

Féidearthachtaí as Cuimse
Infinite Possibilities

CYBER ATTACK CASE STUDY

How we responded to an attack on our systems

Richard.dunne@tudublin.ie



**CYBER
SECURITY
SUMMIT**

T
DUBLIN
OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
TECHNOLOGICAL
UNIVERSITY DUBLIN

Presentation Outline

- A brief history of TU Dublin
- The cyber incident
- Activating the incident response plan
- The role of the Cyber Security Incident Response Team (CSIRT)
- Working through the incident & core challenges
- Lessons learnt
- Biggest take away: Protect your privileged identity

A Brief History



T
OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
DUBLIN

*Institute of Technology
Lanchardstown
Institiúid Teicneolaíochta
iLle Bhlainséir*

TECHNOLOGICAL
UNIVERSITY DUBLIN

TU Dublin in Numbers

3,500
Staff

30,000
Students

80,000
Accounts

45,000
Devices

The Cyber Incident: Unauthorised Access

During Easter week, both TU Dublin Tallaght campus and NCI were hit with RYUK ransomware

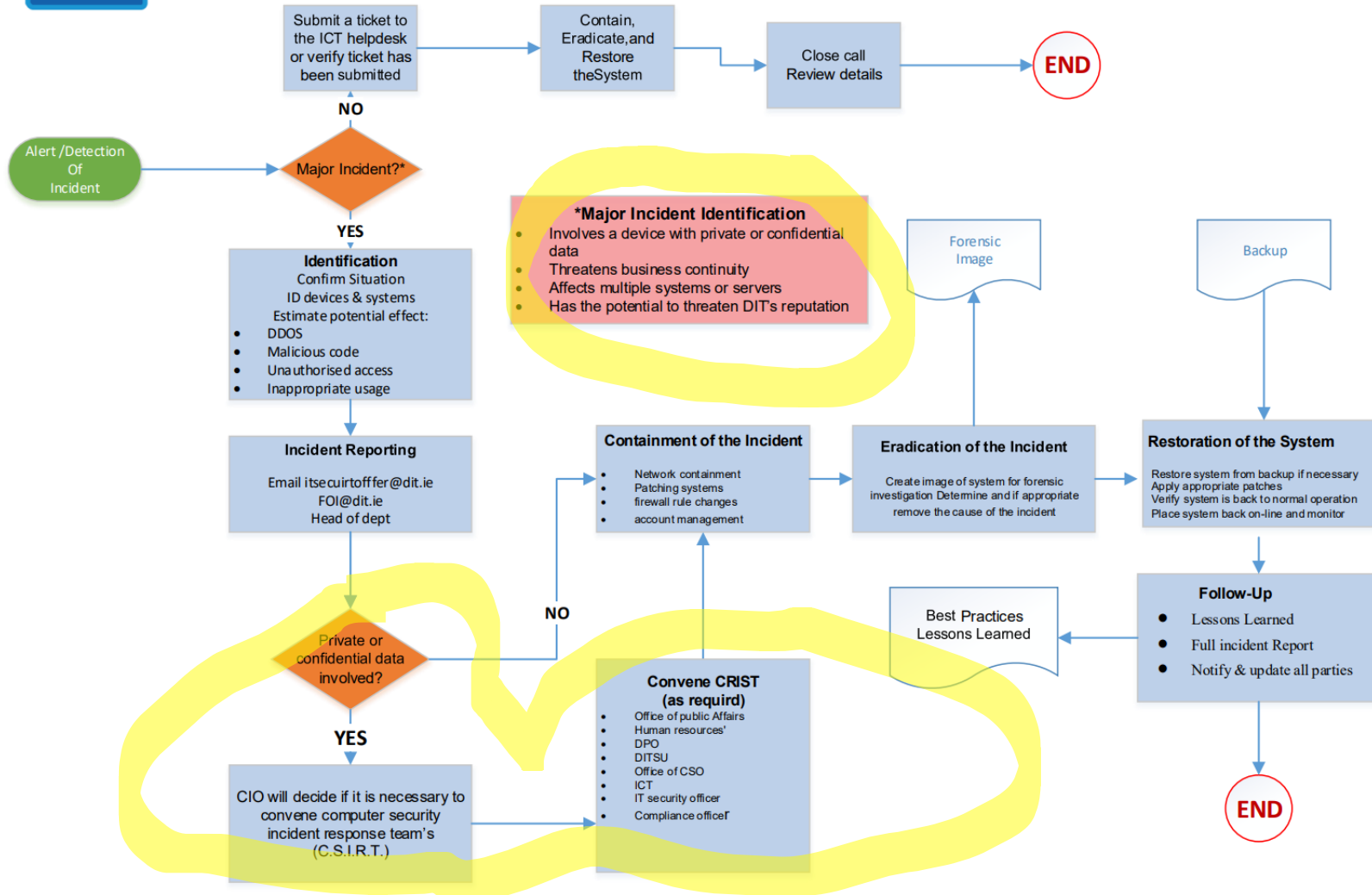
TU Dublin City started to audit and review our AD set up

