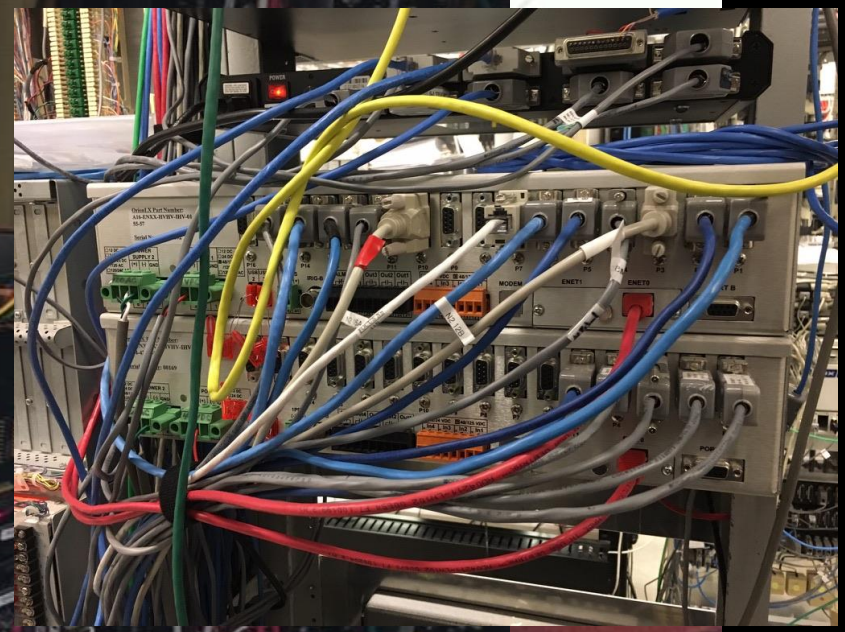
PRODUCT SECURITY CONSIDERATIONS FOR OT SECURITY APPLIANCES

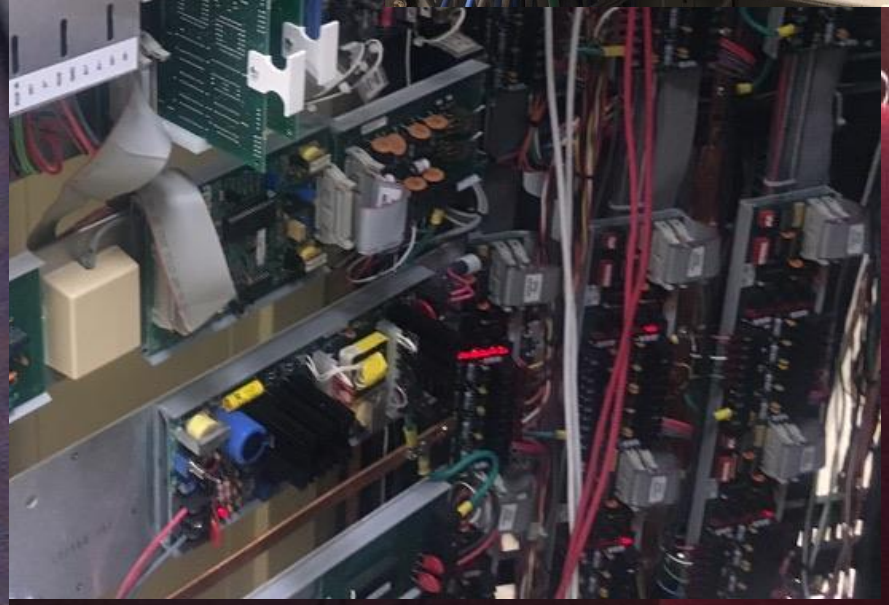
Robert Landavazo

Brandon Dudley


EMC
SYMMETRIX


19,200 7.E.1 HARDWARE
PASSWORD: 0000(ZEROS)

