SECUDEA
Security Ideas & Consulting

DIY Insider Threat Detection

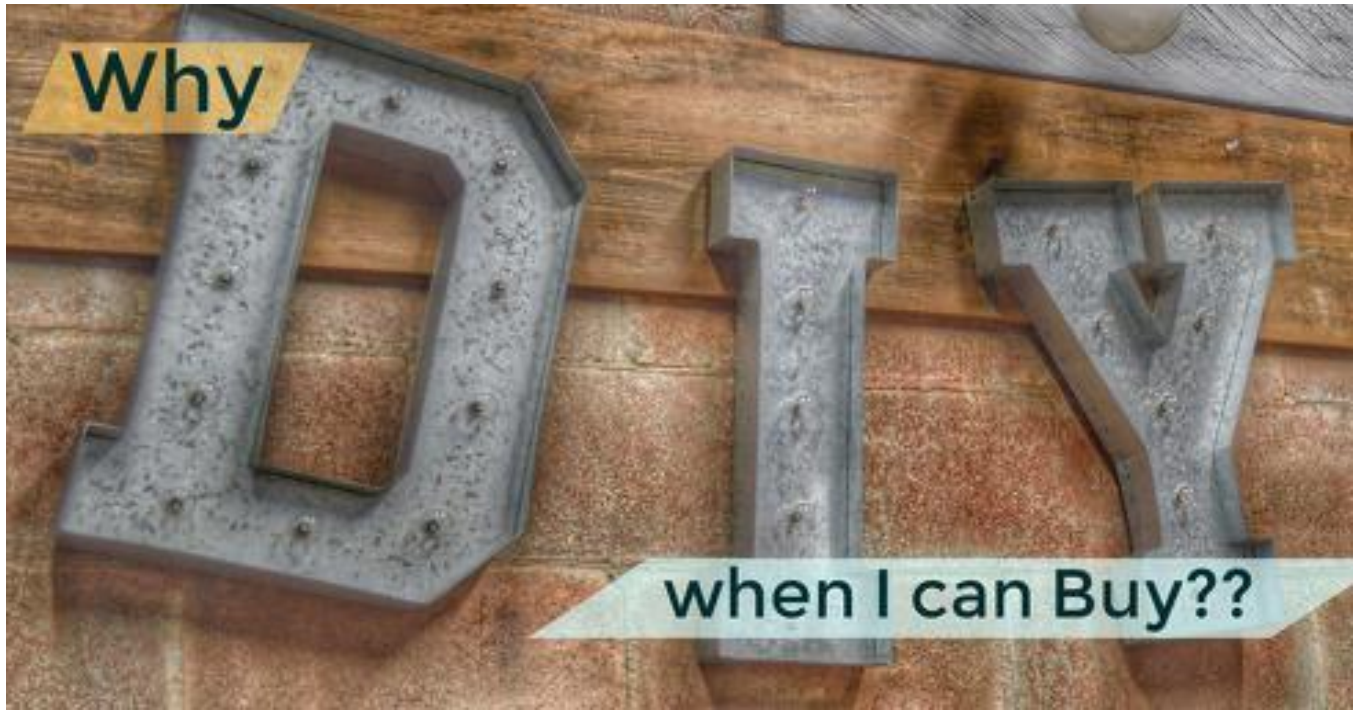
Technical perspectives and considerations within ICS environments

Dieter Sarrazyn

dieter@secudea.be

@dietersar

https://be.linkedin.com/in/dietersarrazyn


Why
DIY
when I can Buy??

(what is an) Insider …

Insiders …

http://fedtechmagazine.com/article/2016/04/commerce-state-departments-take-steps-combat-insider-security-threats

Insiders …

*"an insider is a person that has been **legitimately empowered** with the **right to access, represent, or decide** about one or more **assets** of the organizations environment"*

"Countering insider threats" - Dagstuhl Seminar Proceedings, 2008

http://drops.dahstuhl.de/opus/volltexte/2008/1793

Insiders …

- (compromised) Employees
- (compromised) Contractors/Vendors
- Cleaning crew
- Visitors

- People (ab)using unlocked systems

Insiders …

Can be triggered by …

- Social unrest
  - Strikes / people being laid off
- Compassion / alternate beliefs
- External uncontrollable events
  - Can cause new insider threats

"trusted" people can quickly become untrusted

Some scenario’s

What are the "goals" of the insider threat actor?

