Security Metrics

ⓘ

How vulnerable are we?

07 Vuln Remediation- Are we remediating known vulnerabilities in a timely fashion

- High and critical Vulnerabilities
- Patches

ⓘ

How vulnerable are we?

12 SRM - How effective are the security risk management and assurance processes in identifying, responding, reporting risk and providing assurance?

- Cyber Security Risk Assessment
- Policy Exemptions
- Security Standards

ⓘ

How vulnerable are we?

10 DP - Are we safeguarding our data from threats?

- Encryption

05 Asset Classification - Do we know the critical assets to protect from threats?

- Security classifications

ⓘ

What are the key threats & how are we managing them

H 04 Protective Technologies - How effective are we at threatening external threats at early stages?

- Malware on Microsoft Servers

ⓘ

What are the key threats & how are we managing them

03 Cyber Safety Culture - Are we adequately training our workforce about relevant cyber security threats?

- Phishing insights
- Phishing Incident raised
- Cyber Awareness Training

ⓘ

Are we Prepared to manage the consequences?

14 Detection - Are we monitoring our environment to detect cyber threats and events that may lead to?

- Blue and Red Incidents.

ⓘ

Are we Prepared to manage the consequences?

14 Detection - Are we monitoring our environment to detect cyber threats and events that may lead to ?

- Business Continuity
- Disaster recovery

NOTE: Please click on (i) button for more detail information

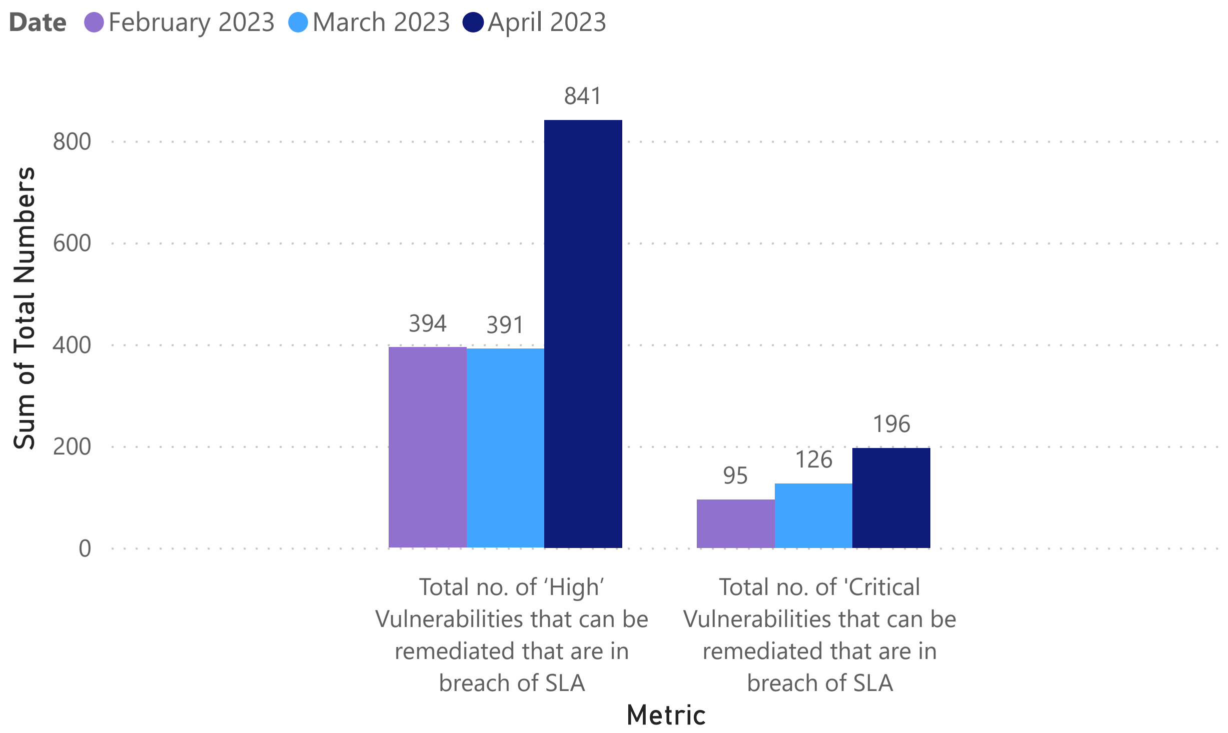
Home

Are we remediating known vulnerabilities in a timely fashion?

