# Practical attack simulations in CNI

How NOT to blow stuff up.

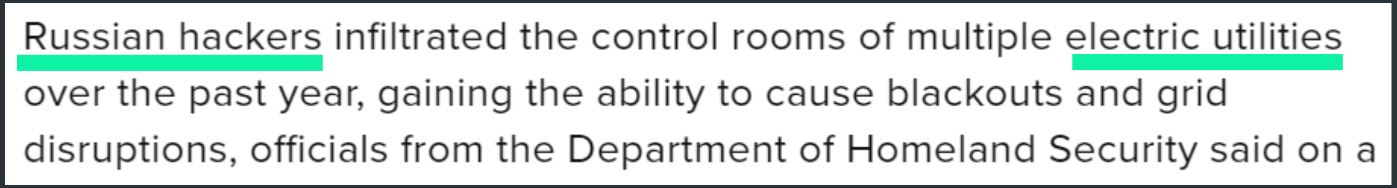
# whoami

- James Coote
- Consultant with MWR
- Focus is on whitebox attack simulations

james.coote@mwrinfosecurity.com

# Why bother with attack simulations?

“

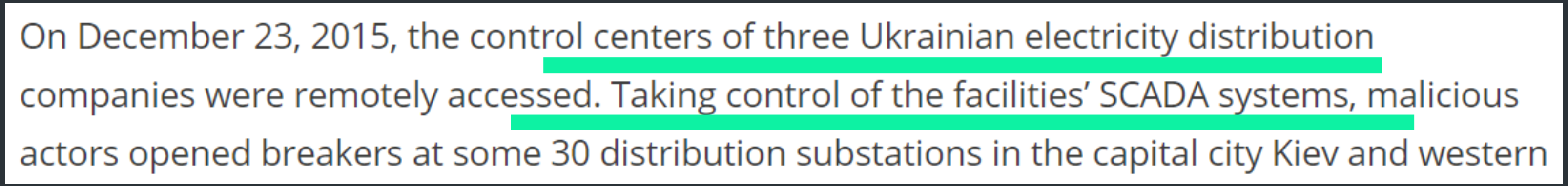


Russian hackers infiltrated the control rooms of multiple electric utilities over the past year, gaining the ability to cause blackouts and grid disruptions, officials from the Department of Homeland Security said on a

”

https://www.utilitydive.com/news/russian-hackers-infiltrated-utility-control-rooms-dhs-says/528487/

“

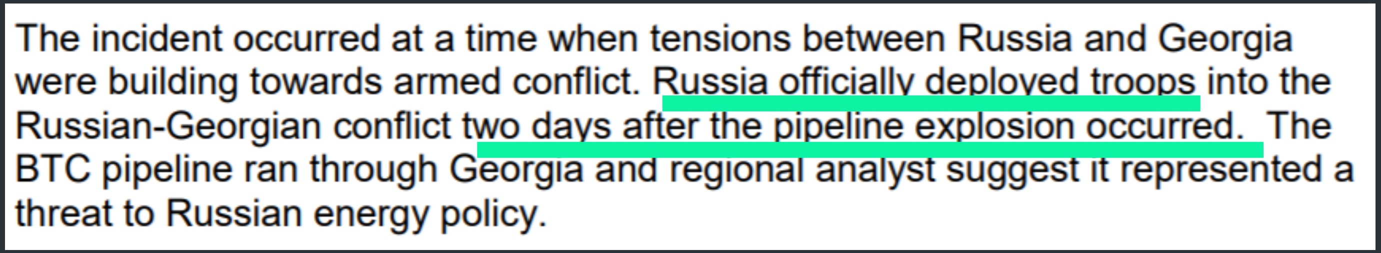


On December 23, 2015, the control centers of three Ukrainian electricity distribution companies were remotely accessed. Taking control of the facilities' SCADA systems, malicious actors opened breakers at some 30 distribution substations in the capital city Kiev and western

”

https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

“



The incident occurred at a time when tensions between Russia and Georgia were building towards armed conflict. Russia officially deployed troops into the Russian-Georgian conflict two days after the pipeline explosion occurred. The BTC pipeline ran through Georgia and regional analyst suggest it represented a threat to Russian energy policy.

”

