Empowering Executives with Security Evidence

Mark Bagley
Vice President, Products
Verodin, a FireEye Company
linkedin.com/in/lmbagley
mark.bagley@verodin.com

About me…

- Better part of 2 decades in cybersecurity and data protection
- Started career in operational IT back in the 90s – networks and datacenters
  - Was often the guy “Security” got dropped on in those days
- A “builder” by core motivation and always in search of “why”
- Alumnus of some great organizations I helped build the offerings for:

CISCO Symantec EMC² splunk>

- Not here to sell you something – here to talk about why evidence is crucial

The Balancing Act

- **Build a strong, mature security program across our people, processes, and technology**

I. Where do we focus our attention?

II. Are the investments we make worth it?

III. Do we offload our risk to cyber insurance?

FUNDAMENTAL CHALLENGE

Assumption Based

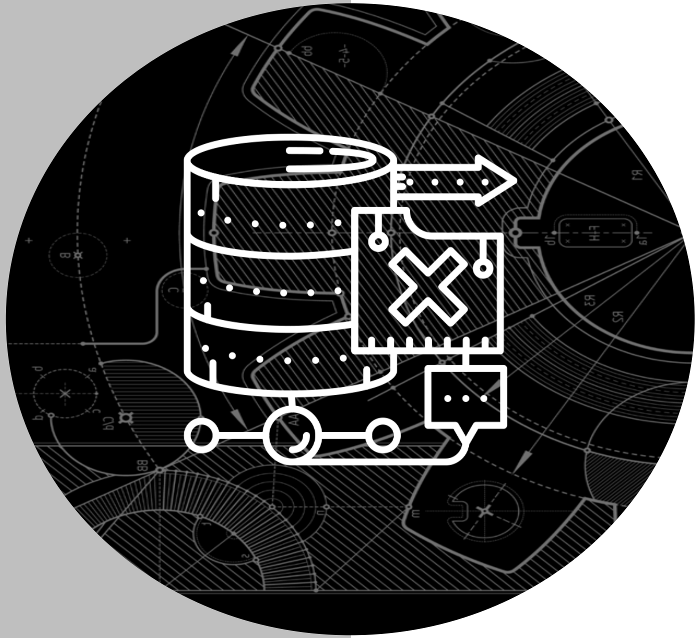
WE ASSUME:
Technologies work as vendors claim

WE ASSUME:
Products are deployed and configured correctly

WE ASSUME:
People are correctly handling events and processes

WE ASSUME:
Changes to the environment are properly understood, and communicated

WHAT IS SECURITY INSTRUMENTATION?

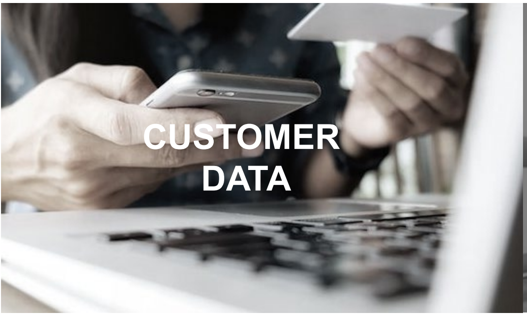


Security Instrumentation is a method that provides organizations with the evidence needed to measure, manage, improve, and communicate their cybersecurity effectiveness.

CYBERSECURITY'S GOAL: PROTECT CRITICAL ASSETS

Across all verticals, businesses rely on **business continuity and critical assets** to gain competitive advantage, drive revenue, protect shareholder value, and deliver services. As a result, many have made significant investments to protect these assets.

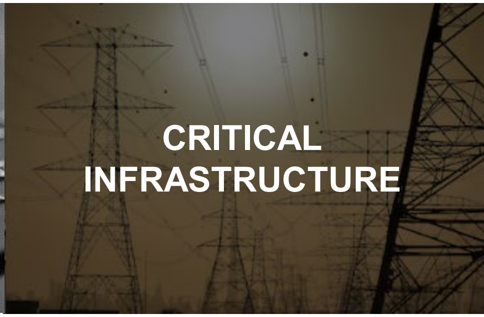
INTELLECTUAL PROPERTY



CUSTOMER DATA

PATIENT DATA

SERVICE / SALES DATA



CRITICAL INFRASTRUCTURE

Demand for EVIDENCE OF EFFECTIVENESS

SHIFTING SECURITY TO A MEASURABLE INVESTMENT

Executives rely on **evidence** to drive decision-making, optimize operations and ultimately improve their organizations over time. Security Instrumentation allows you to elevate cybersecurity to an **evidence-based, data-driven** business function.

