5 Steps to Validation
Understanding Cybersecurity Effectiveness

Maj. Gen. Earl Matthews (Ret.)
VP, Strategy Officer
DISCLOSURE

Case studies and examples are drawn from our experiences and activities working for a variety of customers, and do not represent our work for any one customer or set of customers. In many cases, facts have been changed to obscure the identity of our customers and individuals associated with our customers.
OODA – The Need for Speed

Spin your loop faster than your adversary!

When you’re doing OODA ‘loops’ right, accuracy & speed improve together; they don’t trade off.
Challenges to Cyber Speed

Need to run to the fire of innovation – accelerate.

Info Technology will continue to transform
The adversary is constantly innovating
Regulation complexities and costs are rising
Scarcity of skills remains a top challenge
Amount of Data continues to grow exponentially
IoT / IoE exponentially connecting
Requirement: Demand to See the Evidence

Organizations exhaust an enormous amount of time, taxpayer money, and public resources to defend critical assets against well-funded nation-states, hacktivist groups, and careless employees.

However, even after all of this effort, cybersecurity programs still cannot produce the evidence required to determine if their people, policies, and controls are effective until after an incident occurs.
The Industry, government and public sector are dependent on digital assets to support critical infrastructures such as energy, transportation systems, communications, and financial services.

Any improper access, modification, or destruction of these assets can have a devastating impact on national security, economic well-being, and public health and safety.

Primary Objective: Protect Critical Assets
The Result of Cybersecurity Left Unchecked

- Excessive Tool Overlap
- Underutilized Controls
- Poor Change Management
- Heightened Risk of Data Loss
Establish KPIs for Measuring Cybersecurity Effectiveness

A holistic understanding of cybersecurity resilience can only be achieved with **key performance indicators** for measuring people, processes, and technology.

How well am I preventing exfil of PII data?
Without the ability to **quantify impact**, cybersecurity leaders are understandably **reluctant** to remove legacy products.

Controls are left **severely underutilized** due to weak out-of-the-box configurations and a lack of **resources** to tune, resulting in wasted money and unnecessary infrastructure complexity.
Managing the effectiveness of a multi-faceted cybersecurity program requires the perfect alignment of mission leaders, defense, offense, and threat intelligence.

Community research, industry-standard models, and customized test sequences are essential ingredients to challenge and verify the defenses safeguarding critical assets.
Government IT environments are dynamic and constantly shifting. Cybersecurity leaders are burdened with the responsibility of protecting the environment without the corresponding authority to control it.

To gain complete control, layered defenses must be continuously tested for unintentional configuration changes and errors that put mission-critical assets at risk.
Without the ability to make evidence-based decisions, cyber risk strategies are largely reliant on assumptions.

Risk models, questionnaires, and checklists cannot provide organizations with hard proof that the risk assumed is the risk taken.
Conclusion: Questions & Additional Resources

Related Resources:

- Video: The Case for Continuous Security Validation and Why it Matters to You
- Forbes Article: 2020 Will Be The Year Of Security Validation
- Learn More: About how Mandiant Security Validation (formerly Verodin) can help you validate security protocols and protect critical assets

Maj. Gen. Earl Matthews (Ret.)
VP, Strategy Officer
Email: earl.matthews@verodin.com
LinkedIn: https://www.linkedin.com/in/earlmatthews
## Cyber Top 10

<table>
<thead>
<tr>
<th></th>
<th>1. Cyber Hygiene</th>
<th></th>
<th>6. Workforce</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Revector Focus (Hunting vs. Blocking)</td>
<td></td>
<td>7. Strategic Plan</td>
</tr>
<tr>
<td></td>
<td>3. Application Security</td>
<td></td>
<td>8. Culture</td>
</tr>
<tr>
<td></td>
<td>4. Data Security</td>
<td></td>
<td>9. Internet of Things (Threats)</td>
</tr>
<tr>
<td></td>
<td>5. IT Modernization</td>
<td></td>
<td>10. Risk Management</td>
</tr>
</tbody>
</table>