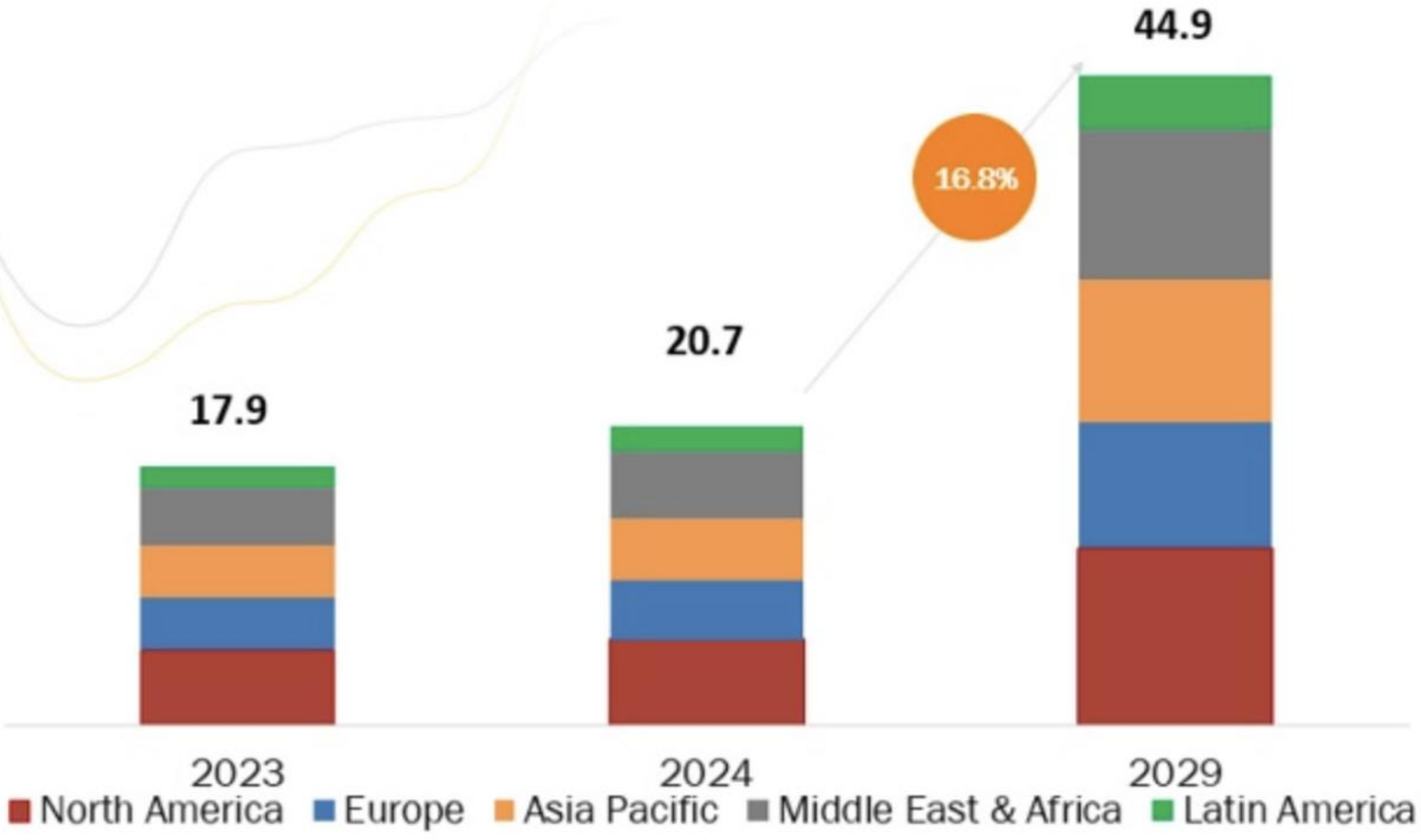




OPERATIONAL TECHNOLOGY SECURITY MARKET GLOBAL FORECAST TO 2029 (USD BILLION)

CAGR OF
16.8%

The Operational technology Security market is expected to be worth USD 44.9 billion by 2029, growing at a CAGR of 16.8% during the forecast period 2024-2029



WHAT'S AN ICS SECURITY APPLIANCE?

