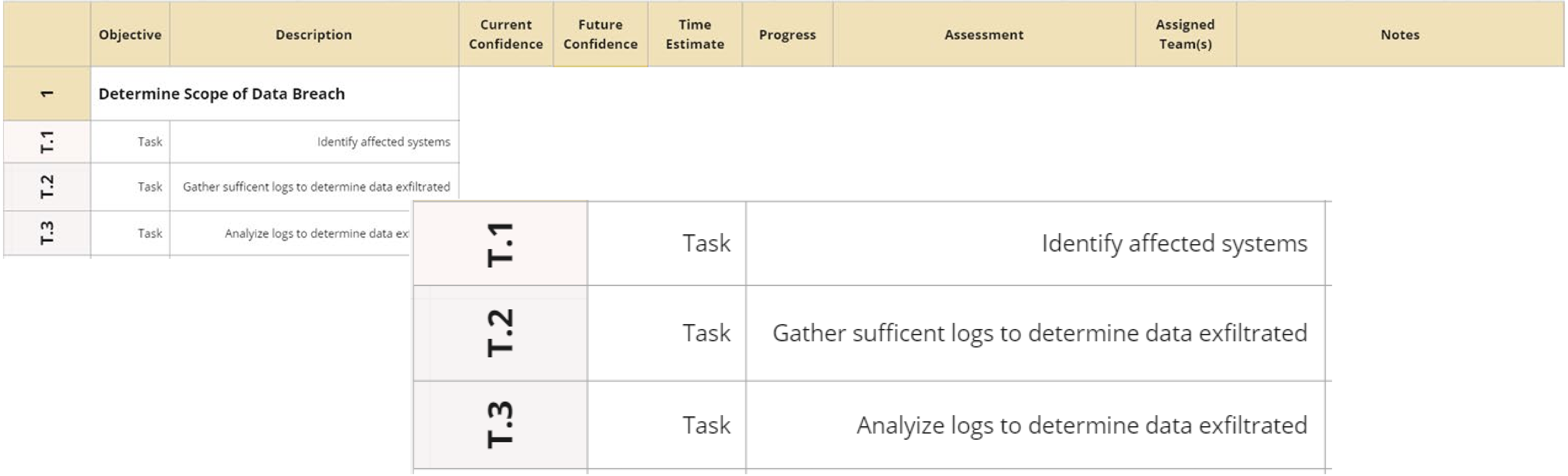
	Objective	Description	Current Confidence	Future Confidence	Time Estimate	Progress	Assessment	Assigned Team(s)	Notes

Create the first objective



	Objective	Description	Current Confidence	Future Confidence	Time Estimate	Progress	Assessment	Assigned Team(s)	Notes
1	Determine Scope of Data Breach								

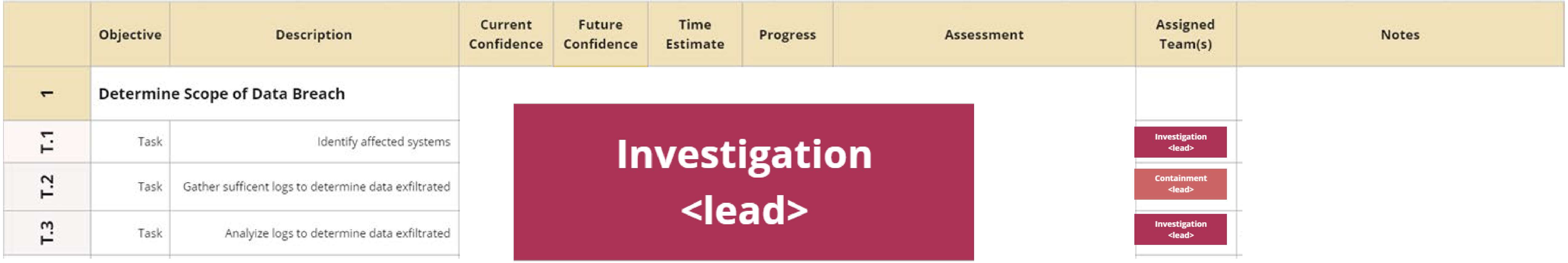
Identify the Tasks to complete the objectives



	Objective	Description	Current Confidence	Future Confidence	Time Estimate	Progress	Assessment	Assigned Team(s)	Notes
1	**Determine Scope of Data Breach**								
T.1	Task	Identify affected systems							
T.2	Task	Gather sufficent logs to determine data exfiltrated							
T.3	Task	Analyize logs to determine data ex							

