deepwatch

Security Operations Modernization

Five Pillars for Driving Differentiation

Agenda

1. Introduction
2. Meaningful Sources
3. Curated Content
4. Effective Prioritization
5. Platform and Function
6. Shifting Response “Left”

Customization in a Commoditized World

Introduction

Daily operations have become, and look to remain, one of the most complex functions in today’s competitively resourced and budget constrained cyber security space.

The SecOps space is served by a variety of providers and internal efforts, varying in approach (product vs. service), delivery models (common vs. bespoke), and effective capabilities (shared vs. custom).

With a focus on standardized, repeatable performance, how can organizations maximize their personal effectiveness and agility?

“Bring Me Solutions!” – The Basics

Identifying these common issues is easy. Understanding how organizations can deal with them is where gains are made.

Organizations must **identify** and **prioritize** needs before they start down the path of deciding to insource or outsource security operations.

Selecting a delivery and consumption model should be based upon **outcomes**. What do we need to achieve? How do we plan to consume the results?

Choose appropriate service model(s) from the selection of **technology-based**, **services-oriented,** or **hybrid solutions** to determine which best meets the organization’s needs.

Outsourcing is here to stay, and it is often the most cost effective solution. The **responsibility**, however, remains, and **RACIs** are critical from the start.

Meaningful Sources – Focusing on What We've Got

Equality
Not all data sources bring the same level of meaningful capabilities.

Validity
Consumption of available data is not something we can assume to be "easy."

Data sources matter, and with an ongoing focus on technology sprawl, the ability to identify, prioritize, and drive meaningful outcomes from the myriad origination points that we have available for use in security operations can be, at best, confusing, and, at worst, counterproductive.

Applicability
Even where data is available, our ability to manipulate, apply, and drive meaningful results from it is questionable.

Overlap
More is not always more, and noise is often just noise.

“Bring Me Solutions!” - Sources

Selecting appropriate data sources can be a confusing effort, especially when outcomes are often unknown.

Review the available use cases to help identify which log sources are most critical.

Sources should be **prioritized** to maximize outputs. The simple existence of a source does not make it a great candidate, although, as the service matures, this can change.

Sources often provide similar information. **Duplication** of data, while sometimes helpful at filling gaps, must be considered as a cost.

Standardized behaviors can often be **customized**, with an increase of upkeep costs being the most common requirement. These should be carefully considered.

Curated Content

Every detail that we can bring in is better, right? Doesn't it improve the fidelity of our analysis?

- The availability of content to be ingested is huge, and it grows every day.
- Consumption can drive cost, often without actually providing tangible benefit.
    - Transmission
    - Storage
    - Processing
- Overlapping content can increase overhead, slow processing, and devalue the most critical data.

Cost – How do you pay?

Effectiveness – Is it lightning or just thunder?

> **"You were so preoccupied with whether or not you could, you didn't stop to think if you should."**
>
> **Dr. Ian Malcolm, Jurassic Park**

“Bring Me Solutions!” - Content

With the incredible optionality available for ingested content, organizations must carefully select what they add into their solutions.

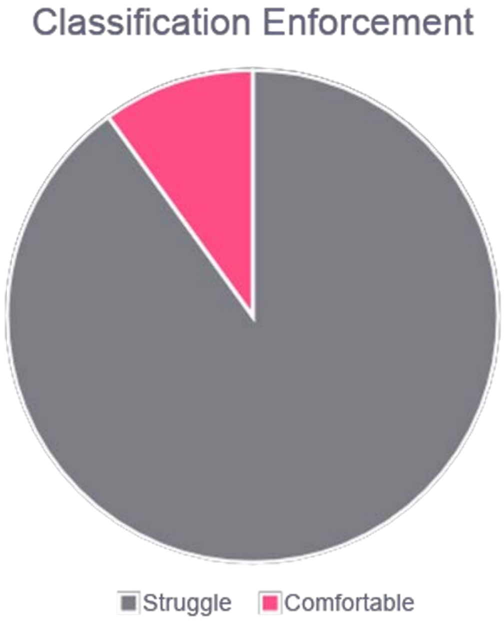
Organizations should understand the value of ingested data to avoid letting their consumption **grow** by orders of magnitude.

Speed of **processing** can be affected by the amount of data assessed. This consideration further drives the need to prioritize both the sources and content of data streams.

Data integration brings cost, often driven by **storage** and **transmission** fees. Budgets matter, and these costs must be balanced against the value that the data brings.

Content that may address the same activity from differing viewpoints must be **normalized** to prevent duplication of alerting and slow investigation and remediation.

Effective Prioritization – What Matters Most?



“The State of Data Security in 2022”, BigID

- Identification remains difficult / contentious
- Fluid attack surface drives constant modifications
- Application of actionable results requires increasingly large teams

"Bring Me Solutions!" - Prioritization

"All animals are equal, but some animals are more equal than others."

