Using Endpoint Security: Control Real Cyber-Threats to IT/OT Convergent Infrastructure

Integrated Cyber 2019

Ron Brash

VERVE

Agenda

1. Introduction
2. Summary of IT/OT/IoT cyber threats and scenarios
3. Defining concrete IT/OT use-cases for success
4. Use-cases and threat coverage (or lack of)
5. Gaining incident context through data convergence
6. The anatomy of an effective end-point solution
7. Lessons learned deploying OT-first security solutions

VERVE

Who Am I?

VERVE

Director of Cybersecurity Insights at Verve Industrial

- Ex-Tofino Security Developer, ICS/SCADA critical infrastructure DPI fanatic, pcap jockey, security architect, embedded Linux/RTOS guy, researcher and technical lead
- Creator and developer of the ICS Detection Challenge (x2)
- Bachelor in Technology (BCIT)
  Thesis under NDA, prototyped packet flow anomaly detection for ICS network traffic with minimal false positives on xScale hardware (2010)
- Master in Computer Science (Concordia)
  (again under embargo), prototyped and formally validated secure technology transitions using hybrid protocol gateways for legacy infrastructure; very SDN-driven (2017)

Why we do this?

"The greatness of a community is most accurately measured by the compassionate actions of its members"

Coretta Scott King

VERVE

Defining Threats

VERVE

Cyber? Threats? Scenario?

What is a **cyber**?

- It's that computer-connected thing with lines blending physical and electrical

What is a **cyber-threat**?

- Effectively, the potentiality of an action that would have negative effects on an organization or system(s) through cyber as a vector

How does that differ from a **threat scenario**?

- Not all organizations and systems are alike, and so the threats in a specific scenario (context or story) may be relevant to one, but not the other!
- And therefore, threats can be shared amongst scenario(s), but not limited too!

What is a **Vulnerability** vs. an **Exploit**?

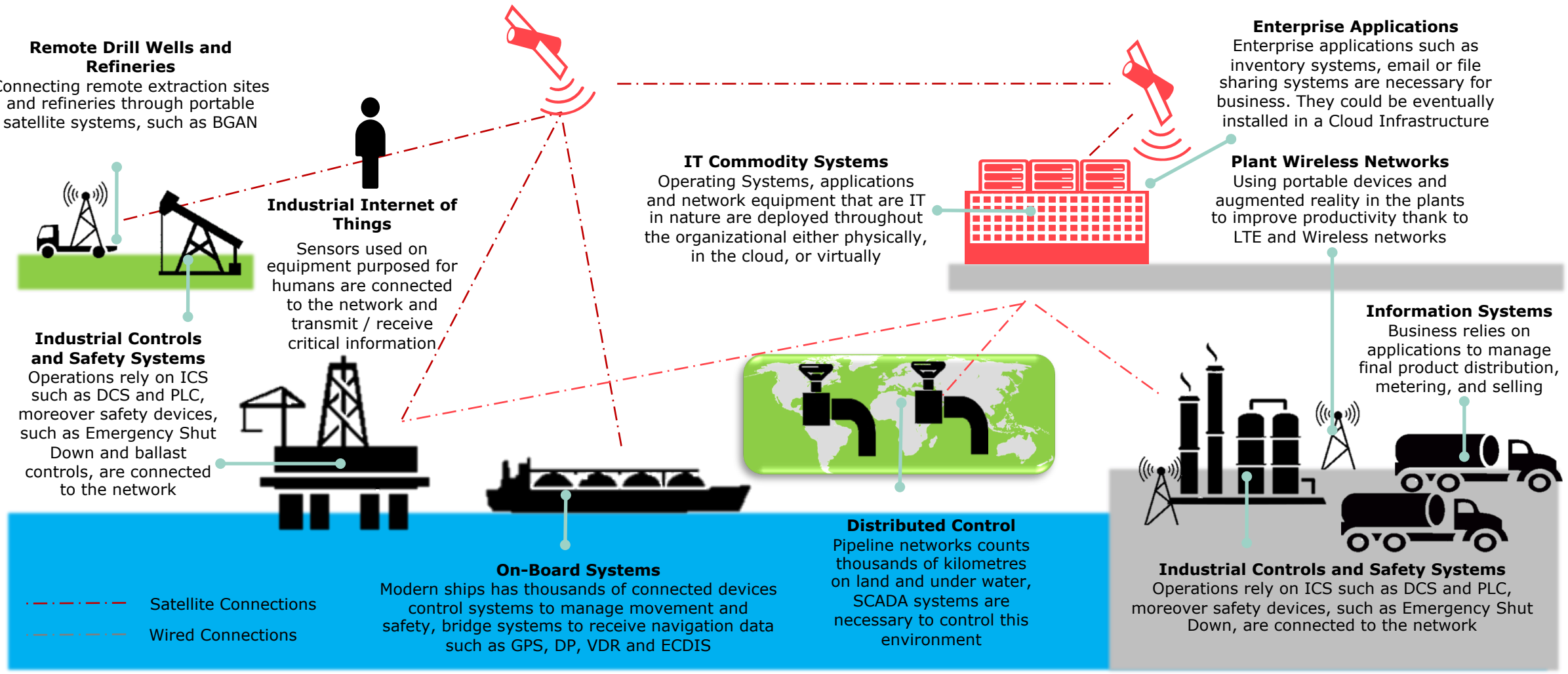
- A **vulnerability** is a potentiality (known or unknown) that could be **exploited** by an **actor**
- **An exploit is the successful execution of that vulnerability**

And importantly, consider that:

- **Cyber-threats are often a chain of vulnerabilities exploited by 1 or more actors**
  Consider that vulnerability is often multi-stage (chained), and also in BUSINESS terms
- E.g., one CVE does not equal a compromised process – it is often an unpatched system with a known exploit, no monitoring, poor access control, and non-existent Incident Response (IR) that RESULT in a successful compromise

VERVE

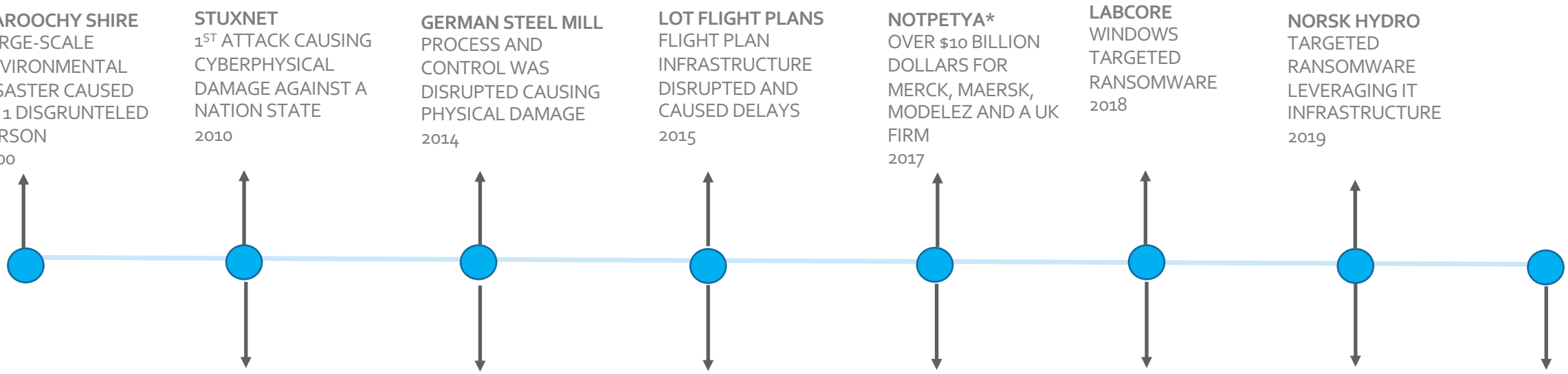
Considering Traditional IT/OT Convergence (Oil & Gas)