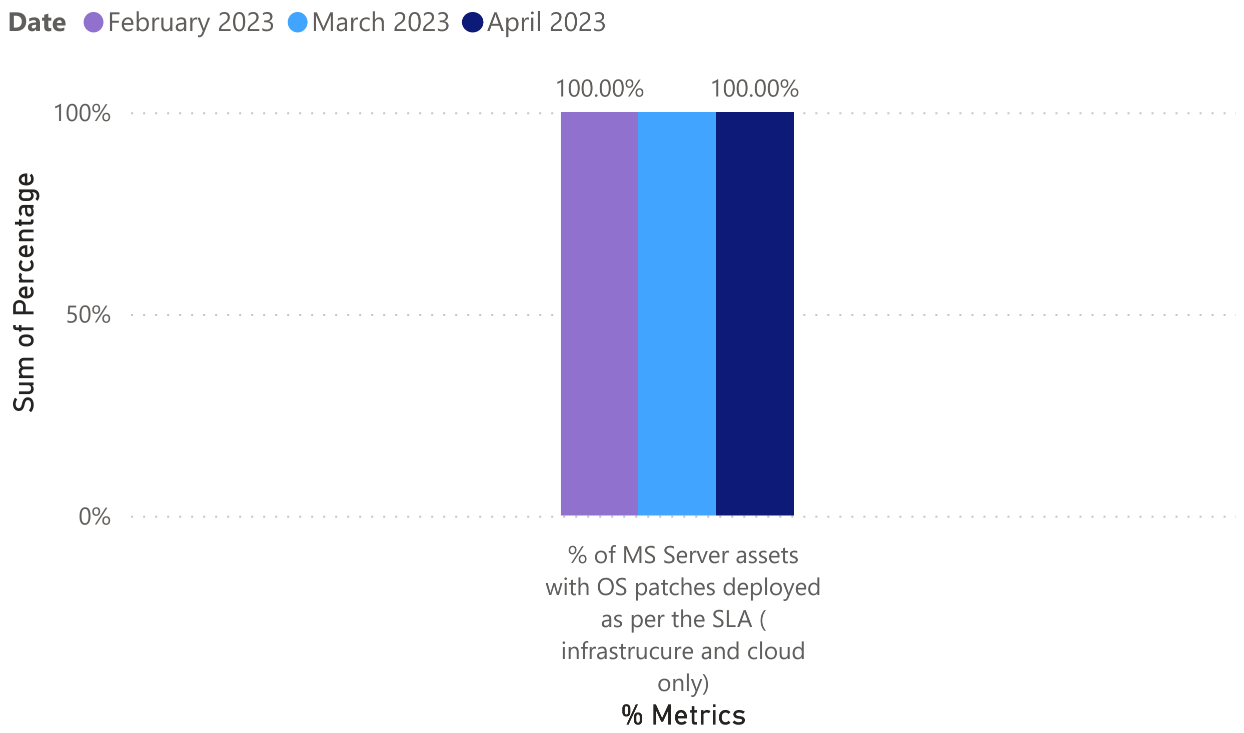
How vulnerable are we?

1/1/2023 12/31/2023

High and Critical Vulnerabilities



Patches deployed to MS assets Microsoft Servers



Vulnerabilities & Critical Events SOC

% Metrics	February	March	April
⊞ Total no. of 'High' Vulnerabilities that can be remediated that are in breach of SLA	394.00	391.00	841.00
⊞ Total no. of 'Critical Vulnerabilities that can be remediated that are in breach of SLA	95.00	126.00	196.00

Patches - SLA

% Metrics	February	March	April
⊞ % of MS Server assets with OS patches deployed as per the SLA (infrastrucure and cloud only)	100.00%	100.00%	100.00%

Home

12 SRM - How effective are the security risk management and assurance processes in identifying, responding, reporting risk and providing assurance?