- Traditional:

  switches, routers, firewalls

- Non traditional:

  Sensors, diodes, taps, aggregators

  -(usually) white labeled OEM hardware

  -Linux flavor of the month

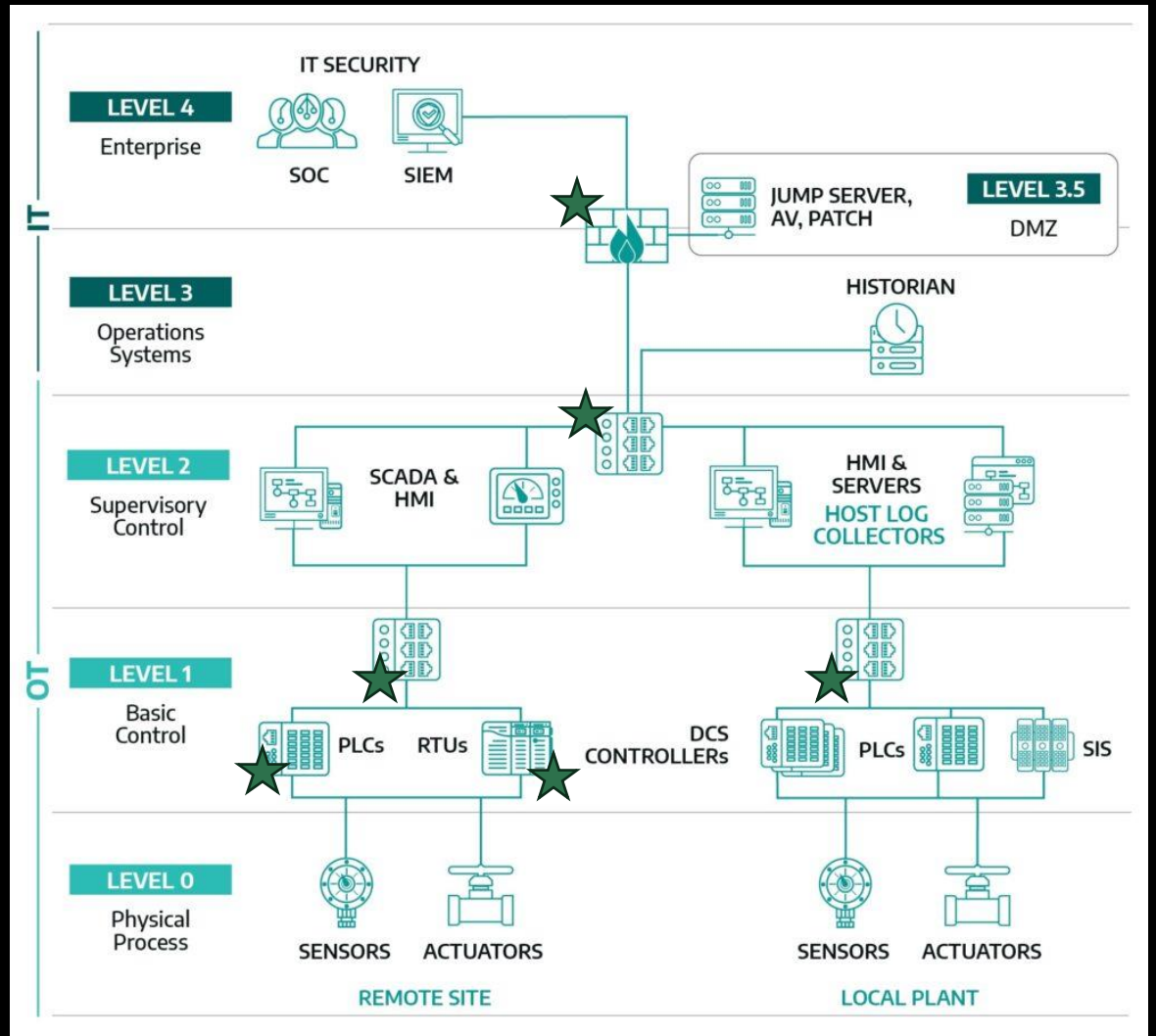
  -OSS

  -Frequent dependencies on cloud

  -Sometimes physically hardened

  -Not security hardened enough

WE PUT THESE THINGS WHERE?



ICS SECURITY APPLIANCE BUYER'S GUIDE

WEAK
- Inspect Secure Software Development Practices

MEH
- Adherence to secure design practices and certifications
  - ISO and ISA/IEC 62443

BETTER
- Review vulnerability disclosure practices
- SBOM

STRONG
- Contractual obligations and RFP/RFI process
- CIP-013

BEST
- Perform independent assessment
  - more on this soon

POST PURCHASE PRACTICAL CONTROLS

- Isolate management and out of band management (OOBM) interfaces from control network
- Monitor the appliances
- For appliances leveraging SPANs

  Configuration monitoring of switch interface configs to prevent misconfig of monitor session interfaces