Summary of Threats (classified by environment)

Attack type	Name	IT	OT	IoT/cloud
Targeted ransomware affecting ICS	NorskHydro	YES	YES	
Commodity malware with ICS support	VPNfilter	YES	NO*	YES
Ransomware	Labcore	YES		
Specialized ICS attack	Trisis	YES	YES	
Ransomware	Merck	YES	YES	
Ransomware	Maersk	YES	YES	
Botnet	Mirai	YES		YES
ICS attack	Water Plant	YES	YES	
DOS	Polish LOT	YES	YES	
ICS attack	German Steel Mill	YES	YES	
ICS attack	Ukraine Power Grid	YES	YES	
Targeted malware	Shamoon	YES	YES	
ICS attack	Stuxnet		YES	
Insider	Maroochy		YES	

Timeline of Threats



Or IoT/IIoT, and Cloud

Cloud-stored OT Telemetry & Predictive Maintenance
Relaying, storage and processing of OT related data for analytics, triage and more

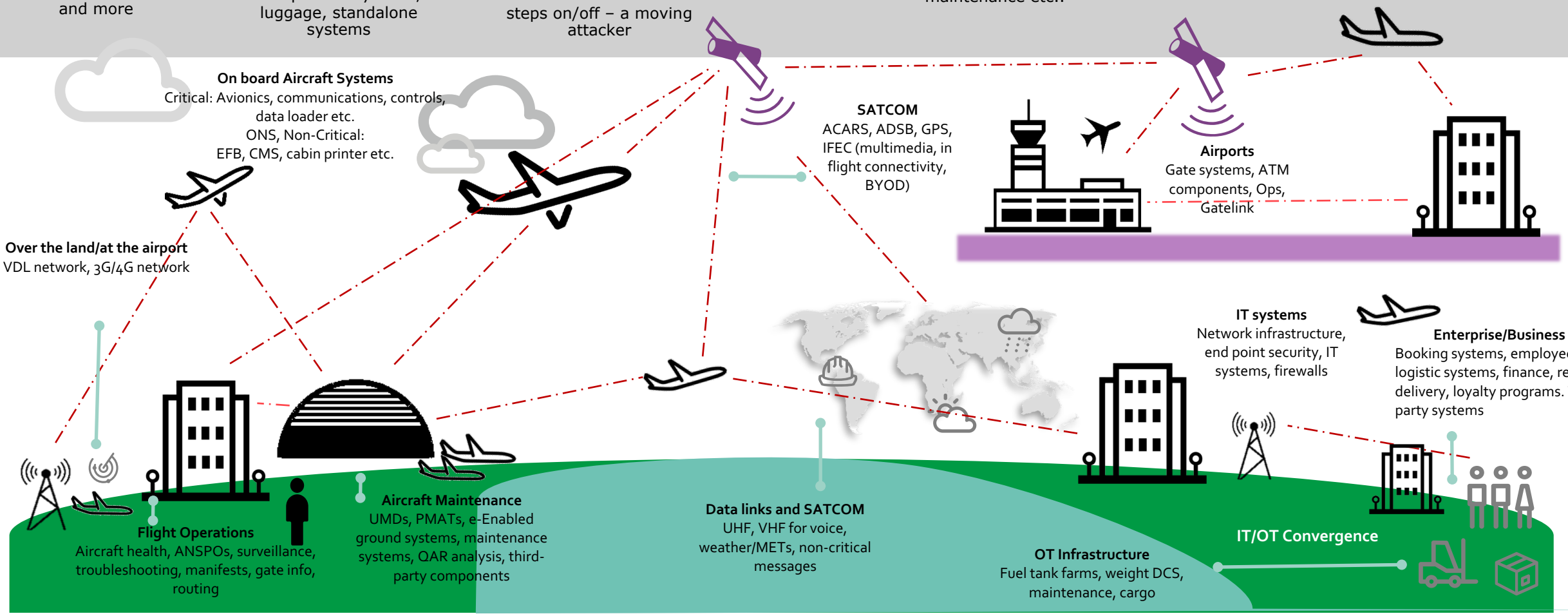
Industrial Internet of Things (IIoT)
Sensors or devices with resources that can be used to provide telemetry where there was previously none; luggage, standalone systems

Internet From Gate-to-Gate/Inflight Wireless
WIFI aboard aircraft, seamless gatelink for when the plane lands, or when the customer steps on/off – a moving attacker

Cloud-infrastructure Integrated for IT/OT
Virtualized and cloud-hosted data centers off premise, software part libraries, archives for maintenance etc..

Cloud-based Access Control
Cloud-based Windows AD/Azure and other federated identity management

Cloud-based Business Applications
Reservation systems, API gateways, sales and transactions, portals to OEMS



The Challenge of Applying Risk to IT/OT Cyber Threats?

While IT cyber-risk is relatively well understood, establishing probability, and impact for OT-related threats is trickier for several reasons:

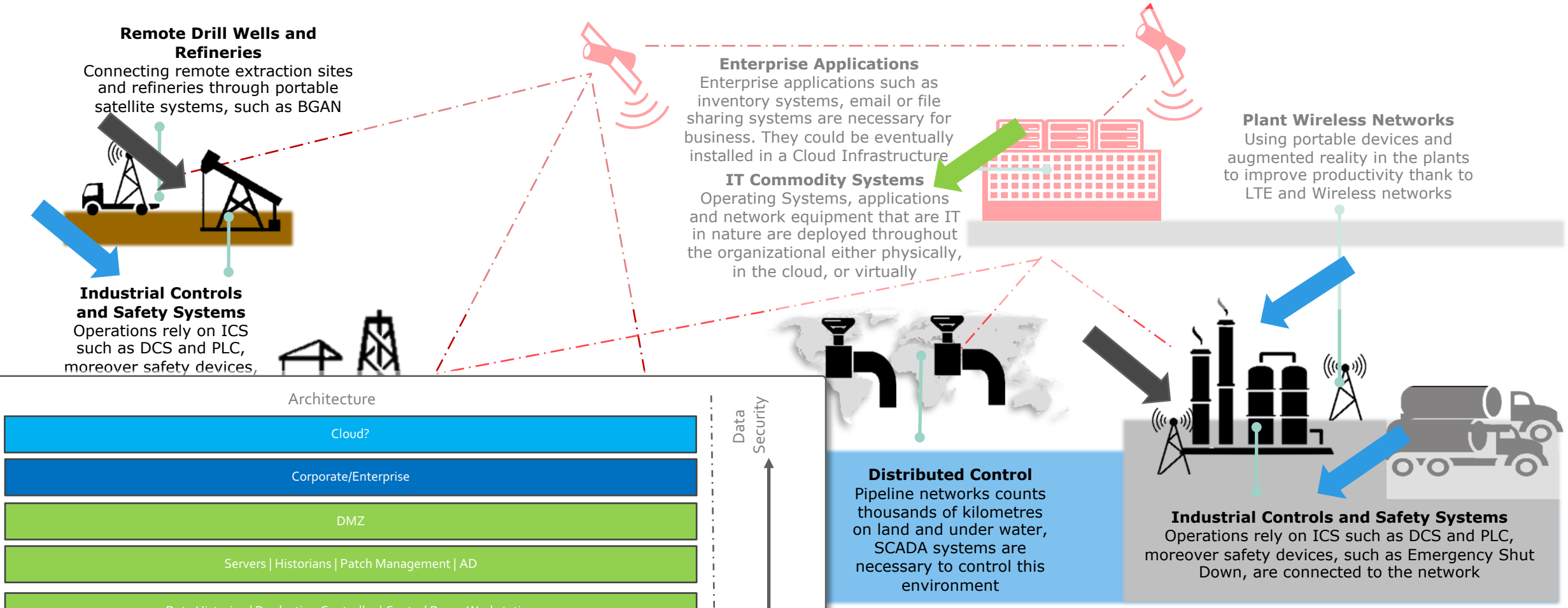
- ✓ Product lifecycles (e.g., hardware EOL)
- ✓ Supply chain and inventories
- ✓ Operational environments (e.g., downtime or certification)
- ✓ Risk of OT disruption (Safety, Reliability and Productivity)
- ✓ Security of day-to-day data isn't the priority; integrity is
- ✓ Process visibility & supervision trumps IT
- ✓ Personnel and skillset differences

