rubrik | Zero Trust Data Security™

Secure your data.

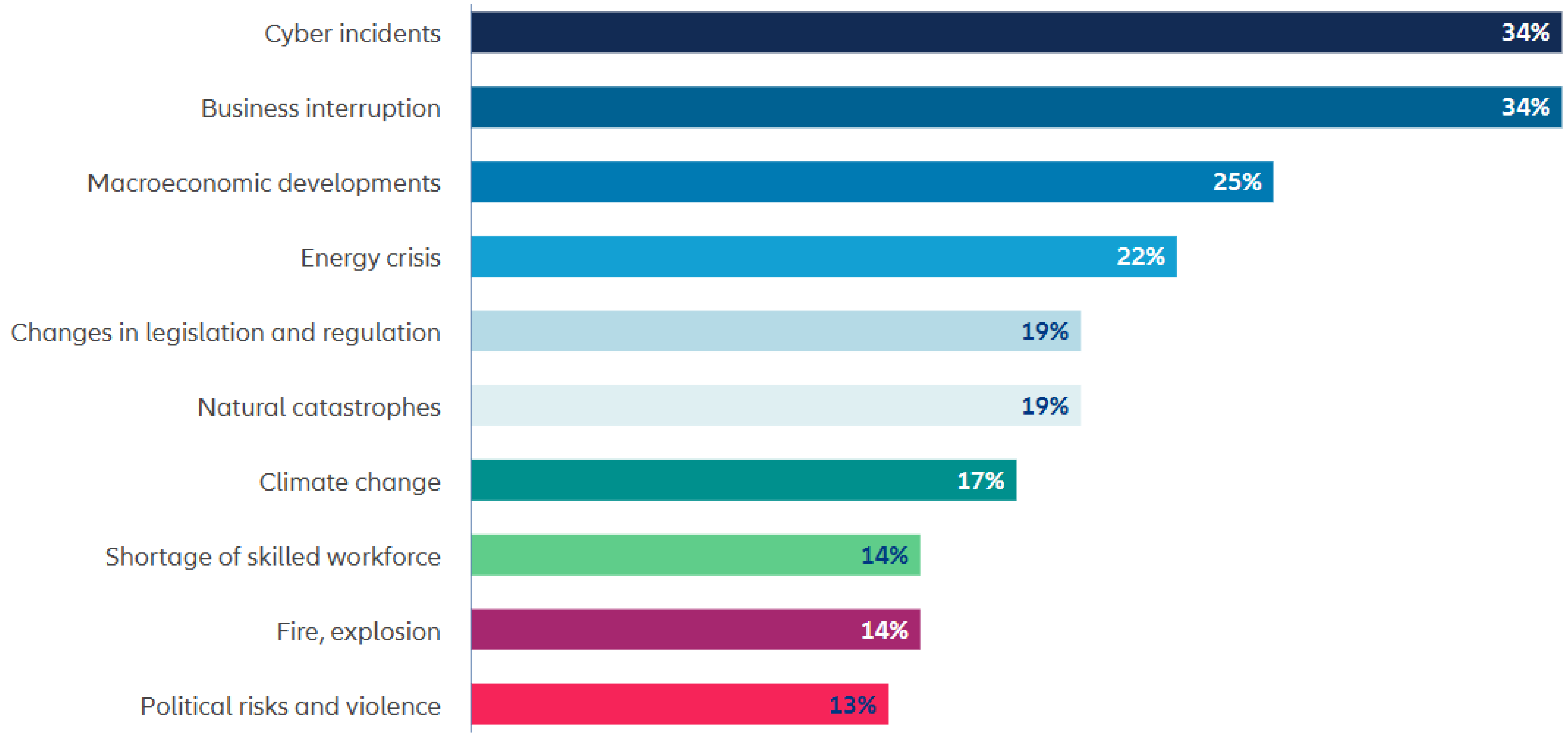
Secure your business.

Nicolas Groh
Field CTO EMEA - Rubrik

Closing the NIST loop

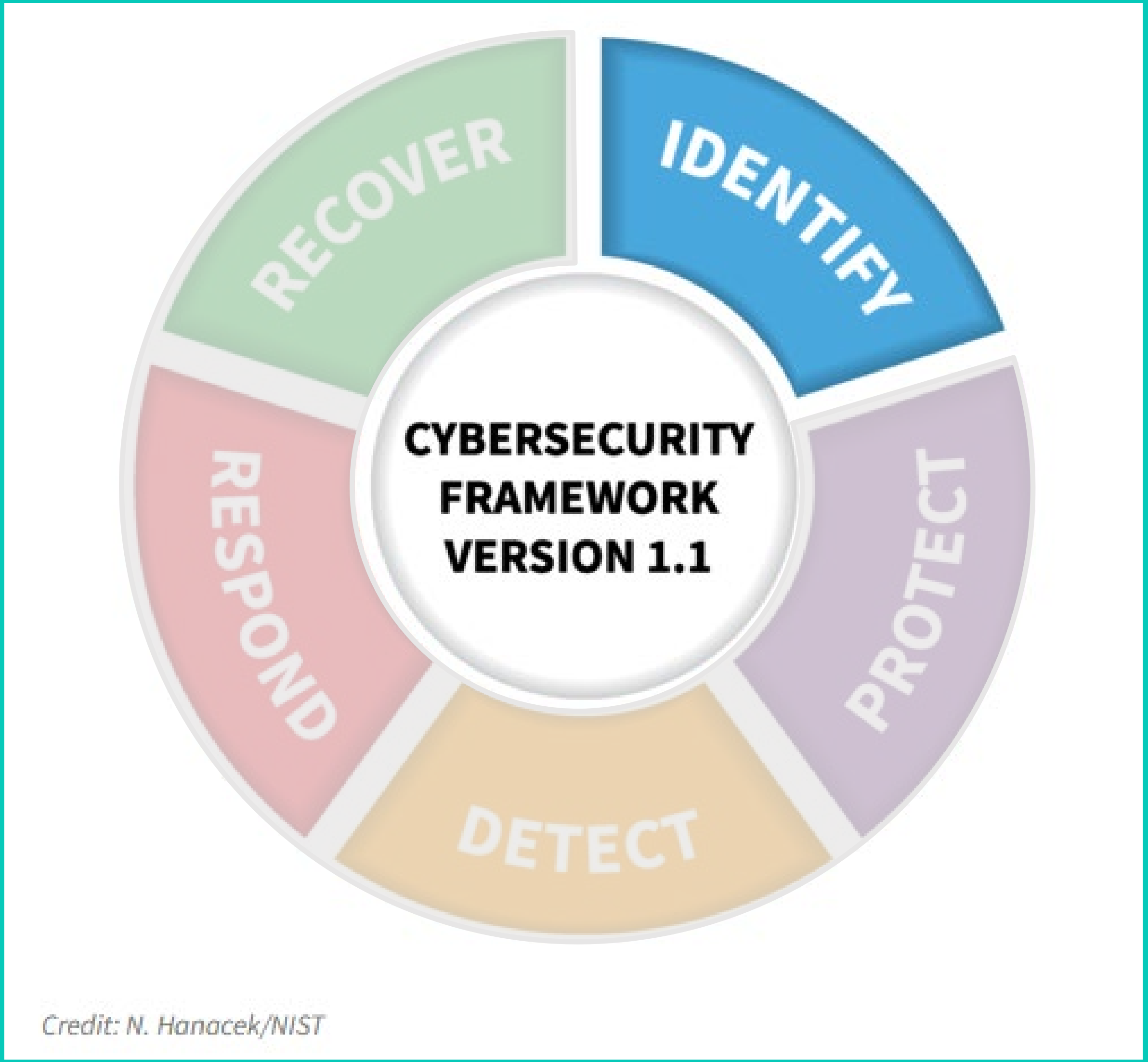
How to make sure, recovery is ensured ?