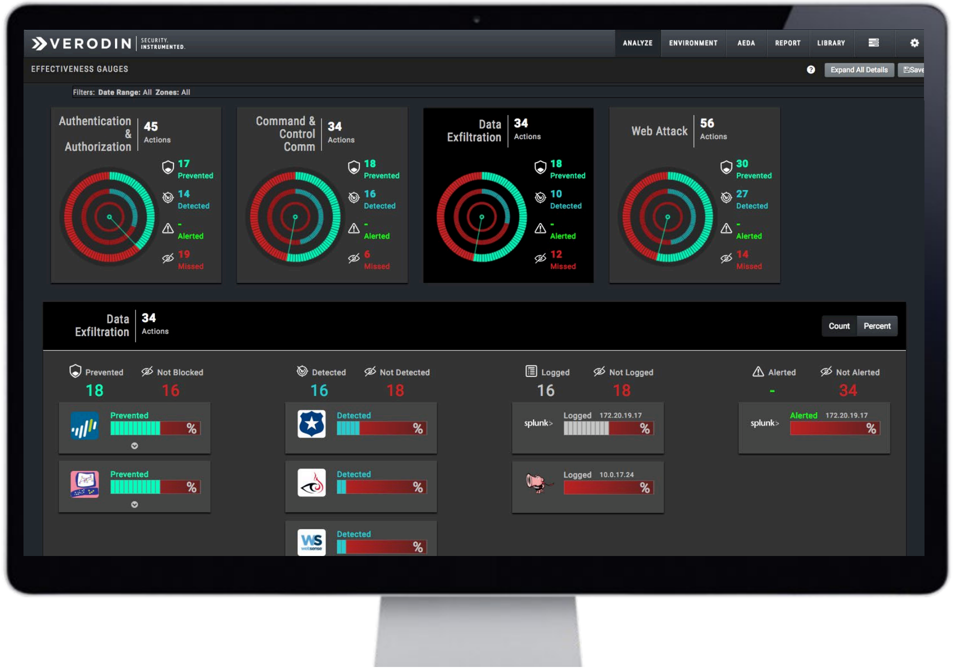
FINANCIAL PERFORMANCE

SHAREHOLDER RETURN

COST OF GOODS SOLD

PATIENT MORTALITY RATE

EQUIPMENT FAILURE RATE



EFFECTIVENESS GAUGES

Filters: Date Range: All Zones: All

Authentication & Authorization 45 Actions
17 Prevented
14 Detected
- Alerted
19 Missed

Command & Control Comm 34 Actions
18 Prevented
16 Detected
- Alerted
6 Missed

Data Exfiltration 34 Actions
18 Prevented
10 Detected
- Alerted
12 Missed

Web Attack 56 Actions
30 Prevented
27 Detected
- Alerted
14 Missed

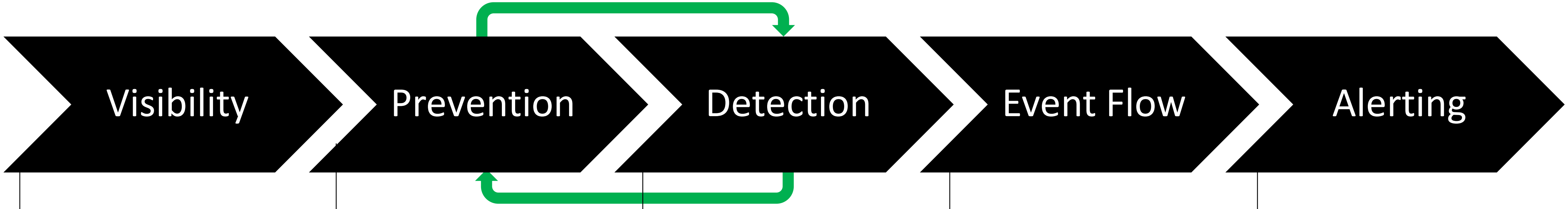
Data Exfiltration 34 Actions

Prevented	Not Blocked	Detected	Not Detected	Logged	Not Logged	Alerted	Not Alerted
18	16	16	18	16	18	-	34

Prevented %
Prevented %
Detected %
Detected %
Detected %
Logged 172.20.19.17 %
Logged 10.0.17.24 %
Alerted 172.20.19.17 %

CYBERSECURITY EFFECTIVENESS

EFFECTIVENESS VALIDATION PROCESS (EVP)



Visibility

- Are tools seeing traffic between zones as expected?
- Are comm direction and port/protocols allowed expected?
- Inline vs. tapped / spanned expected?