And again, the **formulas used for establishing the threat of risk, the probability of risk, the impact of risk and residual risk after mitigations (if any) becomes a challenge** that not just any organization can determine as often they are **SPECIFIC to the OT environment, and IT factors increasingly integrated** into today's IT/OT converged organizations.

- **And can be referred to as Cyber Risk/Cyber Threat Use Cases (UCs)**

VERVE

Threat Relevancy Dependent on Scenario



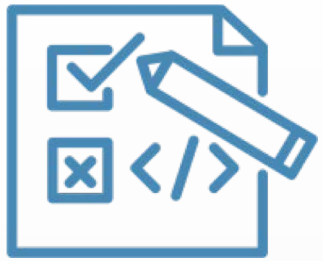
"The idea is to start somewhere based on what keeps the business operating and separate FUD from value"

Use-Cases For Security

VERVE

What is a Use-case

When we think of a use-case, normally a description looks like this:



- **Use X technology to do Y for the business**

However, if we apply a type of gamification:

- We can use use-cases to:
  - **Define exactly how an organization would detect, identify, contain, and respond to a negative event**

- **Use STORY-like narratives** that can be utilized by all three avenues:
  - People, Process and Technology

Therefore, **a use-case is a useful tool** to define:

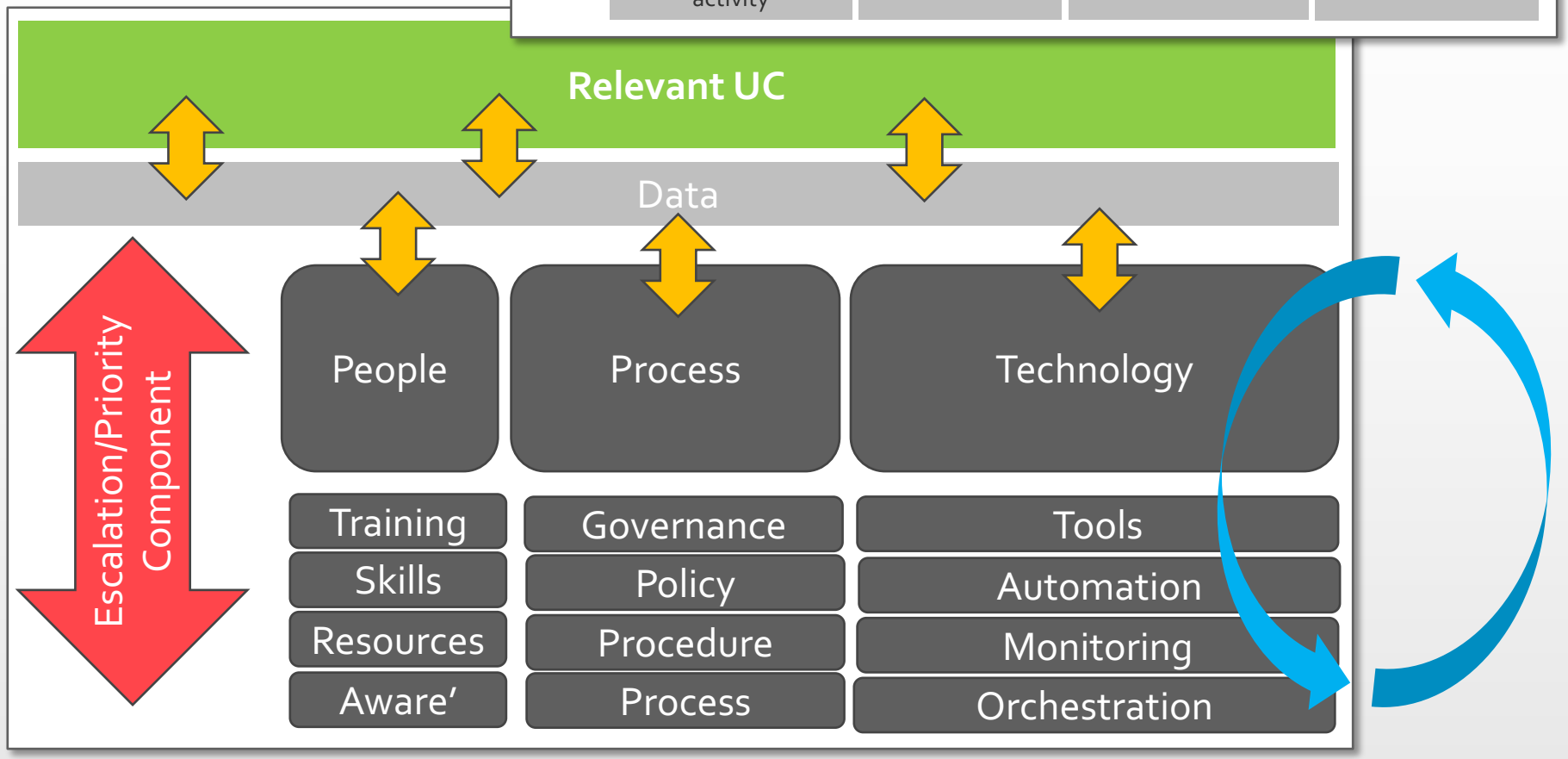
- The requirements, workflow, skills and response to an event

- E.g., similarly to how a software developer would create application's functionality to handle failed login attempts

VERVE

Defining a use-case? Think like a Dr.

	Symptoms	Diagnosis	Prescriptive Treatment	Treatment Execution
⊘	Runny nose	Could be anything	Go away	Left untreated or disappears
✓	X malware signature on hosts Unusual network activity Unusual host activity	Windows Malware on Critical Host/Segment	Comprehensive steps and guidelines	Successfully eradicated by repeatable process



