SECURITYWEEK

ICS CYBER SECURITY CONFERENCE

USING ATTACK PATH MAPPING TO REDUCE RISK AND COST IN ICS ENVIRONMENTS

October 19th 2020

By SEAN RAFFETTO

F-Secure

TODAY'S AGENDA

- Who is F-Secure and what do we do?
- What is Attack Path Mapping?
- What does a typical CNI/ICS environment look like?
- How can we reduce risk when testing?
- What are some common Attack Paths in these environments?
- Case Study – Global Energy Distributor
- Q & A

Who am I?

- Sean Raffetto, Strategic Business Manager
- Working in Cybersecurity for ~8 years
- NJ Native – beach bum
- Equal parts athlete & techy
- Avid soccer player, snowboarder, fiction reader, video game player

F-Secure

F-SECURE IN SHORT

We focus exclusively on cybersecurity
Resulting in a more specialist and tailored service for our customers

We work with the most targeted organizations
For whom technology provides the greatest opportunity, and cyber attack poses a significant risk

We solve the most complex security challenges
Applying the best minds to unsolved, often emerging security problems, while leveraging technology to deliver security at scale

Our **strength** is our **people**

Approximately **300 cyber security consultants** worldwide

1,700 person-strong global business company, operating from 29 offices

F-Secure

RESEARCH-LED CONSULTANCY

Giving consultants the skills and expertise to solve **complex** and **novel** client challenges.

LABS

20+ years of technical **research** and **information** sharing

Discovered **critical design flaws** affecting **millions of locks worldwide**.

Radisson HYATT Sheraton

150+ advisories released in common applications and products

300+ publications including blog posts, articles and whitepapers

>150,000 hours research performed each year

30+ security tools made available for public use within the security community

F-Secure

DIVERSE CAPABILITY

Security Architects
skilled in securely designing and configuring systems and networks

Security Analysts
responding to alerts and implementing effective monitoring solutions

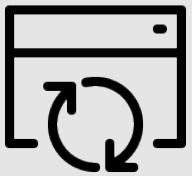
Offensive Security Testers
ethical hacking heritage

Security Researchers
skilled in breaking down hardware and software products

Incident Responders
forensic analysis and combating "hands-on-keyboard" attacks

Tactical Defense Unit
perform technical threat intelligence gathering, and rapid malware triage

Threat Hunters
Proactively hunting for threats while iteratively improving automated detection

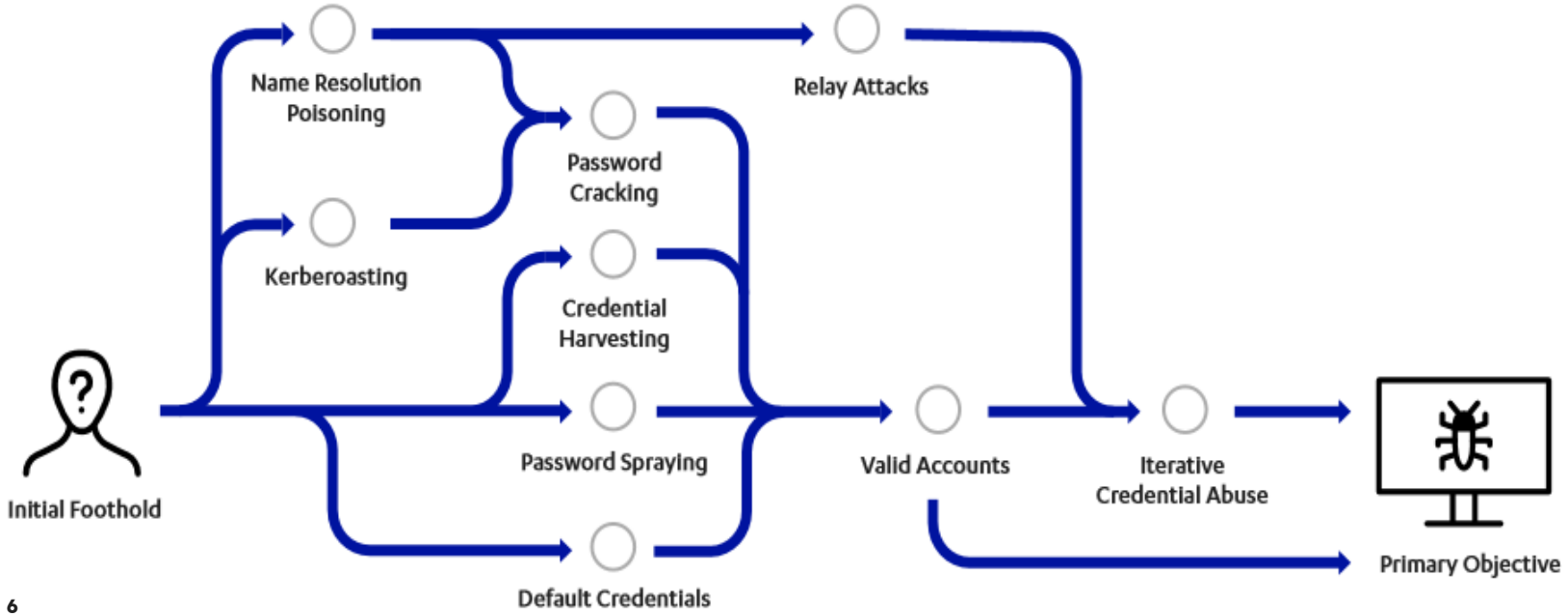


Software Engineers
with knowledge of secure product and application development principles and best practice

F-Secure

ATTACK PATH MAPPING

- Why bother with Attack Simulations?
- "We are Compliant/Certified" – That isn't enough!
- We need to simulate real threats to understand the real risk!