Scenario's

disgruntled employees abusing (ex-)rights

Energy

An oil-exploration company hired a temporary consultant to assist in setting up a Supervisory Control and Data Acquisition (SCADA) system that enabled communication with offshore platforms and detection of pipeline leaks. When his contract was about to expire, he requested permanent employment. The request was rejected and his contract ended. For two months following termination, ***he planted malicious programs on the organization's systems that temporarily disabled the SCADA system****.*

Water

An electrical supervisor developed applications for a SCADA system used by the water industry. After termination, he installed a ***malicious program*** *on one of the organization's critical systems,* ***damaging the SCADA system****.*

https://insights.sei.cmu.edu/insider-threat/2012/09/insider-threats-evident-in-all-industry-sectors.html

Scenario’s

Stuff begin dropped on the network

Scenario's

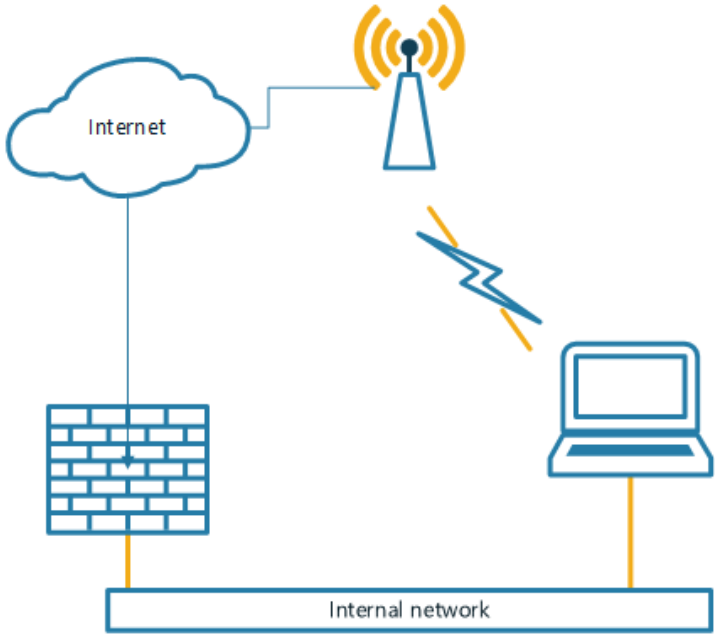
Contractors/visitors/…

- connecting laptops (local or remotely)
- using unauthorized usb sticks

Scenario's

Backdoor(ed) connections

- DSL often with WiFi enabled
- Bridging to the internal network possible
- Remote access



Considerations

Detecting, preventing and/or deterring insider threats

Considerations

Baseline your environment - network

Do you know your network ?

