ASMGi ONEteam

ARCTIC WOLF

MDR/MSOC

The Foundation of Your Security Arsenal

November 19, 2020

MDR/MSOC *plus* - The Foundation of Your Security Arsenal

Tim Smoot
Senior Presales Engineer
Arctic Wolf

Steve Roesing
President, CEO
ASMGi

ARCTIC WOLF

ASMGi
ONEteam

Agenda

- *Why are Cyber Security Operations so critical?*
- *What does the current landscape look like?*
- *What are the components of a Total Solution?*
- *How is MDR/MSOC the foundation of my Cybersecurity arsenal?*
- *What is* ONEteam MDR/MSOC *plus and how does it protect me?*
- *Key Takeaways*
- *Q & A*

CYBER SECURITY SOLUTIONS

Why are Cyber Security Operations critical?

Why are Cyber Security Operations critical?

August 2020

1TB Stolen, Including Cloud-Based Assets Were Accessed In Jack Daniels Breach

Hackers had access for over a month before detection and intervention.

2017

Equifax Announces Cybersecurity Incident Involving Consumer Information

Flaw was known by vulnerability management tools, but the patch was never installed.

2019

Hackers Gain Access to 100 Million Capital One Credit Card Applications and Accounts

Misconfiguration in cloud service went unnoticed despite availability of monitoring products.