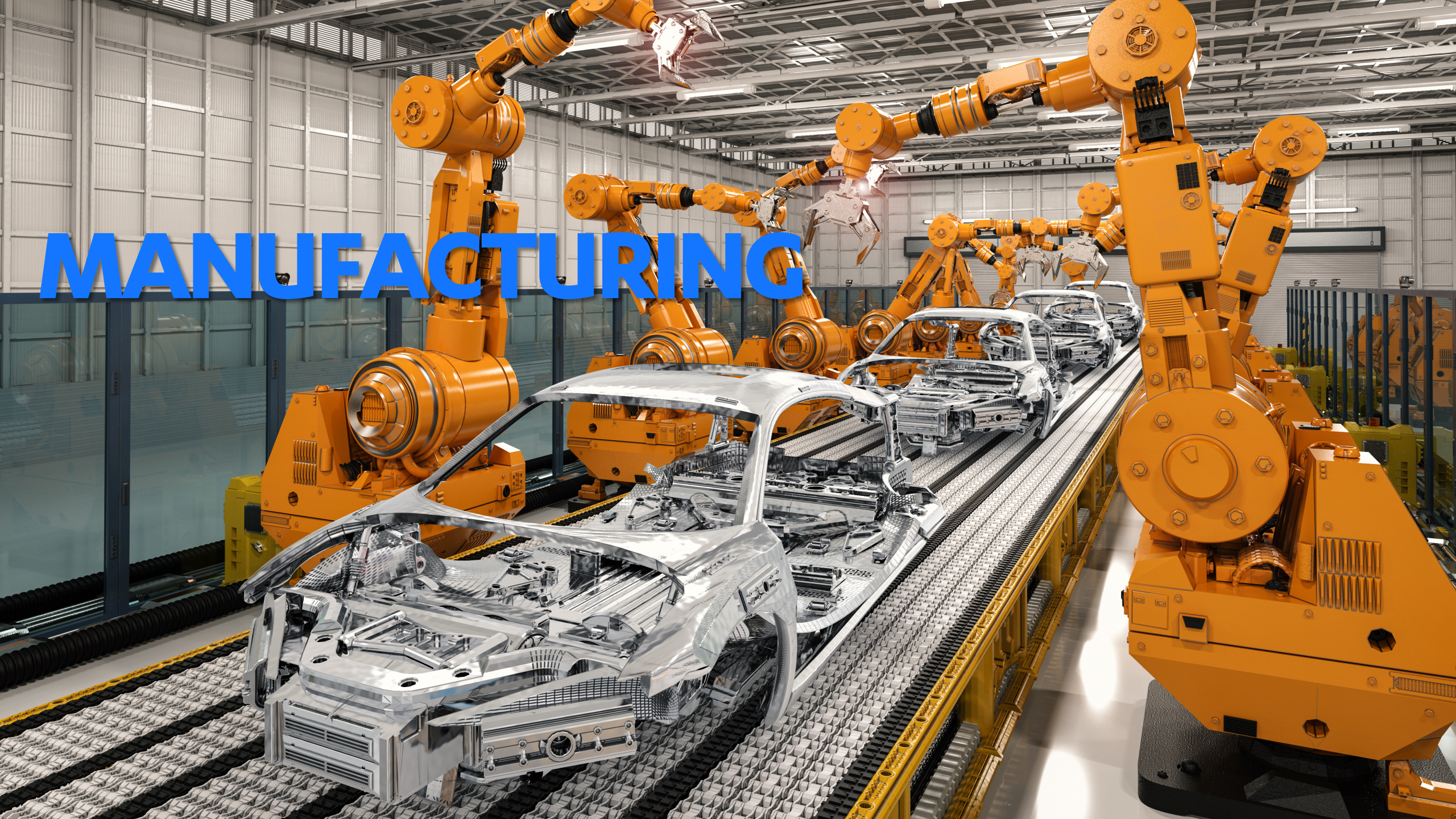
APM

- Dynamic, collaborative approach that uncovers the most likely attack paths an attacker could take to achieve one or more pre-defined attack objectives
- Uses a combination of interviews with key stakeholders and hands-on technical security testing
- The output of an APM engagement can be used to focus an organizations budget on the systems that will be targeted and the controls that will make a difference