https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf

# Traditional view of ICS

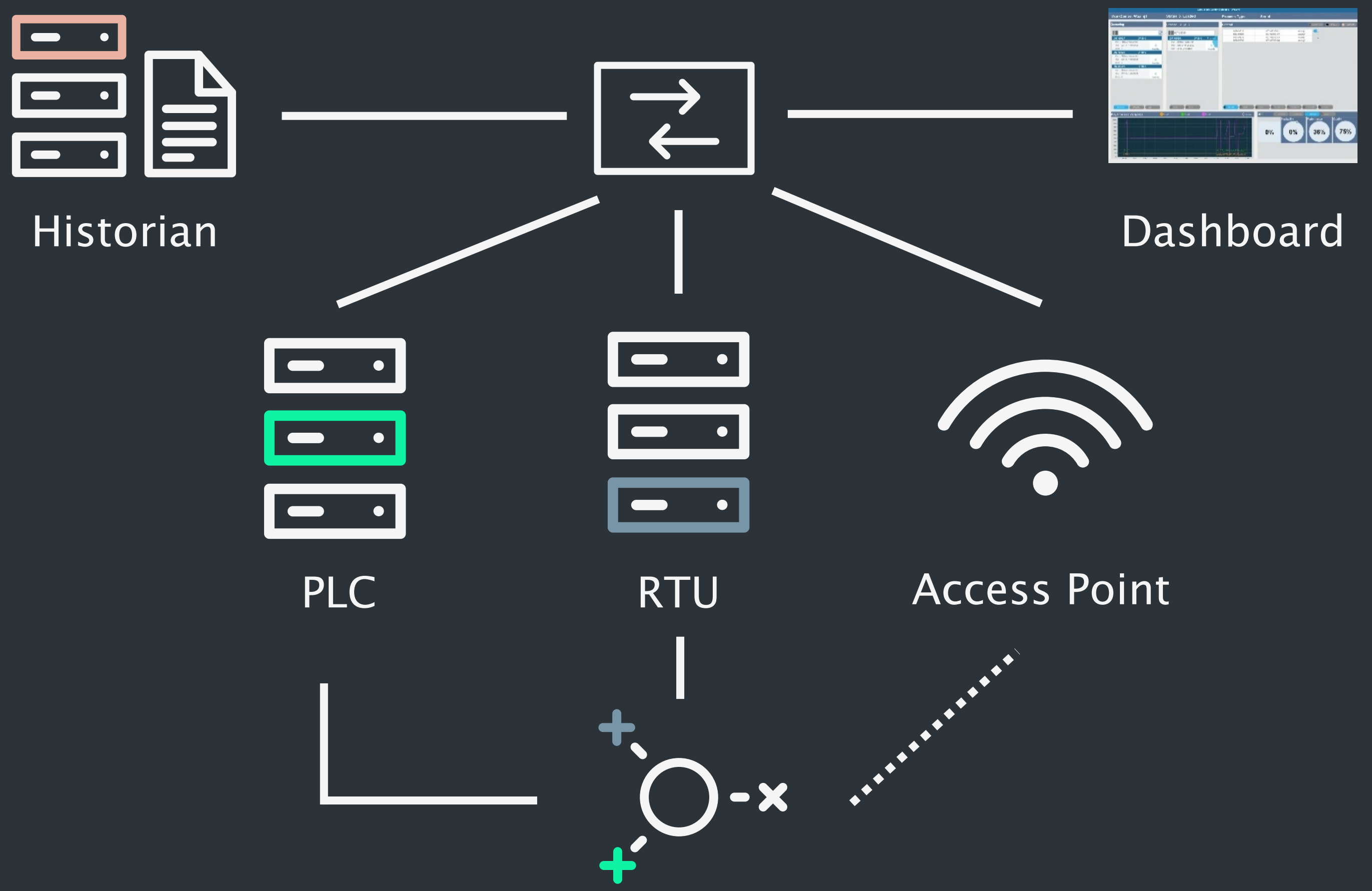
# Threat model

What are we trying to stop an attacker doing?

- Destructive attack
- Disruptive attack
- Information theft

# Typical architecture – Field site

- A field station’s purpose is to manipulate physical processes.
- Water level low? Open the valve and turn on the pump.
- These components are what an attacker is trying to influence.