June 2020

Control Systems Targeted Shutting Down Production In Honda Breach

Attack focused on control systems, in the production line

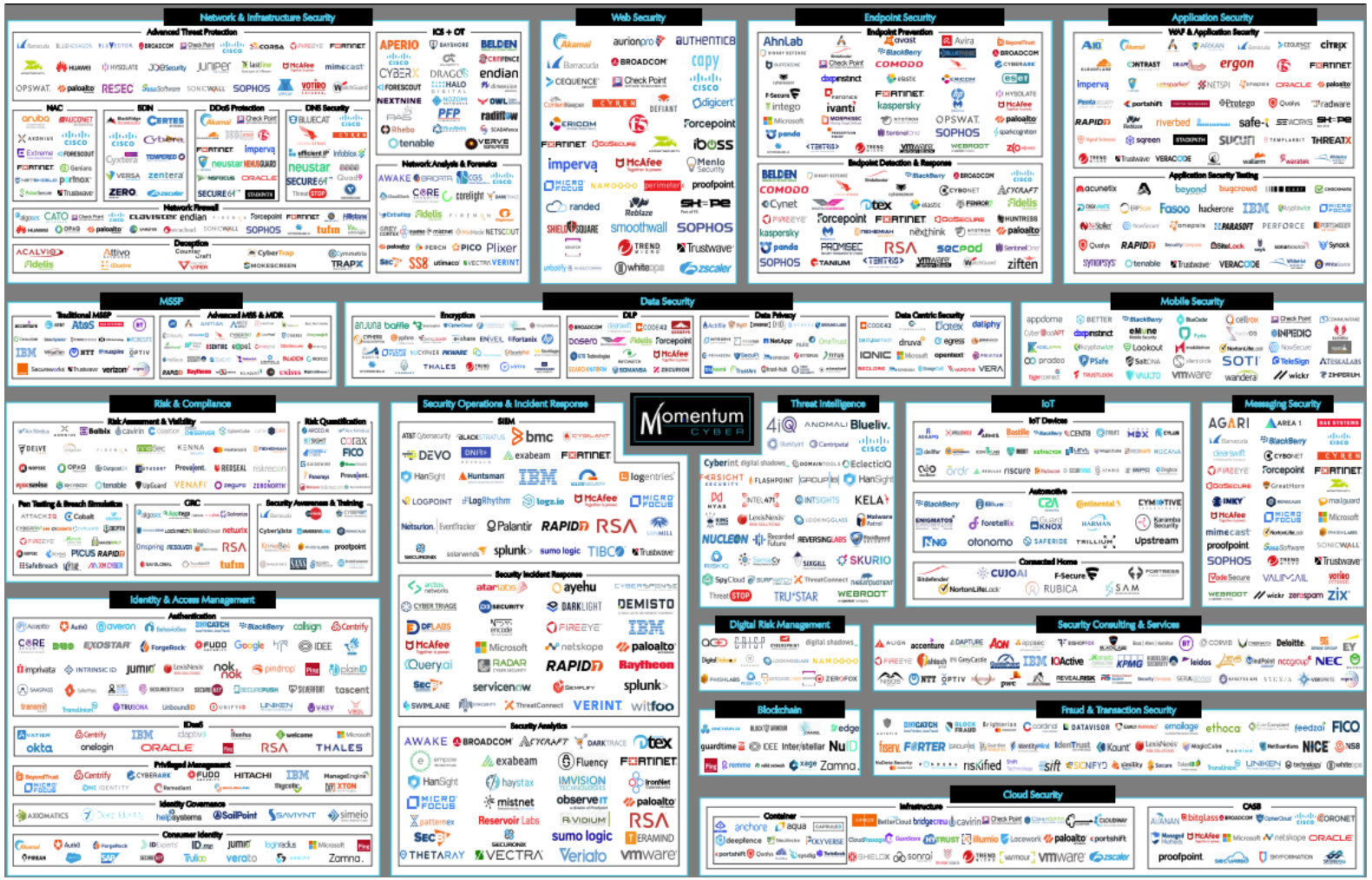
CYBER SECURITY SOLUTIONS

What problem are you trying to solve?

Lots to choose from …

ASMGi ONEteam

ARCTIC WOLF



3,000+
Vendors

18
Categories

$120B+
Total Spend

Lots to choose from …

The Council on Cyber Security Annual 2014 Report coins the term “Fog of More” to describe the “Overload of defensive support…more options, more tools, more knowledge, more advice, and more requirements, but **not always more security**.”

Lots to choose from …

3,000

Vendors

$120B

Total Spend

3,400

Reported Breaches

CYBERSECURITY DOESN'T HAVE AN EFFECTIVENESS PROBLEM. CYBERSECURITY HAS AN AWARENESS, OPTIONS, OR BUDGETARY PROBLEM.

Addressing the EFFECTIVENESS Problem…

Step One: Leverage all logs as a unified actionable dataset ”information is power”

Step Two: Recognize that nefarious actors don’t punch the clock

Step Three: Cybersecurity is not Network Operations, Use the right tool for the job

Step Four: Proper security posture isn’t a destination, it is a journey

Step Five: Effective security posture enables the business, extends its reach, helps it evolve

What are the basic cybersecurity needs?

Without listing acronyms, tool/software types, or features/functionality, let's break it down to simple pieces:

First focus should be on a **Proactive** approach to security posture – With a proactive approach, organizations can eliminate known vulnerabilities, harden threat surfaces, and implement appropriate configuration standards

Next would be a **Reactive** focus for our security posture – A reactive focus keeps organizations safe when those unknown, new, or evolved threats make it through our proactive tools and configurations

Finally, is the implementation of the **Active** component of security posture – The active portion of security posture is arguably the most important. There are multiple reasons for this, but the biggest reason is that the tools/software/configurations/etc. that make up the proactive and reactive elements of a security posture must be monitored, researched, and when necessary, issues remediated.

Matching the focus elements with the tools…

To address the **Proactive** element of security posture common tools would be: Risk or Managed Risk, and IPS

Addressing the **Reactive** elements of security posture would include tools like: Managed Detection and Response, and IDS

The **Active** component of security posture includes not only tools like a SIEM, and MFA, the most critical part is in fact the people and the process! There is no shortcut with respect to the human element, and without the active component of security posture, other investments typically are not effectively leveraged which makes further investments in security very difficult.