T.1	Task	Identify affected systems
T.2	Task	Gather sufficent logs to determine data exfiltrated
T.3	Task	Analyize logs to determine data exfiltrated

Assign the lead workstream for each task



	Objective	Description	Current Confidence	Future Confidence	Time Estimate	Progress	Assessment	Assigned Team(s)	Notes
1	Determine Scope of Data Breach								
T.1	Task	Identify affected systems						Investigation <lead>	
T.2	Task	Gather sufficent logs to determine data exfiltrated						Containment <lead>	
T.3	Task	Analyize logs to determine data exfiltrated						Investigation <lead>	

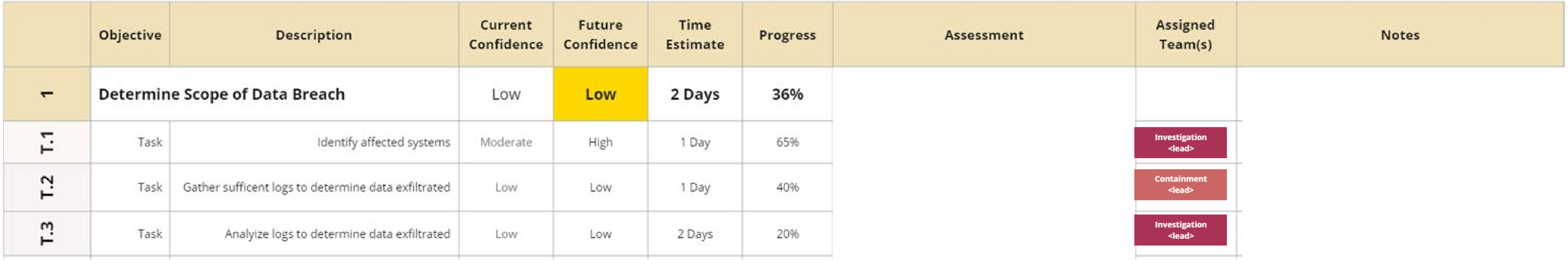
Investigation
<lead>

Containment
<lead>

Investigation
<lead>

Workstream leads provide:

