OT Security & Risk Metrics

Dale Peterson
Founder, S4 Events

We Know Very Little

- What can we say that is supported by data?
  - Ransomware on IT is the most common cyber incident cause of outages
  - Unsecured Internet accessible OT is being exploited by hackers & adversaries
  - A strong security perimeter between IT and OT has prevented many IT cyber incidents from spreading to OT
  - Removable media controls and endpoint detection have reduced walk-in malware from the most common OT cyber incident to number 2 or 3
  - Consequence reduction has direct and measurable impact on risk reduction

Most Everything Else Is An Unproven Assumption

Not Knowing Is Dangerous

- Misallocation of time and money
- Inability to perform effective risk management
- False sense of security

Even Worse … Unwarranted Certainty

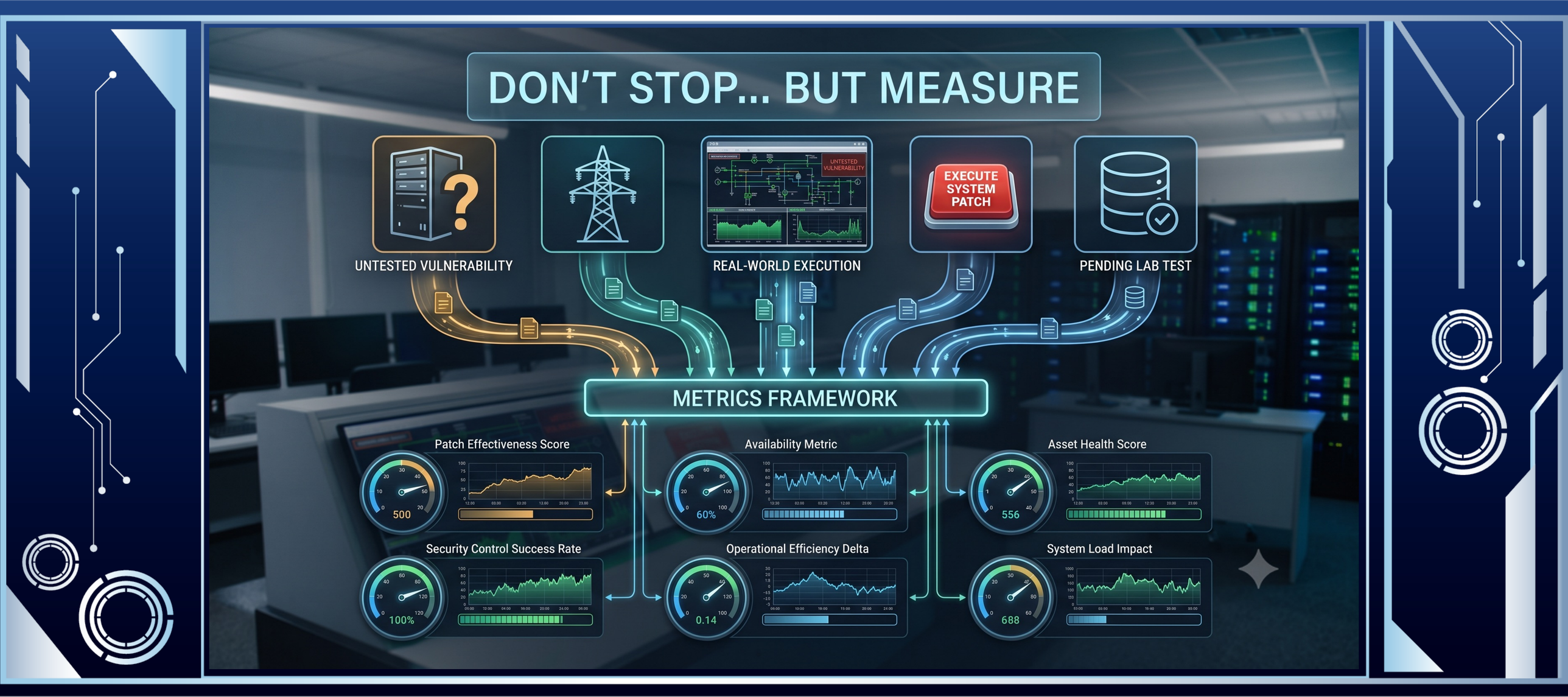
Example: Asset Inventory

- You can’t protect what you don’t know
  - Safes, locked rooms, firewalls, …
  - Why do countries still have power and water? Factories producing?
  - Why do we have air conditioning and power in this building?
- You can improve protection if you know what you are protecting?
  - How much better and at what cost?
- And what does ”know” mean?

