Role of the **network** in a **Zero Trust World**

Radu Niculita

Cybersecurity R&D, Siemens Romania

SIEMENS

my $5000 oscilloscope can't connect to the network because a wifi-enabled lightbulb stole its fixed IP address. the future is f****** stupid

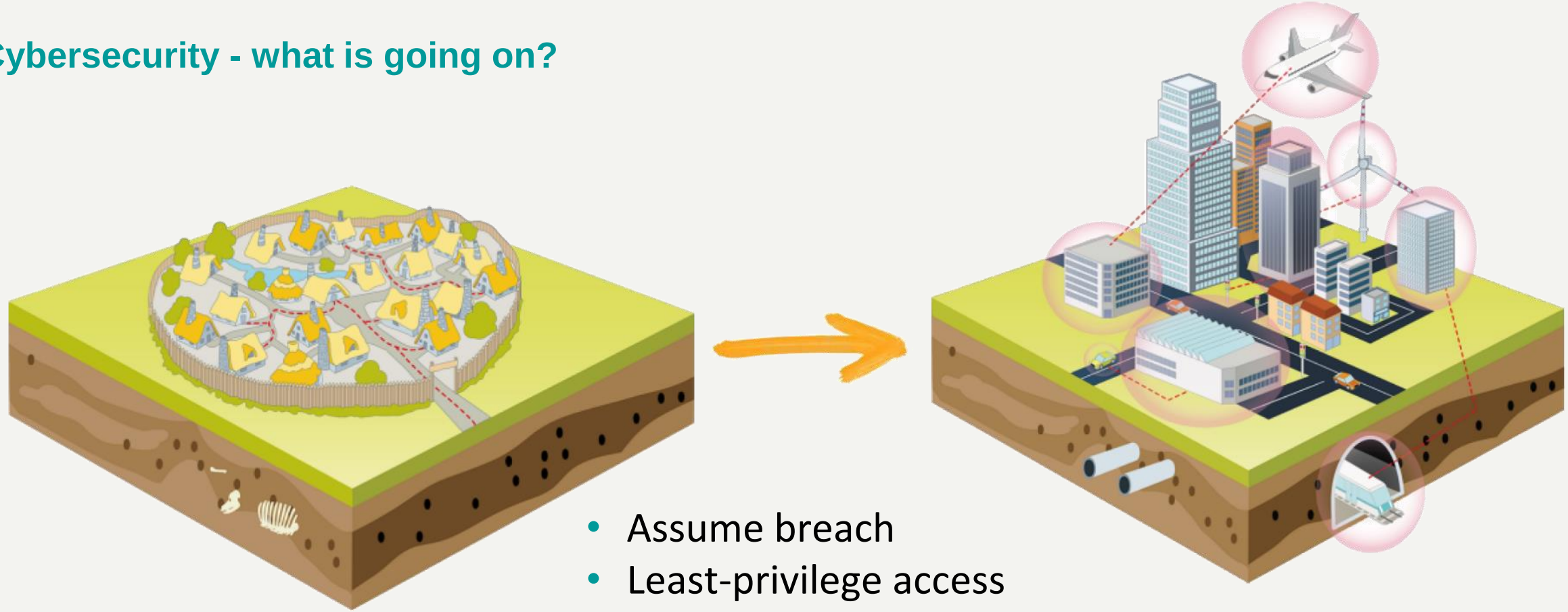
*(IoT smart device landscape in the 2020s)

my toilet paper holder just tweeted that I am out of paper


Everything changes.
Everything is connected.
Pay attention.
*(definition of Zen)

SIEMENS

Cybersecurity - what is going on?



- Assume breach
- Least-privilege access
- Micro-segmentation
- Multi-factor authentication
- Device authentication, authorization, integrity, posture
- Logging and monitoring

SIEMENS

Zero Trust principles (in Siemens)

NIST SP 800-207

1. Connecting from a particular network does not determine which service you can access.
2. Every access request must be authenticated and authorized adopting the least privilege principle.
3. Access policies are composed of rules over attributes of users, devices and trusted information sources.
4. All network traffic shall be End-to-End encrypted
5. Log and inspect all security relevant events and communication meta data.