For more details click on the bars in the diagram



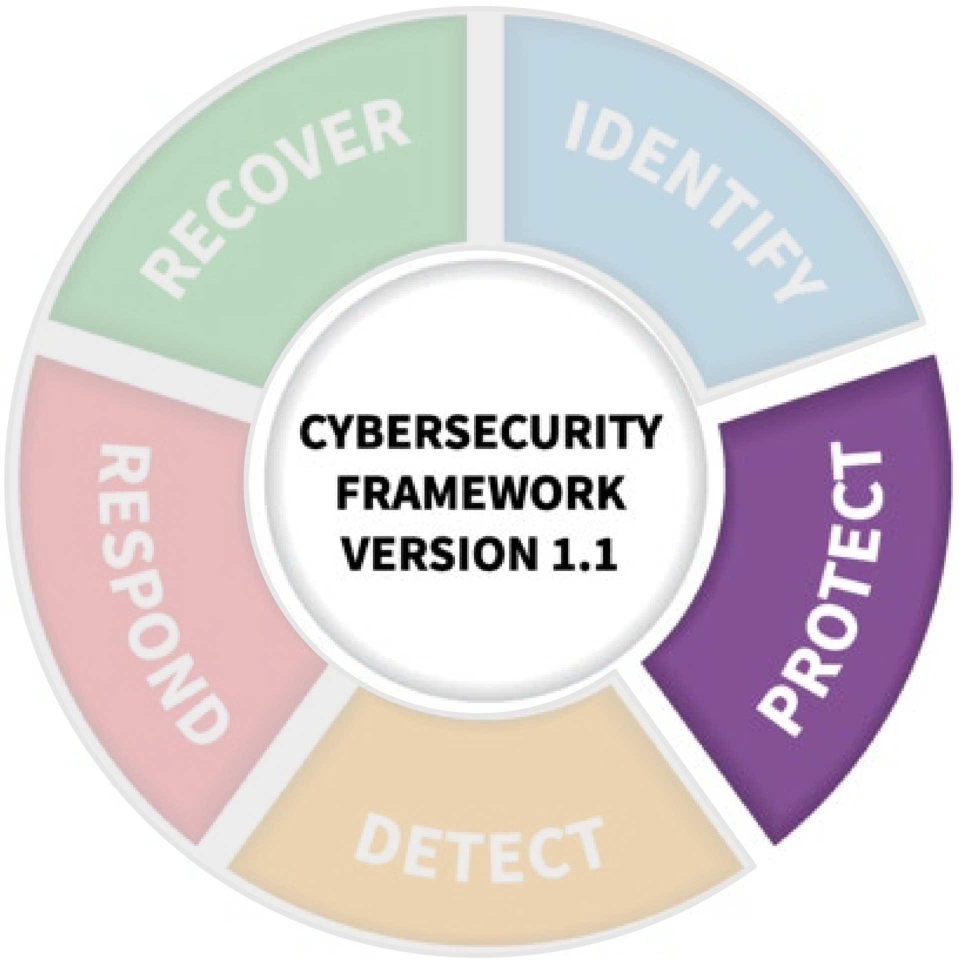
Source: Allianz Risk Barometer 2023
The numbers represent the percentage of all participants who responded (2,712). The numbers do not add up to 100% because more than one risk could be selected.

NIST Framework:



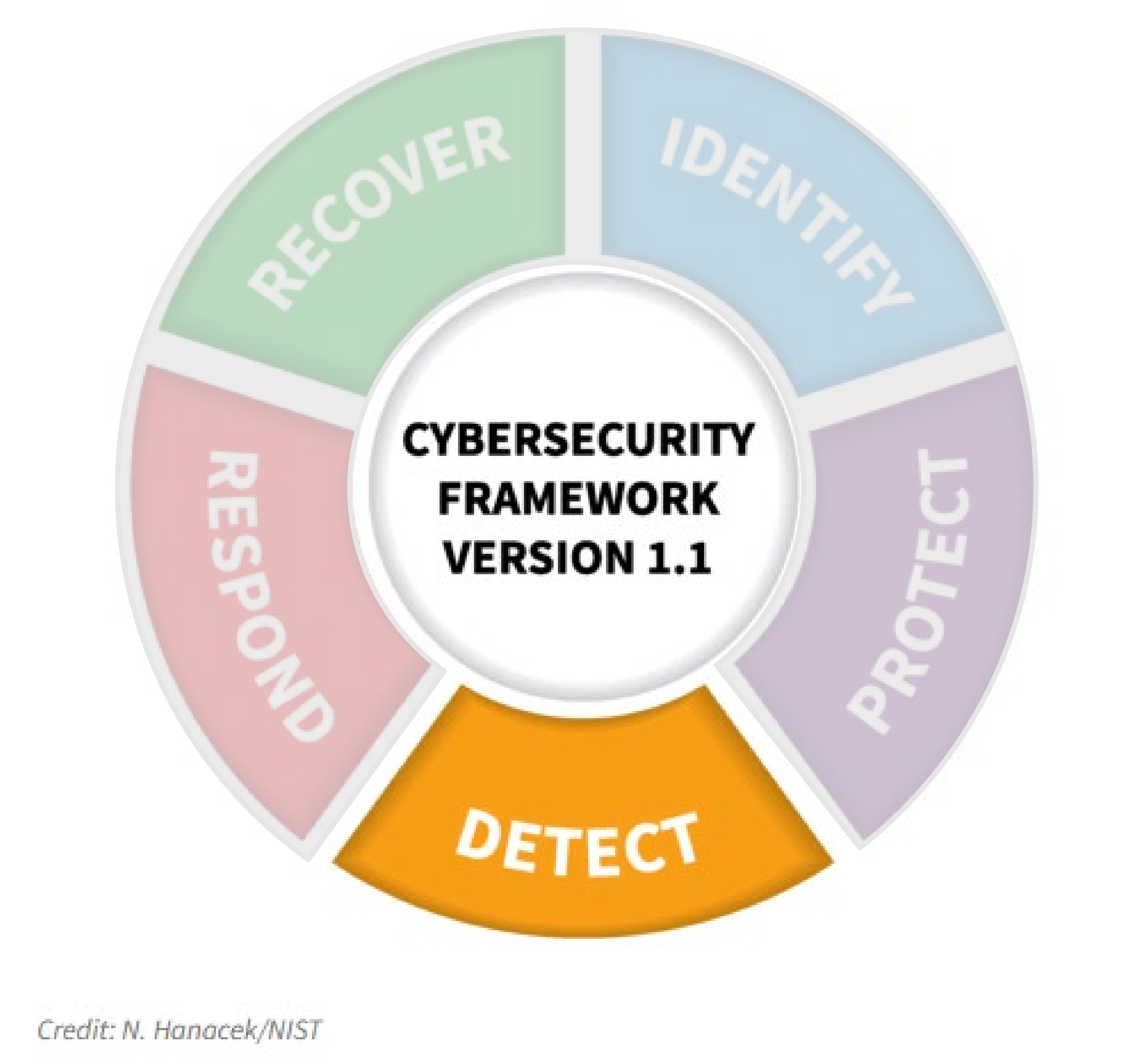
Credit: N. Hanacek/NIST

NIST Framework:



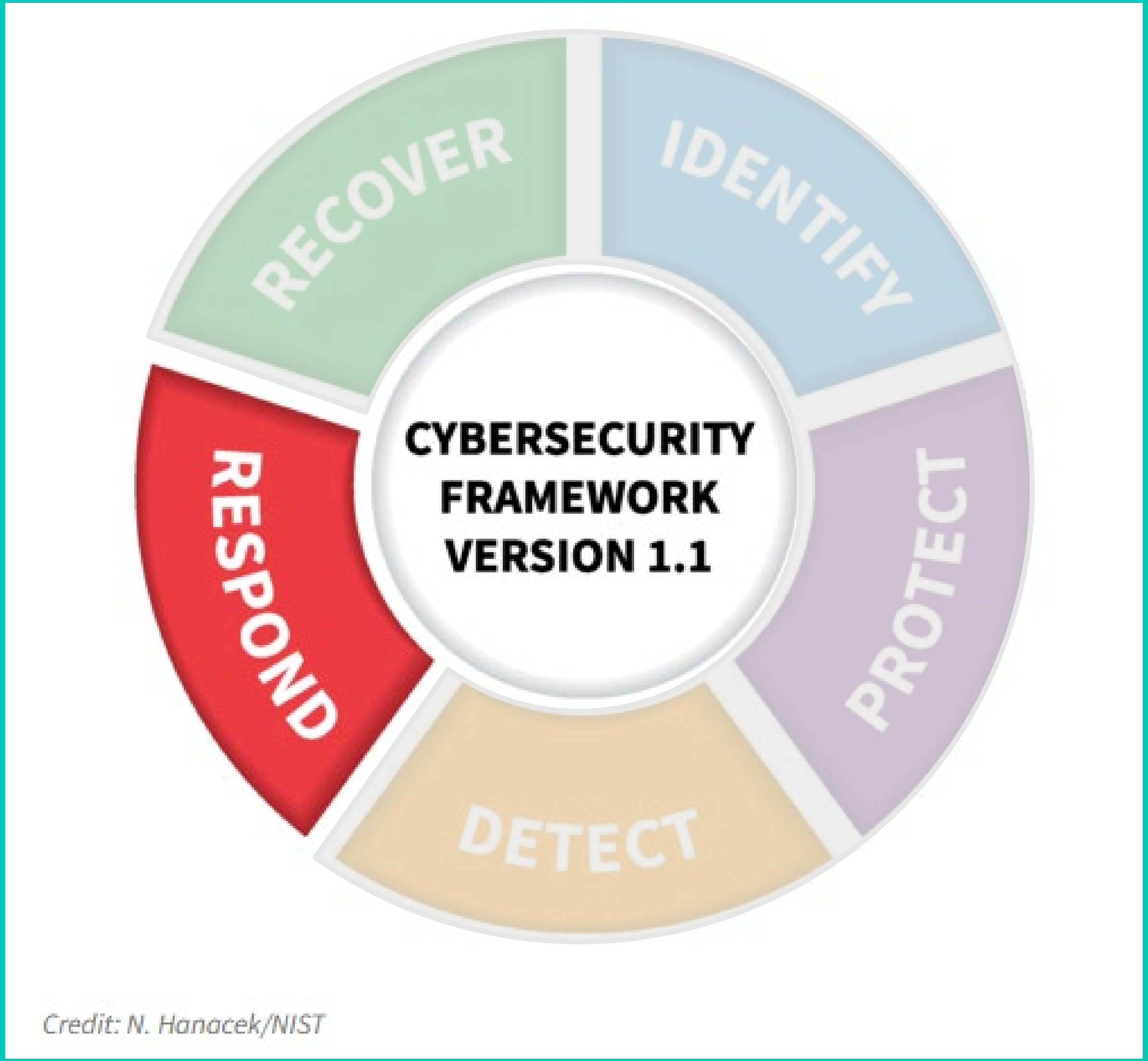
Credit: N. Hanacek/NIST

NIST Framework:



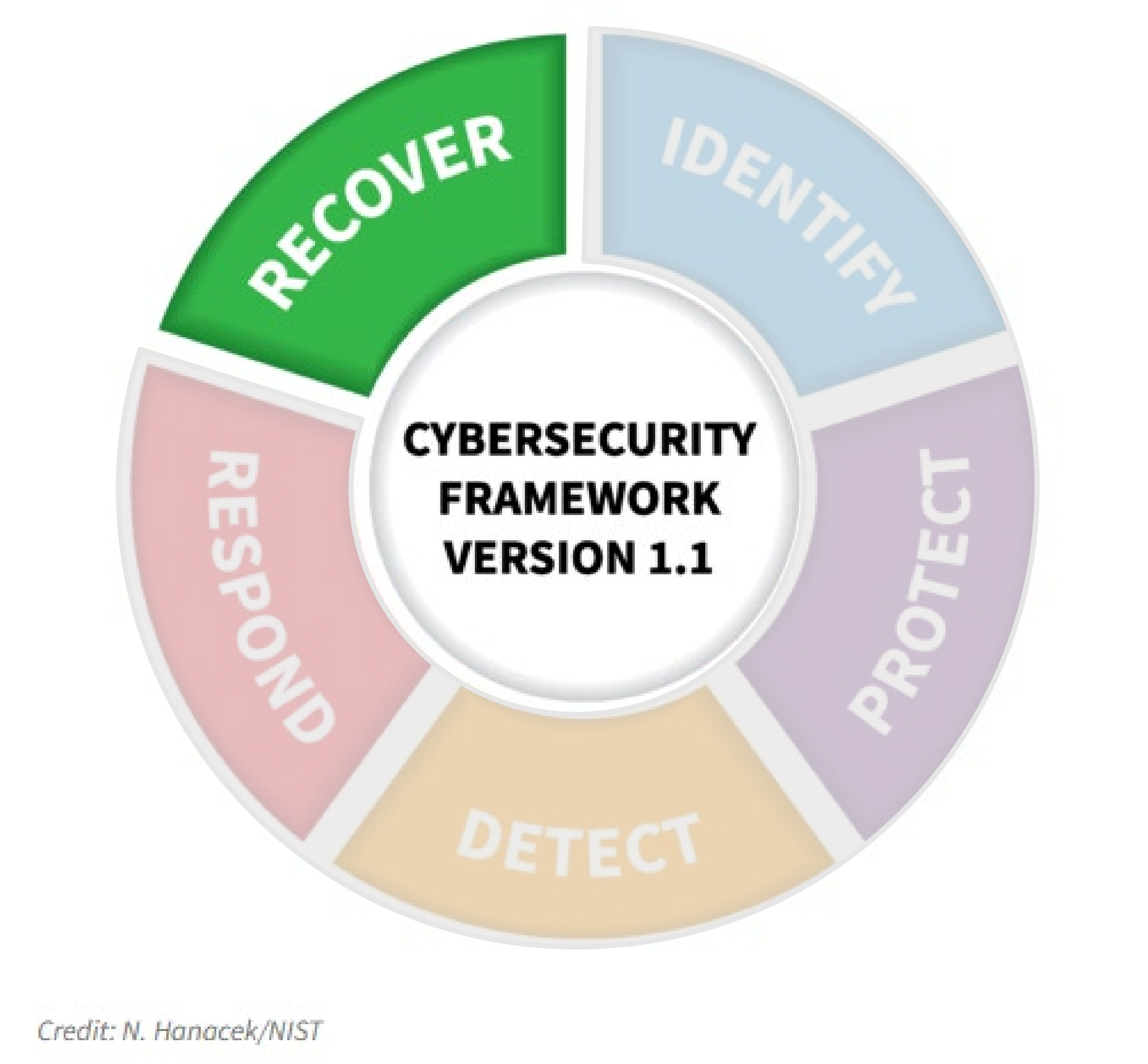
Credit: N. Hanacek/NIST

NIST Framework:



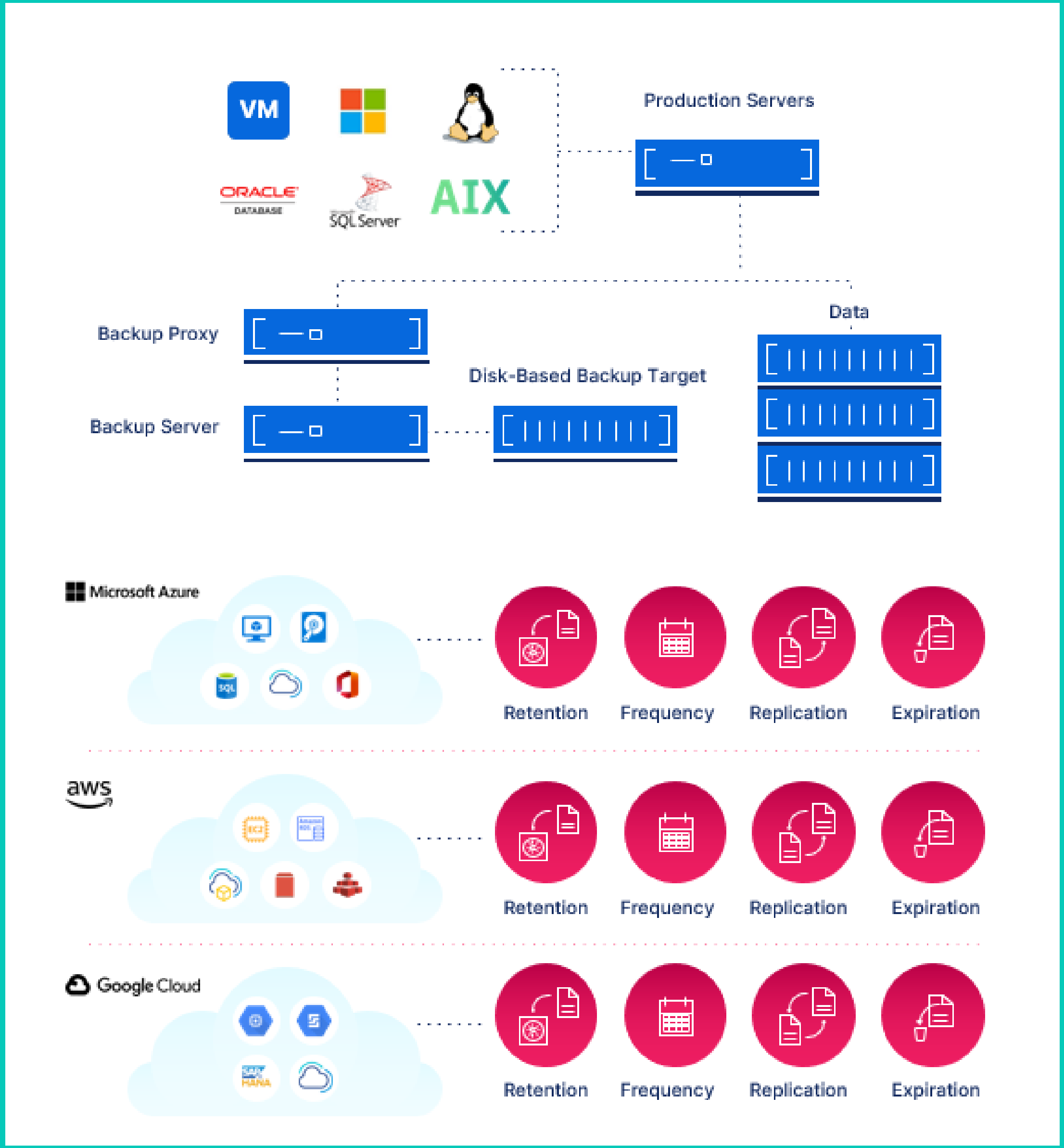
Credit: N. Hanacek/NIST

NIST Framework:



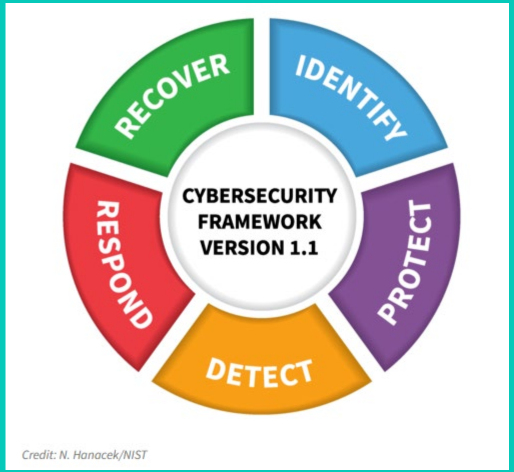
Credit: N. Hanacek/NIST

Recovery ≠ Cyber Recovery



New Questions

- What exactly do I recover?
- Was sensitive data in scope?
- How do I ensure I don’t restore the malware?