Cyber Security – ONEteam Principles

The Old Way: Point-Solution Mindset

- Reactive
- Focus on Individual Controls
- Fragmented and inefficient
- Spend a lot and not necessarily improve security

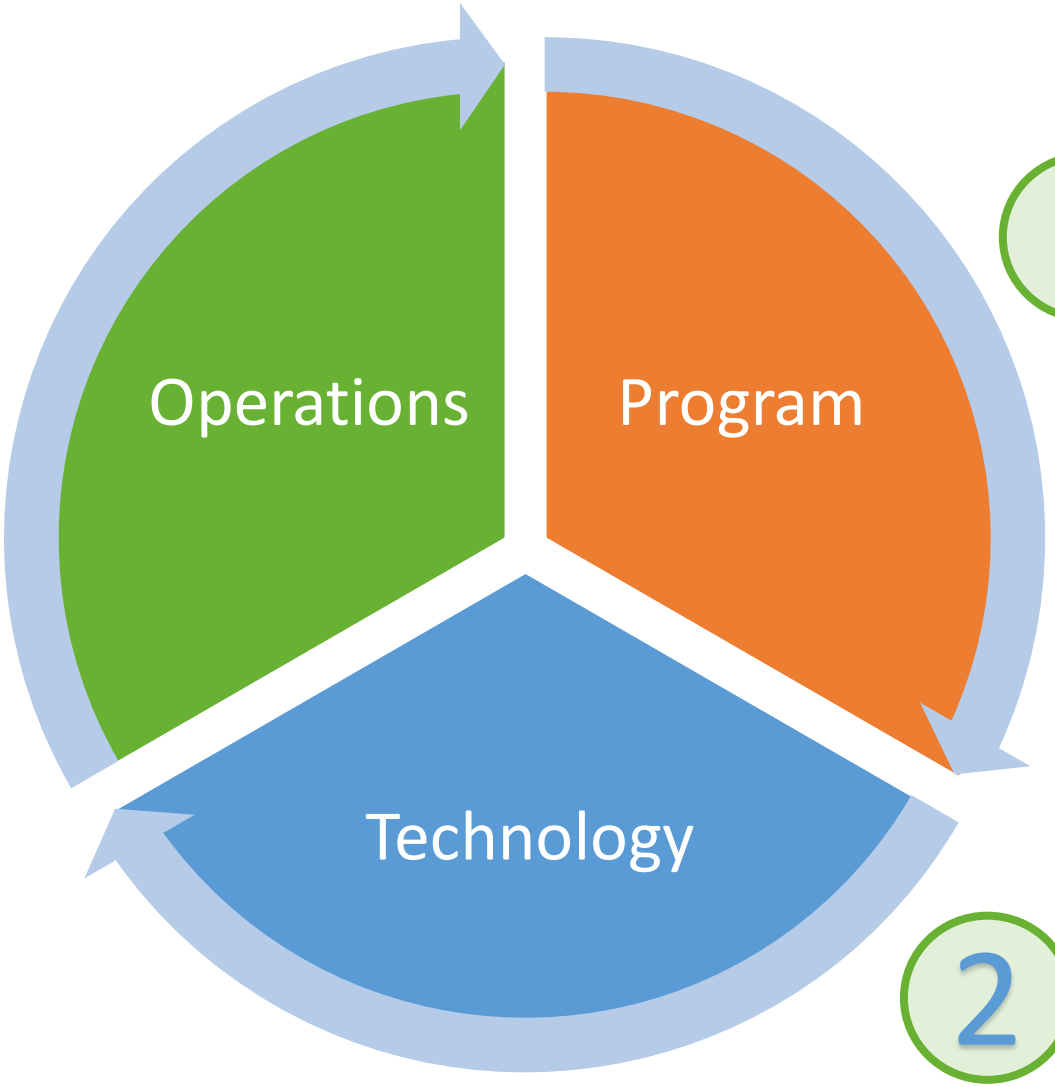
The New Way: Holistic Security Mindset

- Proactive
- Focus on Total Solutions
- Gap-Based & Risk-Based
- Spend less and improve security more