F-Secure

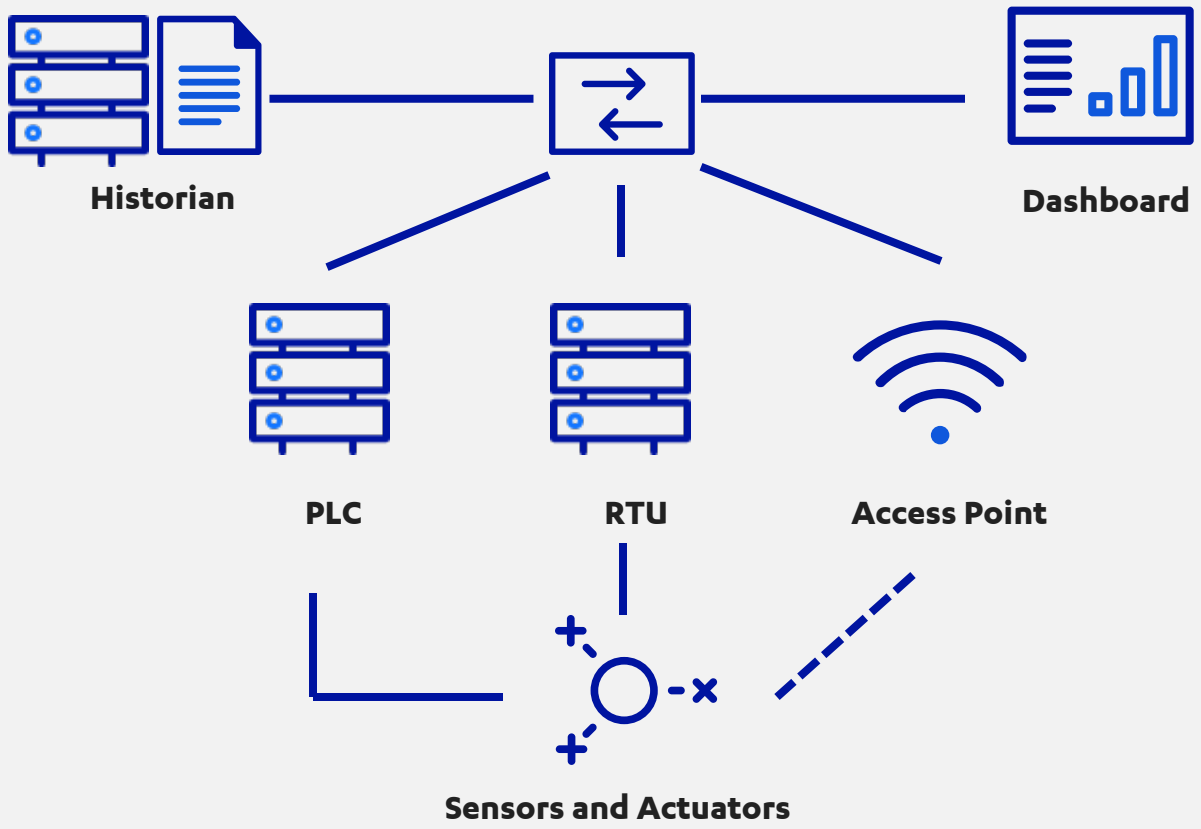
TYPICAL ARCHITECTURE


CRITICAL
INFRASTRUCTURE


MANUFACTURING

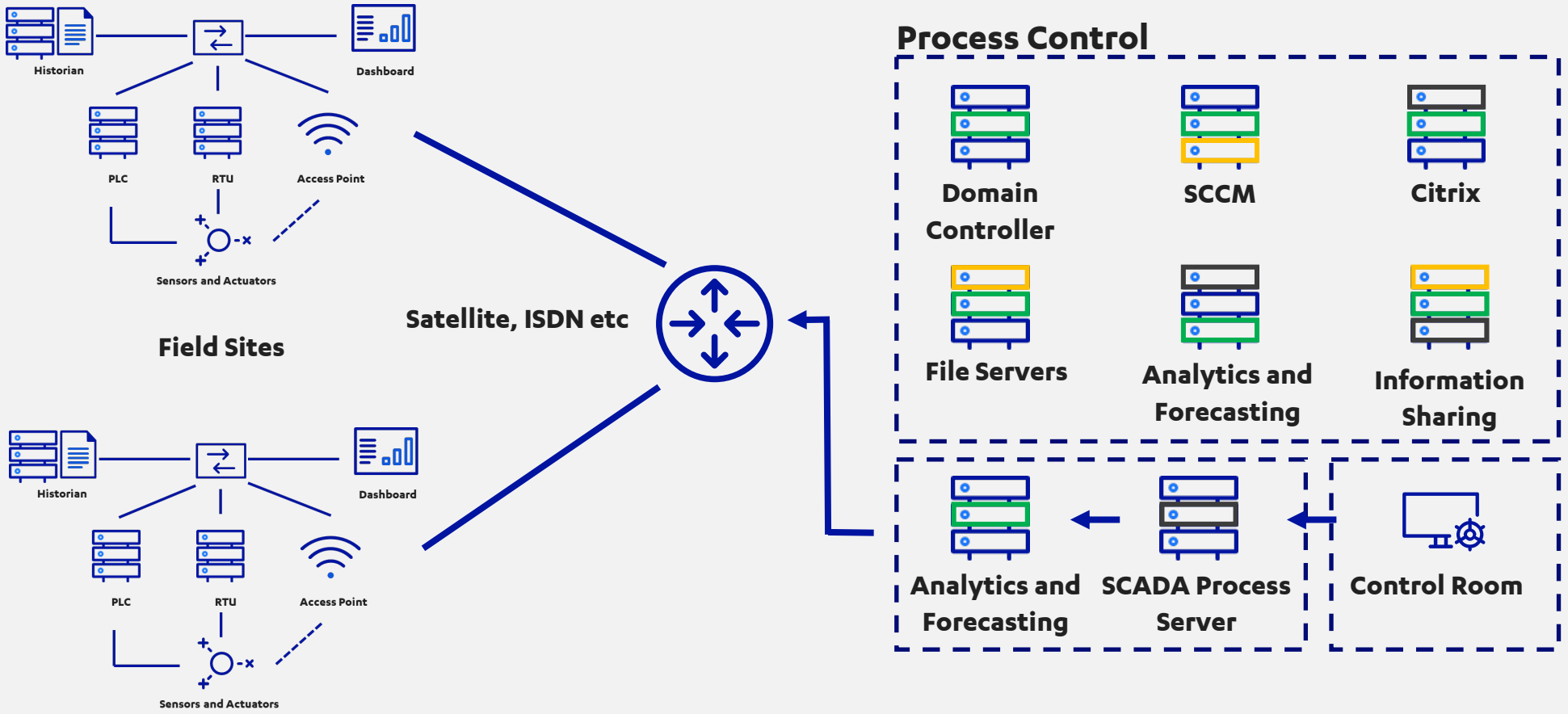

SHIPPING

ARCHITECTURE – FIELD SITE



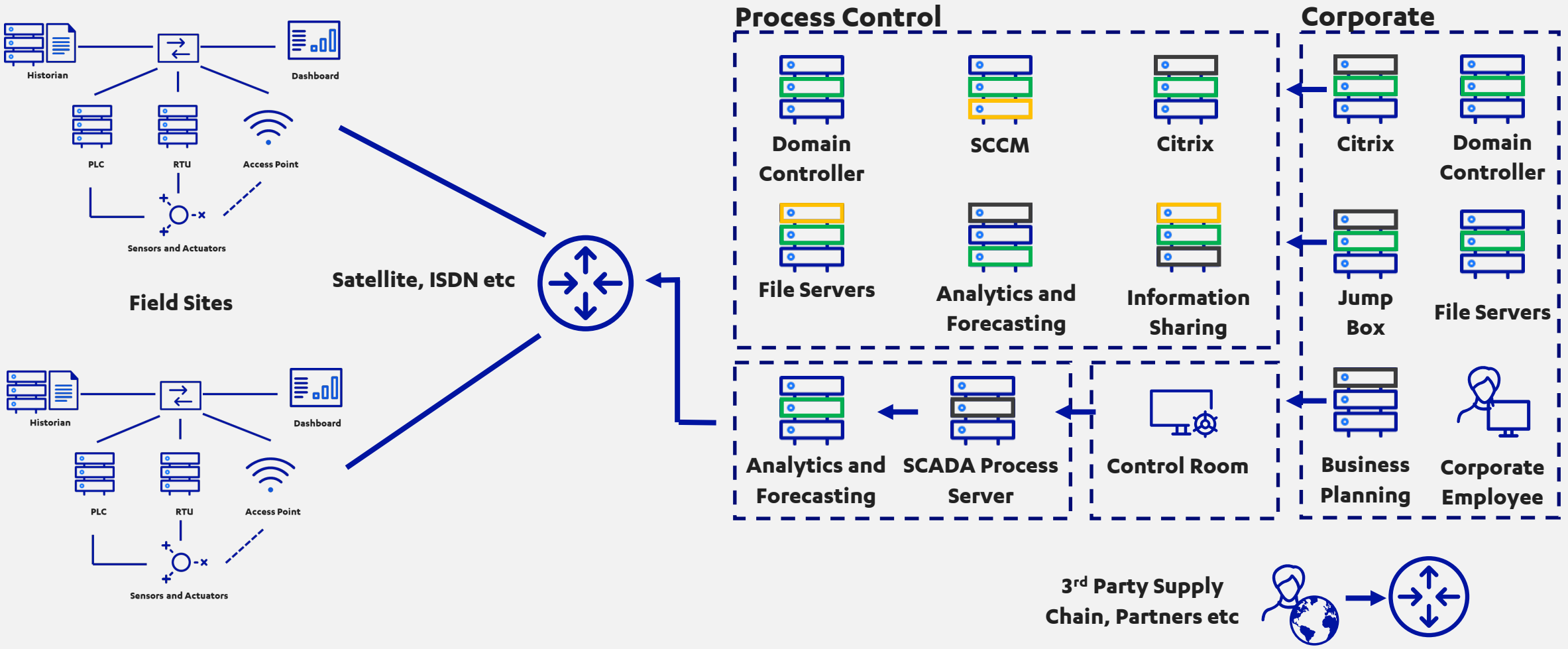
F-Secure

ARCHITECTURE – PROCESS CONTROL



F-Secure

ARCHITECTURE – COMPLETE PICTURE



F-Secure

REDUCE TESTING RISK

REDUCE TESTING RISK

01 Model your threat actor

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

02 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

03 Take the ego out of testing

- Why are you doing X? To demonstrate impact or satisfy your ego?
- Will testing the secondary or failover environment provide the same value?
- If you need to de-chain… ASK!

04 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 understanding of ICS infrastructure and traditional consulting skills