Our Security team spotted unauthorised access within active Directory with evidence of lateral movement

Our antivirus logs showed attempts of malware activity in the week before Easter



DIT Security Incident Response Procedure



Cyber Security Incident Response Team (CSIRT)

Primary Members

CTO
IT Security Manager
System Administrators
Network and Systems Team
Desktop Support
Compliance office
3rd party Disaster Recovery Coordinators

Secondary Members

Management Team Sponsor
Local Site Technical Staff
Estates Office
Human Resources
Public Affairs Office
Finance
Legal

What the CSIRT Provides

Brings governance to the actions of the team

Opens the internal channels of communications within the university

Manages Stakeholder engagement within the incident

Deals with comms, external and internally

Frees up tech team to do tech work

Gives structure to the incident

What actions did we take?

1-24 hours

- Reset and recreated all privileged accounts ,
- imaged PC showing unauthorised access,
- take FW, PC, server logs
- Take servers off line

25-48 hours

- Review of logs showed antivirus did its job
- no malware installed,
- FW logs showed no C&C traffic or exfiltration of data
- moved into incident review stage

Working Through the Incident & Core Challenges



Working with our
insurance cyber
teams



Containment
stage



When do you trust
your systems
again?

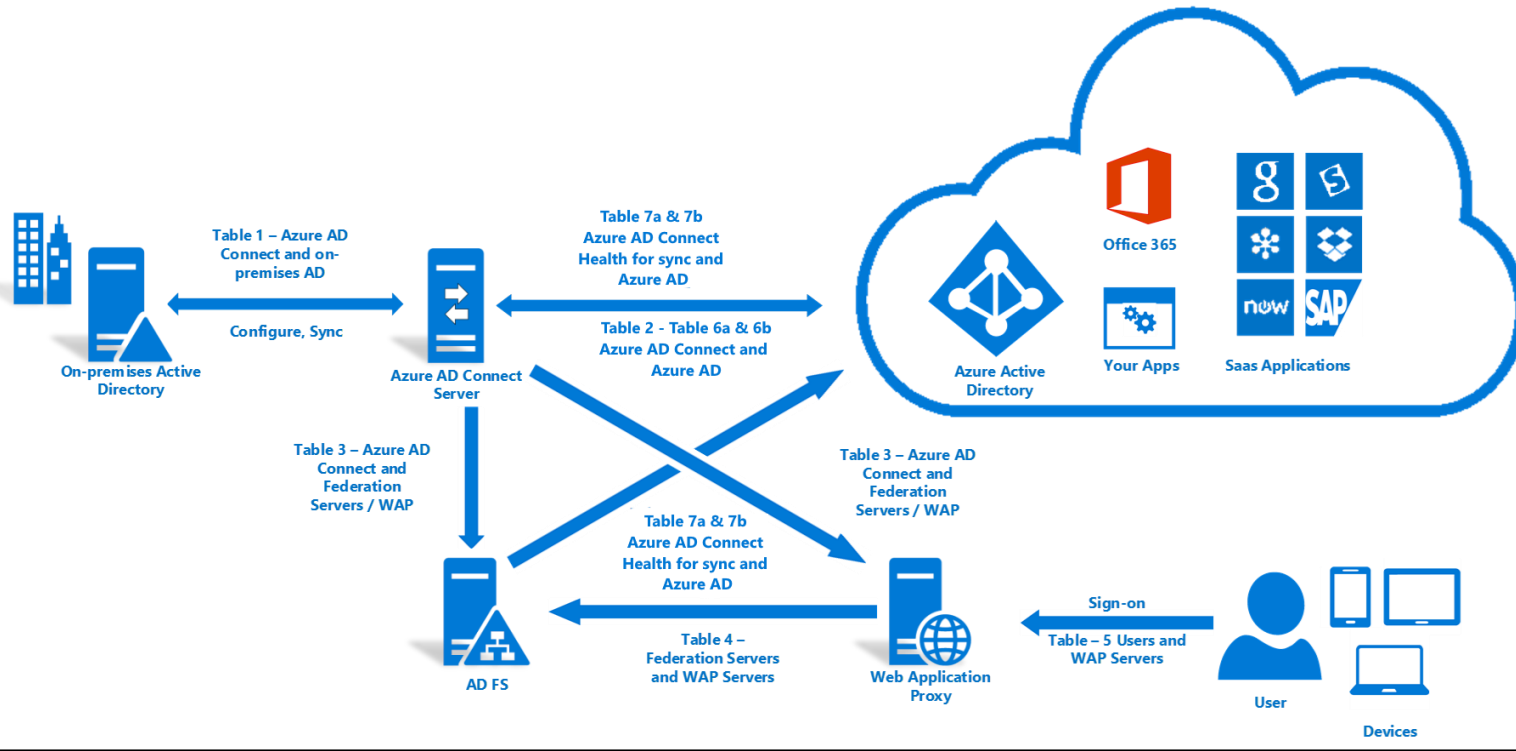


How did they do
it?



Do we assume all
passwords are/will
be compromised?

Hybrid Identity



Containment
in a
Hybrid World

Learning our Lessons

- Lack of analysis of logs
- Lack of EDR on servers and desktops
- Need for complete separation of AD tiers
- Need to upgrade AD (LAPS, protected users)
- Audit of AD
- Review containment issues (on prem/Cloud)
- We don't work 24/7



test.mysmartlogon.com - Healthcheck analysis

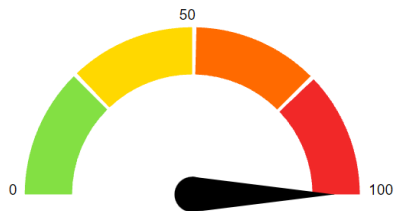
Date: 2021-07-28 - Engine version: 2.10.0.0

This report has been generated with the Auditor Edition of PingCastle [?](#)

Active Directory Indicators

This section focuses on the core security indicators. Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

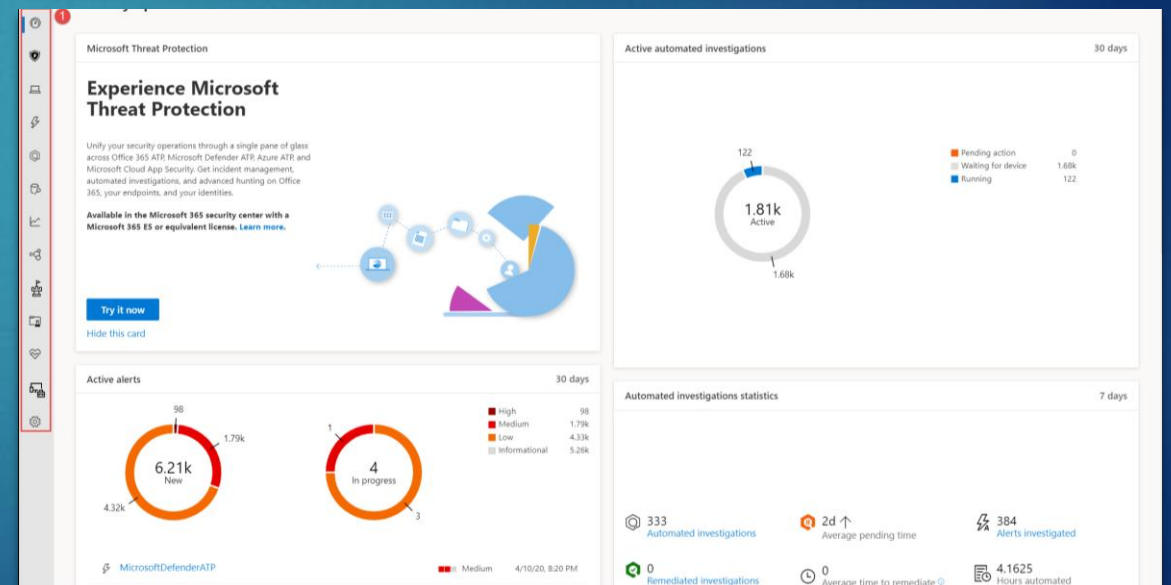
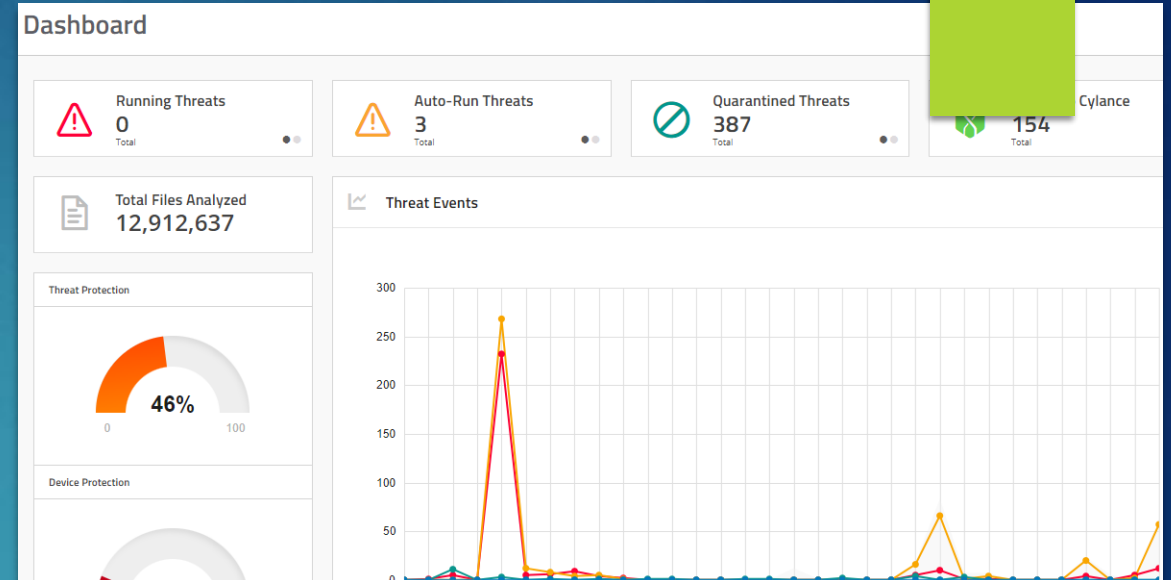
<p>Stale Object : 100 /100 12 rules matched It is about operations related to user or computer objects</p>	<p>Trusts : 100 /100 4 rules matched It is about links between two Active Directories</p>
<p>Privileged Accounts : 100 /100 19 rules matched It is about administrators of the Active Directory</p>	<p>Anomalies : 100 /100 27 rules matched It is about specific security control points</p>