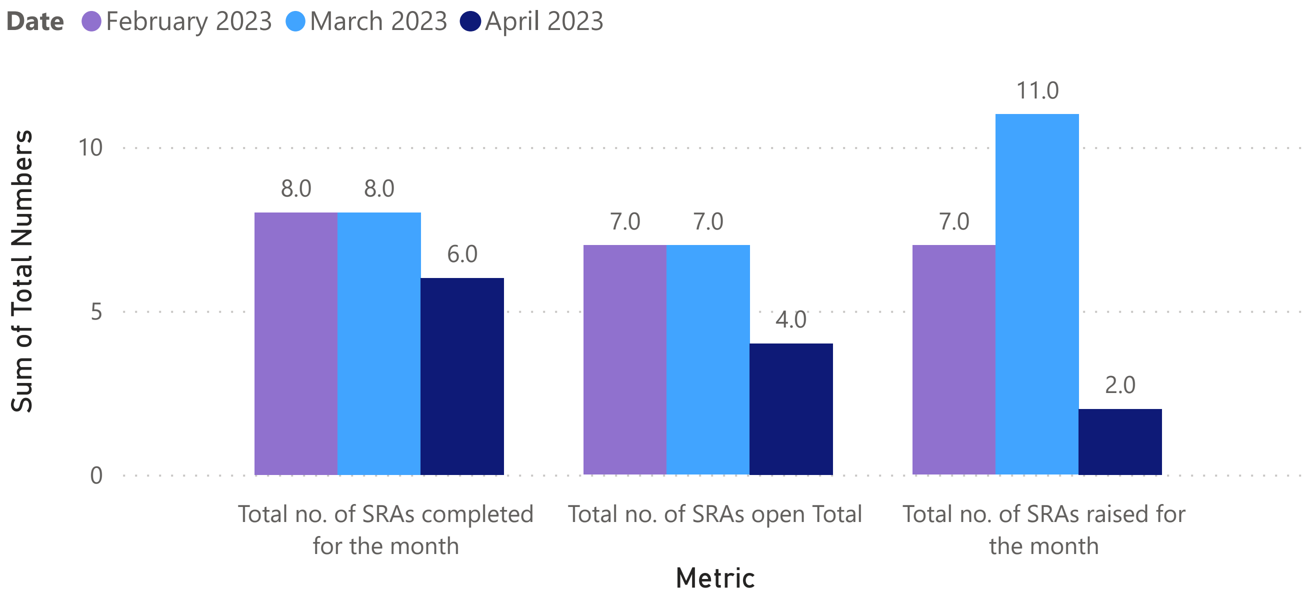
How vulnerable are we?

1/1/2023 12/31/2023

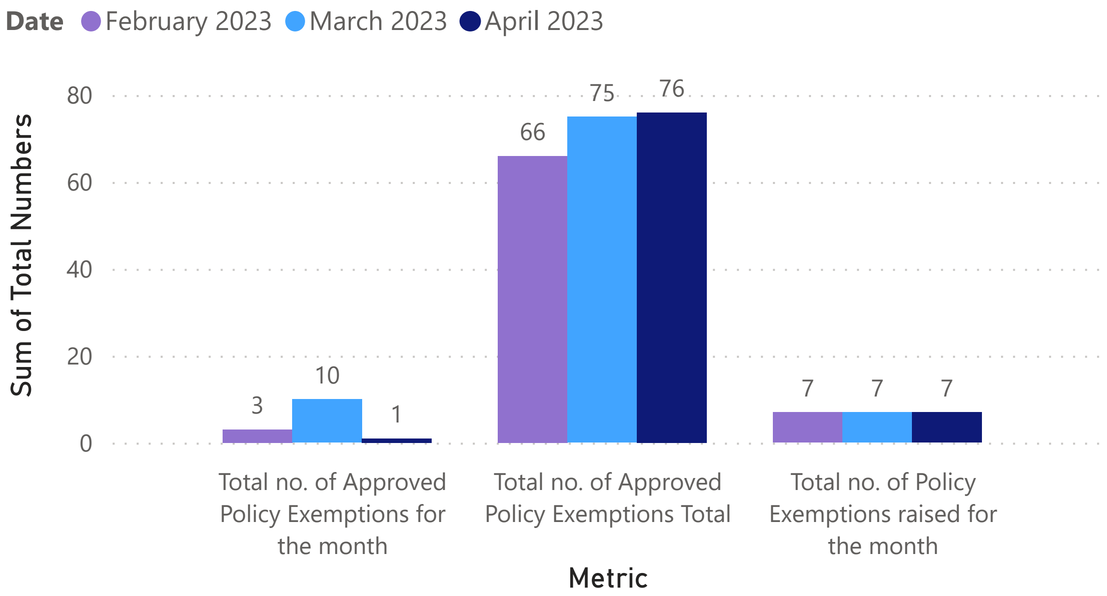
Have we reviewed our Security Standards in the last 12 months?