05 Find a security champion

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

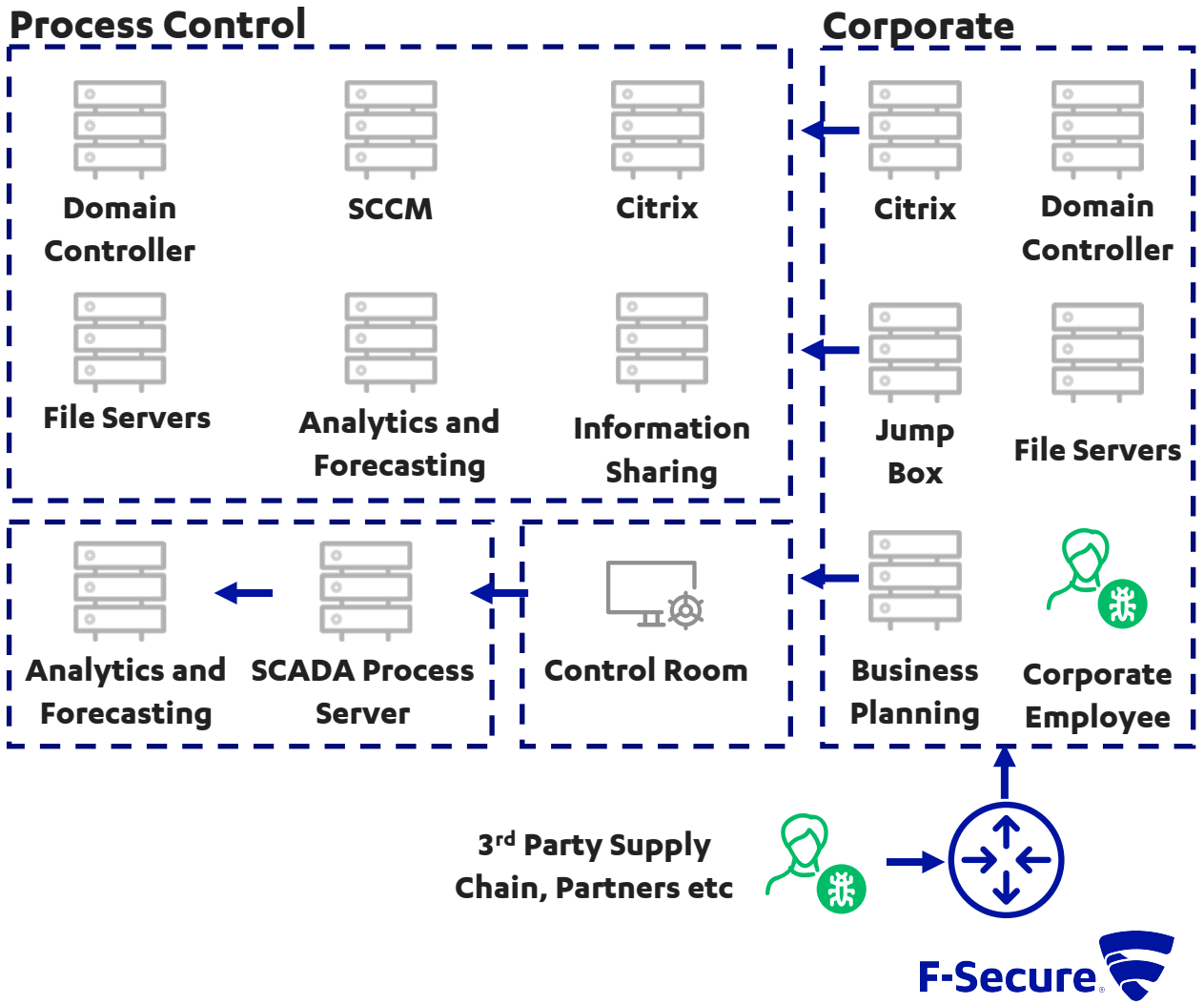
F-Secure

GETTING INTO OPERATIONAL TECHNOLOGY

F-Secure

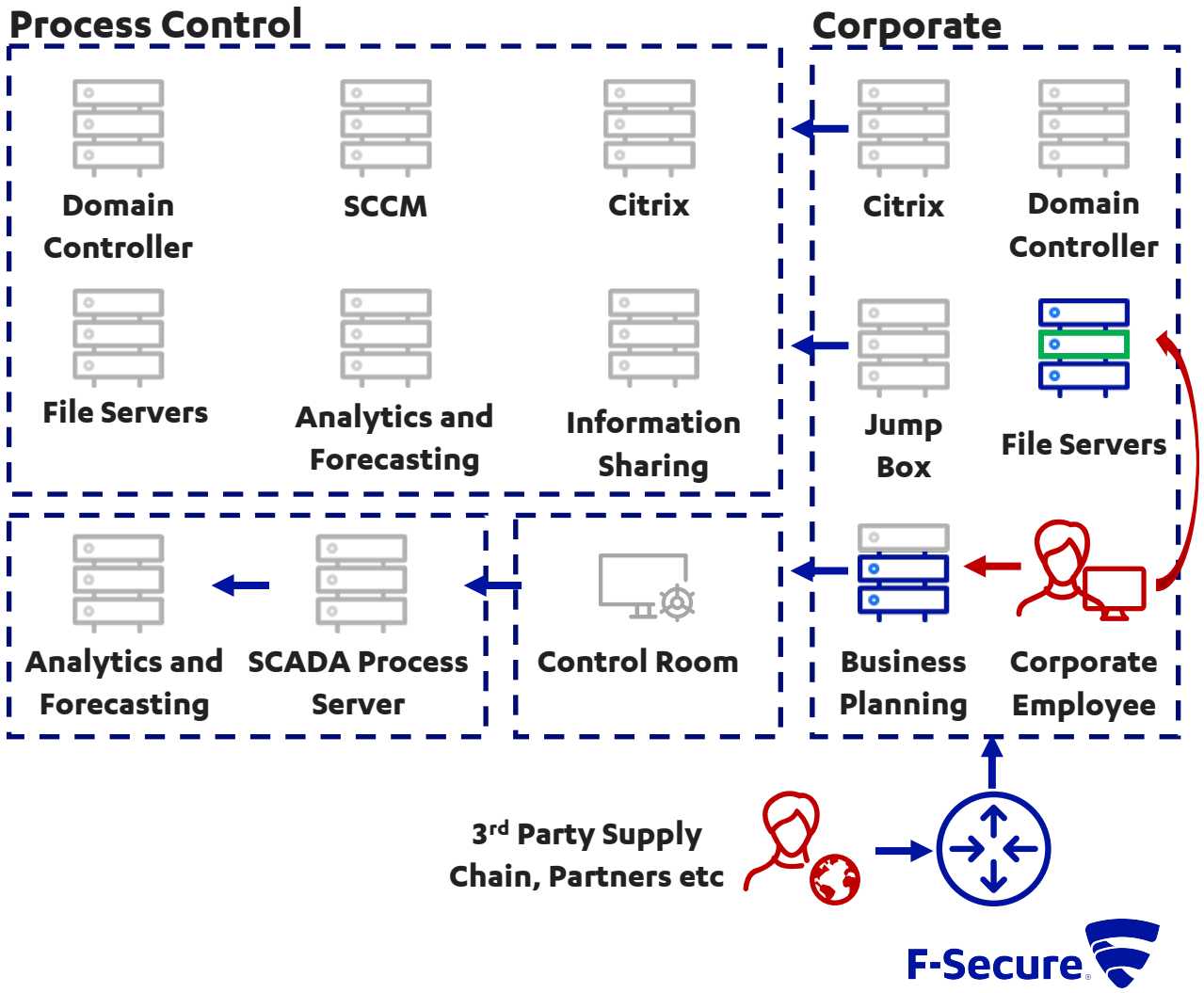
GETTING INTO OT – STEP 1

- Start from the position of an assumed compromise:
  - **Corporate employee**
  - **3rd party supplier**