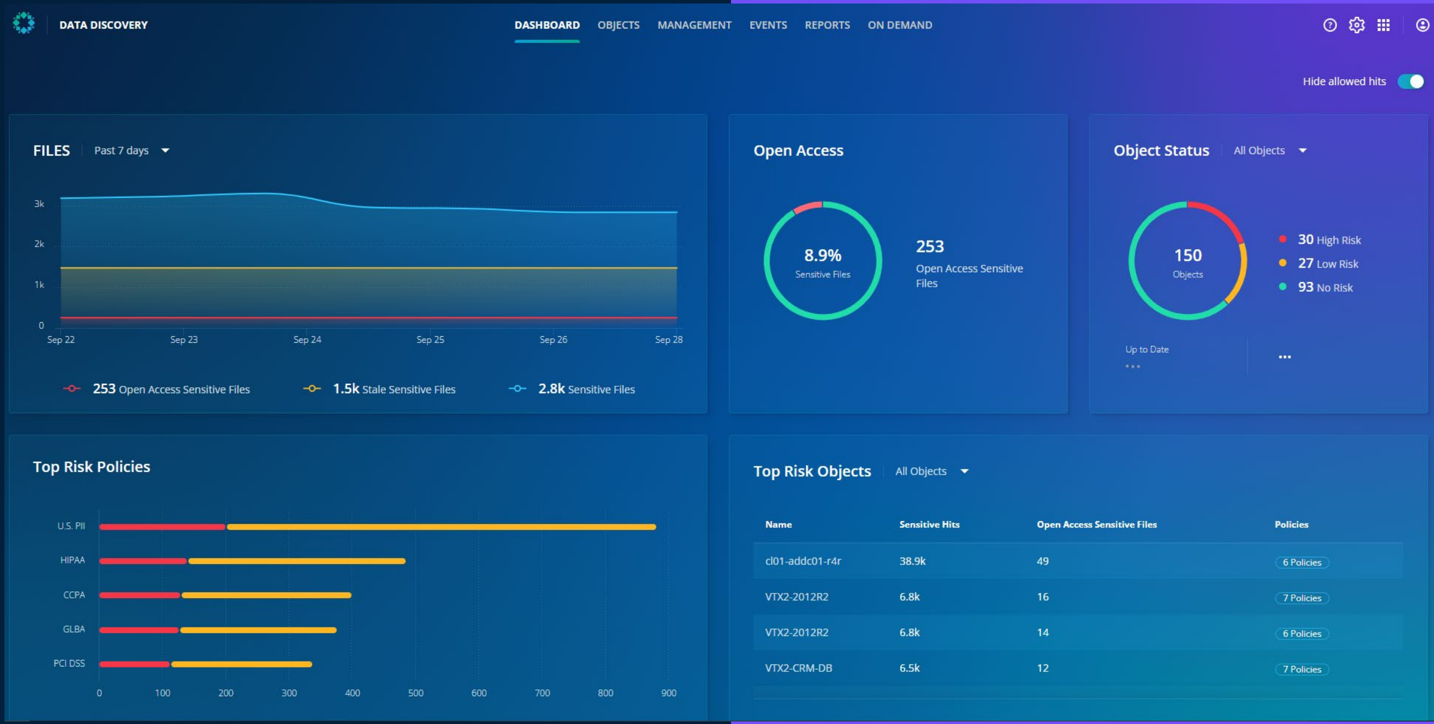


Credit: N. Hanacek/NIST

Sensitive Data Discovery

Reduce sensitive data exposure by discovering what types of sensitive data you have, where it lives, and who has access to it

- Discover sensitive business data
- 60+ built-in analyzers
- Assess risk of exfiltration



253 Open Access Sensitive Files

1.5k Stale Sensitive Files

2.8k Sensitive Files

253 Open Access Sensitive Files

30 High Risk

27 Low Risk

93 No Risk

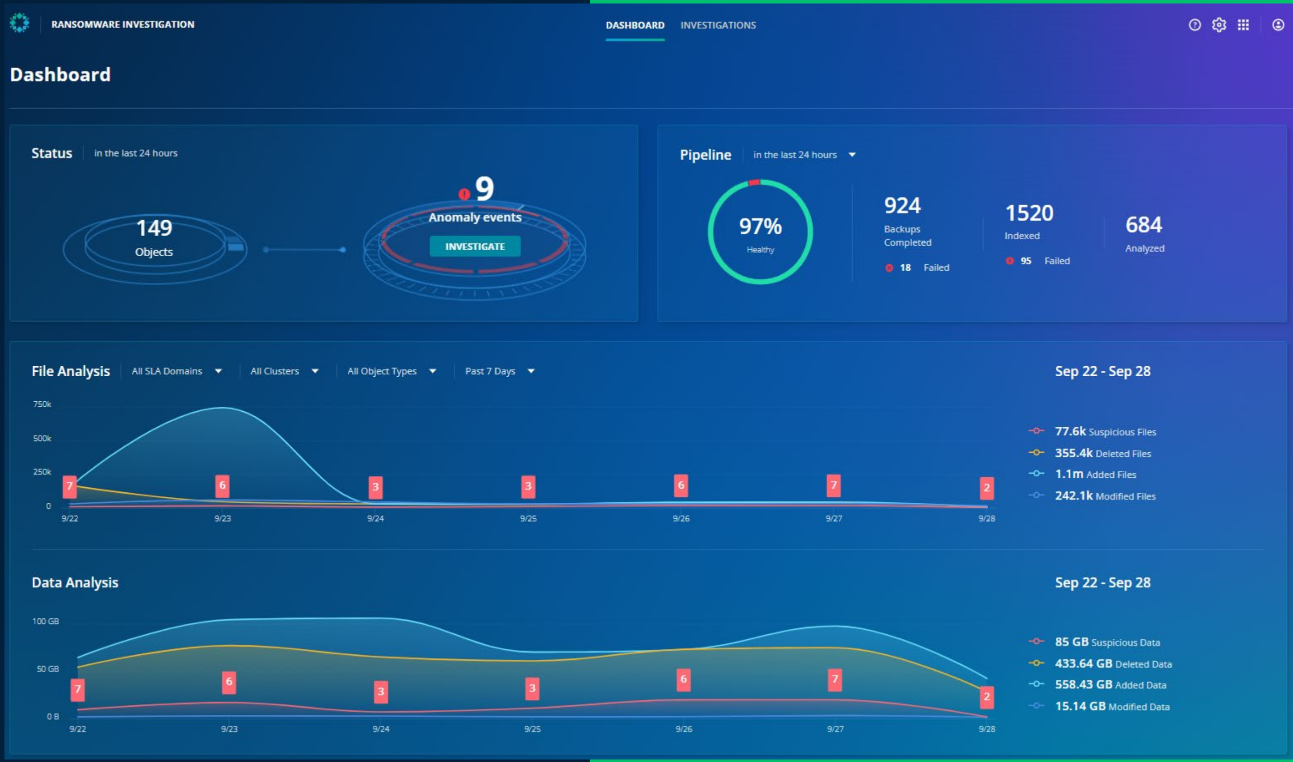
Top Risk Objects — All Objects

Name	Sensitive Hits	Open Access Sensitive Files	Policies
cl01-addc01-r4r	38.9k	49	6 Policies
VTX2-2012R2	6.8k	16	7 Policies
VTX2-2012R2	6.8k	14	6 Policies
VTX2-CRM-DB	6.5k	12	7 Policies

Ransomware Investigation

Determine the scope of ransomware attacks, using high fidelity machine learning to detect deletion, modifications, and encryptions

