Q4 2018

Cyber Force Multipliers

SCIS SECURITY

E Enhance security operations

H Hybrid Use Case Content

A AI Enabled Technologies

Force Multipliers

TRUE SECURITY IS A TALL ORDER FOR ANYONE.

Before you select or evaluate yet another "MSSP" consider this:

- What's their primary function and revenue generation? – Many IT and Consulting firms claim security consultation and services but often make most of their revenue off resells and deployments.
- Can they explain how security has ROI beyond cyber programs? – Often, security teams are seen "at odds" with other IT groups and departments as restrictions vs. enablers.
- Can they help you prioritize your risks? –Many MSSP's want to sell a service or product only and seal the deal. An MSSP is not always the right fit for the need.
- What is their customer transparency and visibility? – Often, customers are left in the dark and rely on the "magic" of a solution or service to catch all threats. If the vendor can't show you what is happening, what are they actually analyzing?

Enhancing Sec Ops

WHAT IS IN YOUR STACK AND WHAT CAN BE AUGMENTED?

With the growing threats in the market to all verticals, companies large and small are turning to service providers to act as their force multipliers. The CXO needs to carefully evaluate what existing technologies can be leveraged, maintained, and determine tools efficiency. If you can't measure it, it's not worth keeping.

So how do you measure "security" from an MSSP? Security is about risk reduction and threat action prevention. So the KPI is damage control and loss mitigation. Think about your costs associated with what was "missed" from your last security related incident which covers ANY form of availability, integrity, or confidentiality.

Enhancing Sec Ops [2]

PRODUCT OR SERVICE (CAPEX VS. OPEX)

When evaluating if you need a specific product to add to your technology stack vs. a service, consider the following:

- Do you have the current head count and resources to operate, maintain, and tune what you'll purchase?

- Do you have to spend specific funds in certain "pools" each FY?

- Do the prices change beyond inflation for your product or solution YoYr?

- What are the "hidden" hurdles when going with a product or technology including: learning curve, scaling, integration with other new technologies, and end user acceptance?

If you're having doubts about any of the above questions. You may want to consider some form of staff augmentation or service enhancement. Chances are your budget won't get increased in exponential fashion YoY and the more you add to your program, the more resources are needed to keep it running smoothly.

So what is a CXO to do if purchasing technologies or tools aren't a viable option due to needs or budget? Consider a long-term service augmentation with a long-term end goal. Figure out your highest threat surface and risk for your enterprise and what existing tools "work" and what could use a boost.

Use intelligence reports such as the Verizon Data Breach Reports each year to help ascertain insights for your vertical. Consider how a managed service or staff augmentation offering could have helped. In the 2018 report, Hacking and Malware related actions took the majority of breaches reported.

As the cyber defense industry matures, SCIS Security has seen the evolution of technology; however the sheer amount of data generated from that mature technology is overwhelming. Additionally, most security operations programs only deal with just detection and simple response. More technical expertise, visibility, and coverage is needed including active response and forensics.

Enable Other Teams with Hybrid Use Cases

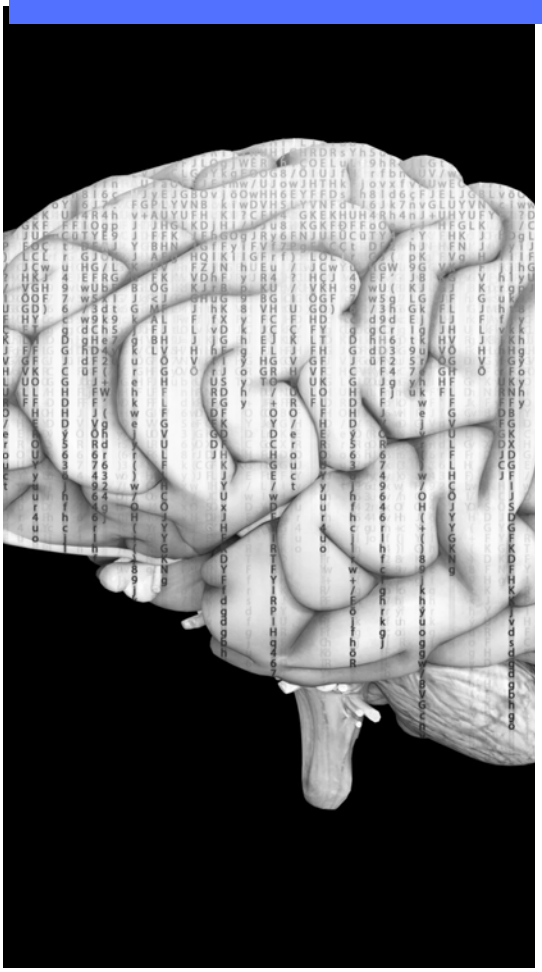
01 Focus on technologies or services that simplify, automate, and visualize data events