VERVE

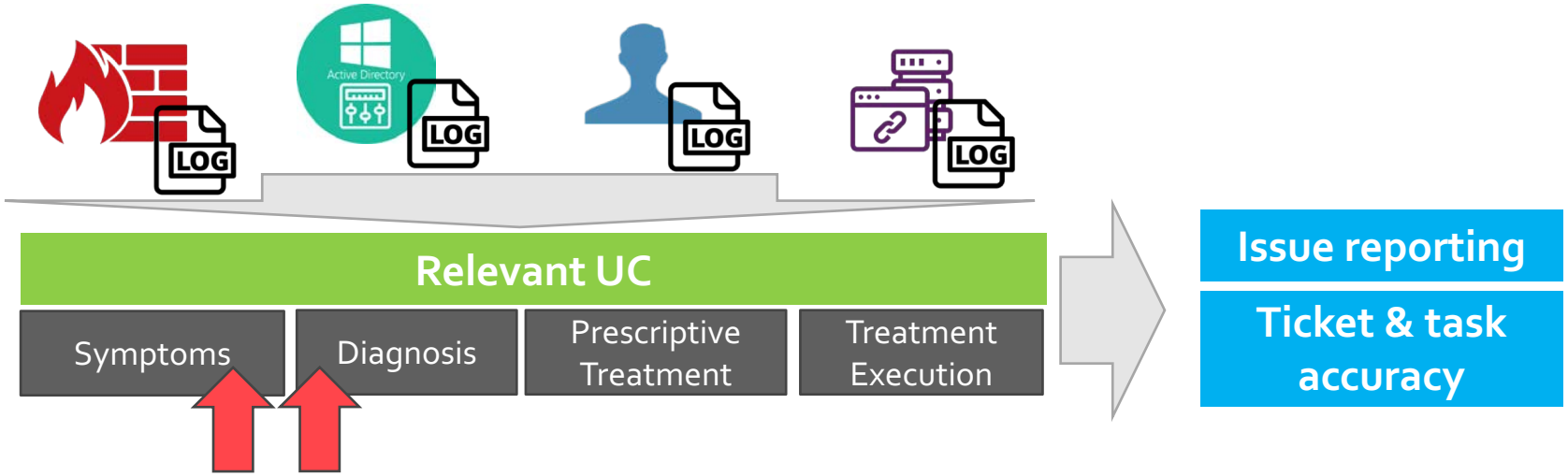
Supplementing Use-cases with data

When approaching use-case data considerations:

- Is it single mode? Or does it need to be multi-modal?
  - **Single mode – single source**
  - **Multi-modal – multiple sources or types (correlation is hard)**

- Again a UC is only as accurate as the data used to:
  - Detect and identify
  - Analyze and triage
  - Contain and remediate

- Reduces incident response time immeasurably, and increases effectiveness of:
  - Teams and resource skills
  - SLAs and SLOs
  - Technology investments



VERVE

Industry 4.0 UC

Example: Drive4Days automotive component maker

- Has several business units producing several different product catalogs
- Some business units are quite integrated, and others older, lower profit margin
- Has recently acquired an older, but still profitable OEM-parts company

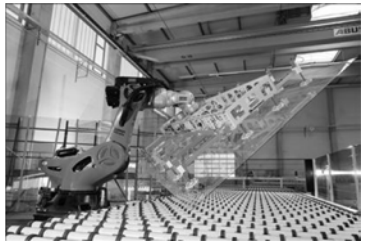
To make the new company more profitable, competitive and reduce any disruptions:

- Enterprise has chosen to integrate vertically reporting to the plant floor (IT/OT)
- Plant must maintain nearly continual operation with a contingency of $10M and burn of $100K/h

Considering the UCs for the organization's bottom line (for security):

- Minimize commodity malware disruptions by patching and monitoring that considers Safety-Reliability-Productivity (SRP)
- Prevent unauthorized/unacceptable system access with standardized software and management controls
- Holistic visibility on all IT/OT assets through aggregation and unified reporting to improve Operations

^ *Notice the language – agnostic of origin for executives/business, engineers and IT; its about keeping jobs…*



VERVE

Example Threat Exercise

Target: Z System (Zsys) HMI Vulnerability at ACME Plant				
Likelihood: High (score 6)	Vulnerability: Low (score 2)	Impact: Medium (score 4)	Mitigation: Limited (score 1)	Normalized Residual: LOW (score 64 or Lvl 2)
Target: Disrupting and compromising Zsys interface				
Actors: ABC Organization, X actors				
Impacts: Legal, financial, brand damage, **potential** safety risk				

Threat Scenarios:		
Scenario	**Likelihood**	Mitigated
Denial of Service – threat actor exploits interface and causes loss of visibility to Operators	High	NO
…	…	…

Remediation & Residual Risk

- Assess additional controls and work with Zsys vendor to close gaps within the next 6 months
- Manager of OT security systems to follow up
- Validate SIS functionality and related incident processes for cyber-exploitation
- Implement and ***Operationalize*** **end-point system protections**

Follow up

- Ongoing use-cases to be integrated into SIEM for continued vigilance and risk monitoring

Leads to Different

Approaches & IT/OT Convergence

Software or hardware

- Does the solution require dedicated hosts?
- Does it need to be installed separately or leverage existing systems?
- Is it entirely an application that can receive information from multiple existing sources?
- Or is it a solution that requires custom hardware in addition?
- Has hardware requirements?

Dashboards or reporting

- Are dashboards targeted to multiple types of audiences?
- Are the dashboards customizable?
- Is reporting automated or real-time?
- Has additional insights and trends?

Agent or appliance

- Network or host-based?
- Can it be installed on existing systems?
- Is it a dissolvable solution?
- Are there host considerations?
- Is it stand-alone?

Active or passive

- Is the solution only a passive monitoring?
- Is the solution able to actively poll information?
- Is the solution able to actively execute security functions?
- Anomaly detection? Heuristics? Or Rule-based?

Administrative

- Patching?
- Capable of applying policy?
- Monitoring of host changes?
- Monitoring of user-behavior?
- Rule-based or trend-based?
- Capable of remote installations?

- Applicability
- Effectiveness
- Accuracy
- Environment
- Features
- Extensibility
- Usability
- Total cost
- Outputs

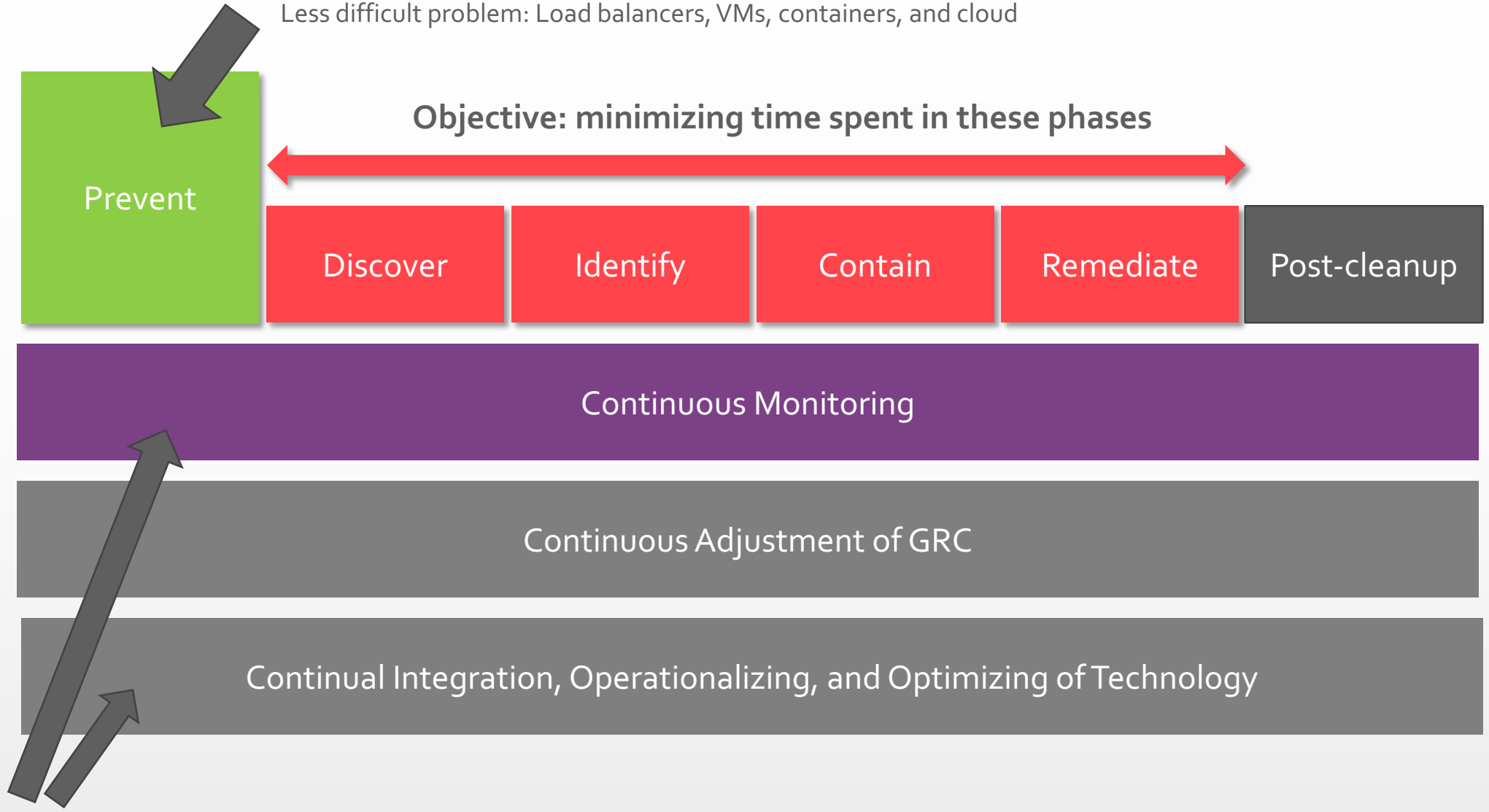
Knowledge, research, hunting, threat intel, services