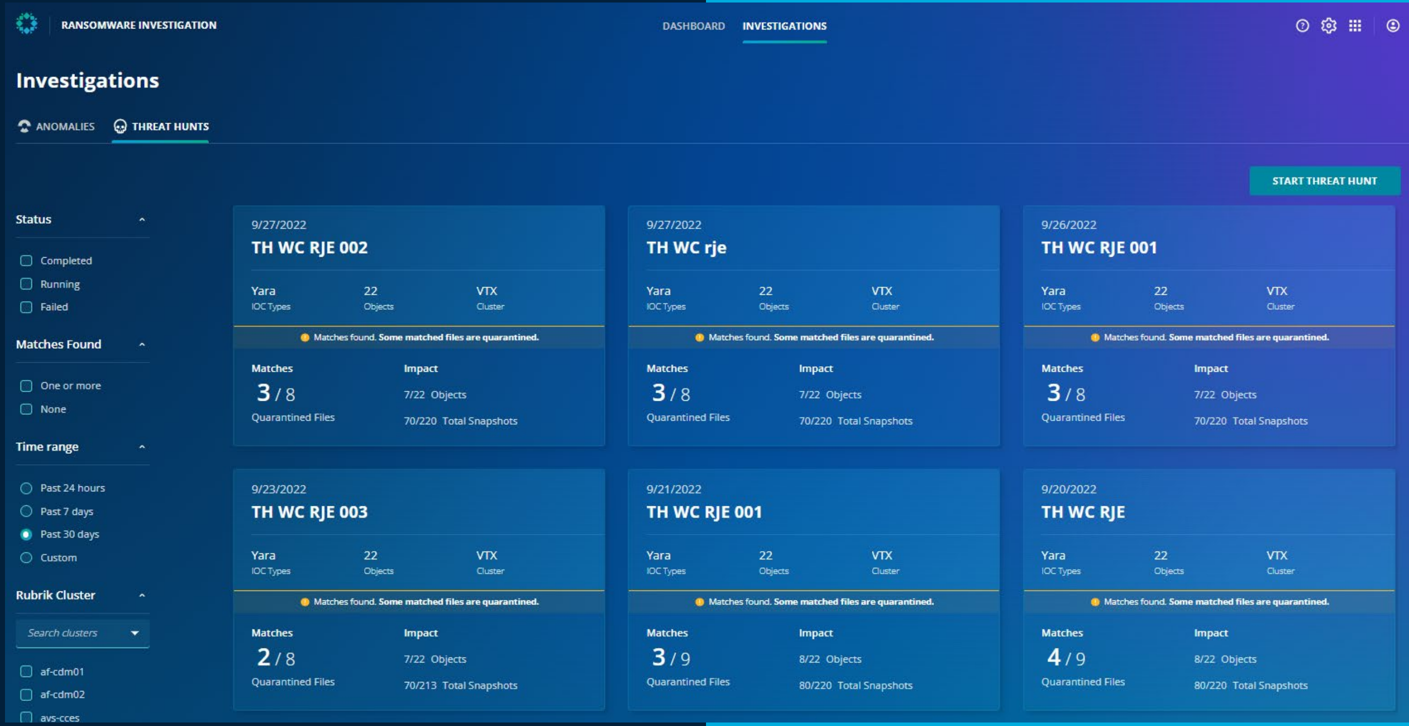
- Detect data anomalies and encryption events
- Determine ransomware infection type
- Assess the blast radius impact



Threat Hunting

Prevent malware reinfection by analyzing the time-series history of snapshots for IOCs to identify initial point, scale, and time of infection

- Scan for threats using known indicators of compromise
- Integrate with application recovery workflows
- Prevent malware reinfection



Investigations

Status
□ Completed
□ Running
□ Failed

Matches Found
□ One or more
□ None

Time range
○ Past 24 hours
○ Past 7 days
● Past 30 days
○ Custom

Rubrik Cluster
Search clusters
□ af-cdm01
□ af-cdm02
□ avs-cces

9/27/2022
TH WC RJE 002
Yara IOC Types | 22 Objects | VTX Cluster
Matches found. **Some matched files are quarantined.**
Matches 3 / 8 Quarantined Files
Impact 7/22 Objects
70/220 Total Snapshots

9/27/2022
TH WC rje
Yara IOC Types | 22 Objects | VTX Cluster
Matches found. **Some matched files are quarantined.**
Matches 3 / 8 Quarantined Files
Impact 7/22 Objects
70/220 Total Snapshots

9/26/2022
TH WC RJE 001
Yara IOC Types | 22 Objects | VTX Cluster
Matches found. **Some matched files are quarantined.**
Matches 3 / 8 Quarantined Files
Impact 7/22 Objects
70/220 Total Snapshots

9/23/2022
TH WC RJE 003
Yara IOC Types | 22 Objects | VTX Cluster
Matches found. **Some matched files are quarantined.**
Matches 2 / 8 Quarantined Files
Impact 7/22 Objects
70/213 Total Snapshots

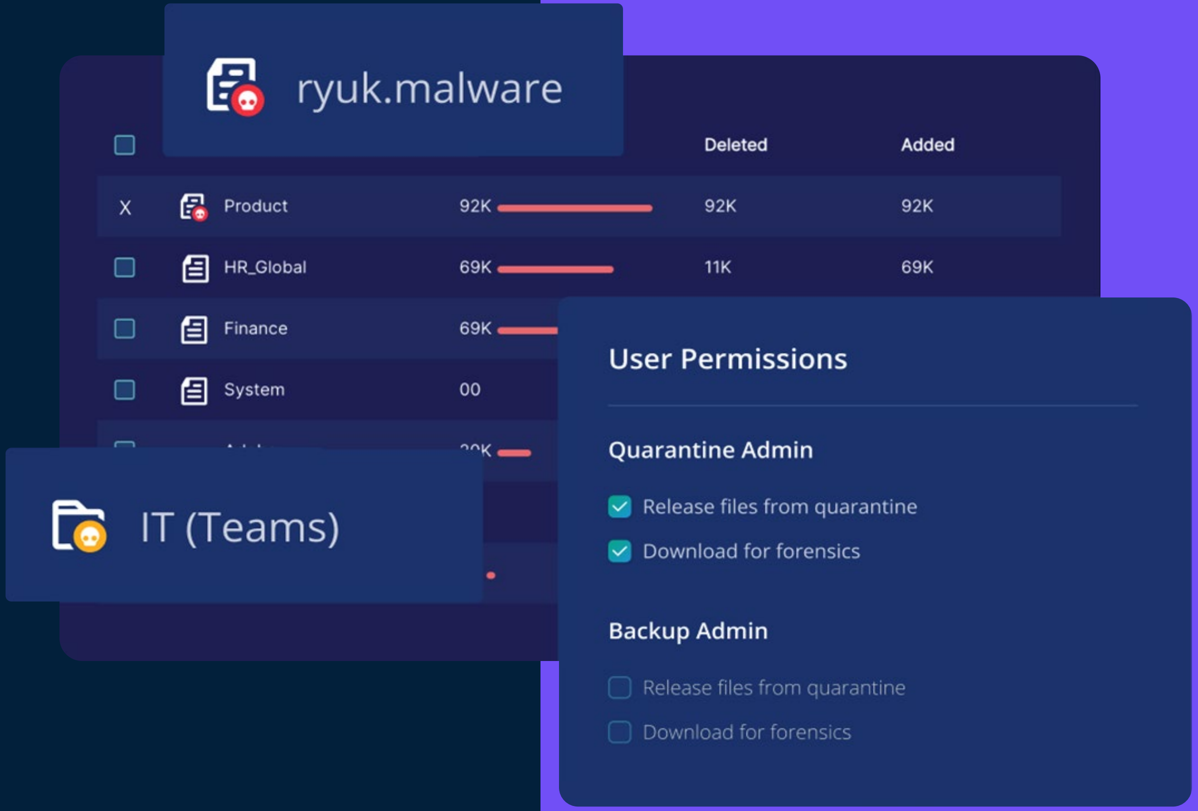
9/21/2022
TH WC RJE 001
Yara IOC Types | 22 Objects | VTX Cluster
Matches found. **Some matched files are quarantined.**
Matches 3 / 9 Quarantined Files
Impact 8/22 Objects
80/220 Total Snapshots