Risk model

Auditing AD

Ping Castle

Endpoint Detection and Response with 24/7 monitoring



Seeing the Benefits

Microsoft Defender for Identity | tudublin | Suspected brute-force attack (LDAP)

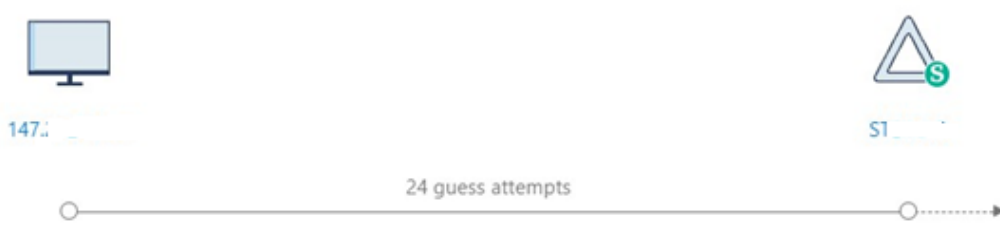
[New investigation experience available. Try it out](#)

[Learn more about this alert](#)

Suspected brute-force attack (LDAP)

An actor on 147.10.10.10 tried 24 passwords on C147101010

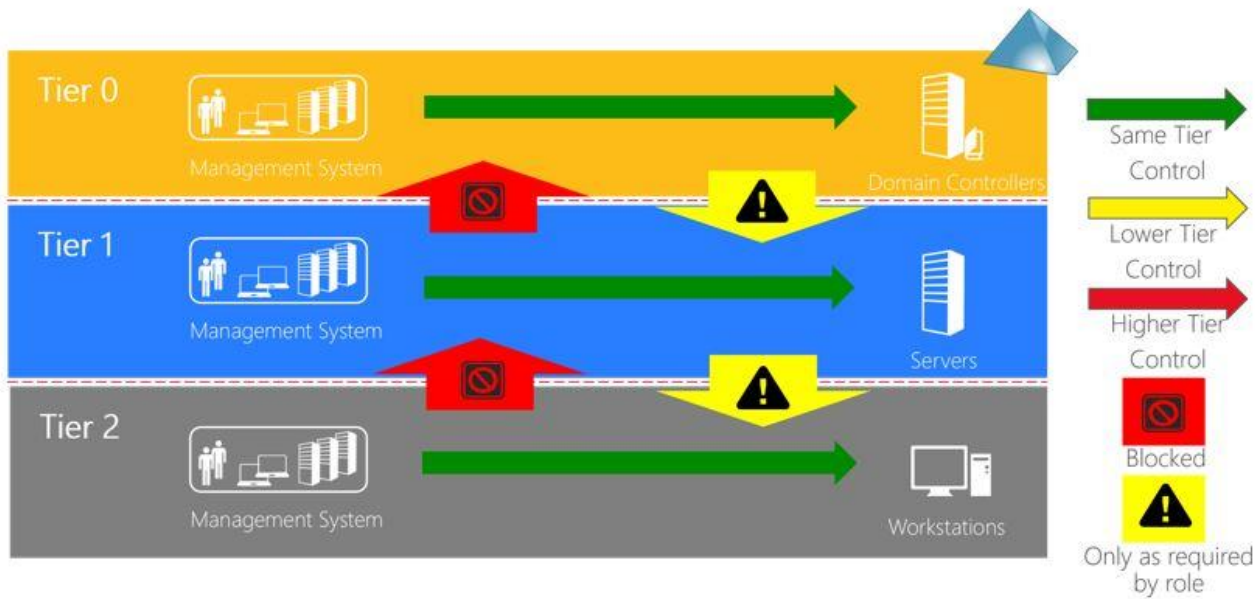
18:12 – 18:20 6 Sep 2021



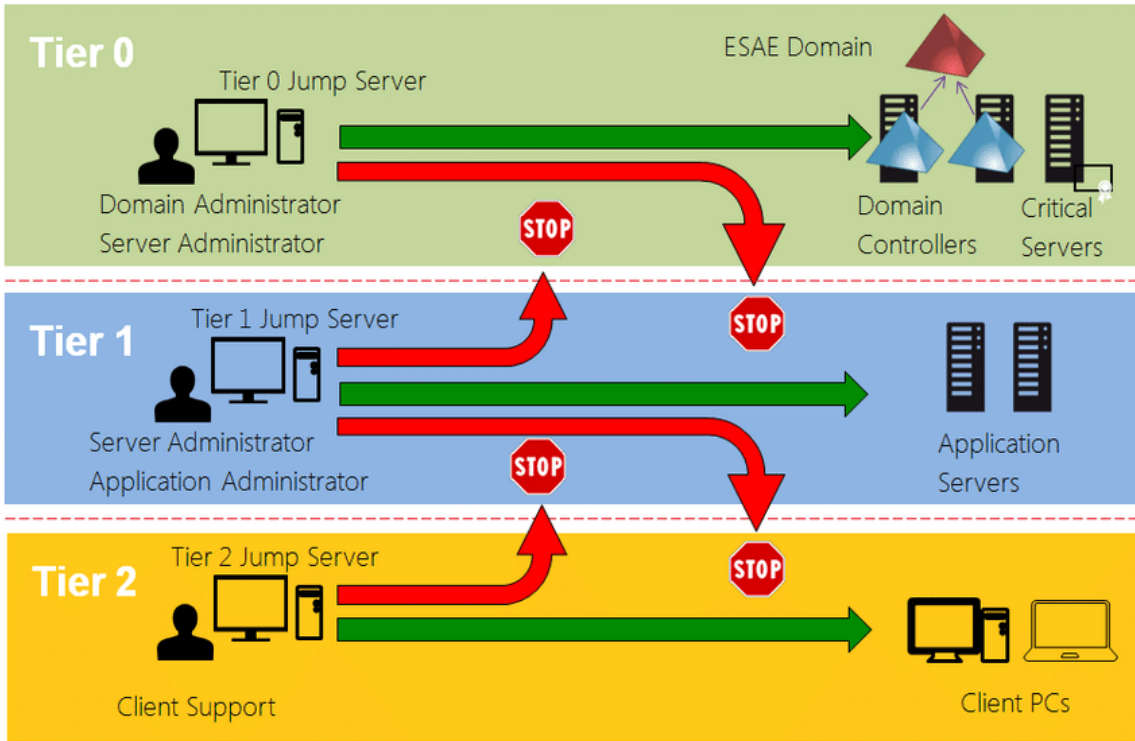
The diagram shows a horizontal timeline with two nodes. The left node is labeled '147.10.10.10' and has a computer icon above it. The right node is labeled 'ST147101010' and has a server icon above it. A horizontal line connects the two nodes, with '24 guess attempts' written above it. The line starts with a solid circle at the left node and ends with a dashed circle and an arrowhead at the right node.

Evidence

- C147101010, not previously observed logging into 147.10.10.10 during the 30 days before this suspicious activity occurred.
- [Details of unsuccessful brute-force attempts:](#)



Protecting Privileged Identity



The Red Forest

Thank You & Questions

Ransomware starts and
ends with AD | LinkedIn