VERVE

#?

(modified) Steps to Threat Management

Problem: Where this get's difficult is with IoT/IIoT and EOL/legacy equipment
Less difficult problem: Load balancers, VMs, containers, and cloud



Relatively Easy & Solvable challenge: integrating multiple data/configuration sources and making sense of them

Friendly advice: Focus on the Quick wins, but also Solid (and small) Wins

VERVE

The Anatomy of End-Point Security

The Anatomy of an Endpoint solution

Cont' Evolution

- Constantly maintained

Usability

- Less hindrance; user friendly

Integrations

- Modular expansion

Training/Support

- Improves org' maturity & skills

Delivery

- **Delivers features effectively***
- Proactive and preventative activities
- Validated activities with rollbacks*
- Timely actions

Insights

- Turns data into usable and valuable insights/alerts
- **Enables productivity***
- Limited false-positives

Features

Enables/Provides:

- Active/passive components
- Logging
- Alerting
- Reporting
- Footprint
- Design
- Automation
- Inputs/Outputs

Relationship

- **Well-engineered**
- **Skills and technology are proven**
- Realistic aims (no buzzword soup)
- Solves org' problems (not vendors)

Approach/strategy

Lessons learned

Intellectual Property

Technology

Skills & Research

Data APIs/Open

VERVE

Threats Addressing When Using **End-Point** Security

Threat	Prevent	Detect	Contain	Respond	Mitigated
Known malware, vulnerabilities	YES	YES	YES	YES	YES*
Ransomware	NO*	YES	YES	YES	YES
Configuration alterations	YES	YES	YES	YES	YES
Unauthorized Software installation	YES	YES	YES	YES	YES
Network traffic anomaly*	-	YES*	-	YES*	-
Data-exfiltration	YES	YES*	YES*	YES*	-
Compromised account	-	YES	YES	YES	-
Anomalous endpoint activity	YES*	YES*	YES*	YES*	-
Policy violation	YES	YES	YES	YES	YES
Network attacks (MiTM, worms)	YES*	-	-	-	-
Incomplete asset inventory	YES	YES	-	YES	YES*
Zero-day	?*	-	-	-	-

Assessing Asset Risk & Applying the Endpoint Security

Threat	Risk	Use-Cases
Known malware, vulnerabilities	**MEDIUM**	• Patch X criticality vulnerability • Detect & respond to AV alert • Alter whitelisting/proxy to alert
Ransomware	**HIGH**	• Validate backup and restore system • Detect & respond to Malware alert • Prevent lateral ransomware movement
Configuration alteration	**MEDIUM**	• Monitor and record configuration changes • Monitor and archive firmware/logic uploads to devices • Archive project file changes • Detect change management violations
Unauthorized Software installation	**MEDIUM**	• Detect, monitor and prevent unauthorized software installation • Update software whitelists • Remove unauthorized software automatically
Policy Violation	**LOW**	• Detect and alert on unacceptable behavior • Detect and alert on policy violations • Detect and alert on user behaviors • Prevent obvious policy violations and alert
…	**…**	• …

What do you notice?
These UC are the same in IT and OT; it's the handling that may change!

VERVE

And Trisis?

The malware—dubbed Triton, Trisis, or HatMan—attacked safety instrumented systems (SIS), a critical component that has been designed to protect human life. The system specifically targeted in that case was the Schneider Triconex SIS. The initial vector of infection is still unknown, but was likely a phishing attack.

- Remote Desktop Protocol (RDP) sessions to the plant's engineering workstations from within the IT network.
- Poorly configured DMZ infrastructure that allowed the attackers to compromise the IT/OT DMZ and pivot to the control network
- Development environment and software being loaded onto workstations
- And the organization's perimeter VPN had been compromised and infiltrated.

Across the network,

- Malware beacons were emanating from the OT network
- And Mimikatz Windows-hacking traffic was spotted by the organization's AV solution in **multiple instances**

While the end-cost and motives are not currently known:

- **The attackers caused two refinery safety events/shutdowns**

Sources: Dark reading, S4x19 presentations and other media

VERVE

Sum(People, Process, and Technology) == (the Role of the Organization)

VERVE

The Role of the organization

ORGANIZATIONAL OWNERSHIP & GOVERNANCE

- Overarching support
- Vision and risk ownership/management
- General direction
- Budget definition and assignment
- Collective body (plants and sites included; especially with convergence)

PEOPLE

- **Task fulfillment**
- **Skills and training**
- Enabling response (proactive and retroactive)
- Validate/execute where human decision is required
- **Needs to abide to policy and process**
- **Enable responsibility and ownership**
- **Limited time and resources**

PROCESS

- **Enables repeatable action**
- **Ensure consistency and clarity**
- **Method for continual improvement**
- **Defines inputs, outputs and expectations**
- Collect, create and report
- Strategy, procedure and guidelines

TECHNOLOGY

- Procurement
- Installation
- **Maintaining**
- Retiring
- **Integration**
- Method of archival/centralization
- Source and method of automation
- **Effectively tools – not silver bullets**

