The danger of ransomware for organizations

Prevention, protection and response

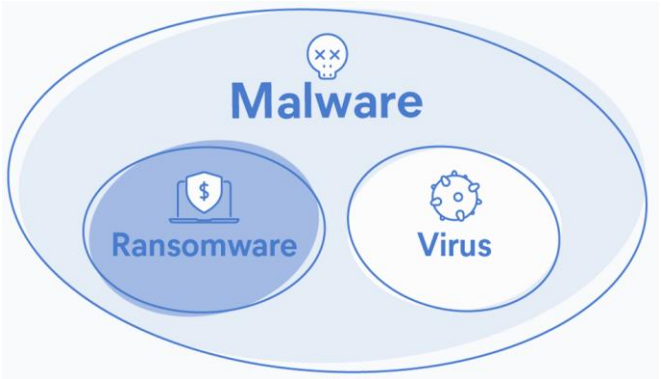
Nicolás D'Alessandro Calderon
Network and System Administration
Universitat Oberta de Catalunya, 2025

1. What is ransomware?

Malware that encrypts or locks systems and data.

Demands payment to gain access.

Affects **all types** of organizations.



2. Types of ransomware

File Encryption
Ransomware locks your files so you can't open them.

Full System Lockout
You lose access to your whole computer or network.

Double Extortion
Attackers steal your data and lock it to ask for more money.

Famous cases: CryptoLocker, WannaCry, Ryuk

3. Impact and consequences

- Major financial losses
- Reputational damage to companies
- Legal sanctions if confidential data is leaked

Around 60% of organizations suffered attacks

4.1 Prevention: Organizational Policies

Least Privilege Access
Give each user only the access they really need to do their job.

Regular Patching and Updates
Keep systems and software updated to fix known problems.

Use of Frameworks like NIST or ISO 27001
Follow trusted guides to improve security and show good practices.

Breaking the network into parts makes it harder for attackers to move and limits the damage.

4.2 Prevention: Awareness

- Ongoing Training
- Phishing Simulations and Campaigns
- Reporting Culture
- Support from Management

Many attacks begin with human error. Investing in training is more cost-effective than suffering operational outages.

5. Active protection

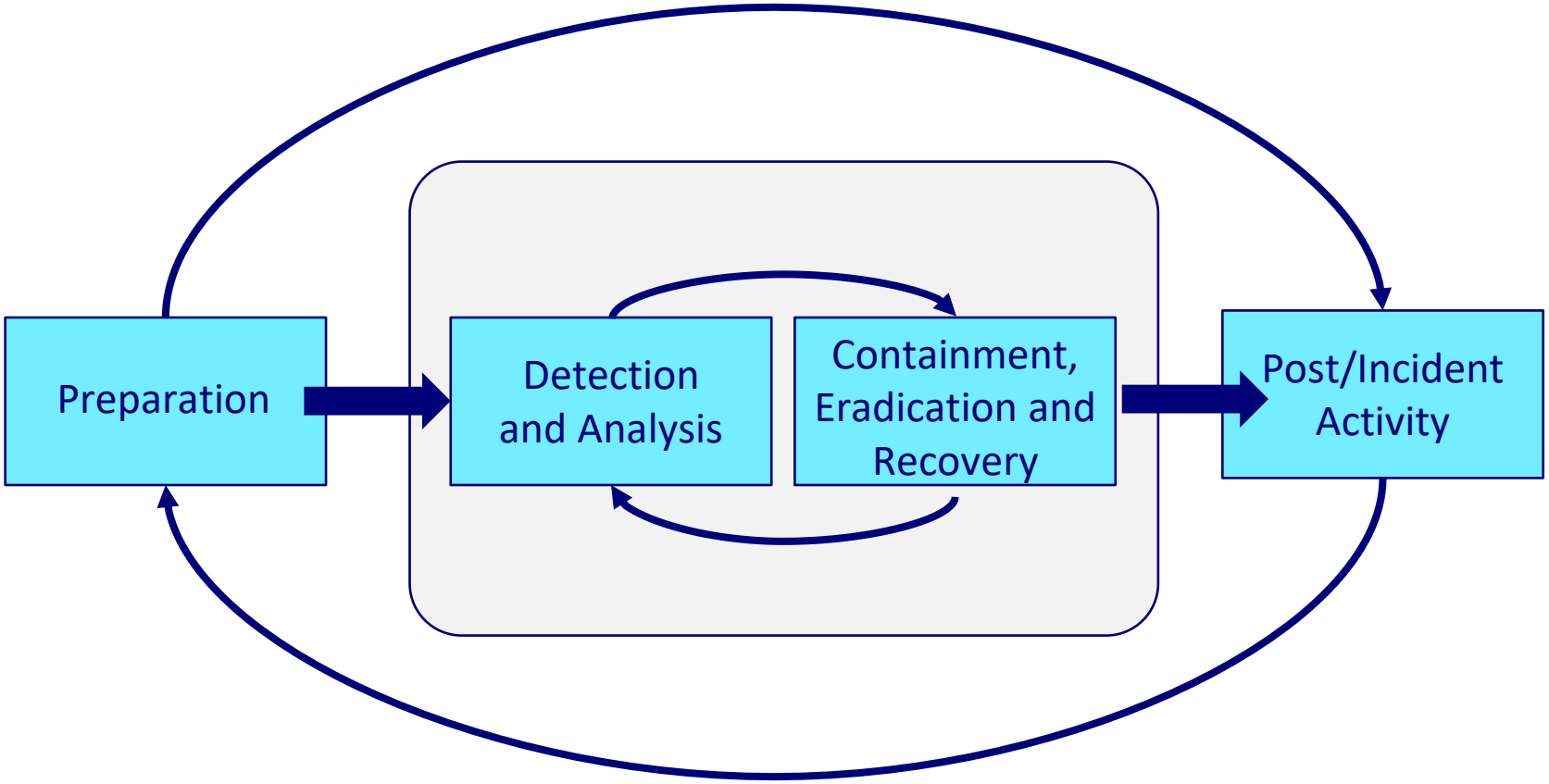
Suspicious Activity Detection (EDR/XDR)
These tools watch computers and servers. They can find strange actions like many files being locked or attackers moving inside the system.

Network Monitoring (NDR)
This tool watches the network traffic. It can find unusual movements, like ransomware spreading or data being stolen.

Immutable Backups
Backups that cannot be changed or deleted for a certain time. Even if ransomware attacks, the backup stays safe.

A coordinated protection system isolates compromised systems in minutes, before ransomware can spread.

6. Response to Incidents



7. Ransom Payment

No guarantees

Funds crime and motivates new attacks

Legal risks

Organizations such as the FBI, CISA and ENISA advise against this practice.

8. Current Solutions Available in the Market

Endpoint protection:

Microsoft Defender, Sophos

Orchestration:

Splunk, QRadar, Microsoft Sentinel

Backup:

Veeam, Commvault, Acronis

Open source:

Wazuh, Zeek, Bacula

Thanks!

Nicolás D'Alessandro Calderon
Network and System Administration
Universitat Oberta de Catalunya, 2025