SIEMENS

Zero trust in Siemens

- The world is changing to everything always connected everywhere
- Industrial devices are moving from physical security to “cloud” accessibility → this is scarry 😨
- Siemens is changing with the world – we want to lead the change, not be a follower

What we do – simplify and control

- Move away from “Castle-and-Moat” security
- “Never trust, always verify“
- Internet everywhere

  …. Including in Siemens campuses
- Cloudify

For Siemens, Zero Trust is the key pillar of the cybersecurity future

SIEMENS

What about the network?

IS NETWORK STILL RELEVANT?

- All these ZT measures seem to cover all angles
- Looking at the network, there are no longer clear locations to place walls

But...

- As long as people write code... it will have bugs
- There are bad guys everywhere while … attack surface is increasing exponentially
- Is client/server and application hardening enough?

We will continue to have non-ZT ready applications for the foreseeable future

Network to the rescue

- First of all – all that you know about network security still stands. ZT is not about *removing* controls, but *evolving*

Important Components of network security in the ZT world

- SASE
- Controlled access to reduce attack surface
- Smart dynamic segmentation
- SD at the center of the new network world

Network Security is a critical tool in the new world

SIEMENS

Components of the Network in a Zero Trust World
SASE

Cisco Umbrella

Harmony Connect

- Somehow misunderstood (as all buzz themes)
- Secure Access What? (Services Edge)

Some confusions:

- SASE is not the same as Zero Trust
- SASE is not a remote access VPN

“Technology used to deliver wide area network and security controls as a cloud computing service directly to the source of connection rather than a data center”

In a nutshell, **SASE is the application overlay**

SIEMENS

Components of the Network in a Zero Trust World
Segmentation

Key pillars

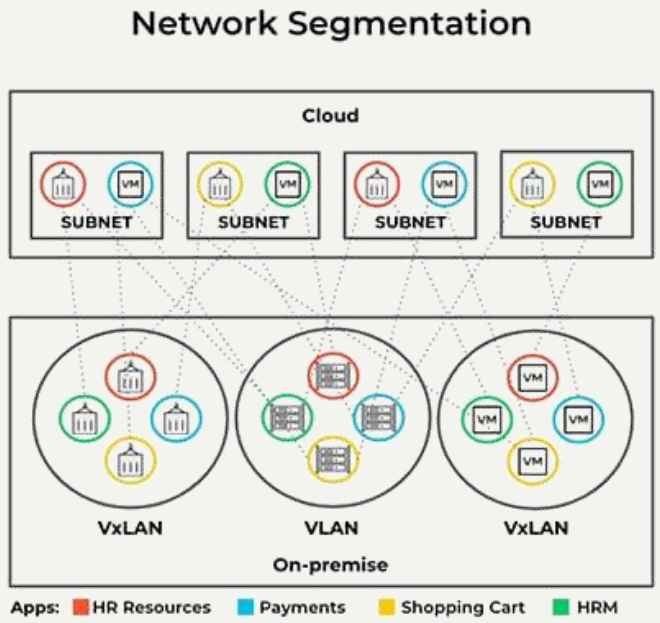
- Controlled access to reduce attack surface
- Smart dynamic segmentation

Macrosegments vs microsegments

Segments

- Agent based
- Network based

Role of the overlay (SD-LAN/VxLAN)



Software Defined Networking is at the center of the new network world

SIEMENS

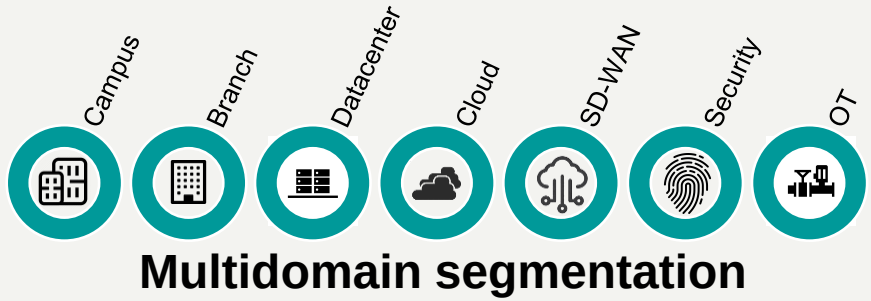
Components of the Network in a Zero Trust World
SD