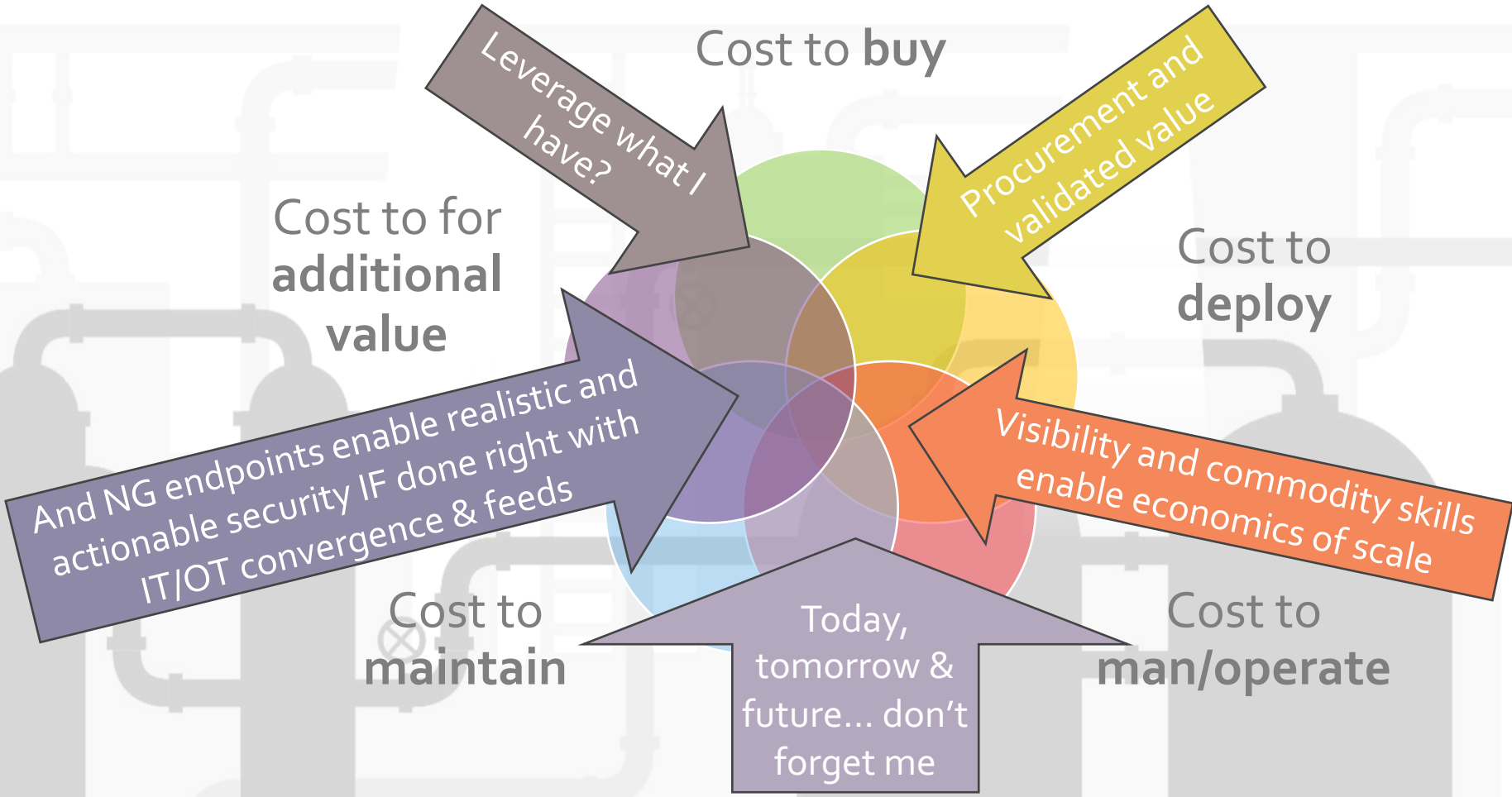
ENDPOINTS

VERVE

And Occam's Razor of Solution Ownership

Again, solutions & assets are not one time investments nor drop-and-forget security.

Total Cost of Ownership (TCO) == COST of (purchase + deployment + operationalizing + maintenance + personnel + additional value generation (integrations and optimizations))

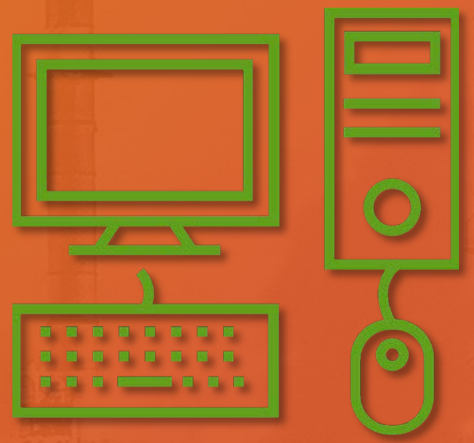


VERVE

Lessons Learned From Reality

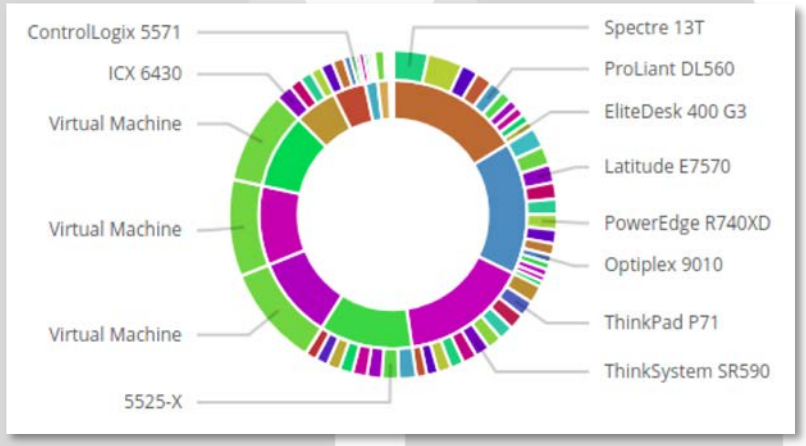
VERVE

IT-esque systems are more prevalent than commonly thought by ICS/OT Sec' vendors



VERVE

- **Commodity** IT systems and hardware are far more prevalent than previously thought:
  - Programming stations, Operator systems/HMIs, Historians, Servers and networking gear
- Despite environment or Operational differences, they still have vast potential to be managed just like Enterprise IT systems:
  - Configuration management
  - Policy enforcement
  - Log retrieval and management
  - Patching
- **And they are subject to a VARIETY of the same threats; EXCEPT the CONSEQUENCES largely DIFFER based on CRITICALITY**



Patch validation is not common

- In typical vulnerability management (VM) the process looks like:

    1. Assess and scan assets (either authenticated or/both non-authenticated)
    2. Assemble data and triage, which known defects can be fixed
    3. Test said fixes/patches
    4. Deploy the fixes
    5. Rescan

- Unfortunately, patching can fail at the deployment phase and often goes secretly unpatched until the Step 1 is completed again.
    - This adds additional frustration for OT and IT teams alike
    - **Reduces effectiveness, and adds risk of exploitation**
    - Complicates upgrade cycles that are limited to specific windows

- **Therefore patch validation and verification after patching activities is necessary; mere deployment does not equal patched.**

    - Patch, validate, patch again if possible to prevent common vulnerabilities from being exploited – stopping attackers from getting a foothold using commodity malware