02 Ensure that interoperability is beyond the Security team such as IT infrastructure tech stacks

03 Tie output of actions from tools or services into sec ops KPI's

Help enable other teams, such as IT, to perform better as CXO's often see IT and Cyber Security as "cost centers." Can a SIEM, Network Tap, Sensor, or Log help make proactive system health alerts and active response actions?

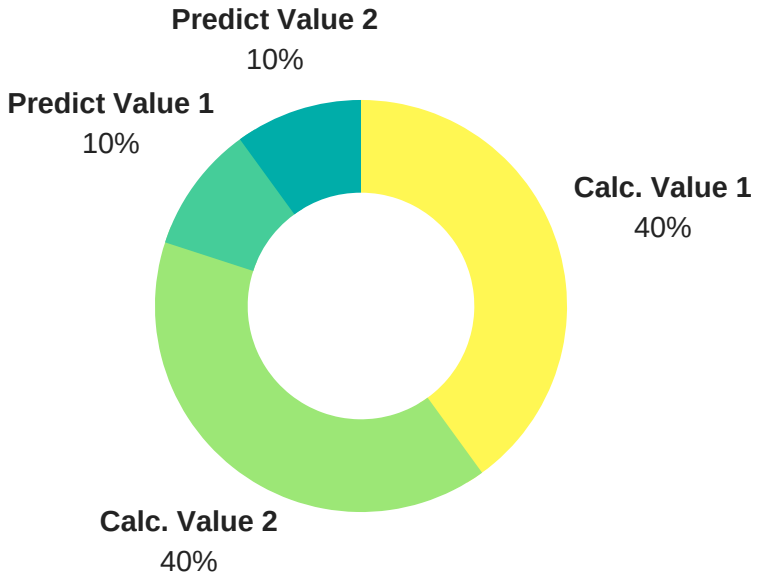
Go in with a game plan and determine if a joint purchase makes sense to make the most ROI from a long-term service or solution commitment.



A.I. Considerations

- Progression – Many solutions for cyber are mainly advanced statistics using different functions. Most of them are predicted only on calculated values such as when linear regression is used.
- Focuses on what signatures/rules leave behind – Many AI enabled solutions don't rely on AI only. Signatures are still used and AI is currently best used for anomalous event detection.
- Garbage In, Garbage Out –Anything AI relies on the quality of data models. Lots of data. If you don't have enough data or good quality data; AI is difficult to help.
- Don't ignore AI – The technology is here and is already used by eDiscovery solutions for document relevance. Analysts can benefit from outlier detection.

SCIS SECURITY MSSP OFFERINGS AUGMENT SIGNATURES AND CORRELATION RULES WITH AI.



SCIS MSSP Force Multipliers

01 Up to a 24x7x365 NSOC Offering with Active Response and U.S. Certified Analysts

02 Endpoint Managed Services with AV and EDR Capabilities

03 Custom dashboards and Portals that provide customer insight and raw event access

It's important that every CXO know what to look for when evaluating suitable MSSP and solutions. We hope this short paper helps to clarify some of the questions when attempting to leverage new services or technology stacks as cyber force multipliers.

SCIS Security helps to provide advanced offerings with high value services to SMB's and Enterprises. Contact us for more details at www.scissecurity.com

- Over 30+ Years of Combined Cyber Security Experience
- Veteran and Prior Service Member Owned
- Solutions and Services That Scale With Your Business
- U.S. based, trained, and certified L1-L3 Engineers and Analysts
- Full Stack Security ONLY Group (Focused on Cyber, Surveillance, and Investigations)
- Best of breed tools with full visibility capabilities for modern threats.
- Experience with HIPAA/PCI-DSS/SOX