Historian

Dashboard

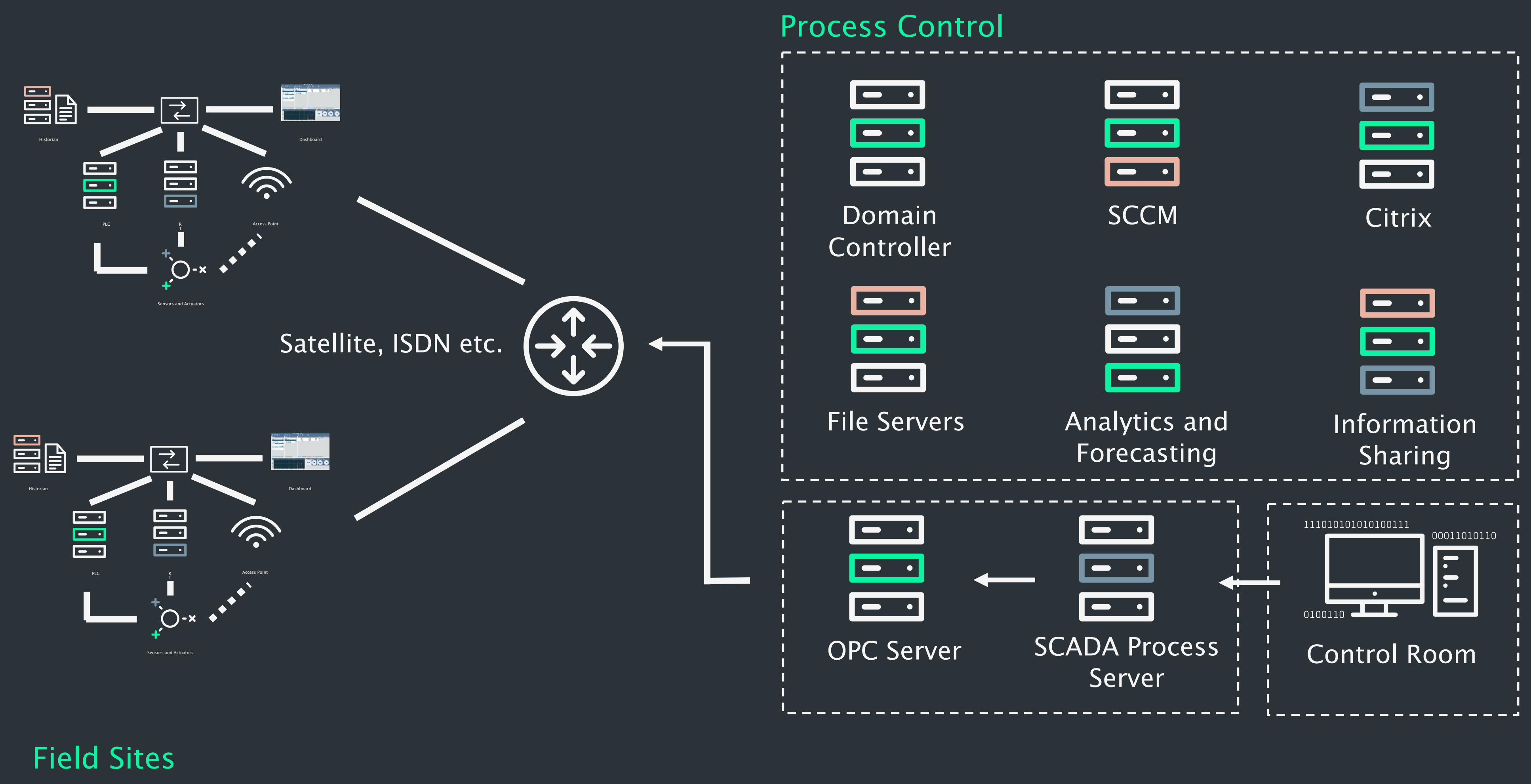
PLC

RTU

Access Point

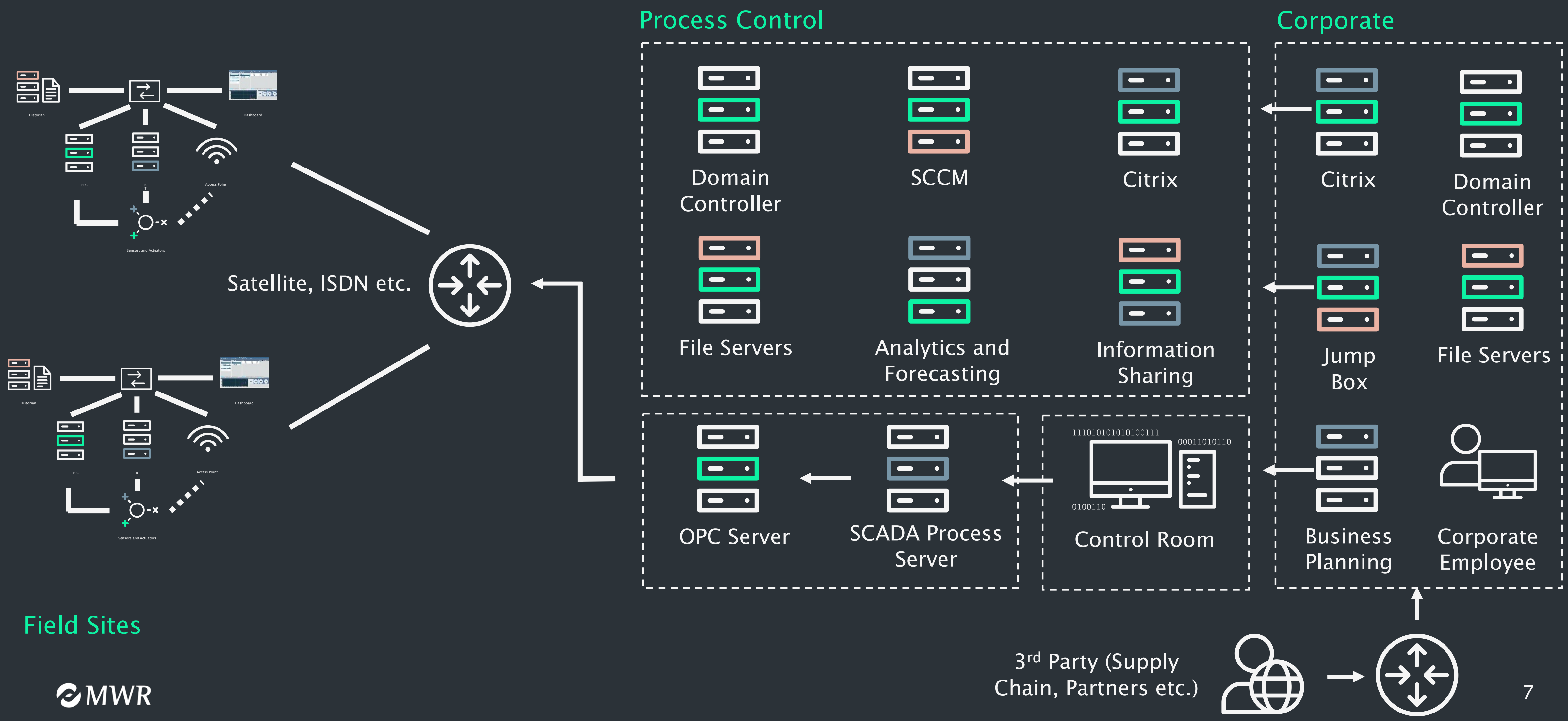
Sensors and Actuators

# Typical architecture – Process control



MWR

# Typical architecture – Complete picture



MWR

# Reduce testing risk

# Model your threat actor

- Know what threat actor you're trying to simulate.
- Use the tools and techniques that align with those actors.
- Tools such as Nmap and Nessus are unlikely to ever be appropriate.

# Whitebox and collaborative

- Conduct interviews with business and technical stakeholders.
- Use this to understand client-specific OT estate and quirks.
- Mimics an attackers reconnaissance phase….just more efficiently and effectively.
- People **WILL** be nervous.

# Take the ego out of testing

- Why are you doing X? To demonstrate impact or to satisfy your ego?

- Will testing the secondary or failover environment provide the same value?

- If you need to de-chain…ASK!

# Pick your team carefully

- They must know their tools and understand their impact.
- They must have an understanding of modern attacker techniques.
- Strive to strike a balance between an understanding of ICS infrastructure and traditional consulting skills.

# Find a security champion

- Identify a senior security champion (think CISO/CRO).
- These should have the authority and autonomy to open doors.
- Pragmatically contextualise risk without fear mongering.