Large & Growing Set Of Unproven ”Good Practice”

Example: Detection

- Detecting attacks is a good thing; you should have a detection capability
- What do you monitor?
  - Minimize false negatives and false positives
  - Resource efficiency
- Armis / Claroty / Dragos / Nozomi / …
  - How much of our OT environment should we monitor … and at what cost?
  - 80 / 20 rule? Why?


DON’T STOP... BUT MEASURE
UNTESTED VULNERABILITY
REAL-WORLD EXECUTION
EXECUTE SYSTEM PATCH
PENDING LAB TEST
METRICS FRAMEWORK
Patch Effectiveness Score
500
Availability Metric
60%
Asset Health Score
556
Security Control Success Rate
100%
Operational Efficiency Delta
0.14
System Load Impact
688

Two Metrics … For Every Project

- Implementation Effectiveness
- Risk Reduction

- Bonus: Tier 2 / Near Misses


FLAWED

Start With A Hypothesis

- What are we expecting the security control to do?
  - Prevent unauthorized access to OT Zone
  - Shorten attacker dwell time
  - Provide data for forensics
  - Prevent lateral movement in OT Zone

Implementation Effectiveness

- How are we expecting it to meet the hypothesis?
- What architecture / design / configuration / human activity is required to support the hypothesis?

JIM MILLER

RATING DEPLOYED OT FIREWALLS' EFFECTIVENESS

Before we start…

- Overall process
  - Rate a firewall from 0-100 (start with 0)
  - Rewarded for secure settings and restrictive rules
- Two sections
  - Configuration (15 points)
  - Rules / Policy (85 points)
- People / Process
  - Not comparing vendors

Implementation Effectiveness

- Alternate approaches
  - Purple teaming … test your security control (action)
  - Lab or third-party analysis
  - Your idea here
- Automate metric collection and display

Risk Reduction (the hard one)

- Did the action we took reduce OT cyber related risk?
- You need data
  - How often did the security control get activated?
  - How often did it work as hypothesized? And not?
  - What was the cost of the consequence prevented?
  - What was the actual cost of failure?

Begin With Your Hypothesis

A firewall at the IT / OT security perimeter
will block all traffic, including attacks,
that is not permitted

Identify Your Data

- Total Number Of Connection Attempts To & From OT
- Blocked Connection Attempts

Identify Your Data

- Total Number Of Connection Attempts
- Blocked Connection Attempts
  - On control system ports (502, 5900, 44818)
  - On control system ports and IP addresses in use
- Blocked Content
- Blocked Exfil Attempts
- Annual Cost (product and people)

Create Your Risk Reduction Metric

(Blocked connections to key resources on dangerous ports
+
(Exfil attempts x 1000))
x
(Consequence / difficulty)
=
Risk Reduction

Create Your Risk Reduction Metric

(Blocked connections to key resources on dangerous ports
+
(Exfil attempts x 1000))
x
(Consequence / difficulty)
=
Risk Reduction

LIFECYCLE COSTS


FLAWED

Begin With Your Hypothesis

Our OT Detection Platform (define)
will detect attacks and allow us to act
to prevent an outage in our Operations.

Identify Your Data

- Number of detected attacks by platform
  - Number of detected attacks likely to succeed
- Number of detected attacks that were stopped from causing an unacceptable impact
- Annual Cost

It Hasn’t Happened Yet

Likelihood & Consequence
Contribution To Risk Reduction

Two Metrics … For Every Project

- Implementation Effectiveness
- Risk Reduction

- Bonus: Tier 2 / Near Misses

The Impact Of OT Cyber Incidents Is Minimal

How Can We Determine Actual Threat?

	API 754
Tier 1	Loss of containment with injury or death
Tier 2	Loss of containment no injury or death
Tier 3	Safeguard is challenged
Tier 4	Process, inspection not happening properly

How Can We Determine Actual Threat?

	OT Security / Near Miss Version
Tier 1	High consequence cyber incident
Tier 2	Access available to cause Tier 1, but didn’t
Tier 3	OT asset compromised, Tier 1 not possible
Tier 4	Cyber maintenance / hygiene failure

You / We Need To Collect Near Miss Incident Data
When There Is Access
Could That Access Cause A Tier 1 Incident
With The Desire & Skill?

THANK YOU