- Most common initial infection vector during F-Secure's investigations
- 100% success rate escalating within corporate environment



GETTING INTO OT – STEP 2

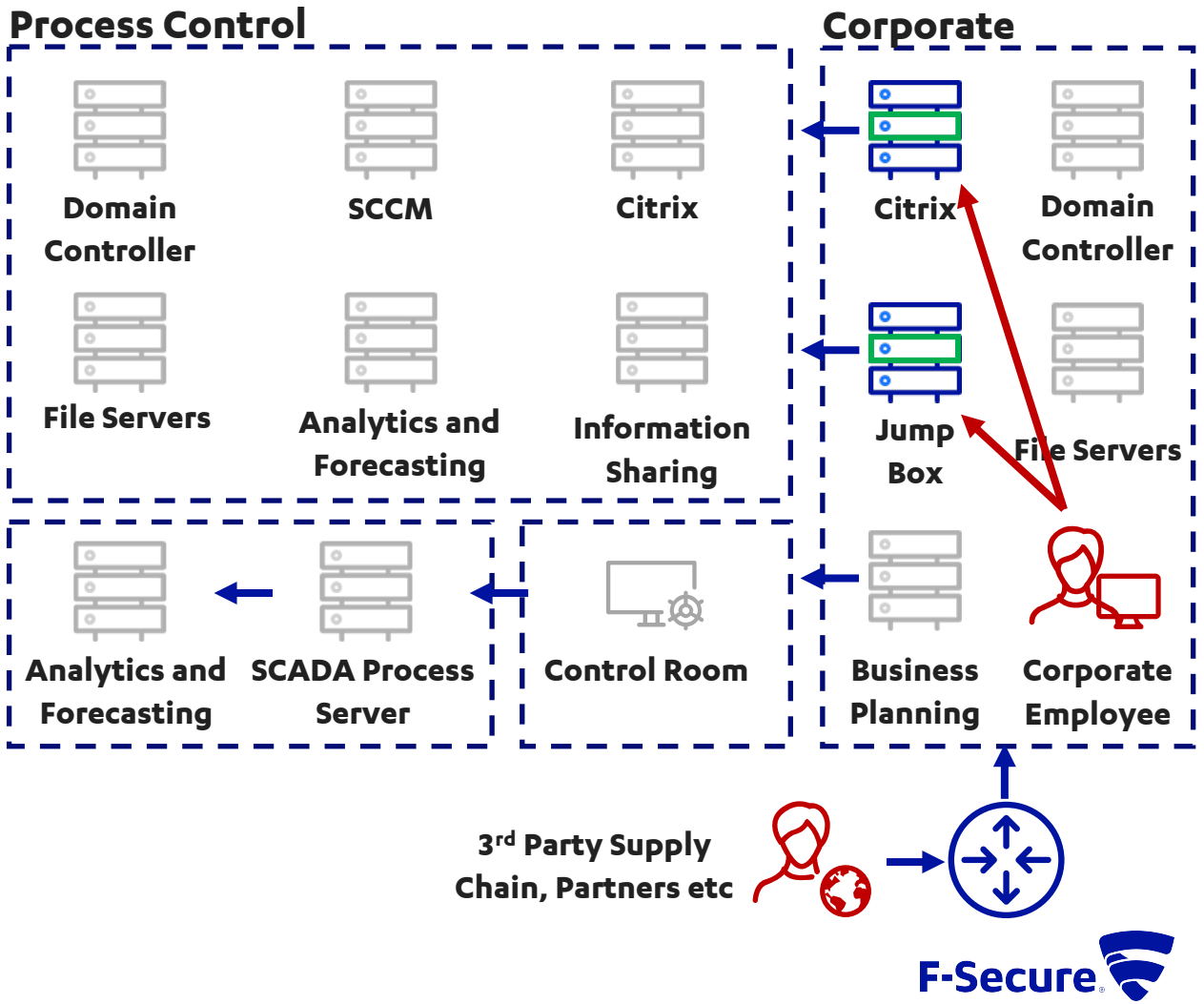
- Devil's Advocate: Do you actually need to get into process control?
- OT-specific data is almost always in the corporate domain:
  - Emails
  - File shares
  - Information repositories
  - Business planning applications