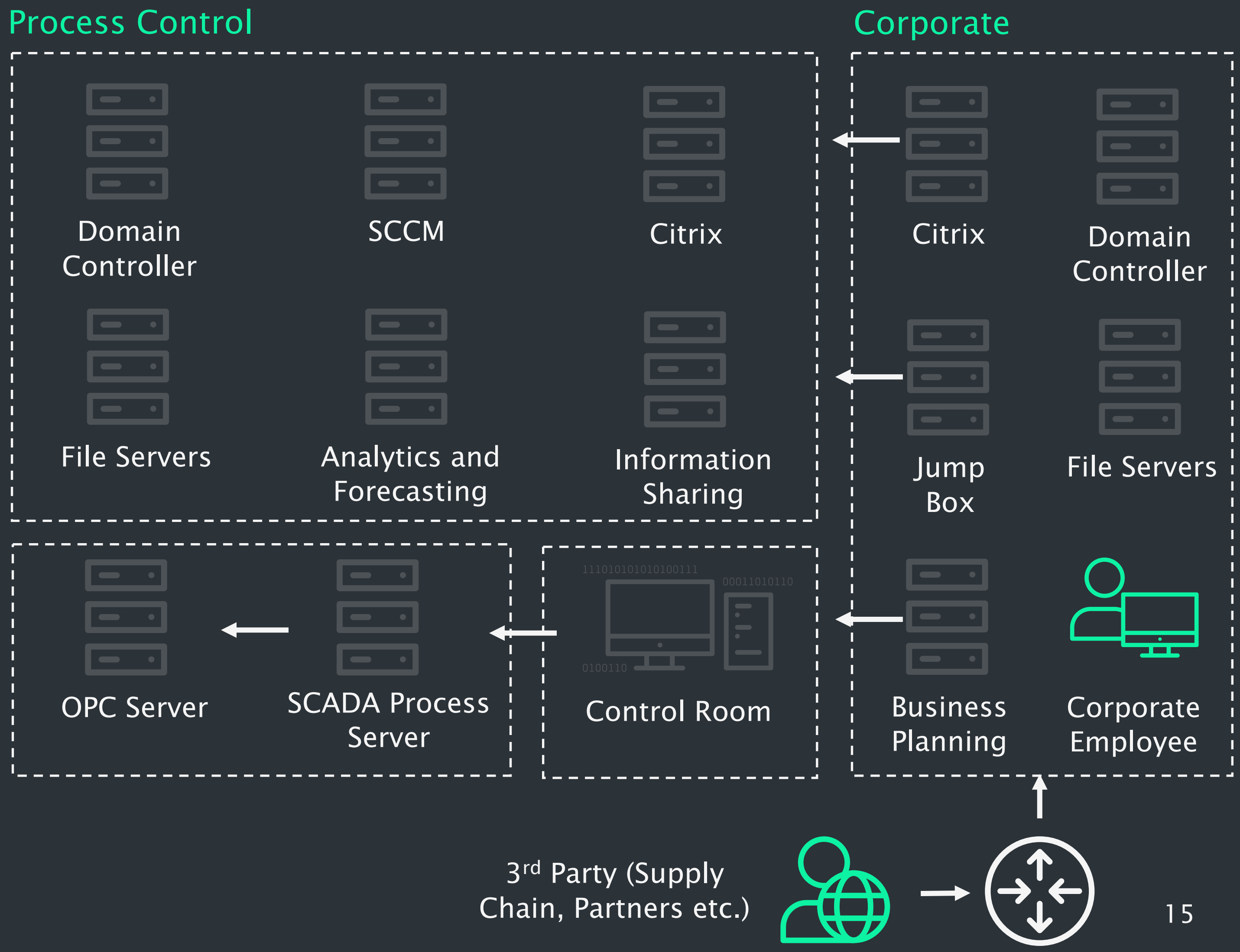
# Getting into OT

# Getting into OT

- Starting from the position of an assumed compromise of a:
  - Corporate employee
  - 3rd party supplier

- Most common initial infection vector during MWR’s investigations.

- 100% success rate escalating within corporate environment.

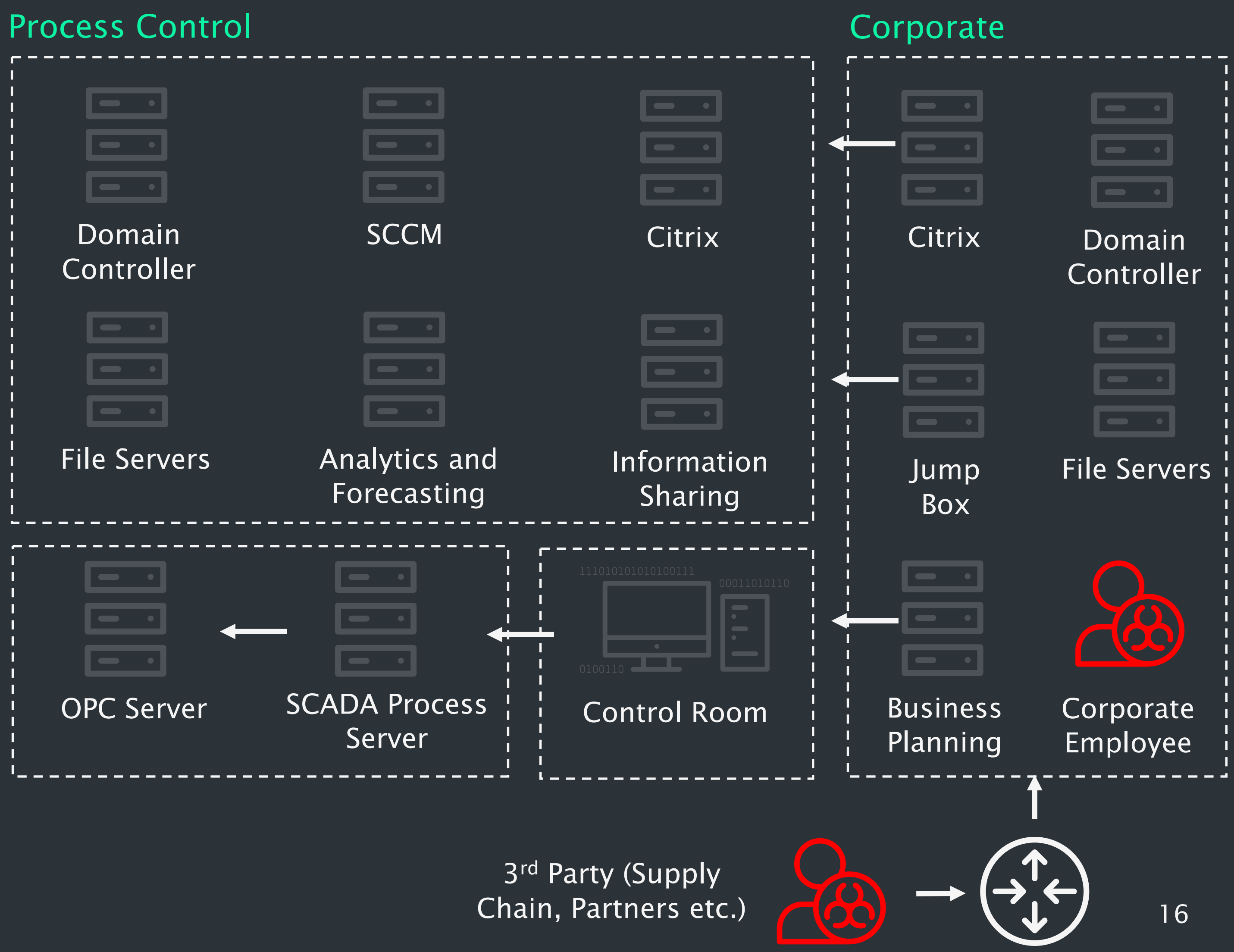


# Getting into OT

- Starting from the position of an assumed compromise of a:
  - Corporate employee
  - 3rd party supplier

- Most common initial infection vector during MWR's investigations.