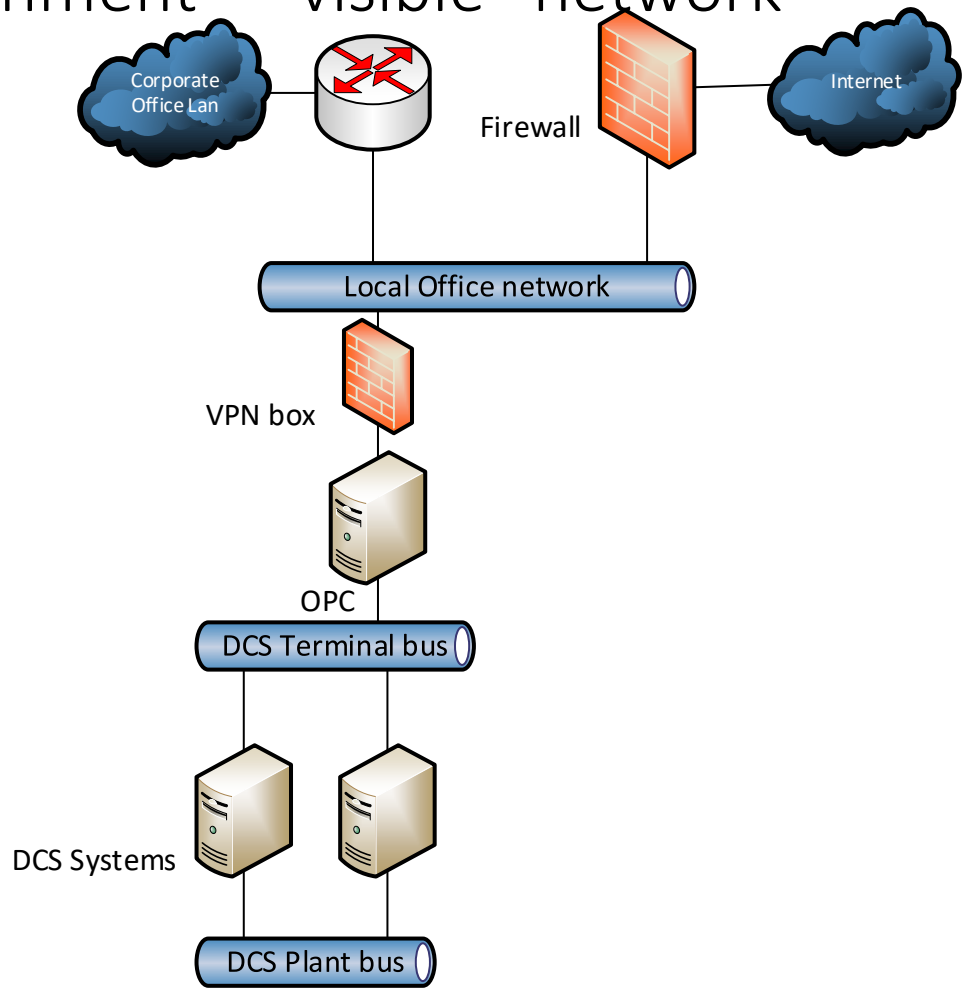
- Asset / inventory management
- Bridge systems
- Remote access