ONEteam Principles – The 3 Pillars

3 Operations

- Operations must meet the requirements and objectives outlined in the Program and align with the Technology. For MDR/MSOC, it must include:
  - MDR / MSOC
  - Incident Response
  - Vulnerability Mgmt
  - Remediation



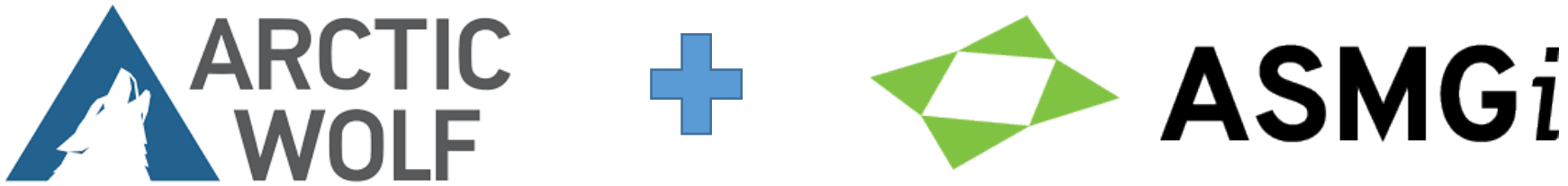
1 Program

- Corporate Objectives
- SLOs / SLAs
- Strategic Goals (tech and operations must meet this requirements)

2 Technology Stack

- Tech Stack must meet strategic requirements and objectives

What is ONEteam MDR/MSOC *plus*?



= ONEteam MDR/MSOC *plus*

TOTAL SOLUTION:

ONEteam MDR/MSOC *plus*

- Security Operations Centers (SOCs)
- Managed Detect and Response
- Managed Risk Services
- Managed Cloud Monitoring
- Cyber Incident Response / Forensics
- Vulnerability Management and Remediation

3.5 Incident Handling Checklist

The checklist in Table 3-5 provides the major steps to be performed in the handling of an incident. Note that the actual steps performed may vary based on the type of incident and the nature of individual incidents. For example, if the handler knows exactly what has happened based on analysis of indicators (Step 1.1), there may be no need to perform Steps 1.2 or 1.3 to further research the activity. The checklist provides guidelines to handlers on the major steps that should be performed; it does not dictate the exact sequence of steps that should always be followed.

Table 3-5. Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Key

- Arctic Wolf + ASMGi
- ASMGi

ONEteam MDR/MSOC *plus* defined …

- **Arctic Wolf** provides the "base" technology and is ***complimented*** by ASMGi Programs and Operations (e.g. Services) for:
  - Security Operations Centers (SOCs)
  - Managed Detect and Response (MDR)
  - Managed Risk Services
  - Managed Cloud Monitoring
- **ASMGi** provides complimentary services to the "base" technology and "as-a-Service" for:
  - Cyber Incident Response / Forensics
  - Vulnerability Management and Remediation