9/20/2022
TH WC RJE
Yara IOC Types | 22 Objects | VTX Cluster
Matches found. **Some matched files are quarantined.**
Matches 4 / 9 Quarantined Files
Impact 8/22 Objects
80/220 Total Snapshots

Threat Containment

Ensure safe and quick data recovery by quarantining data infected with malware

- Prevent reinfection during recovery by isolating infected data
- Control access to quarantined data with granular role-based access control
- Download quarantined data to analyze the root cause, point of origin and other details



ryuk.malware

□			Deleted	Added
X	Product	92K	92K	92K
□	HR_Global	69K	11K	69K
□	Finance	69K		
□	System	00		

IT (Teams)

User Permissions

Quarantine Admin

☑ Release files from quarantine

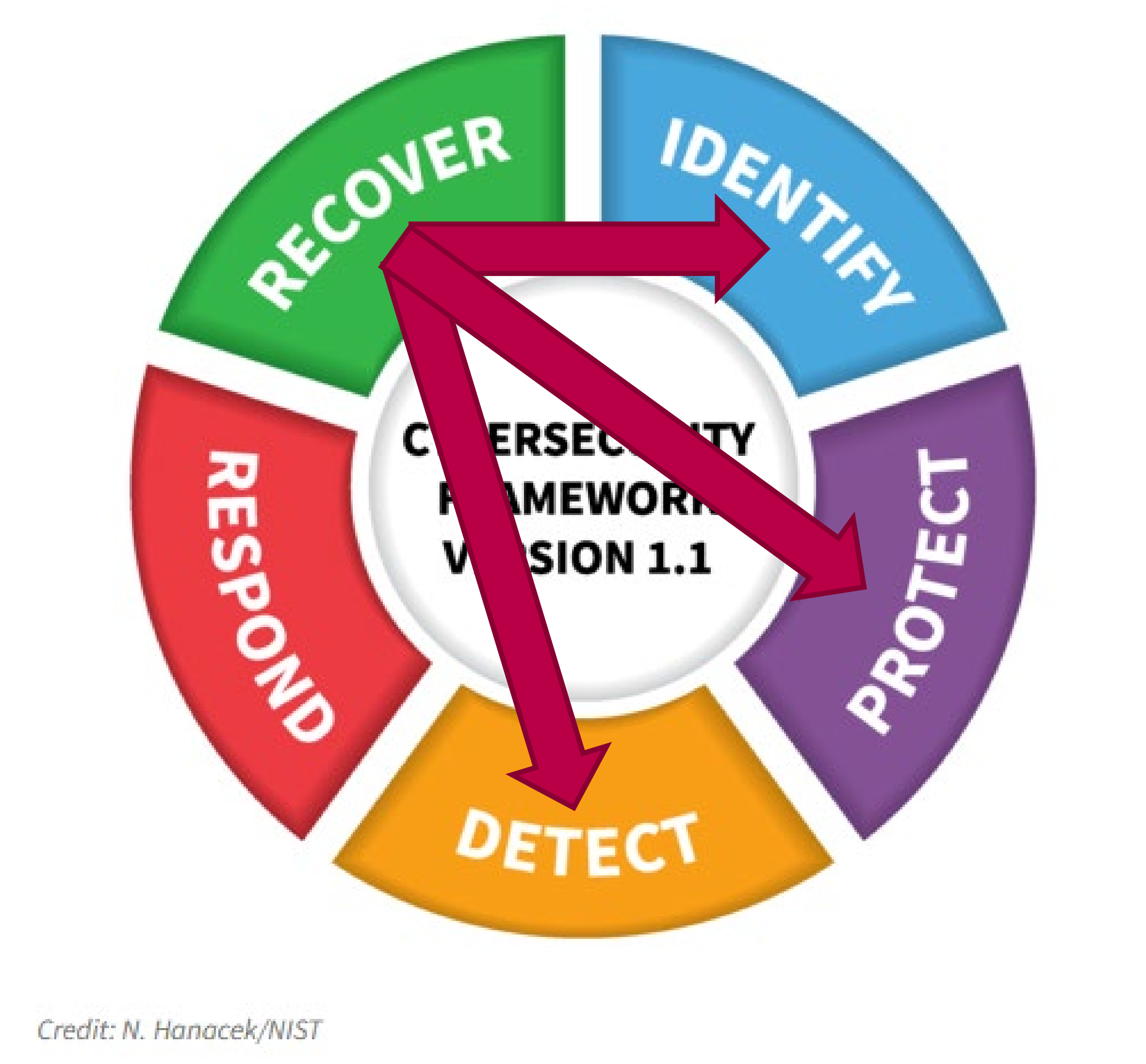
☑ Download for forensics

Backup Admin

□ Release files from quarantine

□ Download for forensics

NIST Framework:



Credit: N. Hanacek/NIST

rubrik Security Cloud™

Thank You