  - i.e. span ingress

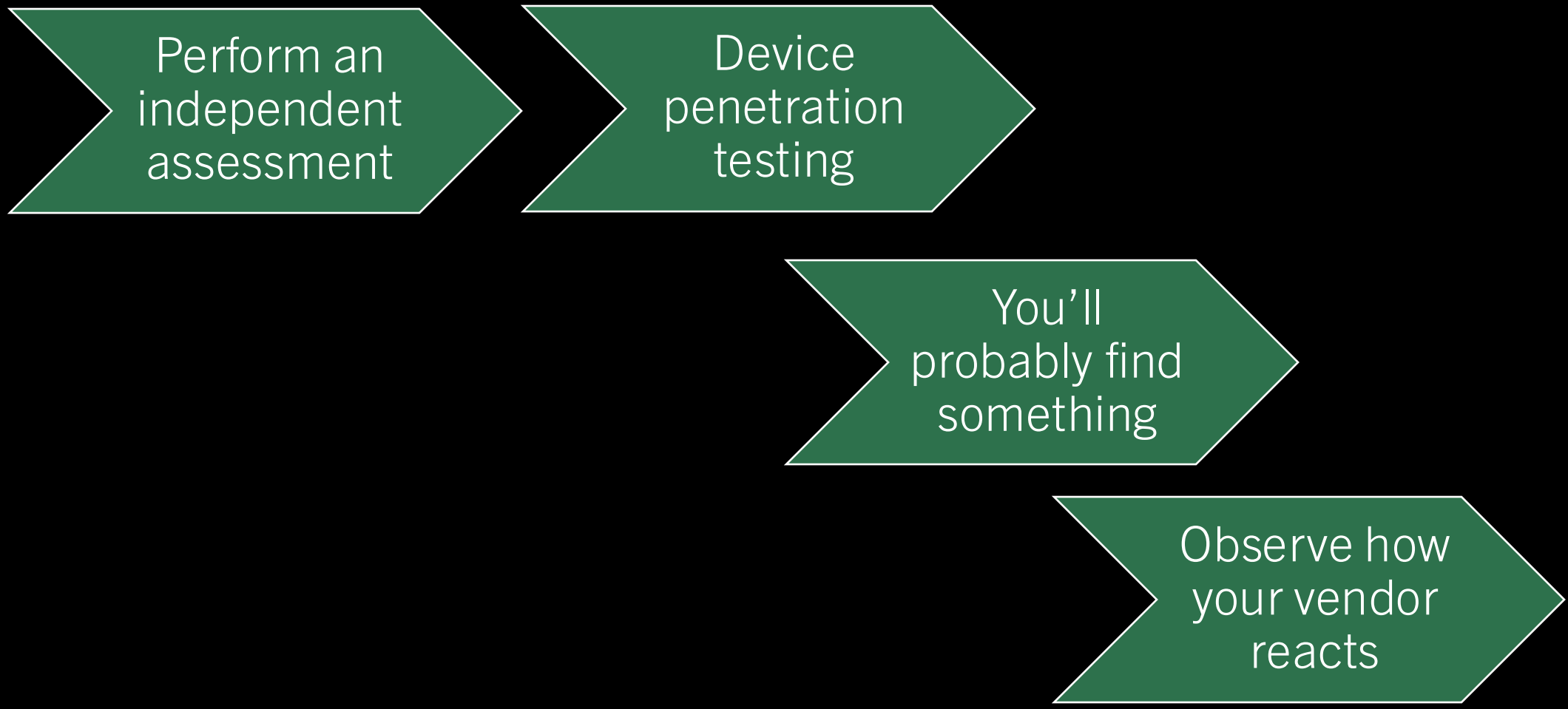
  Consider data diodes for extra insurance

  - There's typically nothing preventing monitor-only interfaces from generating traffic!

    tcpreset == scary?

- Follow ISA/IEC 62443 zoning and conduiting principles (where possible)
- Regulatory compliance

IMPRACTICAL CONTROLS



WHAT IS IMPORTANT?