- Always able to escalate within corporate environment.



Process Control

Domain Controller

SCCM

Citrix

File Servers

Analytics and Forecasting

Information Sharing

OPC Server

SCADA Process Server

Control Room

Corporate

Citrix

Domain Controller

Jump Box

File Servers

Business Planning

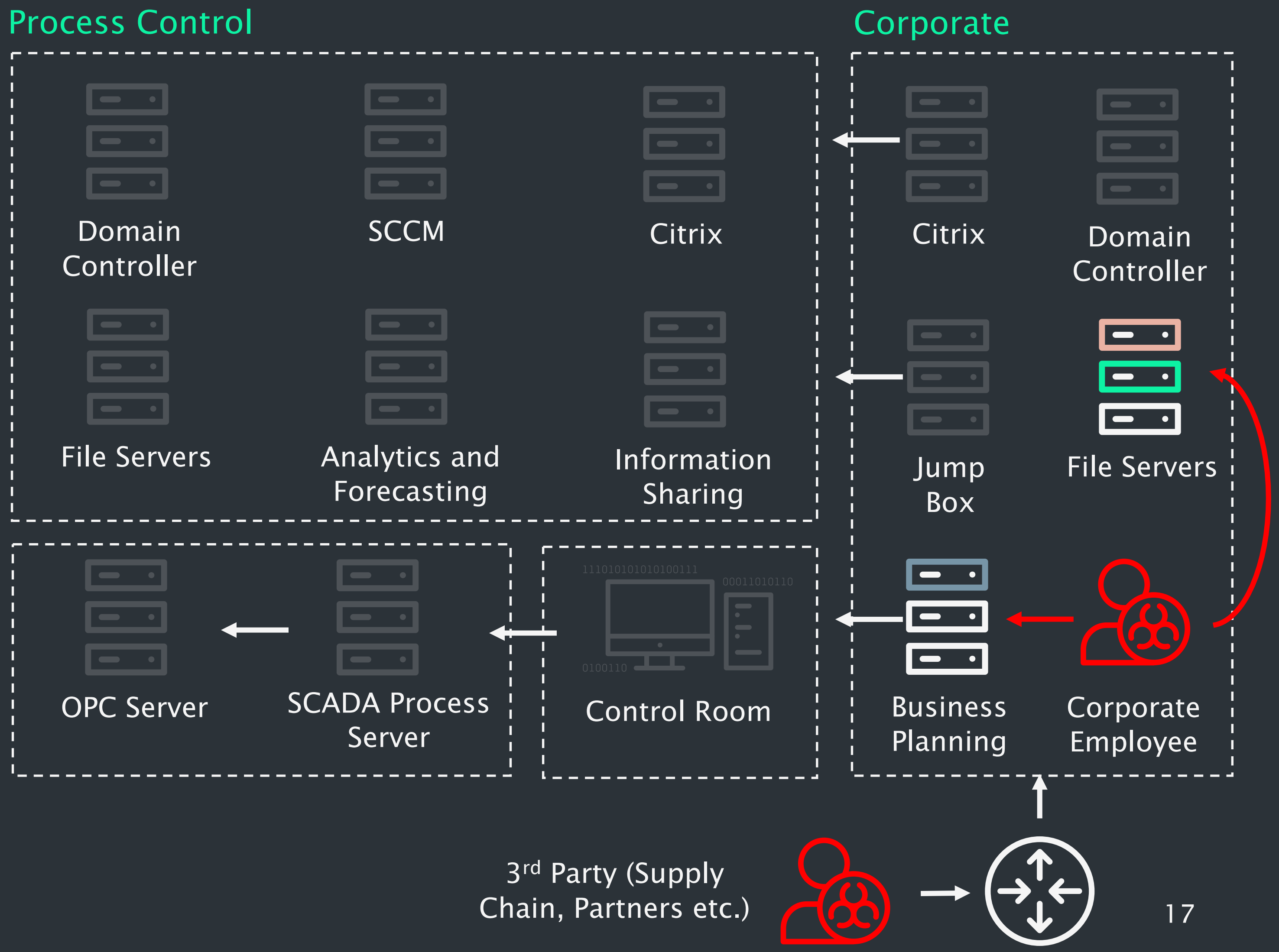
Corporate Employee

3rd Party (Supply Chain, Partners etc.)

# Getting into OT

- Devil's advocate: Do you actually need to get into process control?