F-Secure

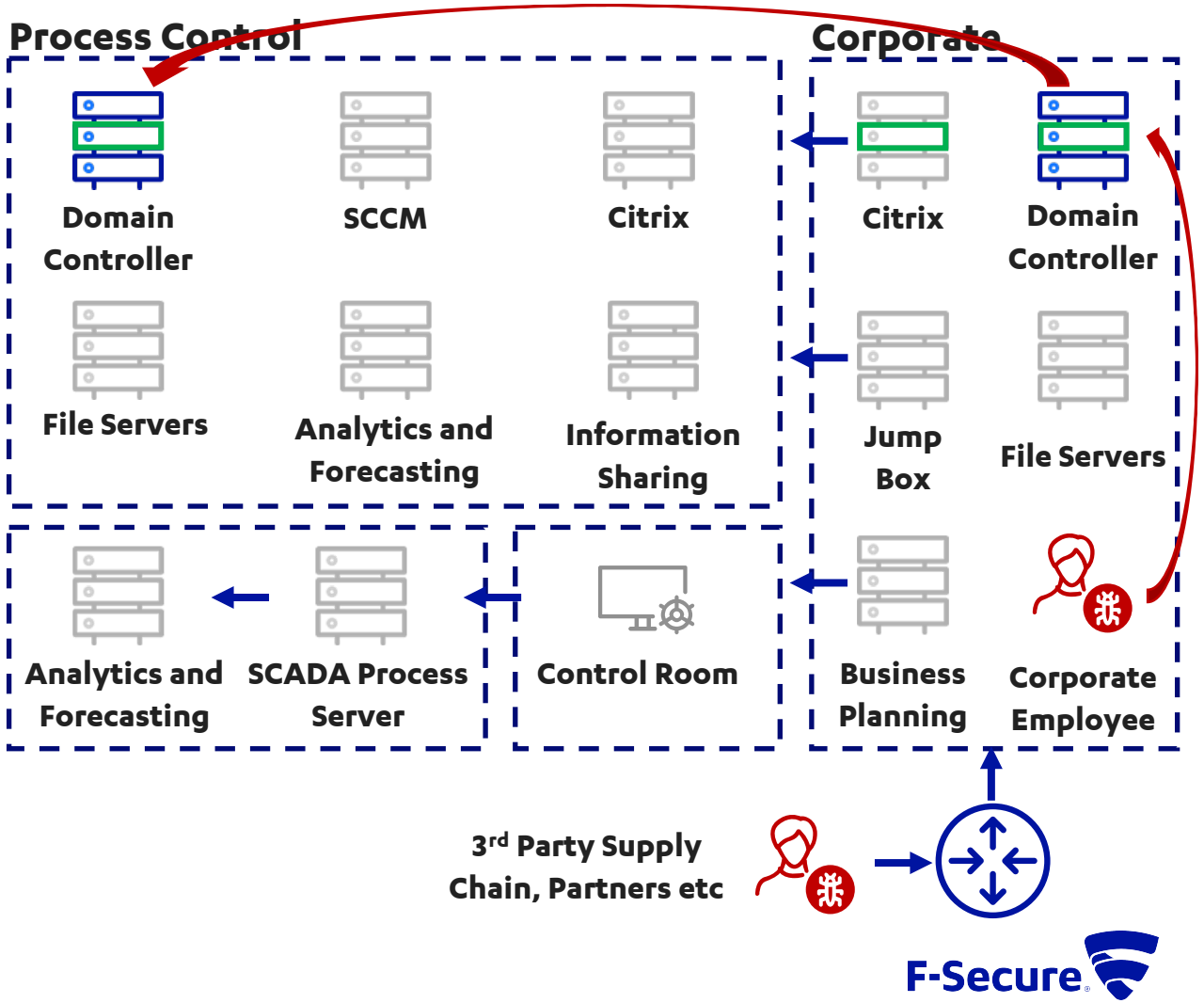
GETTING INTO OT – STEP 3

- 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 an exploit than jump boxes