VERVE

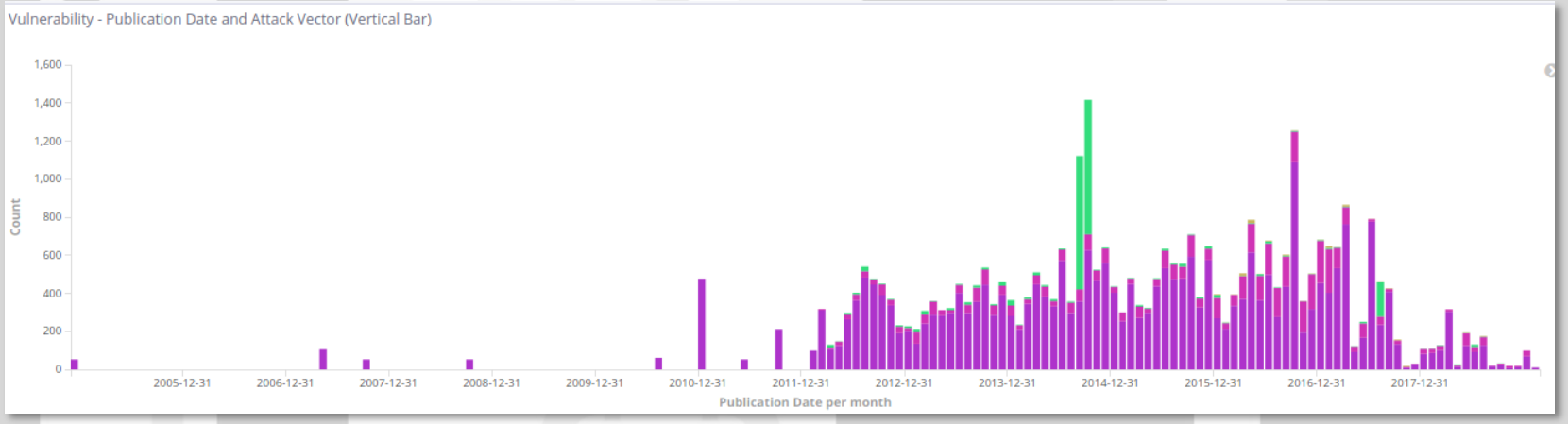
Blatant Security Vulnerabilities Exist Unknowingly

VERVE

- Despite policies and security controls being implemented in a number of facilities – WE FOUND:
  - Common security holes such as an unknown point to point WEP encrypted wireless network that connected the plant to a remote water pump station and exhibited direct bi-directional access back into the plant
  - Discrepancies in firewall rules and zones
  - Multi-NIC/dual-homed devices, and circumventing controls such as data diodes

- For whatever the reason, audits were not performed and as a result, comprehensive solutions have to look at:
  - Host information
  - Networking configurations
  - Application inventories
  - Projects and configurations

- **Using only passive monitoring of network traffic will only provide a fraction of the utility necessary to COUNTER and PREVENT threats EARLY ON**



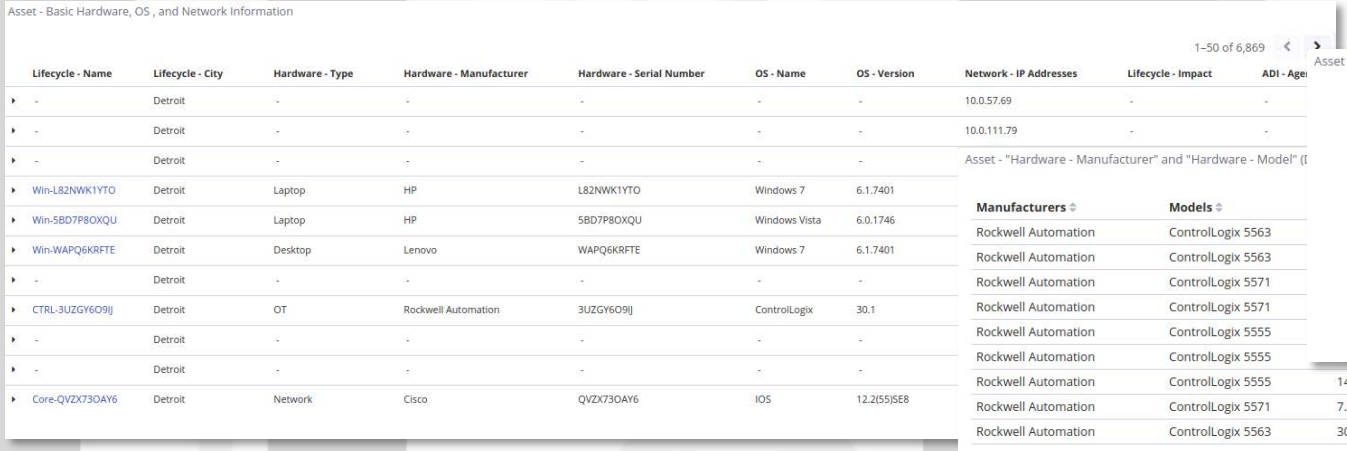
Volumes of data & Usable Reporting

- When you think of the technological scope and asset inventory of an organization:
  - **It's easy to forget the amount of data that is generated** for:
    - Storage and processing
    - And at the network layer
  - This is why careful planning, controls/heuristics, experience and modeling/verification is required to ensure no risks of disruption
  - **And the amount of effort used to validate/utilize any reported information**
- In short – platforms can receive volumes of data and user's are often initially overwhelmed with the alerts or data. This is where it is important to ensure that:
  - The value of accessible, and holistic data and why reporting makes it easies to visualize and understand
  - Automate reporting and trends
  - Minimize duplicates and ensure accuracy
  - Support asset owners with training during project and Operationalizing phases to reduce "shock" factors and fatigue
  - Ensure reliable and timely alerts for EVENTS that MATTER
- **And a good solution provides security controls, automation, and visibility reduces effort WITHOUT being just a check box**

VERVE

Asset Owner Actuality Accuracy

- Considering the scope of OT assets within an organization – there are often gaps for a variety of reasons:
  - Size and remoteness of assets
  - Changing technology environments (e.g., connectivity upgrades)
  - Acquisitions and mergers
  - Skill/technology gaps
  - Retiring of key resources
- In our experience – we have seen (for example):
  - **Comprehensive Asset Inventory from asset owners is usually incorrect. 1 plant owner was over 1200% off of their initial asset inventory.**
  - Asset owner has a misconfiguration or misunderstanding of own assets; DC controller is not primary and needed to be rebuilt!
  - "It worked yesterday" – but in reality, monitoring was neglected and the system was not working correctly for over a month before arrival!

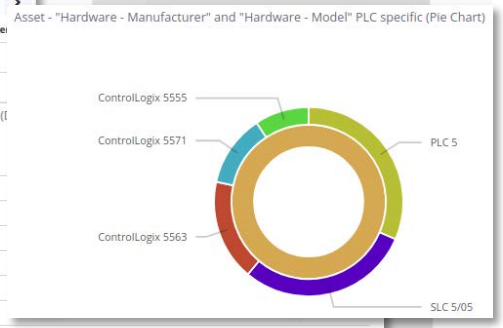

Asset - Basic Hardware, OS , and Network Information

1–50 of 6,869

Lifecycle - Name	Lifecycle - City	Hardware - Type	Hardware - Manufacturer	Hardware - Serial Number	OS - Name	OS - Version	Network - IP Addresses	Lifecycle - Impact	ADI - Age
-	Detroit	-	-	-	-	-	10.0.57.69	-	-
-	Detroit	-	-	-	-	-	10.0.111.79	-	-
-	Detroit	-	-	-	-	-			
Win-L82NWK1YTO	Detroit	Laptop	HP	L82NWK1YTO	Windows 7	6.1.7401			
Win-5BD7P8OXQU	Detroit	Laptop	HP	5BD7P8OXQU	Windows Vista	6.0.1746			
Win-WAPQ6KRFTE	Detroit	Desktop	Lenovo	WAPQ6KRFTE	Windows 7	6.1.7401			
-	Detroit	-	-	-	-	-			
CTRL-3UZGY6O9IJ	Detroit	OT	Rockwell Automation	3UZGY6O9IJ	ControlLogix	30.1			
-	Detroit	-	-	-	-	-			
-	Detroit	-	-	-	-	-			
Core-QVZX73OAY6	Detroit	Network	Cisco	QVZX73OAY6	IOS	12.2(55)SE8			