- Availability
  - Power, water, etc.
  - Life and environmental safety
- Confidentiality
  - IP theft
  - Competitive information
- Integrity
  - Loss of visibility

POTENTIAL IMPACTS OF OT SECURITY APPLIANCE COMPROMISE

- Appliances can act as pivots into production OT networks
  - Active appliances are already configured to touch OT networks
  - Passive appliances can potentially be abused to become active
- Compromise of asset data and vulnerability data
  - Valuable to attackers that want to affect availability (allows them to skip enumeration/scanning)
  - Also valuable to attackers interested in IP theft
- Additional (credentialed) access to third party integrations
  - Active Directory, OIDC, Service Now, etc.
  - Least privilege applies
  - What can these AD accounts do?
- Appliance can become a watering hole targeting users of the appliance

ACTIVE APPLIANCES AS PIVOTS

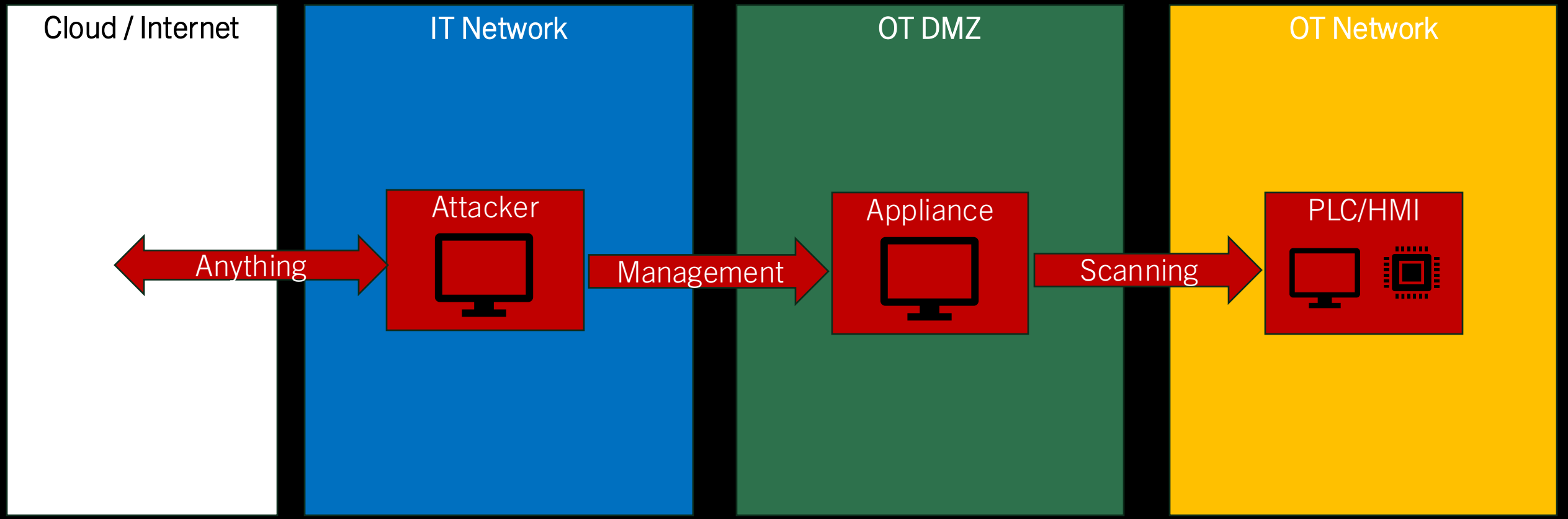
- Configured, by default, to act as pivots into the OT network
- Arbitrary code execution could allow attackers to send malicious traffic from the scanner into the network for enumeration, attack, etc.
  - Use the appliance as intended (loud, but quiet)
  - Abuse the configurations/plugins and make a malicious module
  - Access a shell and write a script
- Proxying of requests could allow attackers to send malicious packets to OT networks
  - Requires very specific conditions for this to be useful to an attacker
  - Attacker has the potential to send packets to the appliance, treating the appliance as a gateway, and have that packet routed elsewhere (requires attacker to be on same layer 2)

PASSIVE APPLIANCES AS PIVOTS

- Requires the right conditions (poor configuration/setup, luck) to be viable, far more difficult to pivot from a truly passive appliance
- Pivoting through a monitoring interface requires a lot of access, and is an additional barrier for the attacker
- Still contains information useful to the attacker (see: use as intended from previous slide, LOTL)

EXAMPLE ACTIVE APPLIANCE PIVOT 1

Attacker identifies management interface on active appliance, pivots through the appliance to OT