Answer
Yes

Cyber Security Risk Assessment



Policy Exemptions Requests



Cyber Security Risk Assessment

% Metrics	February	March	April
⊞ Total no. of SRAs raised for the month	7.00	11.00	2.00
⊞ Total no. of SRAs open Total	7.00	7.00	4.00
⊞ Total no. of SRAs completed for the month	8.00	8.00	6.00

Policy Exemption Requests

% Metrics	February	March	April
⊞ Total no. of Approved Policy Exemptions for the month	3.00	10.00	1.00
⊞ Total no. of Approved Policy Exemptions Total	66.00	75.00	76.00
⊞ Total no. of Policy Exemptions raised for the month	7.00	7.00	7.00

Home

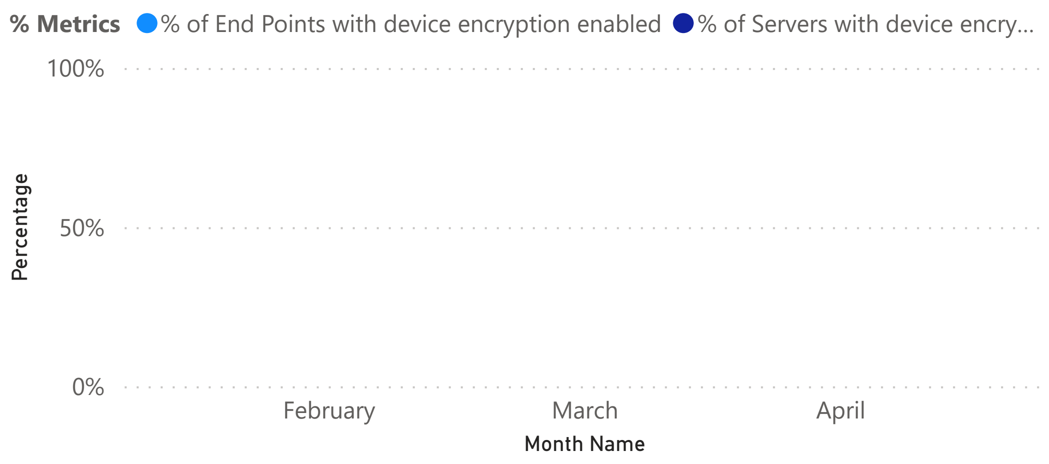
How vulnerable are we?

10 DP - Are we safeguarding our data from threats?

Encryption enabled

% Metrics	February	March	April
⊞ % of End Points with device encryption enabled	0.00%	0.00%	0.00%
⊞ % of Servers with device encryption enabled	0.00%	0.00%	0.00%

Encryption enabled



05 Asset Classification - Do we know the critical assets to protect from threats?

Security Classification

% Metrics	February	March	April
⊞ % of assets with complete security classification attribute(s) in the CMDB	0.00%	0.00%	0.00%

Home

What are the key threats & how are we managing them?