Prevention

- What tests are being blocked and by which technology?
- Which technologies are preventing the most?
- Are the company’s expectations of what will be blocked inline with the results?

Detection

- What detection events are generated?
- What is generating high fidelity events vs. noise or false positives?
- Where am I detecting tests with high fidelity and can quickly reconfigure to blocking? **Optimization**

Event Flow

- Are the detection events going from Sensor > Mgmt. Console > SIEM?
- Are events being parsed correctly?
- Is all the anticipated data present?
- Are the timestamps correct?

Alerting

- Are alerts firing?
- Where can context be increased to make the alert more actionable?
- Are high fidelity/priority detection events alerting?

VERODIN | SECURITY. INSTRUMENTED.

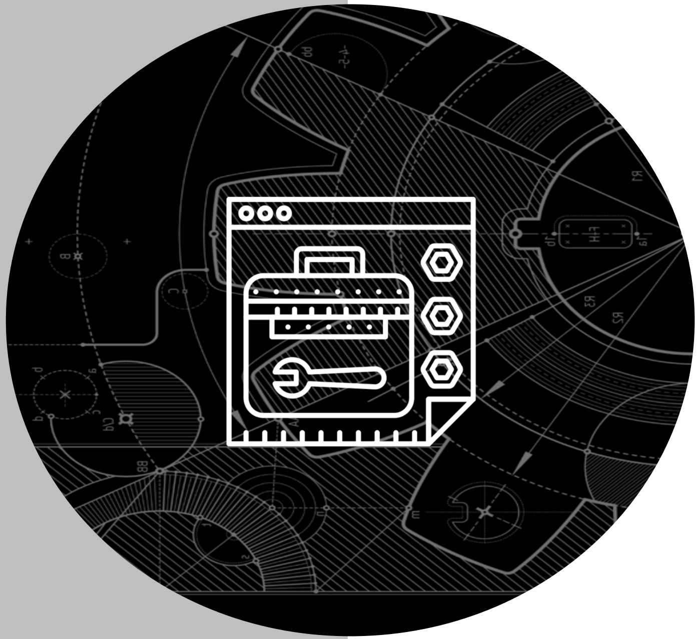
CONFIDENTIAL - NOT FOR DISTRIBUTION

CORE BUSINESS VALUE

Control Effectiveness / Configuration Assurance

- Are our controls working the way we expect them to?
- Are they properly configured?
- Are they effective against the adversary's behaviors?

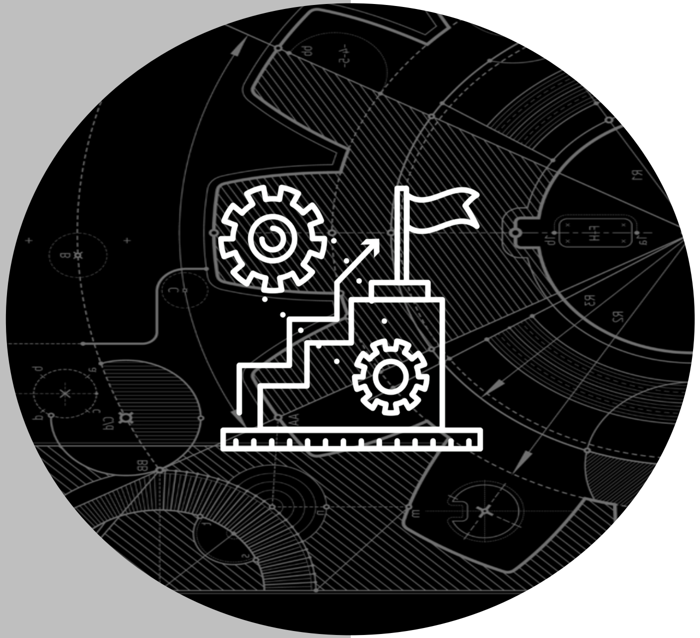
CORE BUSINESS VALUE



Security Tools
Optimization

- Are we able to increase the efficiency of the dollars already spent?
- Are we using the full value of our existing tools?
- Are we maximizing ROI?