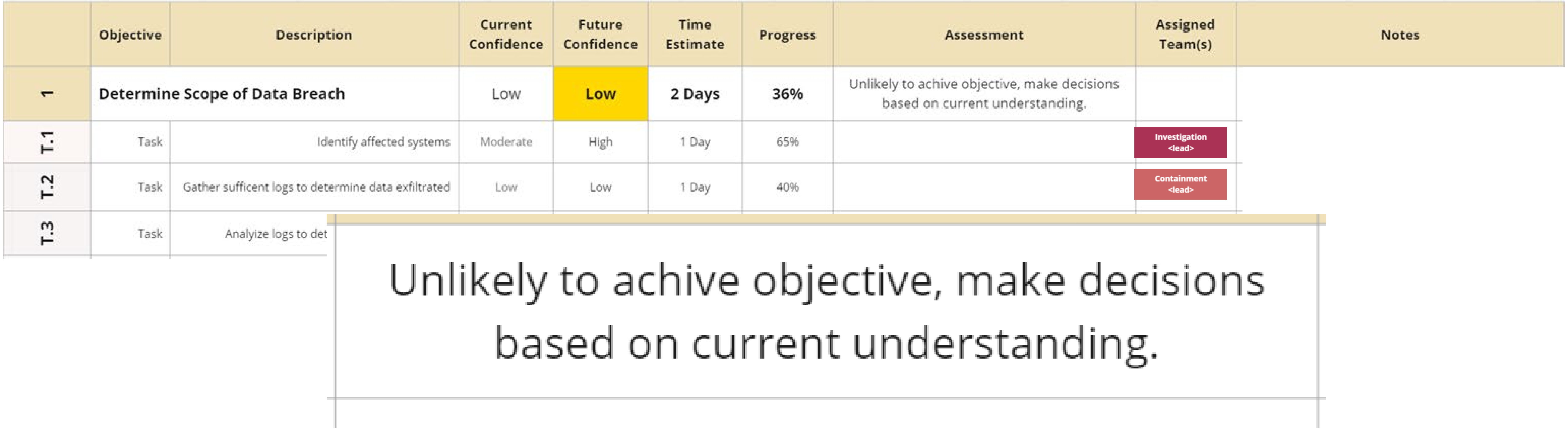
Confidence, Time, Progress



	Objective	Description	Current Confidence	Future Confidence	Time Estimate	Progress	Assessment	Assigned Team(s)	Notes
1	**Determine Scope of Data Breach**		Low	**Low**	**2 Days**	**36%**			
T.1	Task	Identify affected systems	Moderate	High	1 Day	65%		Investigation <lead>	
T.2	Task	Gather sufficent logs to determine data exfiltrated	Low	Low	1 Day	40%		Containment <lead>	
T.3	Task	Analyize logs to determine data exfiltrated	Low	Low	2 Days	20%		Investigation <lead>	

Incident Command w/ Workstream leads

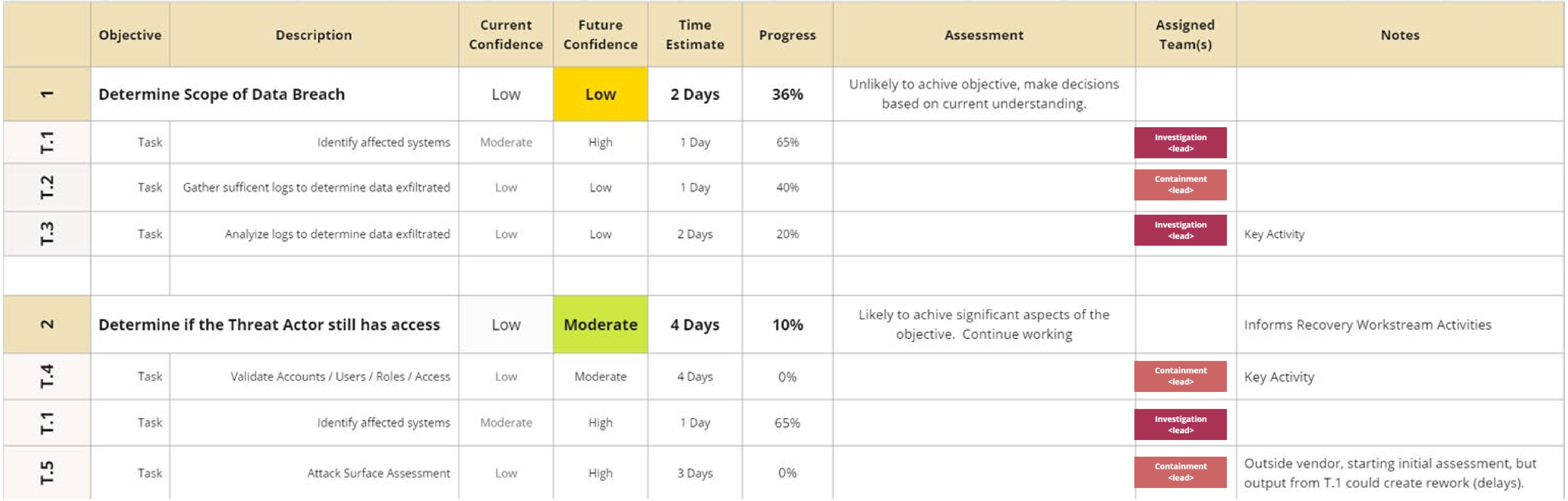
Assess and Recommend



	Objective	Description	Current Confidence	Future Confidence	Time Estimate	Progress	Assessment	Assigned Team(s)	Notes
1	**Determine Scope of Data Breach**		Low	**Low**	**2 Days**	**36%**	Unlikely to achive objective, make decisions based on current understanding.		
T.1	Task	Identify affected systems	Moderate	High	1 Day	65%		Investigation <lead>	
T.2	Task	Gather sufficent logs to determine data exfiltrated	Low	Low	1 Day	40%		Containment <lead>	
T.3	Task	Analyize logs to det							