"visible" network <> "invisible" network

http://www.smartceo.com/kci-technologies-know-who-owns-your-network/

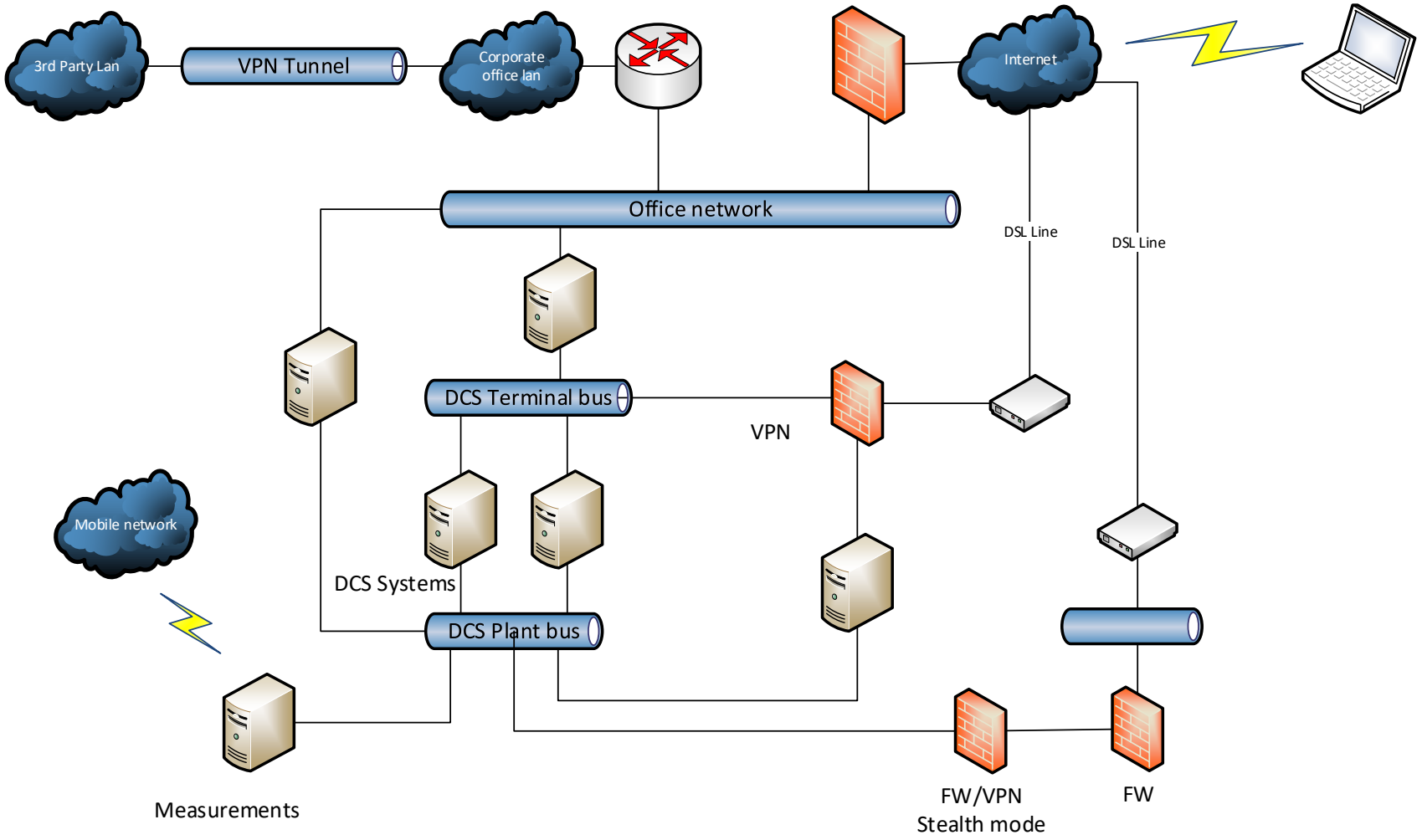
Considerations

Baseline your environment – “visible” network



Considerations

Baseline your environment – “invisible” network



Considerations

Network

- Network volume/usage monitoring
  - (big) usage of gmail, dropbox …
  - Large print jobs
  - A lot of DNS requests …
- Network authentication
- Network segmentation/zoning

- Use honeypots within your ICS network(s)