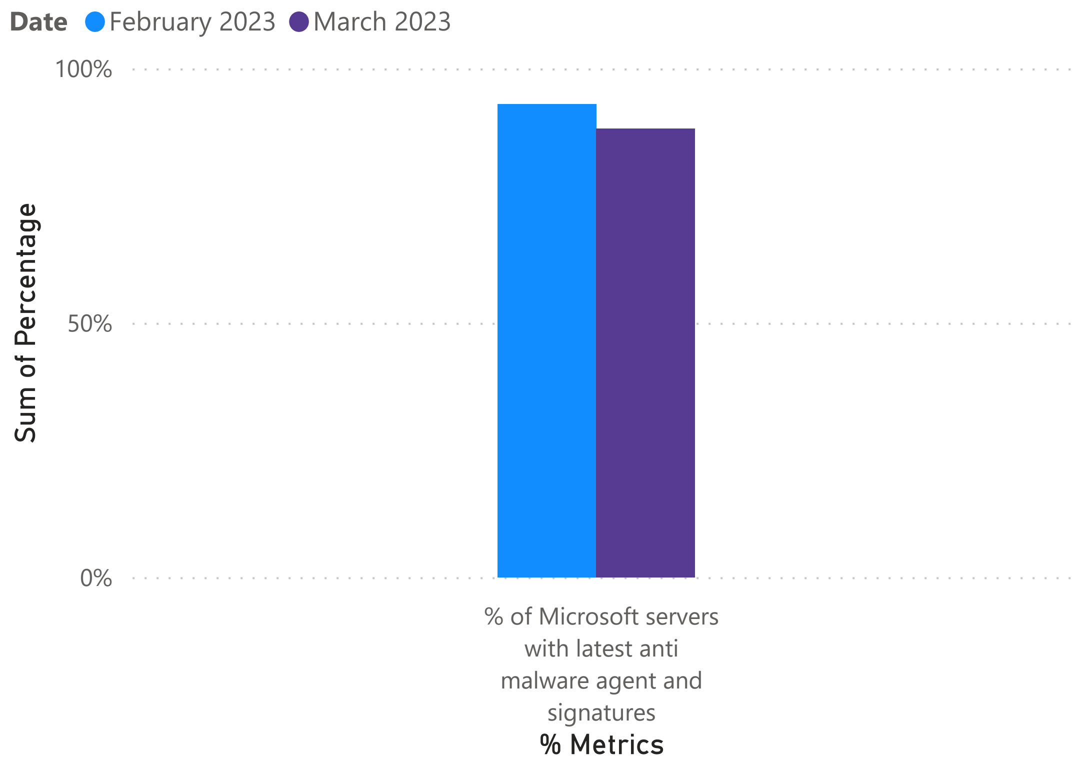
H 04 Protective Technologies - How effective are we at threatening external threats at early stages?

2/1/2023 12/1/2023

Malware

% Metrics	February	March
⊞ % of Microsoft servers with latest anti malware agent and signatures	93.00%	88.20%

Malware on Microsoft Servers



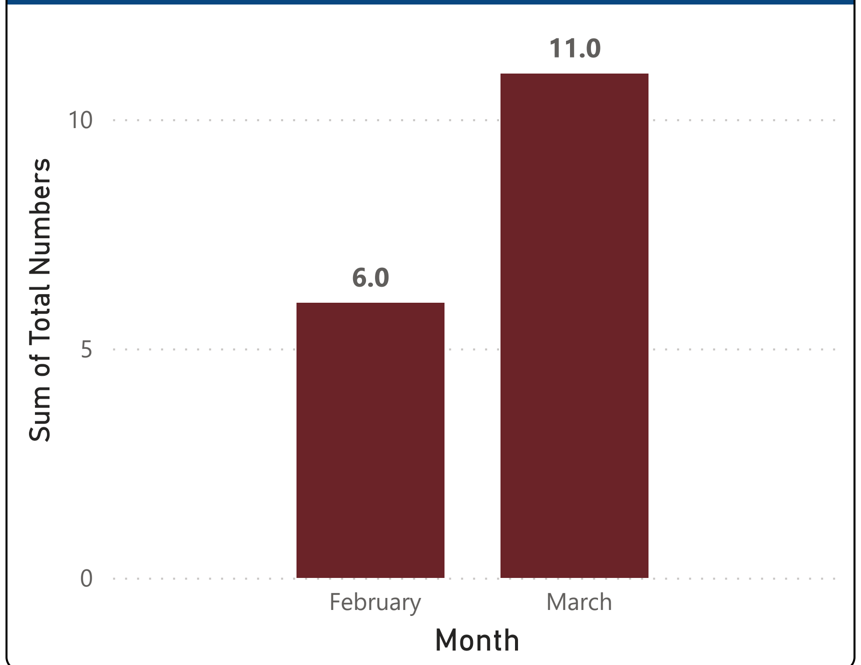
Home

What are the key threats & how are we managing them?