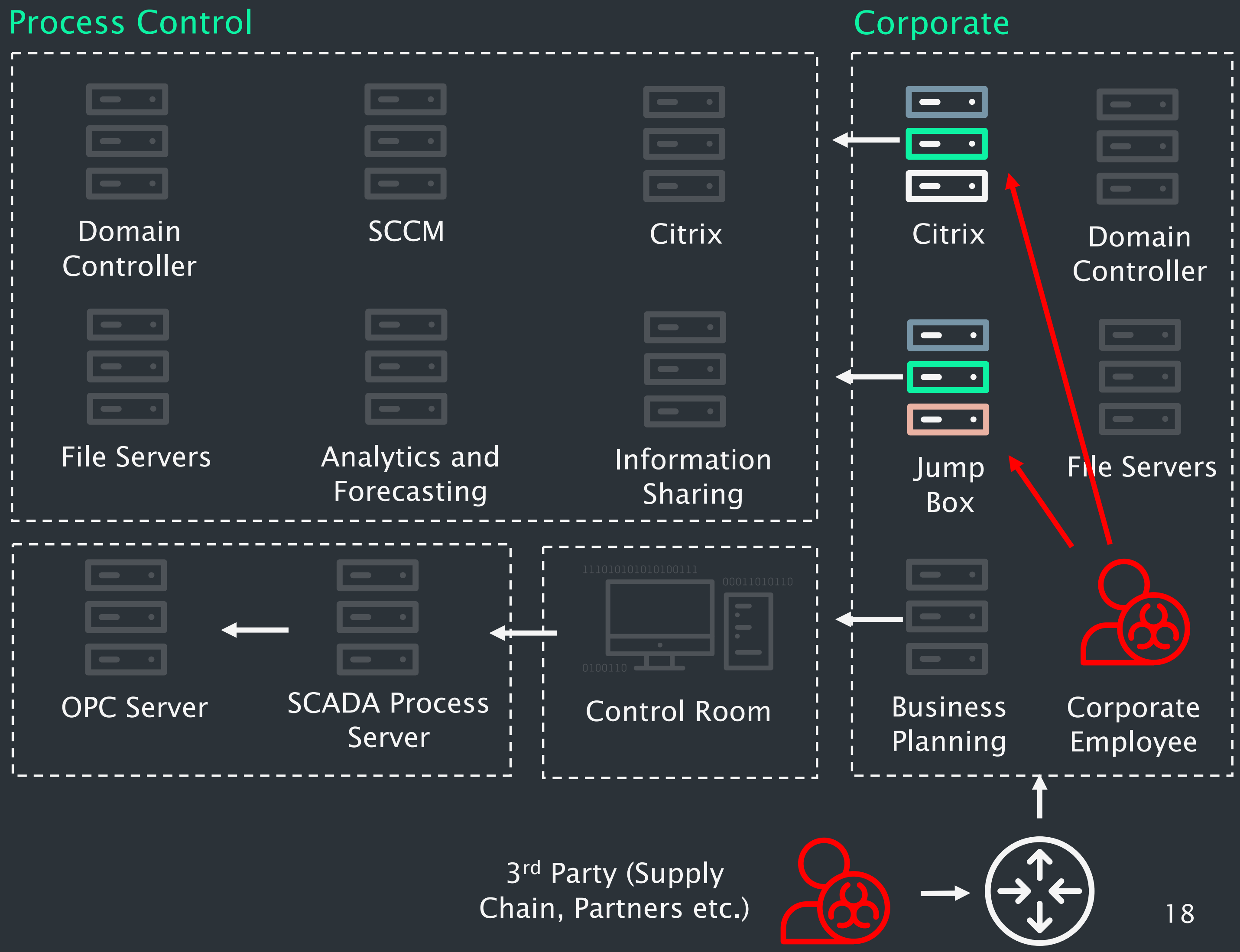
- OT-specific data is almost always in the corporate domain:
  - Emails
  - File shares
  - Information repositories
  - Business planning applications



MWR

# Getting into OT

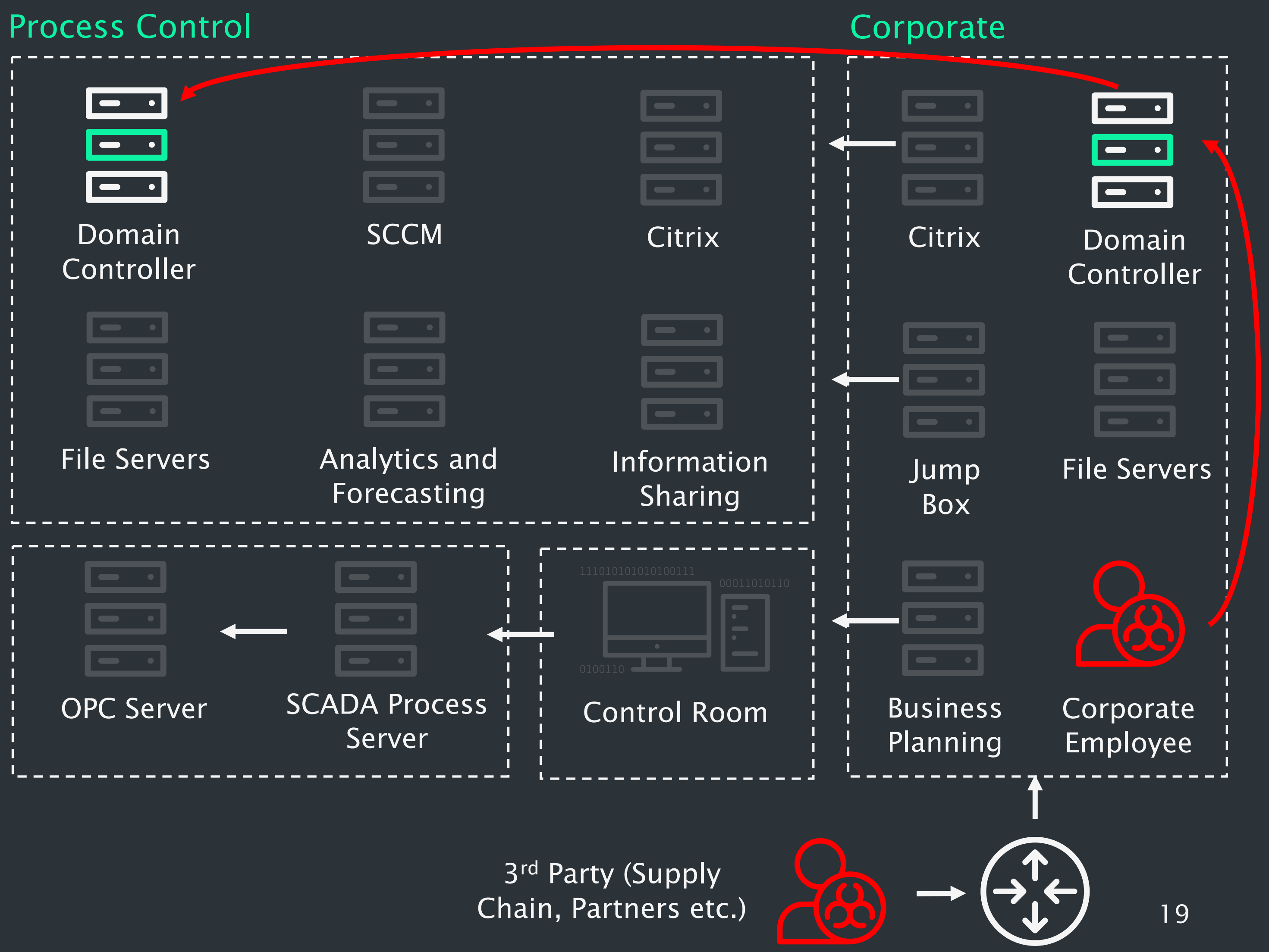
- Citrix is often wrongly considered a security boundary.
- One client was using a unique double-hop architecture:
  - Citrix breakout
  - Privilege escalation
  - Credential dump
  - Credential re-use gave access to OT services
- Easier to find and exploit than jump boxes.