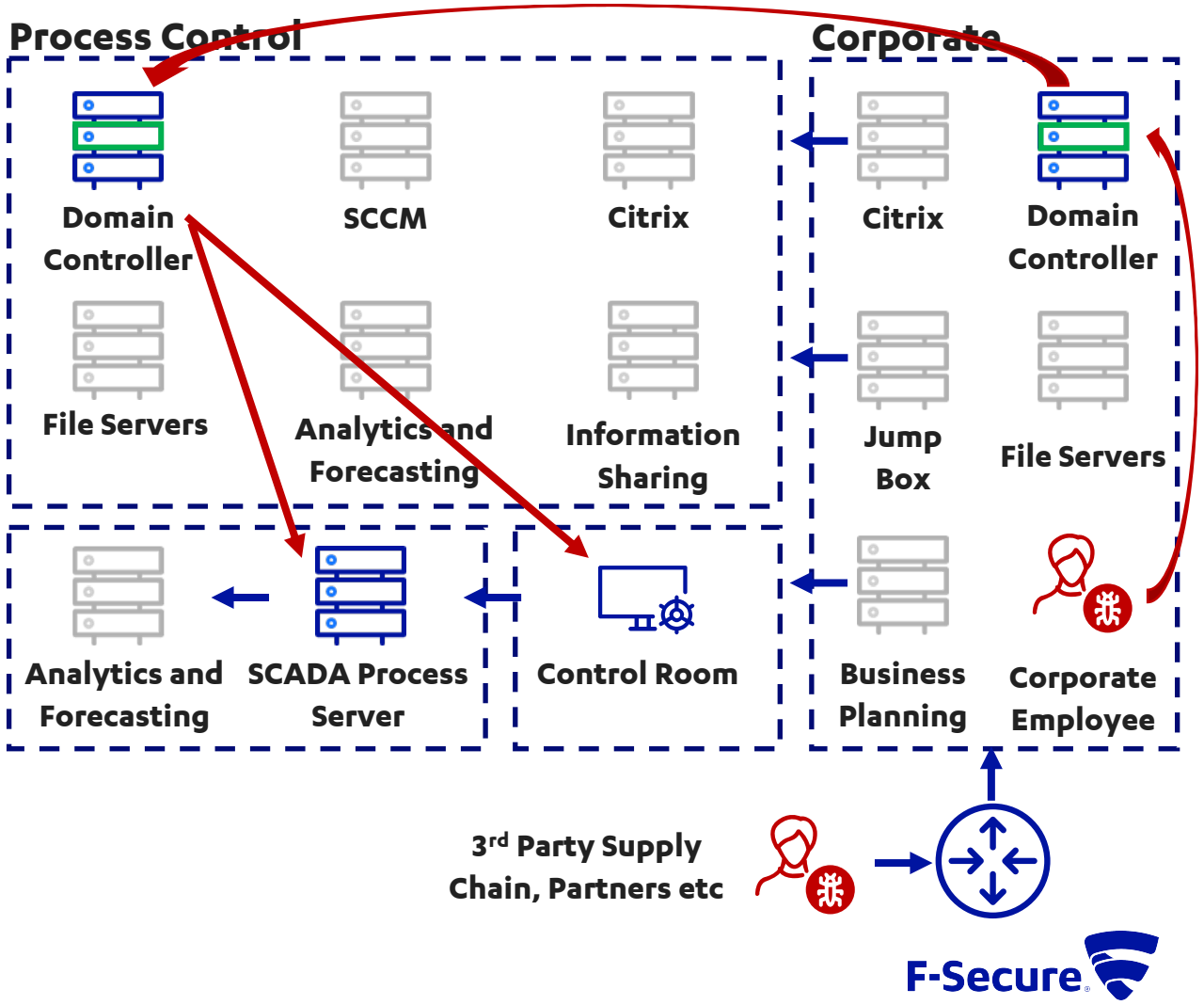
GETTING INTO OT – STEP 4

- 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 compromise of the forest
  - Legitimate firewall rules can be abused to pivot into OT



OT CONTROL CHAIN – STEP 1

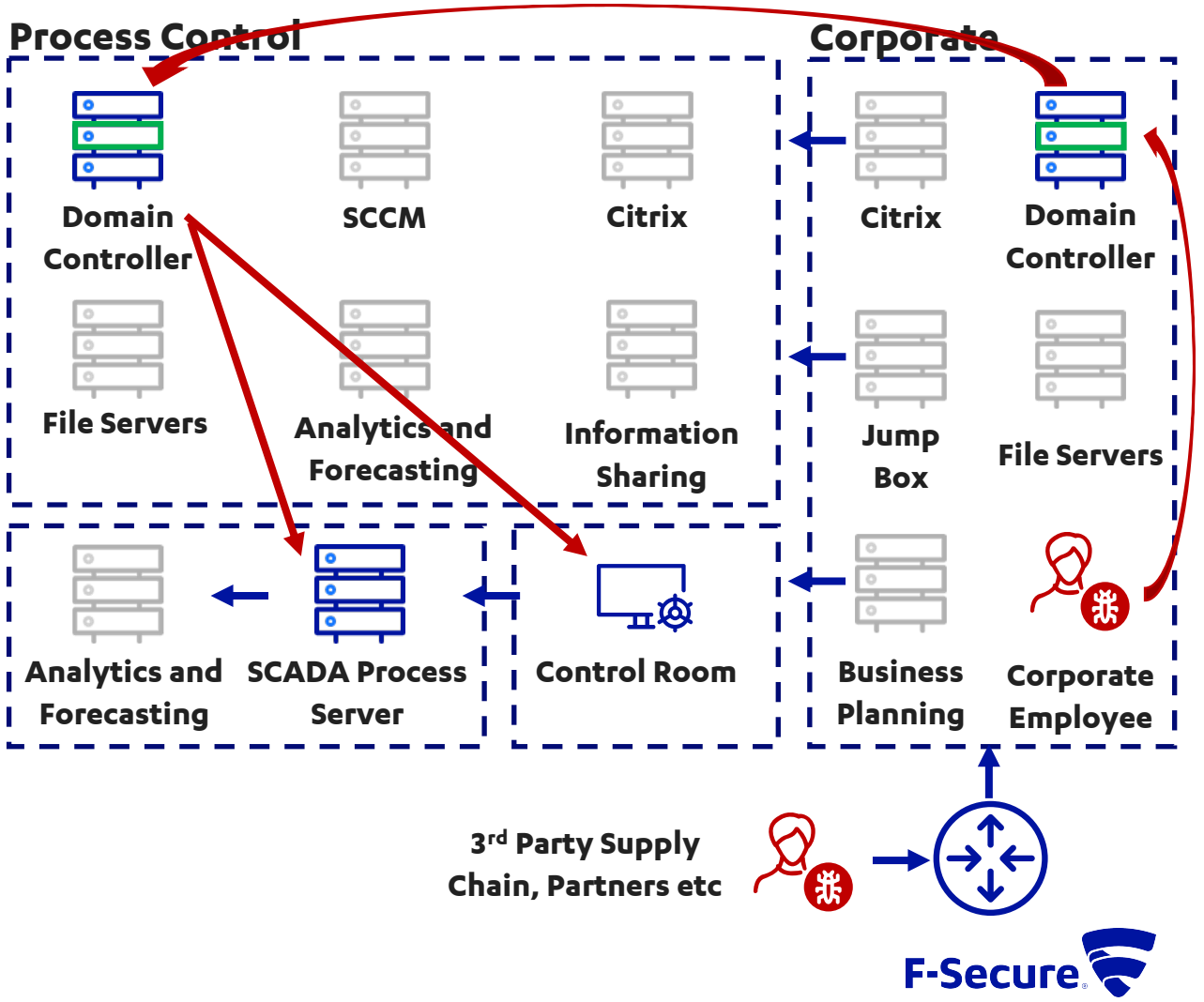
- We're now in the OT environment
- Key assets to compromise:
  - **Control room**
  - **SCADA process server(s)**
- These directly control the physical processes.
- Control room operators often have a false sense of security