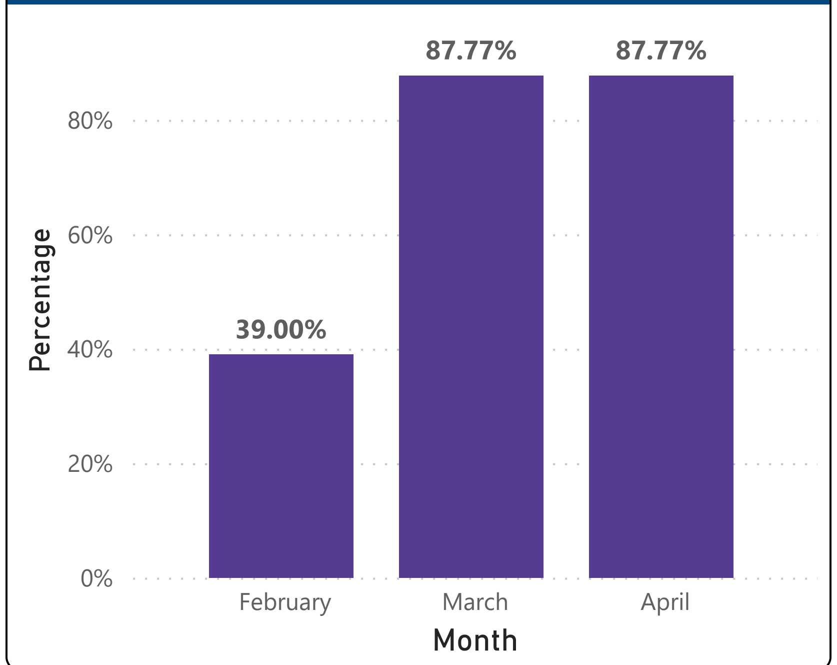
03 Cyber Safety Culture - Are we adequately training our workforce about relevant cyber security threats?

2/1/2023 4/30/2023

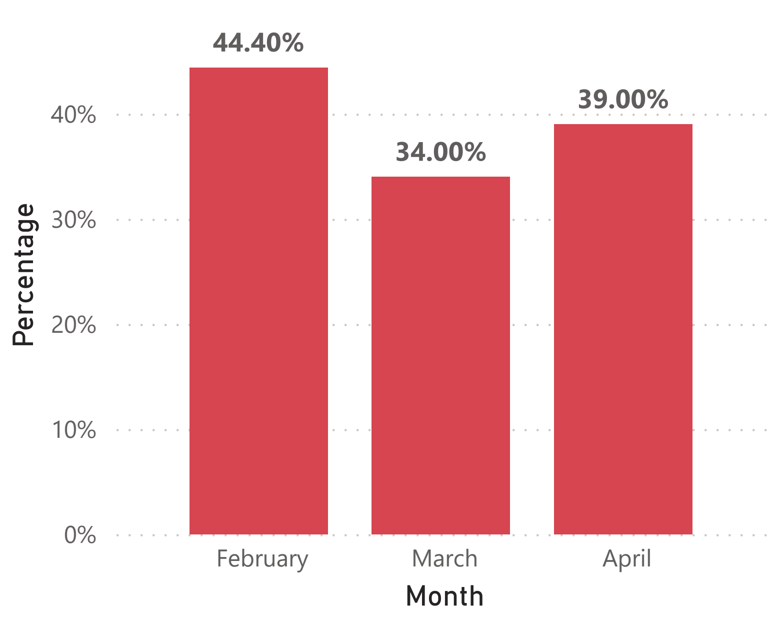
Total no. of Phishing Incidents raised by users



% of Employee completed mandatory training



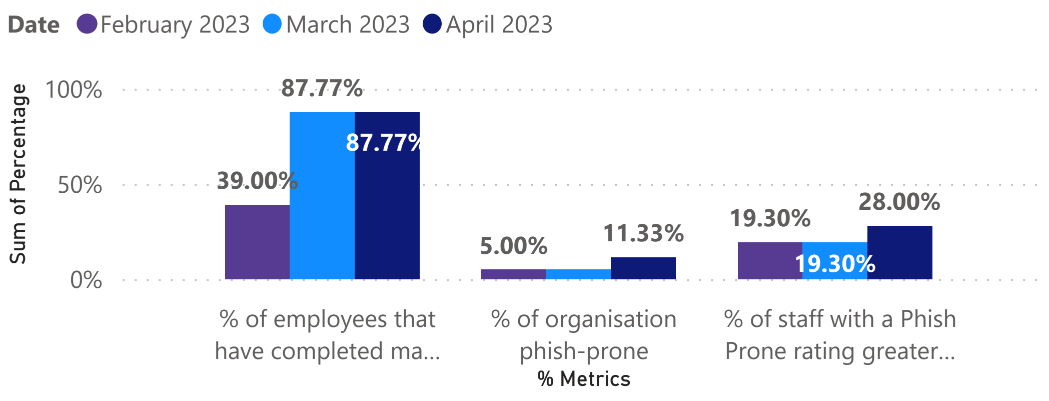
% of 'clickers' that have completed KnowBe4 training



Cyber Awareness

% Metrics	February	March	April
% of staff with a Phish Prone rating greater than 30%	19.30%	19.30%	28.00%
% of people that used the Report Phish function	70.70%	70.70%	14.40%
% of organisation phish-prone	5.00%	5.00%	11.33%
% of employees that have completed mandatory training within the defined timeframe - completed before deadline - cyber security training.	39.00%	87.77%	87.77%
% of 'clickers' that have completed KnowBe4 training	44.40%	34.00%	39.00%

Phishing Insights



Home

Are we prepared to manage the consequences?