MWR

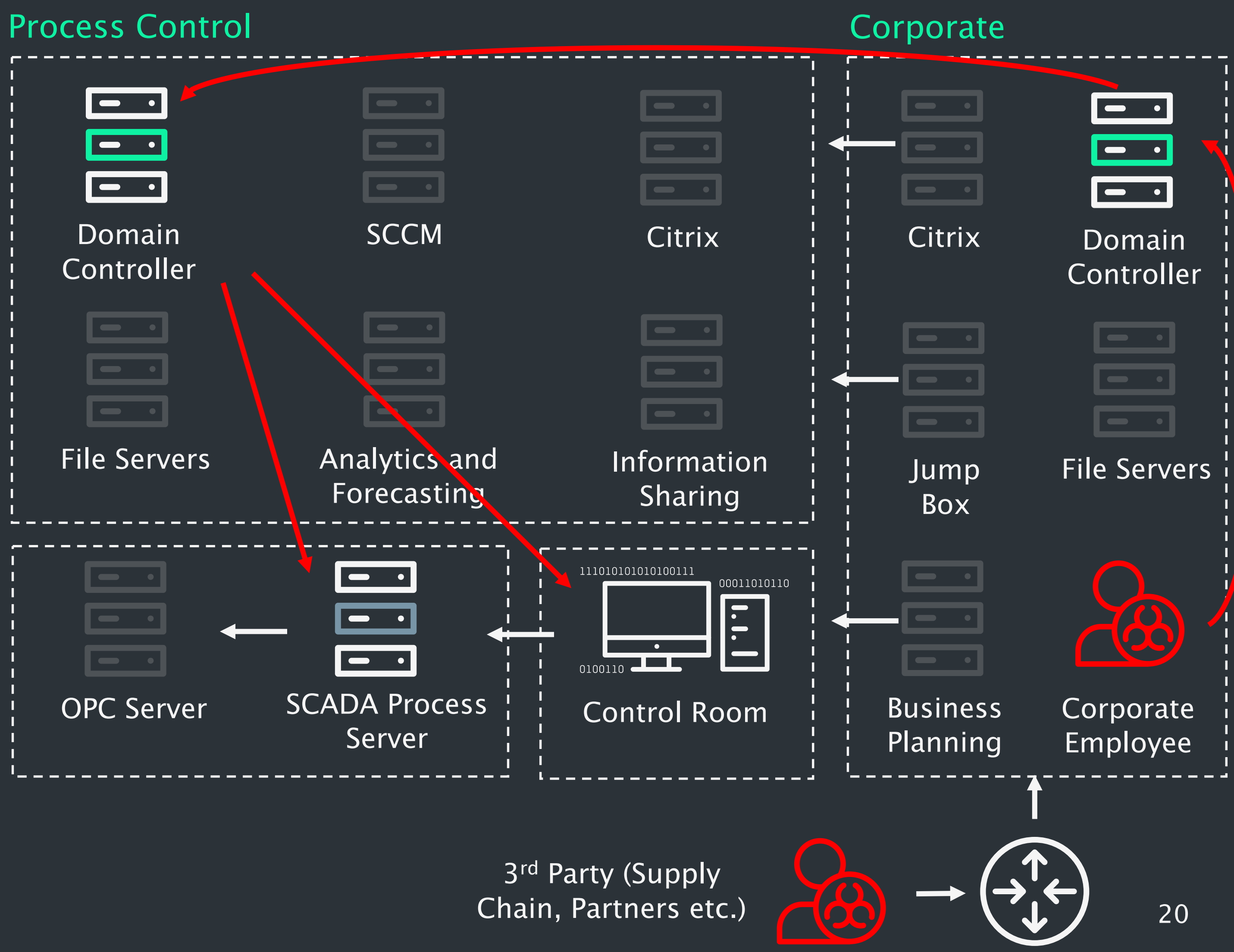
# Getting into OT

- AD architecture is often 'sub-optimal'.
- 100% of CNI clients using the domain as the security boundary.
- High impact:
  - Compromise of any child domain leads to the compromise of the forest
  - Legitimate firewall rules can be abused to pivot into OT



# OT control chain

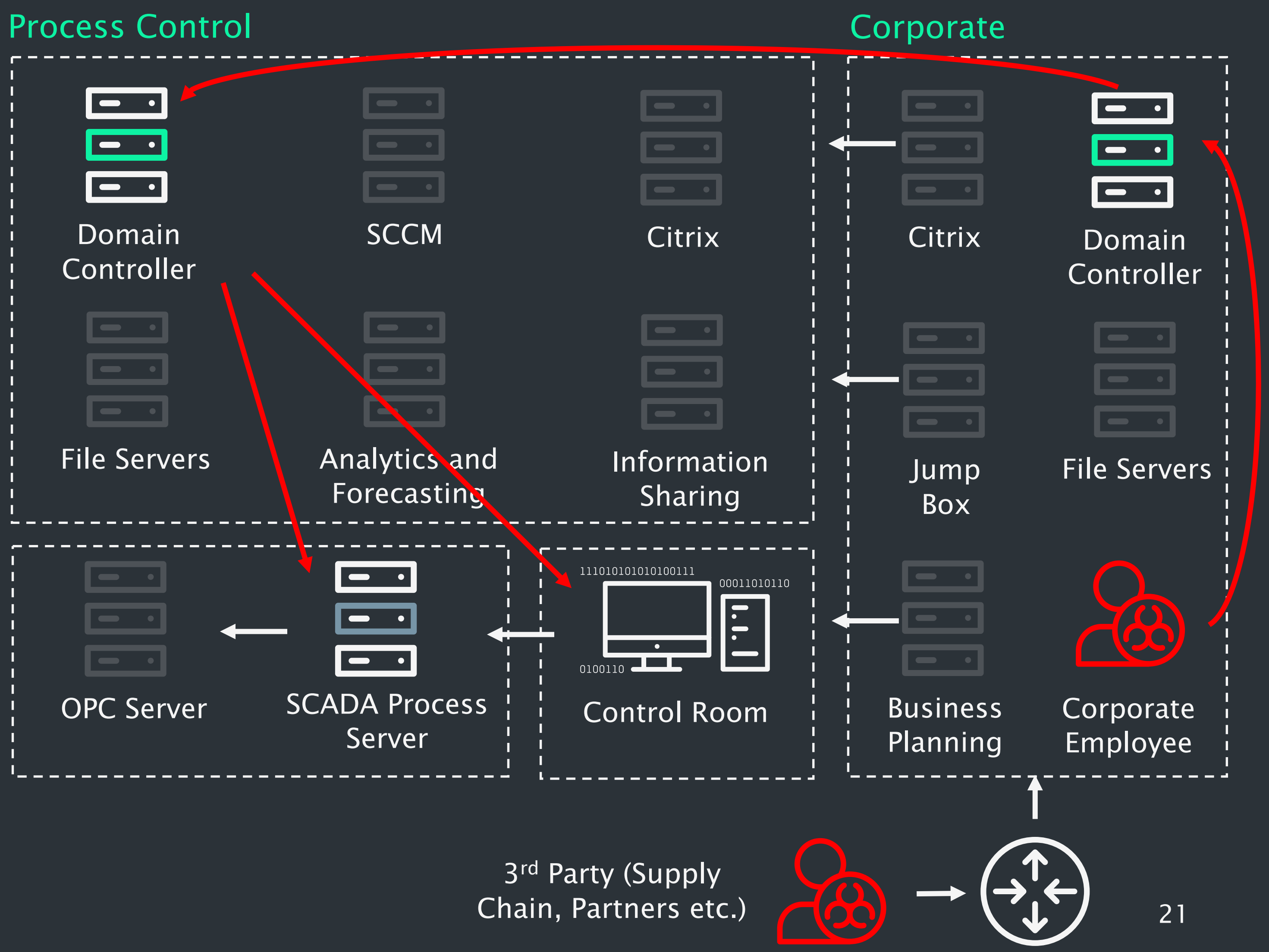
- We're now in the OT environment.
- Key assets to compromise:
  - Control room
  - SCADA process server(s)
- These directly control the physical processes.
- Control room operators often have a false sense of security.