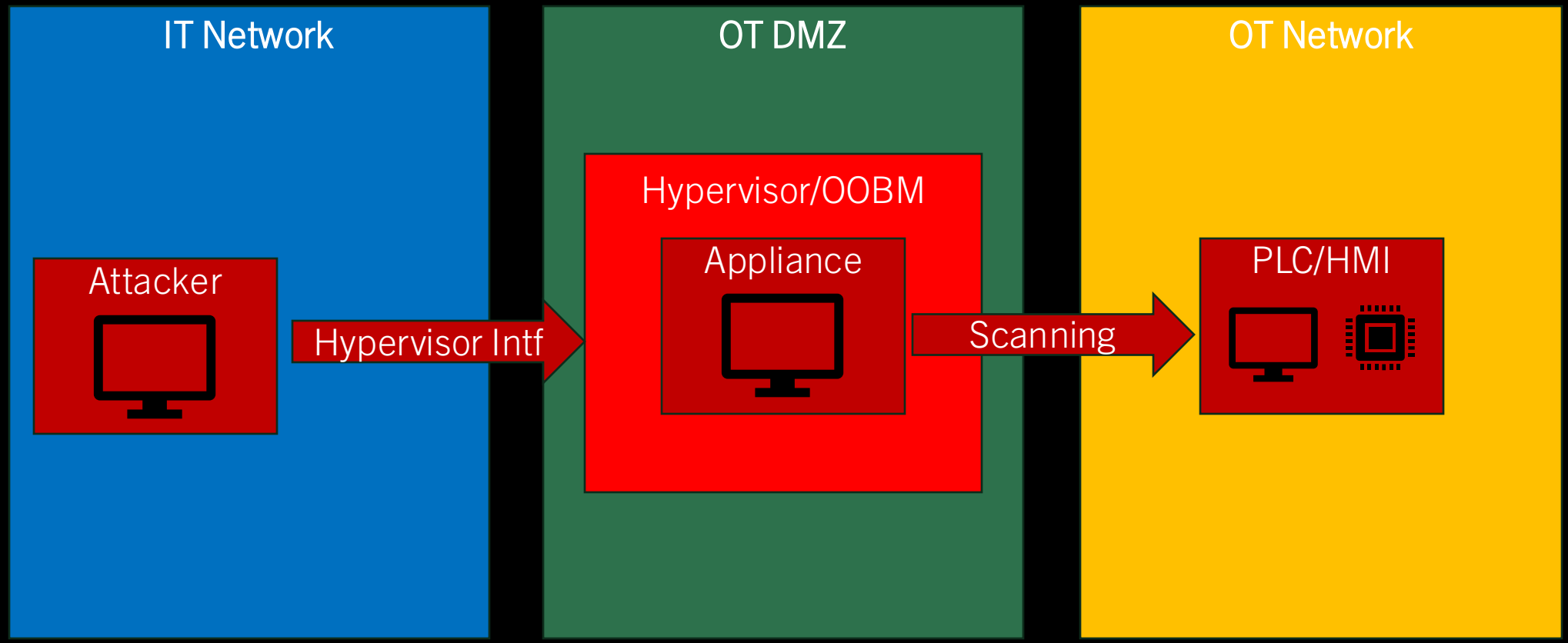


ACTIVE APPLIANCE PIVOT 1 MITIGATION

- Do not allow access to management interface from IT
- Ensure very strong, industry standard, authentication practices are enforced on the security appliance
  - Active Directory (this has implications if AD is in IT, and your IT network is compromised)
  - MFA, OTP – Hardware token
  - Segmentation within IT network: who can access the appliance?
- Remove/disable device when it's not in use
  - If you only scan during maintenance windows, disable all other times