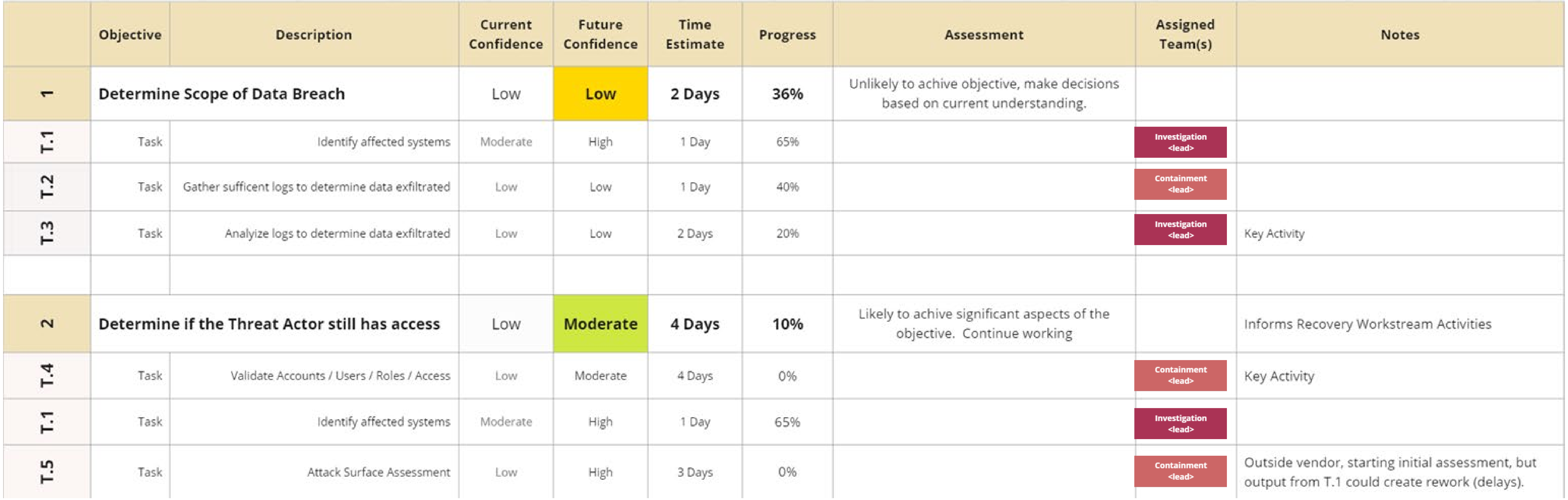
Unlikely to achive objective, make decisions based on current understanding.

Identify remaining objectives and data



	Objective	Description	Current Confidence	Future Confidence	Time Estimate	Progress	Assessment	Assigned Team(s)	Notes
1	**Determine Scope of Data Breach**		Low	**Low**	**2 Days**	**36%**	Unlikely to achive objective, make decisions based on current understanding.		
T.1	Task	Identify affected systems	Moderate	High	1 Day	65%		Investigation <lead>	
T.2	Task	Gather sufficent logs to determine data exfiltrated	Low	Low	1 Day	40%		Containment <lead>	
T.3	Task	Analyize logs to determine data exfiltrated	Low	Low	2 Days	20%		Investigation <lead>	Key Activity
2	**Determine if the Threat Actor still has access**		Low	**Moderate**	**4 Days**	**10%**	Likely to achive significant aspects of the objective. Continue working		Informs Recovery Workstream Activities
T.4	Task	Validate Accounts / Users / Roles / Access	Low	Moderate	4 Days	0%		Containment <lead>	Key Activity
T.1	Task	Identify affected systems	Moderate	High	1 Day	65%		Investigation <lead>	
T.5	Task	Attack Surface Assessment	Low	High	3 Days	0%		Containment <lead>	Outside vendor, starting initial assessment, but output from T.1 could create rework (delays).