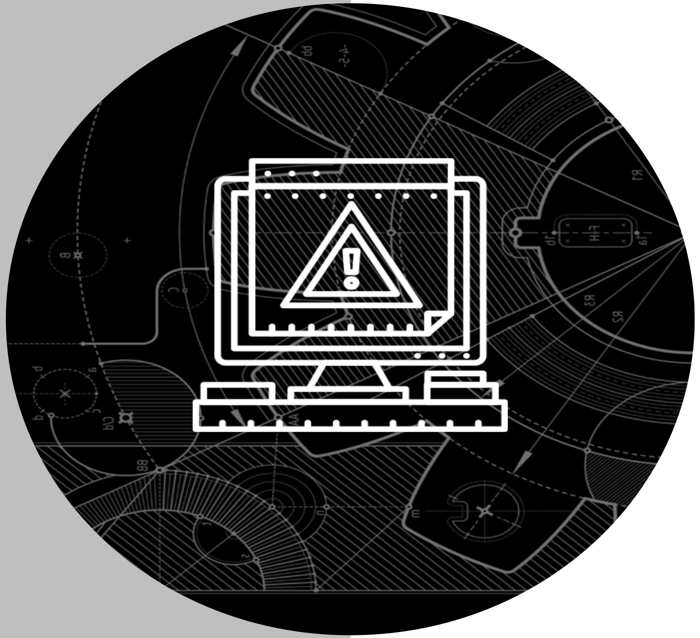
CORE BUSINESS VALUE

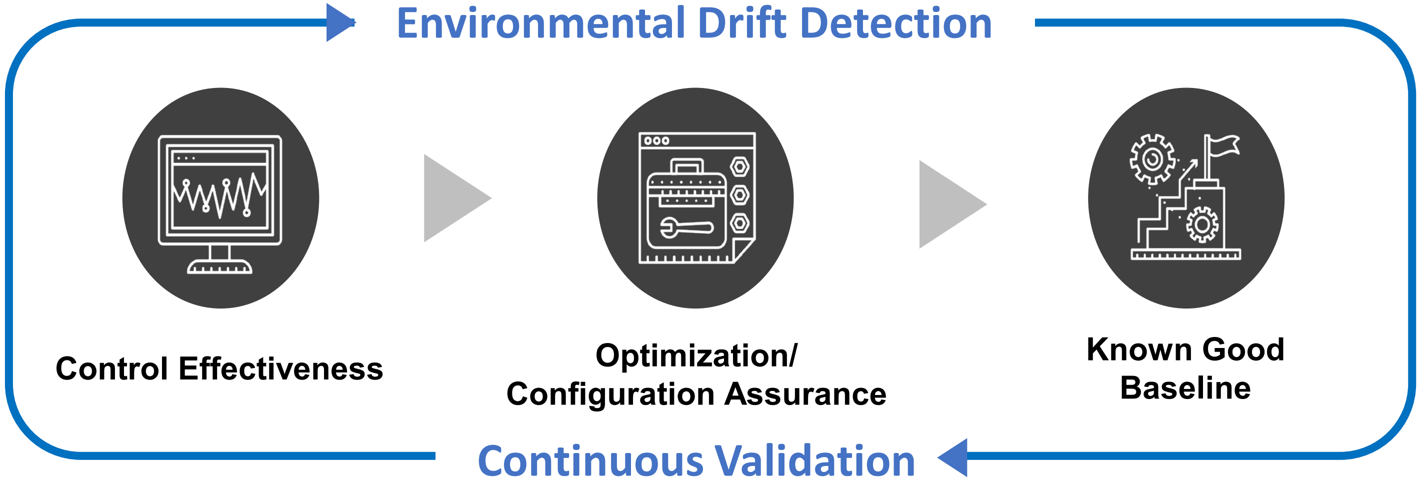


Known Good
Baseline

- Demonstrate improvement over time
- Notifications of when changes occur – both planned and unplanned – quantifying <u>environmental drift</u>