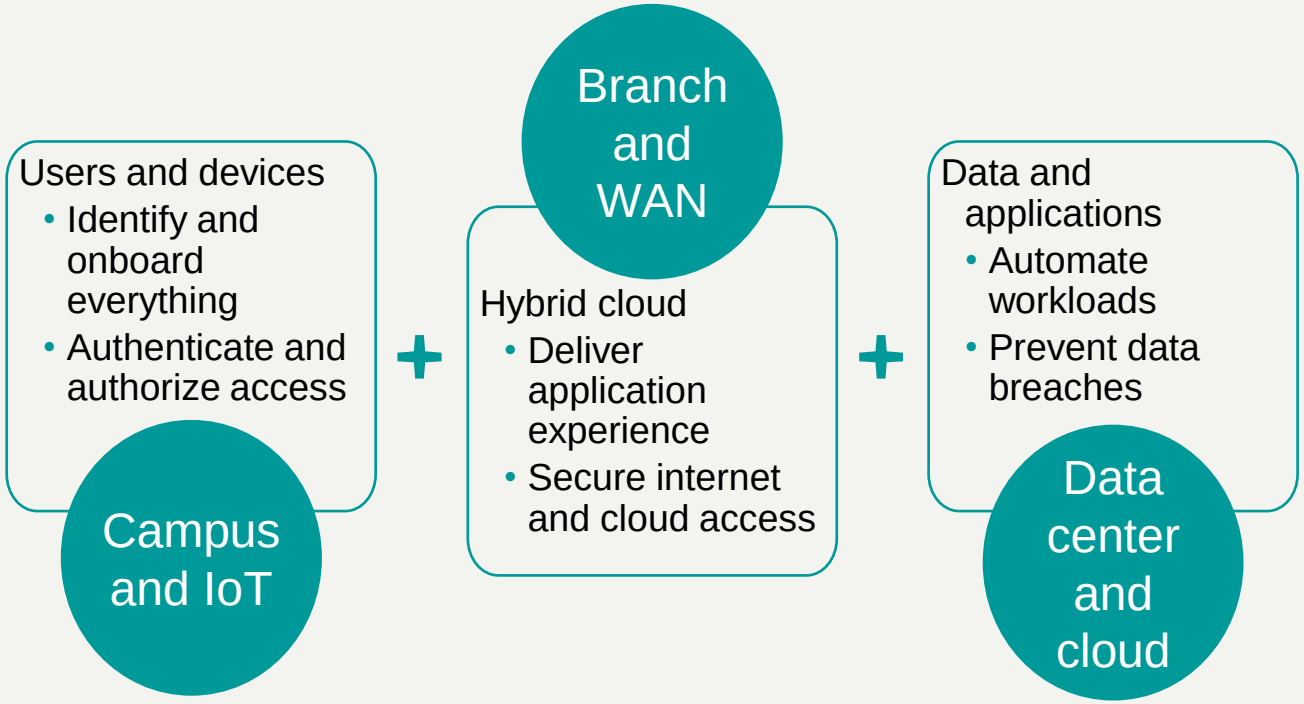
Software Defined Networking is the new norm

- Campus
- Data Center
- SD-WAN
- Cloud

…but why?

- Orchestration
- Automation
- Speed of change
- End to end control
- Assurance
- Visibility





SIEMENS

radu.niculita@siemens.com

SIEMENS

Contact

Published by Siemens Romania SRL

Radu Niculita

Network architect/R&D cybersecurity professional
Siemens Romania R&D
Mobile +40 723 191 094

E-mail radu.niculita@siemens.com

SIEMENS