George Orwell, Animal Farm

Asset criticality is an incredibly difficult thing to accomplish once, let alone continuously. **Classification methodologies**, simple or complex, must be selected and applied.

Criticality should be considered based upon **content**, business **value**, available **attack/vulnerability surface**, and **exposure**.

Organizations must agree upon common **processes**, **nomenclatures**, and agreed upon **ownership** is critical to defining asset prioritization.

Data sources, content, and applied use cases should be **applied** to the most critical assets first, last, and always.

Platform and Function – Our Weapons of War

Technology - The components used to ingest, enrich, analyze, and communicate concerns.

- What is the **purpose** of the SecOps function?
- What identified **functionality** outputs are expected from the chosen platform?
- How is the platform expected to support up and down stream **integration**?
- How do we want to **budget** for the technical outcomes provided?

Staffing – The human element needed to implement, maintain, operate, and respond to alerts.

- Can the organization afford to **recruit** and **retain** resources?
- Are all needed **roles** available to provide well-rounded results?
- Are staff members provided effective **training** and **support**?
- Does the SecOps team have sufficient **environmental familiarity** to provide rapid response?

“Bring Me Solutions!” - Platform

Evaluating, implementing, and maturing the overall platform components used to support an organization’s SecOps capability is the keystone of execution. The technology and staffing aspects must be carefully selected to support the identified needs.

Security technologies vary widely in capabilities. These components must be carefully **selected** to address needs…or those needs must be **modified** to address the available solutions.

Criticality should be considered based upon **content**, business **value**, available **attack/vulnerability surface**, and **exposure**.

Technologies should be chosen based upon their ability to easily **integrate/consume** source data and provide outcomes that can be used to increase **collaborative** analysis.

Regardless of the selected technologies, attending personnel must be knowledgeable, well trained, functionally integrated, and enabled. Organizations must understand and commit to supporting these needs.

Shifting Response “Left”

“Fewer incidents and human interactions are the goal.”

More incidents lead to **fewer** failures over time. SecOps needs to drive meaningful investigation while providing, where appropriate, immediate mitigation.

”We are overwhelmed by alerts and cannot keep up.”

The ability to differentiate YES from MAYBE is critical. Systematic, correlated improvements in the true **positive event rates** must be a constant priority.

“Every day is Groundhog Day around here.”

“Good” yesterday often leads to “behind” today unless the organization adopts a mindset of relentless, **continuous improvement**. Integrating SecOps into the overall security programmatic approach as a thought leader AND a response arm is a simple necessity.

"Bring Me Solutions!" - Speed

SecOps functions cross the spectrum from detection to alerting, from alerting to response, and from response to remediation. Striving for continuous improvement, the goal is to consistently shorten the time of exposure and prevent recurrence of exposure.

Detect = Prevent. One is, honestly, just as important as the other. Organizations must spend equivalent time performing root cause analysis for each to round out their blue team capabilities.

SecOps is no longer just an execution arm. It must be used to **enable**, **drive**, and **validate** security program activities – **tactically** and **strategically**.

Alert fatigue is very real. Baseline data is insufficient and must be enriched with alternative sources and actionable analysis. Know what matters.

There can never be a "good enough." **Knowledge sharing**, **training**, and constant benefit **analysis** are required to retain parity status. **Pressure testing** is more of a requirement to escape guesswork than ever.

deepwatch

Chris Gray
AVP, Security Strategy
chris.gray@deepwatch.com

Thank you

www.deepwatch.com

Call to Action!

Set Goals

Understand what you need. Then act.

Delivery Model

Choose your delivery model based on where you want to excel. ($$$)

Prioritize

Plan to win. Don't fight to lose.

Call to Action!

Select Value

Just because you have something does not mean it is always useful.

Seek Outcomes, Not Features

Choose sources that achieve something more than just noise.

The 80/20 Rule

Implement solutions that drive massive change. After that? Iterate.

Call to Action!

Blinded by the Noise

Sometimes, enough is far too much.

Duplication is the Enemy (Sometimes)

Multiple versions may not add anything of value.

Limits Exist

People, process, money, time. We never have enough.

Call to Action!

Framework

Choose a classification process that fits the organization and its needs.

Crown Jewels

The most effort must be spent to protect what matters the most.

We’re Already Behind

The enemies don’t give up. Improve daily.

Selection

Choose a solution that addresses your fundamental needs. Beauty fades.

People Make You Money

Treat your team's skills like they make you money. They really do.

Integrate Synergistically

Solution your capability (P/P/T) with integration in mind.

Call to Action!

Move Left

Detection must drive quicker response.

Individually Ignorant

None of us are as smart as all of us.

Lifecycle Analysis

Integrate the overall program. Each area should drive greater success.

Call to Action!