EXAMPLE ACTIVE APPLIANCE PIVOT 2

Attacker identifies out of band management accessible from IT, pivots into OT

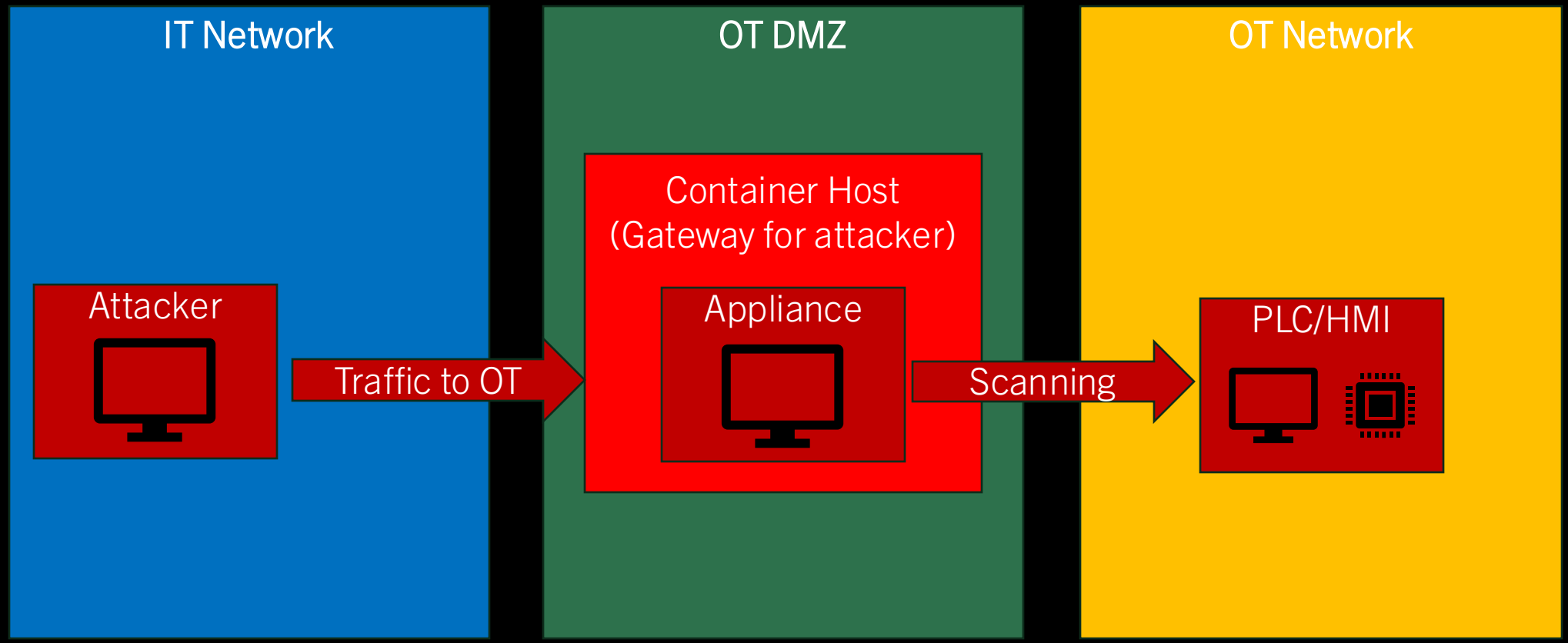


ACTIVE APPLIANCE PIVOT 2 MITIGATION

- Ensure that all access methods (iDRAC, iLO, IPMI, Hypervisor, etc.) are treated with the same sensitivity as the appliance
- Consider disabling/unplugging OOBM if you do not have the resources to secure it
- For virtualization, completely separate hypervisors in OT and IT
- In hypervisor management interface
  - Robust role/permission separation
  - Regular patching