CONPOT ICS/SCADA Honeypot

Considerations

Network – rogue device/AP detection

Enclosure alarm

Rack door alarm

Wifi AP monitoring

US

ARP

https://www.flickr.com/photos/teknyka/6592496831/

Passive device … No introduction of (new) bridges…

Considerations

Network – distributed rogue device/AP detection

ARP/AP probe zone 1

Get ARP DB for zone 1
Get approved AP's

ARP/AP probe zone 2

Get ARP DB for zone 2
Get approved AP's

Considerations

System

Create system security baselines

Use media sanitization techniques

Monitoring on

- Usb usage
- Access rights usage
- Group accounts
- …

Hashing for PLC programs

Logging & Monitoring

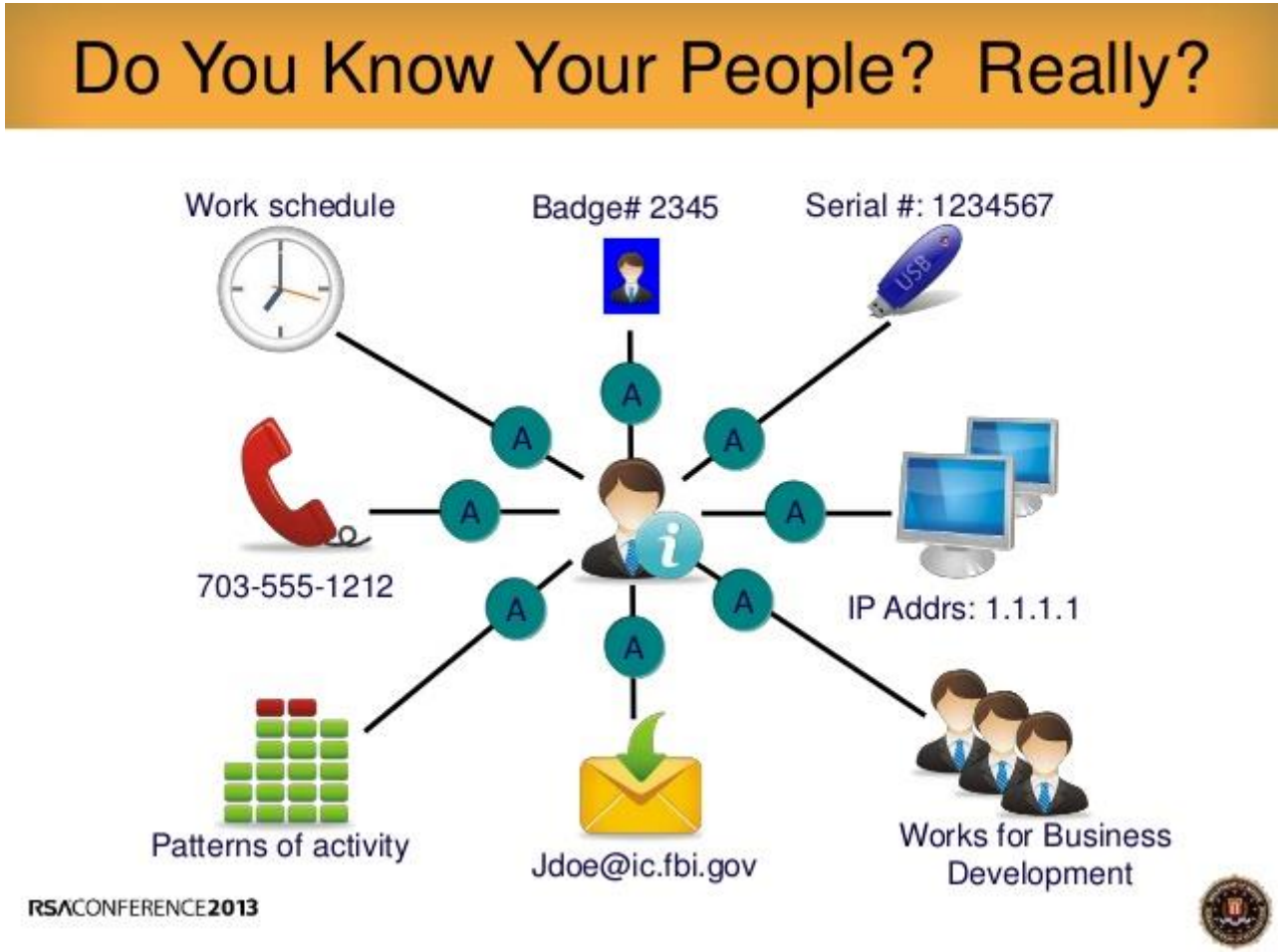
ARP/AP probe

System logs

Honeypot info

Considerations

Users - "baselining"