Different personas are consuming this data



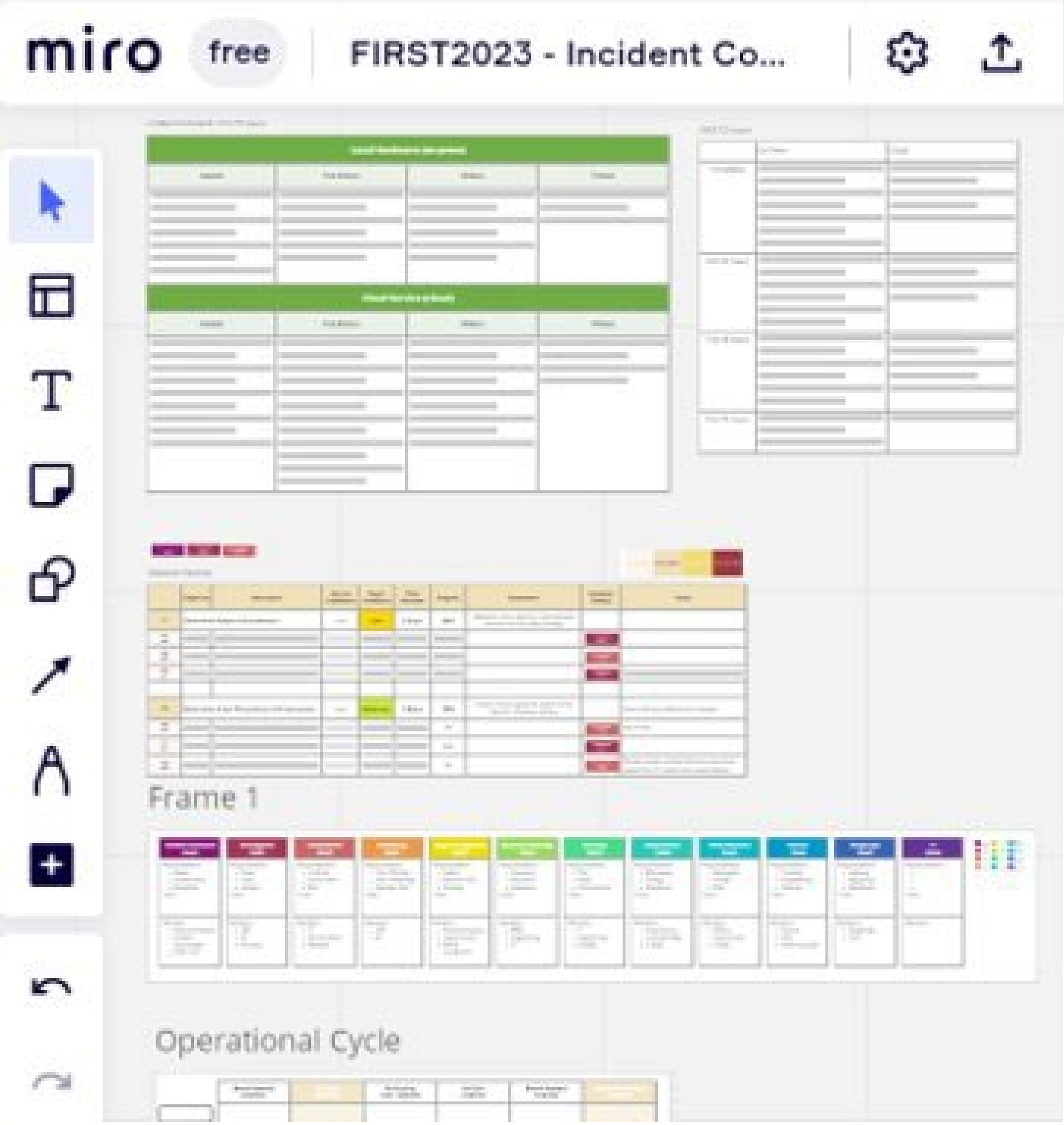
	Objective	Description	Current Confidence	Future Confidence	Time Estimate	Progress	Assessment	Assigned Team(s)	Notes
1	**Determine Scope of Data Breach**		Low	**Low**	**2 Days**	**36%**	Unlikely to achive objective, make decisions based on current understanding.		
T.1	Task	Identify affected systems	Moderate	High	1 Day	65%		Investigation <lead>	
T.2	Task	Gather sufficent logs to determine data exfiltrated	Low	Low	1 Day	40%		Containment <lead>	
T.3	Task	Analyize logs to determine data exfiltrated	Low	Low	2 Days	20%		Investigation <lead>	Key Activity
2	**Determine if the Threat Actor still has access**		Low	**Moderate**	**4 Days**	**10%**	Likely to achive significant aspects of the objective. Continue working		Informs Recovery Workstream Activities
T.4	Task	Validate Accounts / Users / Roles / Access	Low	Moderate	4 Days	0%		Containment <lead>	Key Activity
T.1	Task	Identify affected systems	Moderate	High	1 Day	65%		Investigation <lead>	
T.5	Task	Attack Surface Assessment	Low	High	3 Days	0%		Containment <lead>	Outside vendor, starting initial assessment, but output from T.1 could create rework (delays).

#FIRSTCON23

35TH ANNUAL FIRST CONFERENCE

MONTRÉAL

JUNE 4-9, 2023



Thank you!

Robert.Floodeen@newanderton.com