F-Secure

OT CONTROL CHAIN – STEP 2

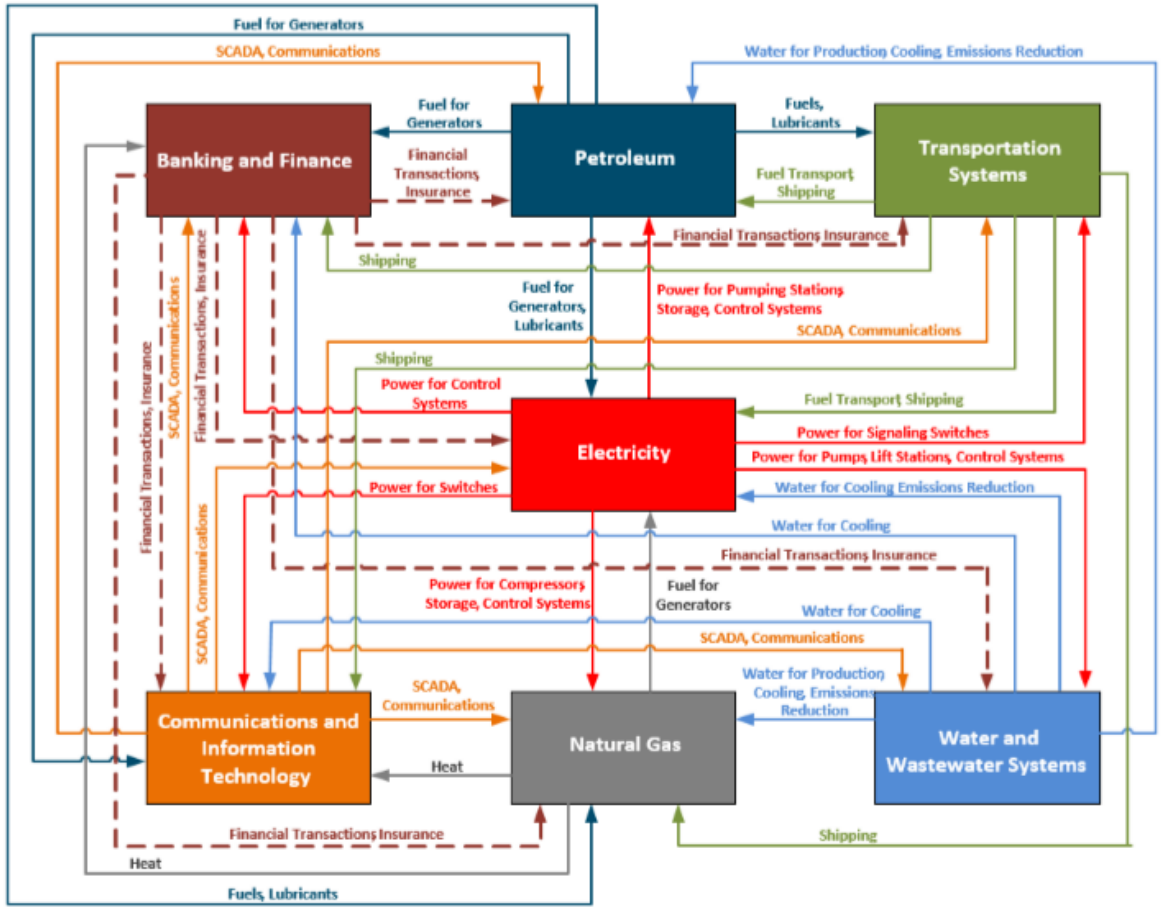
- On the DC? Almost certainly a firewall exception to your objective.
- SMB most likely blocked, but RDP will probably still work.
- WinRM, DCOM?
- Many more:
  - Vulnerabilities in OT specific applications
  - Backups of file servers
  - Dormant support account



GOOD IN THEORY, GREAT IN PRACTICE

Case Study – Global Energy Distributor

- Energy distribution is crucial to most other elements of CNI
- New CISO initiated a "100 Day Program" to get a complete understanding of existing security posture
- F-Secure proposed:
  - External Asset Mapping
  - APM
  - CNI Perimeter Review
  - Cyber Defense Consultancy
- Outputs were integral in establishing priorities and roadmap
- CISO carried this effort to other regions to ensure global standard of security



1 https://www.hybridcoe.fi/wpcontent/uploads/2019/02/Assessing_Energy_Dependency_in_the_Age_of_Hybrid_Threats-HybridCoE.pdf

F-Secure

CONCLUSIONS

"Attack positioning" phase for CNI is 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

F-Secure

F-SECURE CONSULTING

Thank you! Please come speak to our experts at the booth!