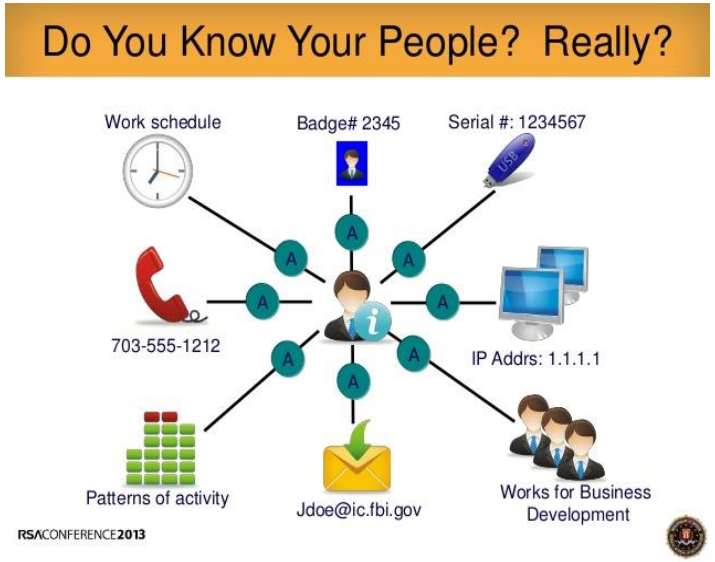


https://www.slideshare.net/SelectedPresentations/ht-t17

Considerations

Users

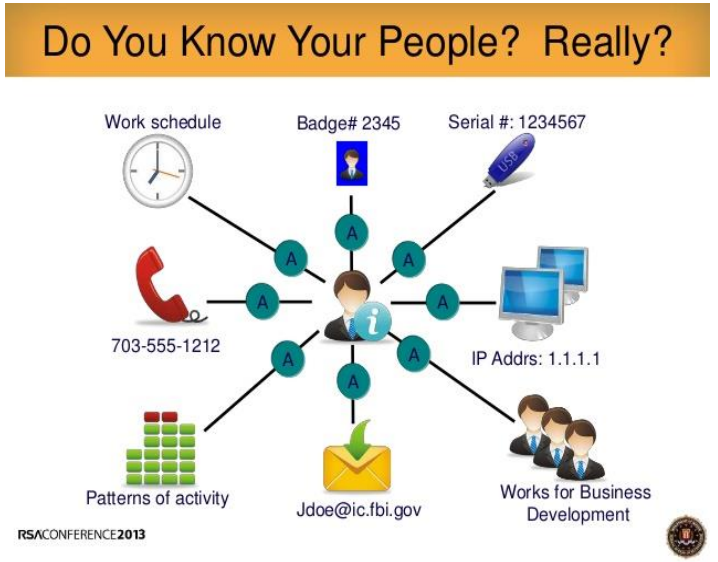
- Behavior related – usage monitoring
  - Logon / logoff hours
  - Websites visited
  - (internal) servers accessed
  - Physical locations visited



Considerations

Users

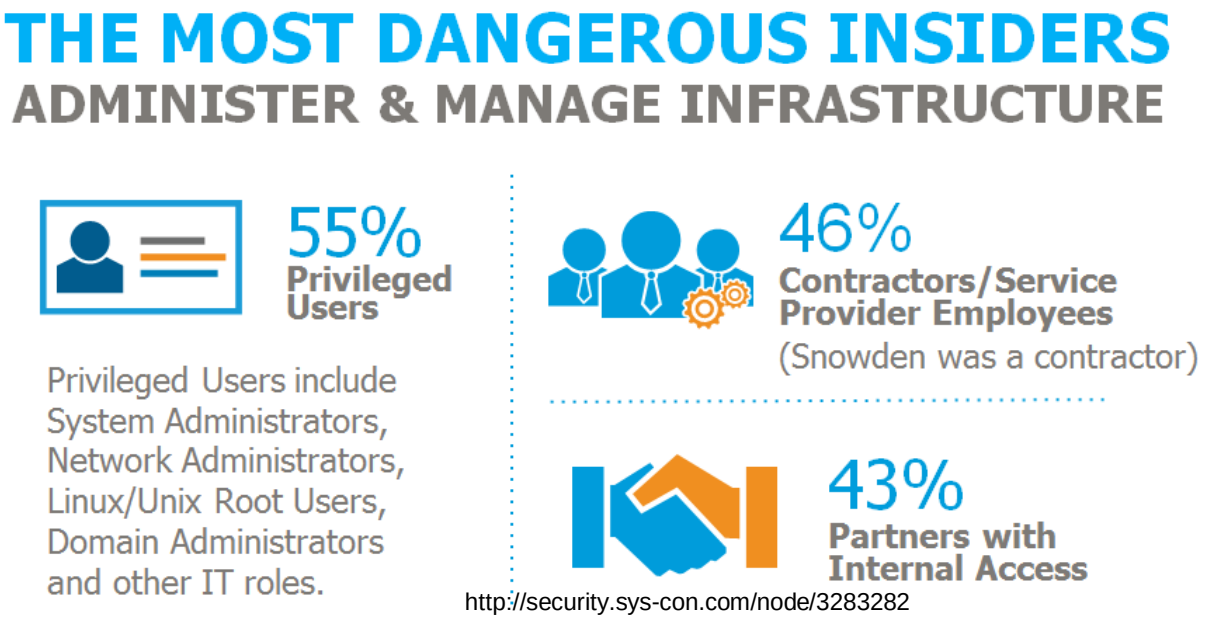
- HR related
  - Background checks during hiring
  - “missed” promotion
  - Radicalization
  - Identify “key personnel”
  - Governance accreditation



Considerations

(Privileged) access

- usage of admin credentials
- (ab)use of (privileged) service accounts
- Revoke (logical) access if role(s) change