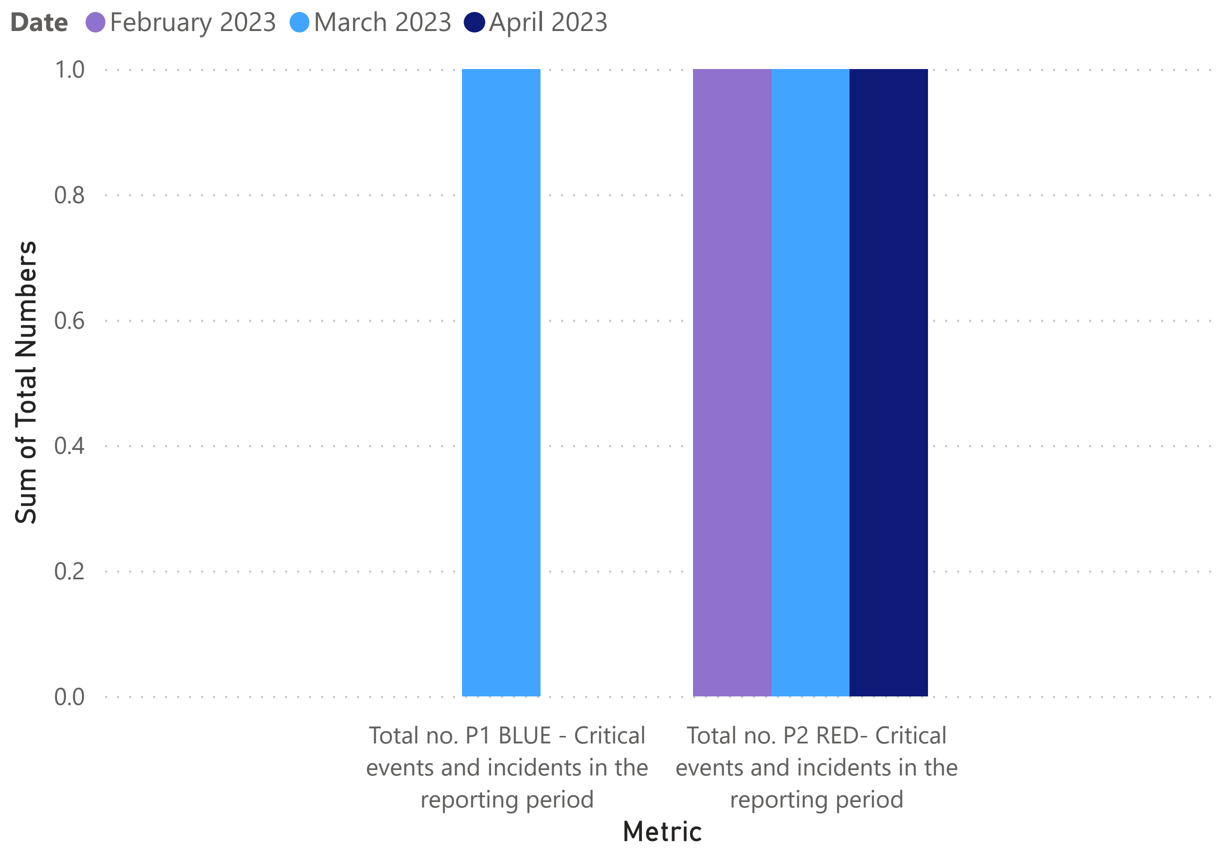
14 Detection - Are we monitoring our environment to detect cyber threats and events that may lead to (4 consequences listed as risk categories)?

1/1/2023 12/31/2023

Red and Blue Incidents

% Metrics	February	March	April
⊞ Total no. P2 RED- Critical events and incidents in the reporting period	1.00	1.00	1.00
⊞ Total no. P1 BLUE - Critical events and incidents in the reporting period	0.00	1.00	0.00

Red and Blue Incidents



Home

Are we prepared to manage the consequences?