CORE BUSINESS VALUE





Environmental Drift Detection

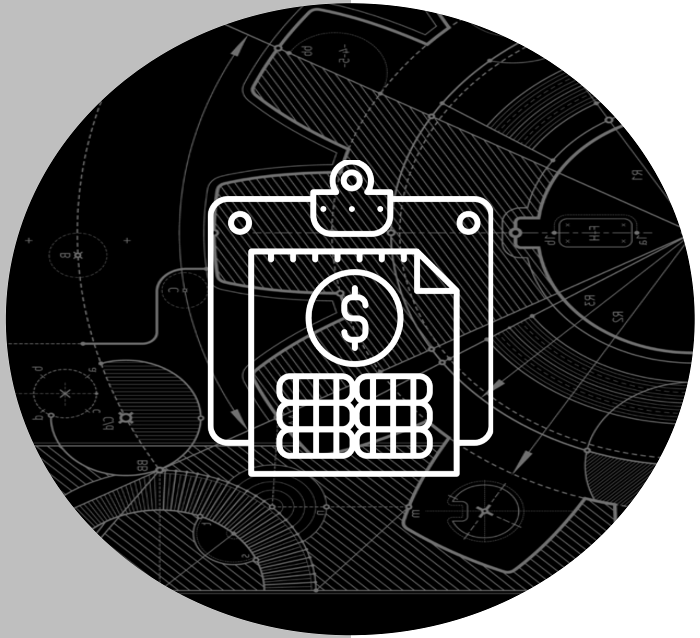
Control Effectiveness

Optimization/ Configuration Assurance

Known Good Baseline

Continuous Validation

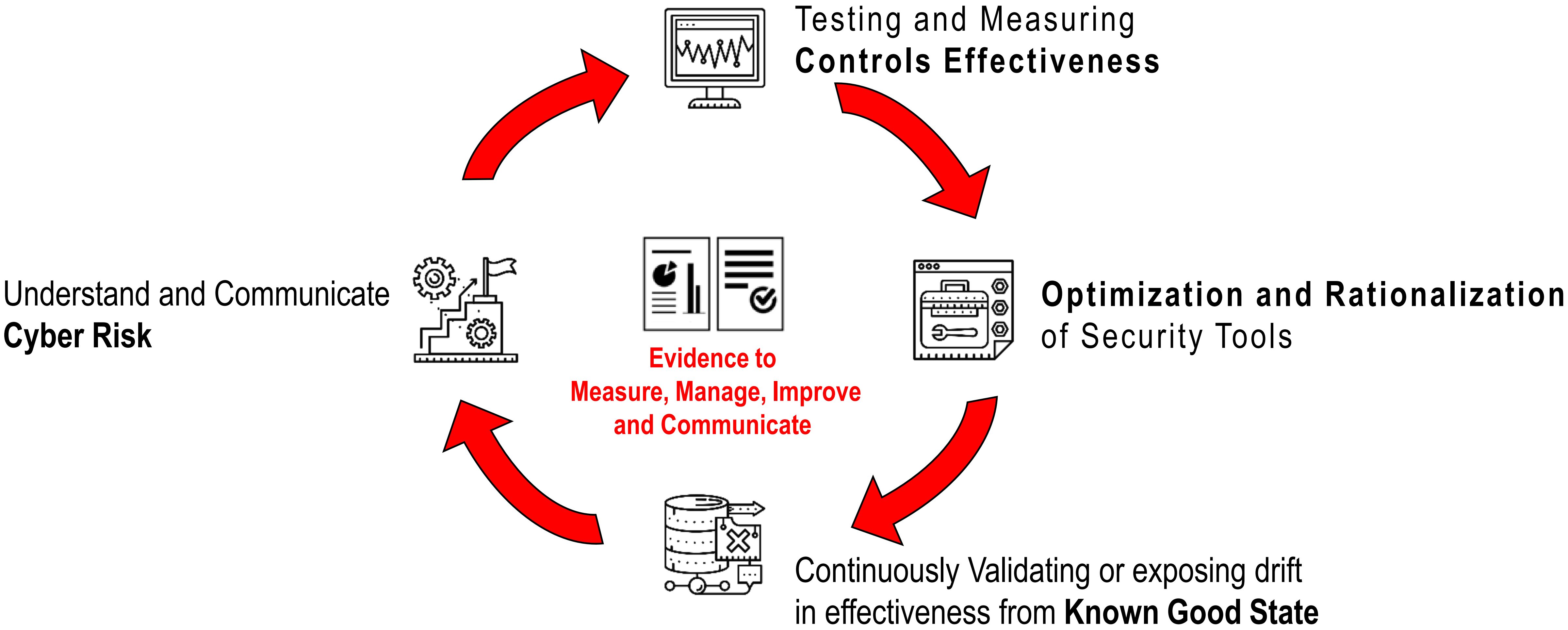
CORE BUSINESS VALUE



Security Tools Rationalization

- Where are overlaps and true gaps?
- Can tools be removed from the stack?
- Can we simplify the environment?

EVIDENCE CAN CONTINUOUSLY IMPROVE CYBERSECURITY



Testing and Measuring **Controls Effectiveness**

Optimization and Rationalization of Security Tools

Continuously Validating or exposing drift in effectiveness from **Known Good State**

Understand and Communicate **Cyber Risk**

Evidence to Measure, Manage, Improve and Communicate

Thank you!!

Questions?