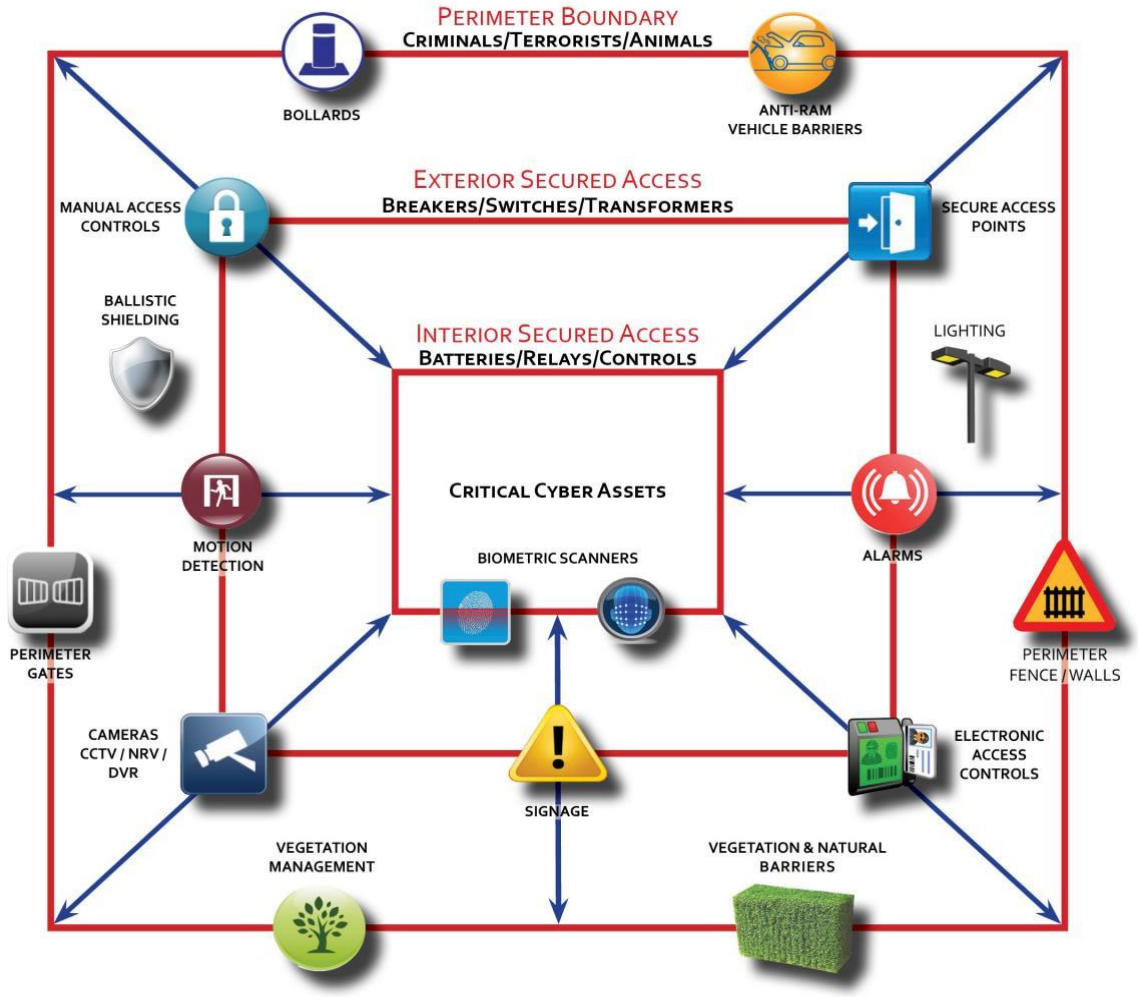


http://security.sys-con.com/node/3283282

Considerations

Physical

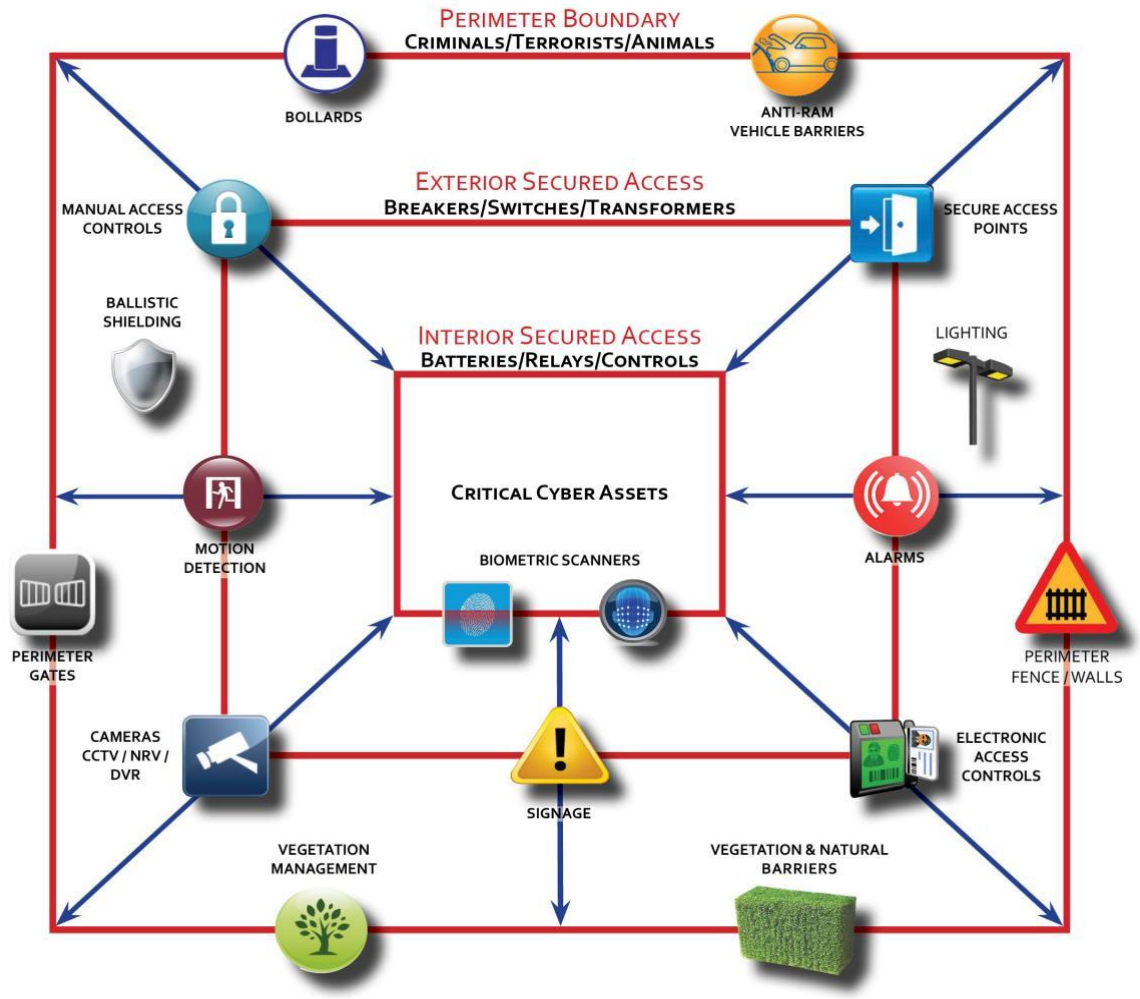
- Verify physical access of everybody
  - Revoke physical access if role(s) change
- Know who is where at what time
- 4 eyes principle
- Camera detection



Considerations

Physical

- Verify physical connections to DSL or other internet lines
- Perform regular physical walkthroughs
- Rack alarms



Considerations

Policies

- Having a (paper) security policy is good
- But should be supported by technical measures

Considerations

ICS Vendor management

Considerations

Training / awareness

Summary

Summary

http://www.csoonline.com/article/3161851/data-protection/how-to-eliminate-insider-threats.html

Summary

https://www.itmg.co/strategic-advising.html

Summary

http://www.rcrwireless.com/20170310/opinion/reader-forum-using-big-data-to-combat-ddos-security-threats-tag10

Summary

- DIY insider threat detection/protection is doable …

- However you need
  - (skilled) People
  - Knowledge/experience
  - Time
  - Management support
  - Equipment & tools
  - Still some Budget
  - To get your IT to know/understand OT

SECUDEA
Security Ideas & Consulting

DIY insider threat detection & prevention

Dieter Sarrazyn
dieter@secudea.be
@dietersar
https://be.linkedin.com/in/dietersarrazyn