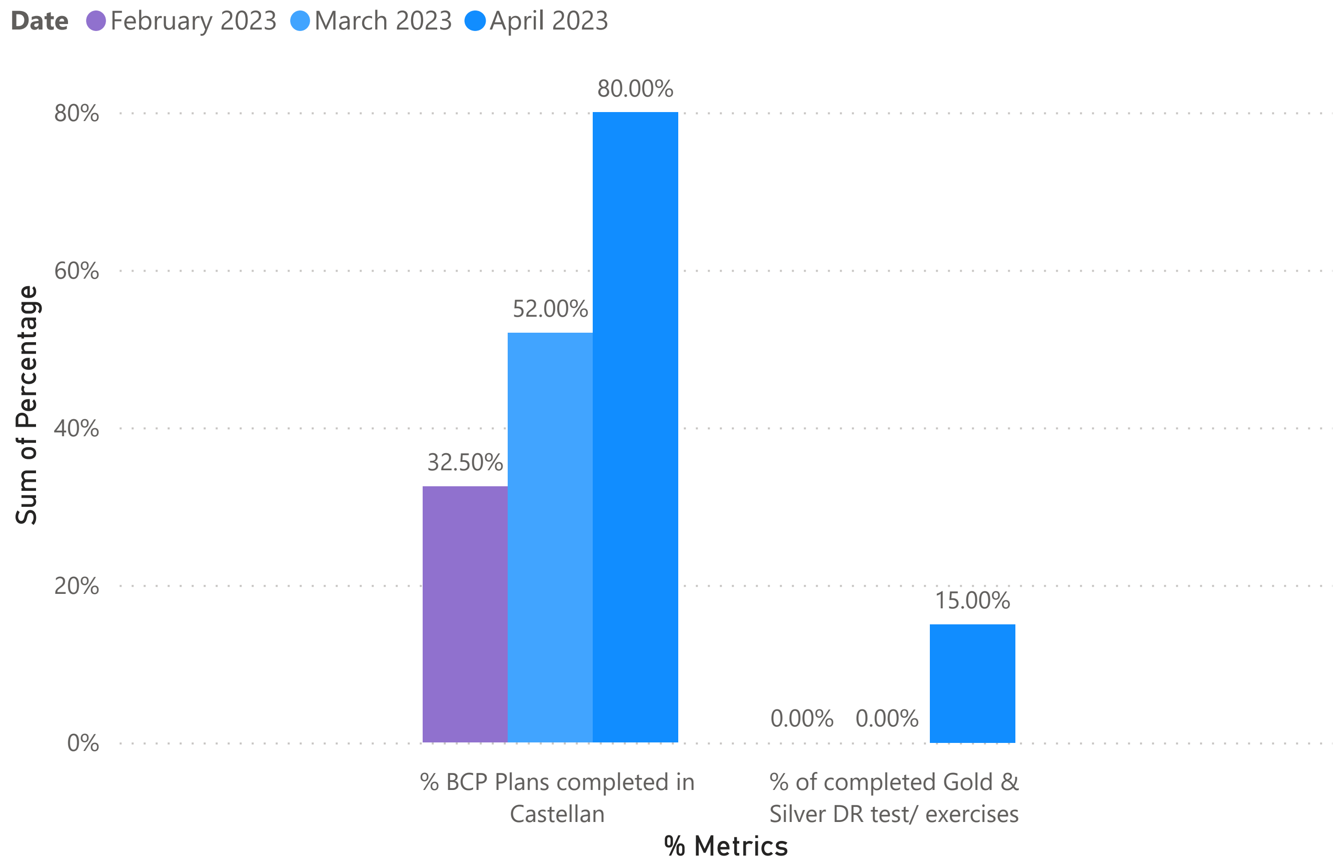
14 Detection - Are we monitoring our environment to detect cyber threats and events that may lead to?

2/1/2023 12/1/2023

Business Continuity and DR

% Metrics	February	March	April
⊞ % of completed Gold & Silver DR test/ exercises	0.00%	0.00%	15.00%
⊞ % of completed BIAs	32.50%	52.00%	80.00%
⊞ % BCP Plans completed in Castellan	32.50%	52.00%	80.00%

Business Continuity Plans


Date
February 2023
March 2023
April 2023
Sum of Percentage
% BCP Plans completed in Castellan
% of completed Gold & Silver DR test/ exercises
% Metrics