Asset - "Hardware - Manufacturer" and "Hardware - Model" ([

Manufacturers	Models		
Rockwell Automation	ControlLogix 5563		
Rockwell Automation	ControlLogix 5563		
Rockwell Automation	ControlLogix 5571		
Rockwell Automation	ControlLogix 5571		
Rockwell Automation	ControlLogix 5555		
Rockwell Automation	ControlLogix 5555		
Rockwell Automation	ControlLogix 5555	14	5
Rockwell Automation	ControlLogix 5571	7.2	4
Rockwell Automation	ControlLogix 5563	30.1	4



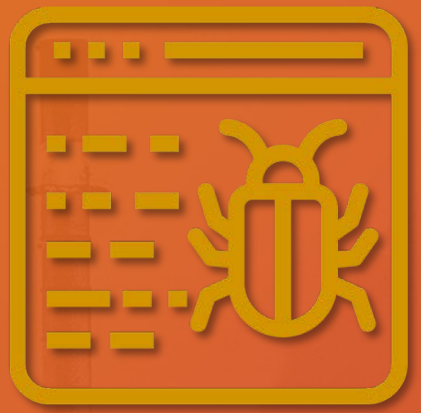
VERVE

Cyber Security Products are Not Drop & Forget

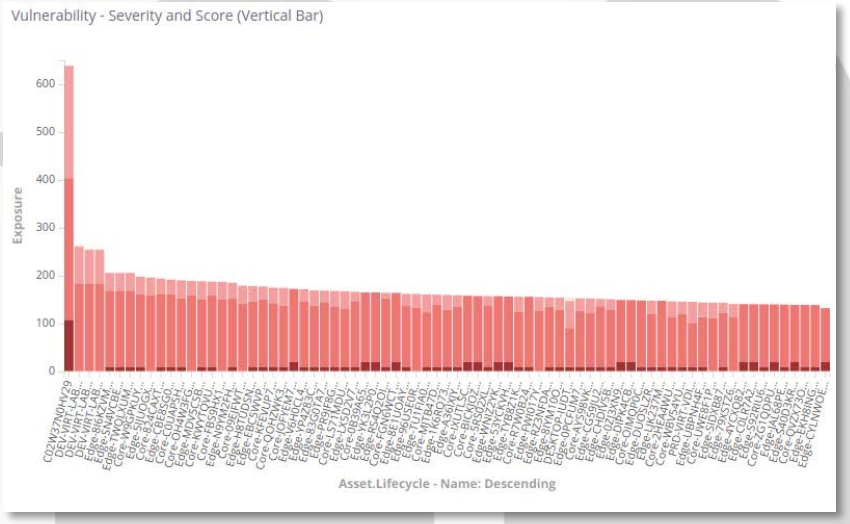
VERVE

- Unfortunately, the industry has a tendency to think that if we just buy this new solution or OT ICS system – all will be protected with a drop of a hat:
  - Not all installations are the same
  - Generalized rollouts at the lower OT layers are not easy
  - Skills, budgets, time, and **SUPPORT** are required to help lift up asset owner teams such that they can control REAL threats to the organization
- **These solutions must also be managed too as part of a Vulnerability Management (VM) program:**
  - It must be seamless
  - It must be tested
  - It must be assured
  - It must not additional risk or facets to the attack surface
  - All are things that need to be considered in the client-vendor relationship from the 1st step & is frequently misunderstood.

Existing Malicious Software Infections

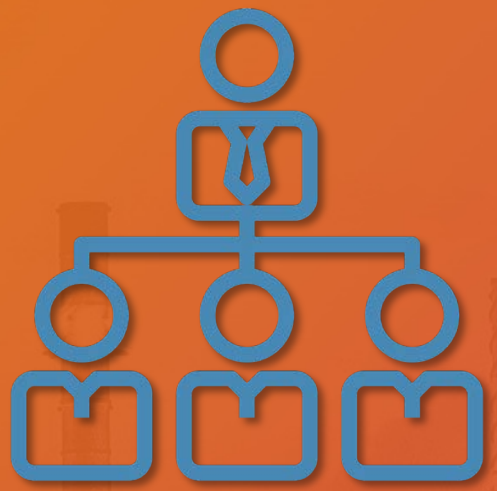


- In some facilities, given the legacy nature of some software and Operating systems – persistent malware continues to exist (for example):
  - Slammer worm
  - Conficker
  - Wrapped and mutated malware
- In these cases, managing endpoints, whitelisting and monitoring any applications/logs/alerts is key!
  - Where Windows XP (and other legacy OS are deployed)
  - Monitoring unsupported applications (e.g., office, or programming software)
  - Being able to enforce policies and gain visibility on Operator actions
- **"Its not doing anything and we won't risk downtime imaging systems"** – large oil producer's security team…



VERVE

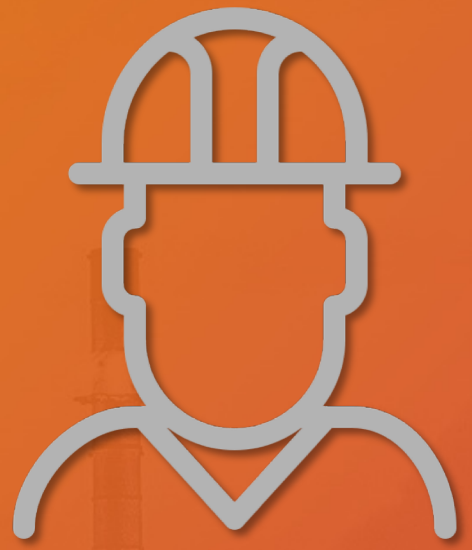
Organizations Need Help!



- Organization's while often having mature IT security and vulnerability management practices – do not necessarily:
  - Have the understanding of OT environment concerns
  - Have control of OT infrastructure (usually site/plant managed)
  - Have a respectable reputation that instills confidence with engineers
- Trust must be earned using:
  - Tools that make sense for IT and OT
  - Training and skill development (for both IT and OT)
  - Proof-of-concepts that demonstrate value organization-wide
  - Ongoing support and relationships
- Organizations – just might not know the threats they are facing and it is hard to separate fact from fiction
  - The threats in one organization are different to another
  - Vendor claims can be skewed due to media and sales pitches
- **And so – independent, or demonstrated thoughtfulness driven by trust, history and reputation are required**

VERVE

User/Operator Creativeness



- Most organization's have a set of acceptable use policies, firewalls and other controls… unfortunately:
  - Administrators, power users and Operators like to get creative!
  - Or are held back from doing their work (or want to ignore normal channels)
- So – software such as Teamviewer, and NMAP are often deployed ad-hoc on systems to "help" with daily activities. The problem?
  - **Ad-hoc applications are not usually removed**
  - **And remain exposing additional potential vulnerabilities**, which the organization then inherits
- Endpoint security helps enforce that fact and can remove them… again, reducing risk and improving enforcement

Questionable Software

Application Name	Version	Count
Advanced IP Scanner 2.5	2.5.3233	2
Advanced IP Scanner 2.5	2.5.3581	1
Advanced IP Scanner 2.5	2.5.3646	1
Angry IP Scanner	3.5.1	2
Angry IP Scanner	3.5.2	2
Nmap 7.70	7.70	3
TeamViewer 13	13.0.6447	1
TeamViewer 13	13.1.3629	1
TeamViewer 13	13.2.26558	1
Bonjour	3.0.0.10	1

VERVE

Questions?

VERVE

Ron Brash
Director of Cybersecurity Insights
rbrash@verveindustrial.com
(+1) 438-394-2868

Twitter: https://twitter.com/ron_brash
LinkedIn: https://ca.linkedin.com/in/ronbrash

VERVE

Credit and References:

Credit to images: various authors on the noun-project & under Creative Commons

VERVE