MWR

# OT control chain

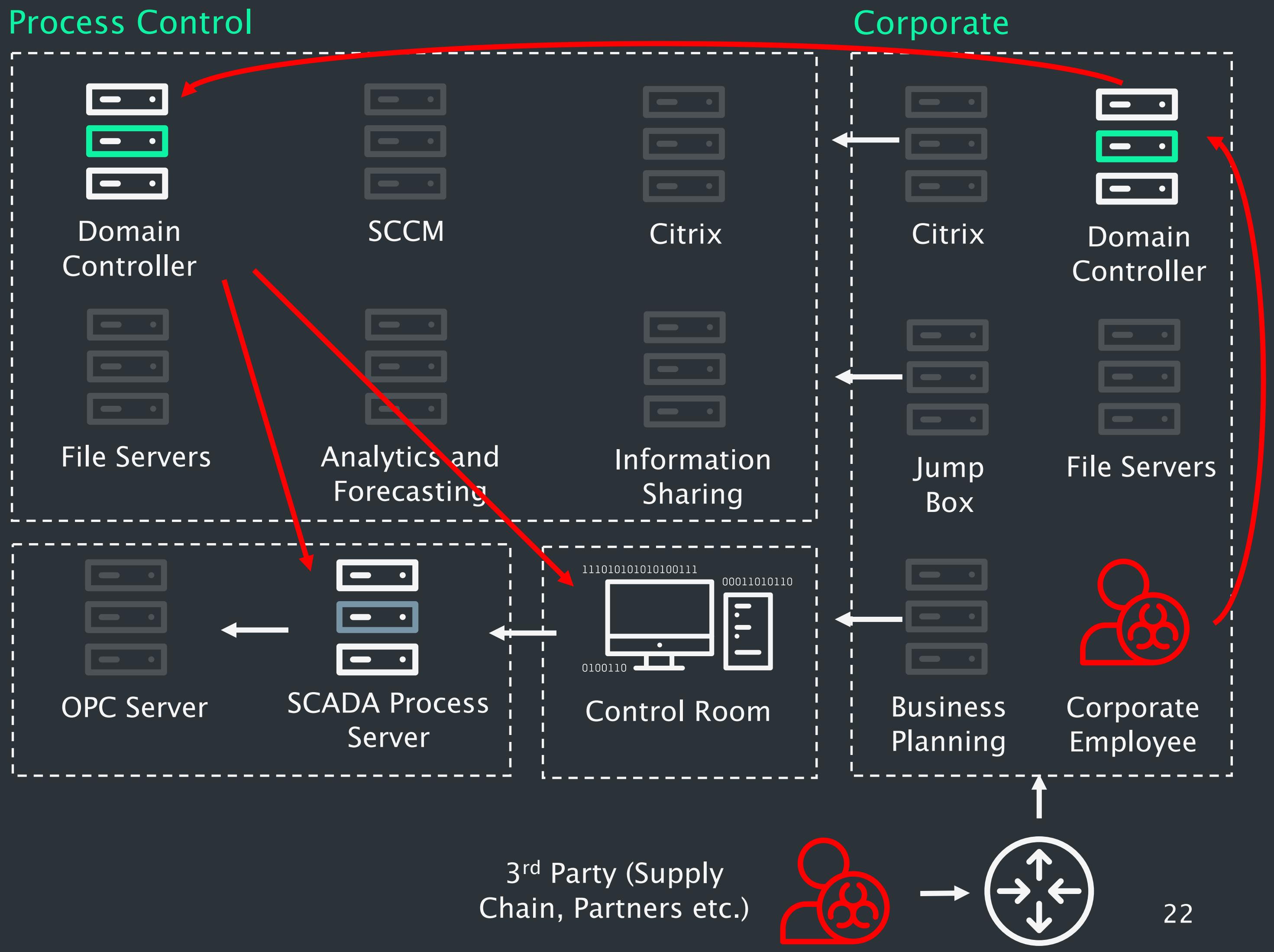
- On the DC? Almost certainly a firewall exception to your objective.
- SMB most likely blocked, but RDP will probably still work.
- WinRM, DCOM?



MWR

# OT control chain

- Lots more:
  - Vulnerabilities in OT specific applications
  - Backups on file servers
  - Dormant support accounts



MWR

# Conclusions

- “Attack positioning” for CNI not as different as many think.
- We need to do more threat-informed and intelligence led testing.
- Collaboration lowers CNI-specific knowledge prerequisites, improves knowledge transfer, and lowers risks.