EXAMPLE ACTIVE APPLIANCE PIVOT 3

Attacker identifies container host (Kubernetes) with gateway mode enabled

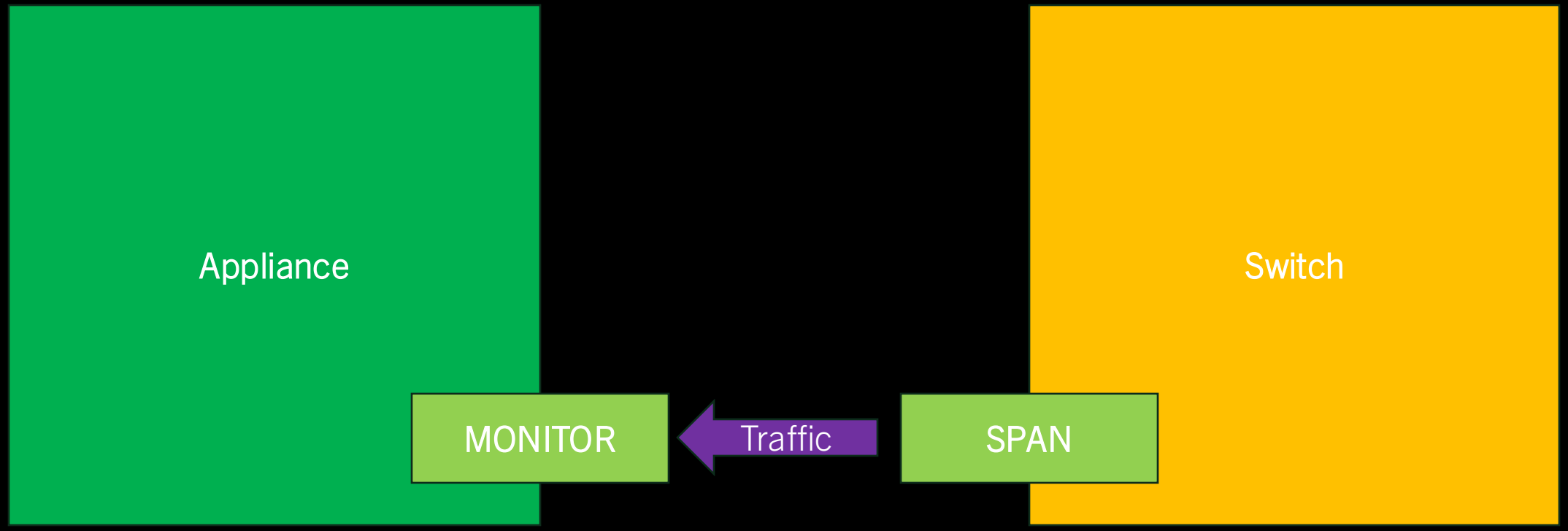


ACTIVE APPLIANCE PIVOT 3 MITIGATION

- Place a layer 3 device between container host and all other hosts (impractical)
- Disable gateway mode for container host

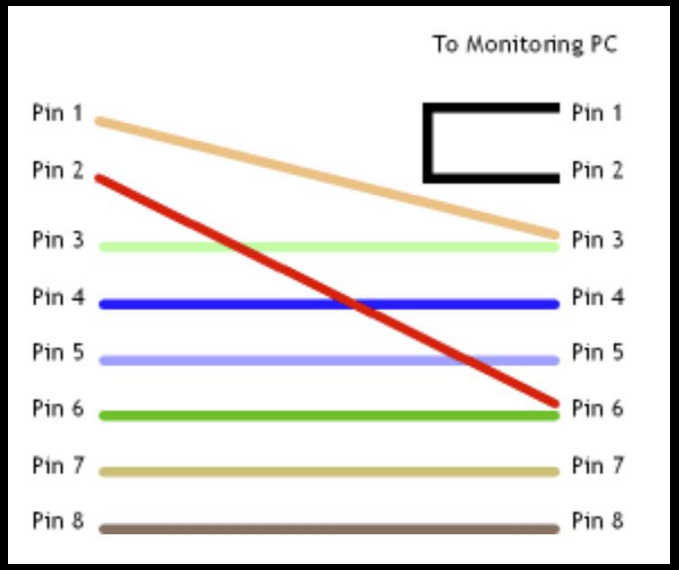
EXAMPLE PASSIVE APPLIANCE PIVOT

Attacker identifies misconfigured traffic producing port, reconfigures appliance port to route traffic



PASSIVE APPLIANCE PIVOT MITIGATION

- Use a TAP that only allows traffic one way
- For older devices, you can make read-only ethernet cables
  - Can break auto-negotiation
  - Doesn't always work, especially with gigabit
- Configure your SPANs properly



TIPS TO IDENTIFY ABUSABLE BUGS

- Always treat the appliance as a computer
- All standard web security practices apply
  - XSS
  - Priv esc
  - etc
- Look for places in the appliance that allow you to configure integrations, especially ones that allow you to enter both IP and port
- Look at the interfaces (sometimes it is easiest to do this physically first)
- See the appliance as its individual components

KEY TAKEAWAYS

- Segmentation
  - Not all OT networks are actually segmented
- Understand your appliance
  - Active or passive?
  - Virtualized, containerized, on metal?
  - OOBM options?
- Capabilities of appliance (explicit and implied)
  - What can it touch in an unintended way, and does that matter?
- What are your priorities? (CIA)

QUESTIONS?

SOURCES CITED

- https://www.marketsandmarkets.com/Market-Reports/operational-technology-ot-security-market-18524133.html
- https://www.dragos.com/blog/improving-ics-ot-security-perimeters-with-network-segmentation/
- https://www.tamos.com/htmlhelp/monitoring/read_onlycables.htm