Services Overview

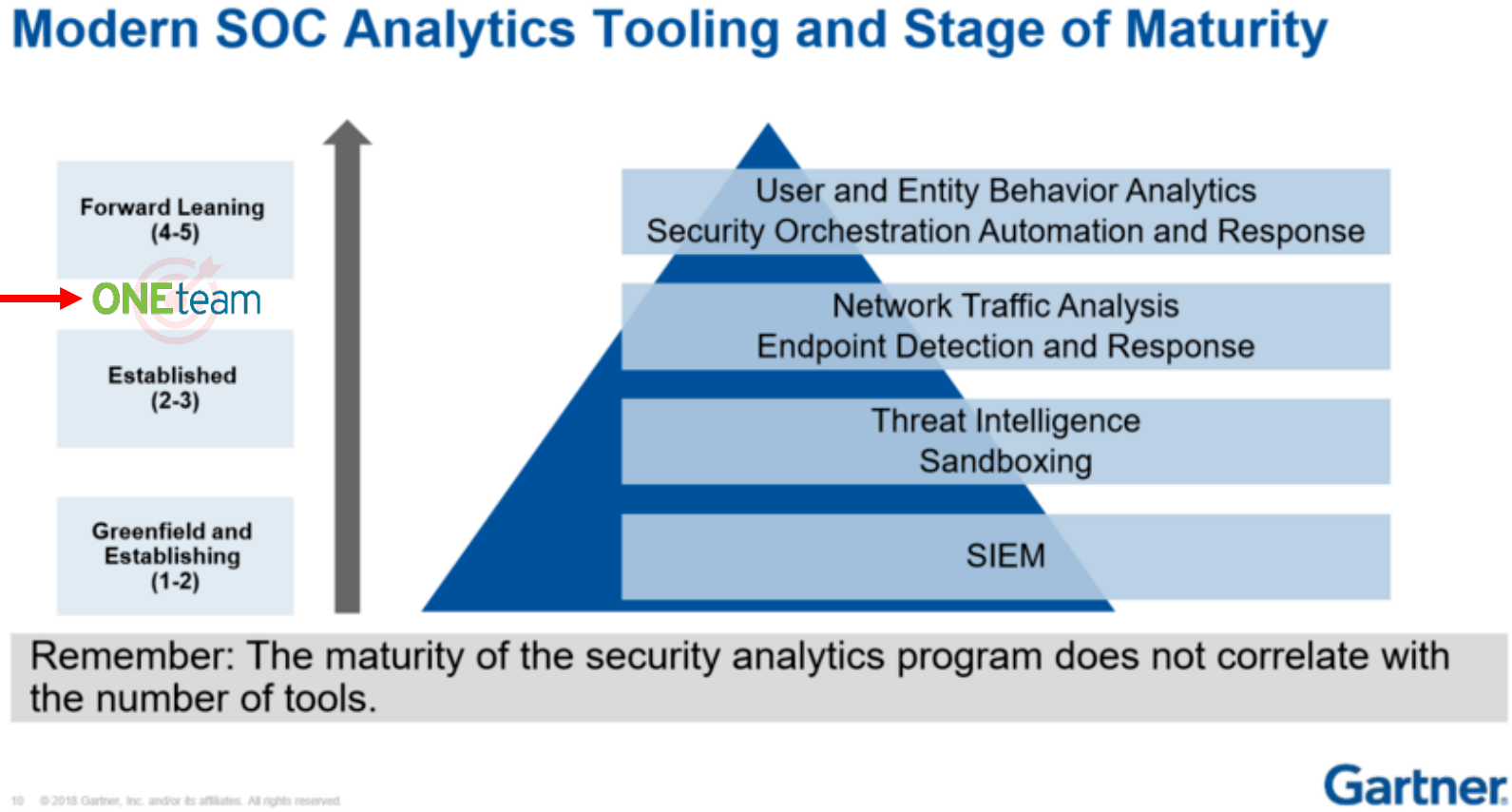
- **Program**
  - Review Existing Client Security Program and/or create Program based on the requirements for each of the Services across the following:
    - Business
    - Compliance and Risk
    - Security
    - Technology
  - Define and establish the Operating Model to support the identified Program Requirements
  - Define the Plan for implementing the Program and Operating Model and the Ongoing “Refresh” of the Model
- **Operations**
  - Execute the Plan for the Onboarding (Non-Recurring) of each Service
  - Deliver the Ongoing (Recurring) Services as defined in the Operating Model
  - Provide “As Needed” Services based on Incidents (as required)

Who is this service for?

- Any company that does not have the resources, either head count or expertise, to do this themselves.
- Size of the company doesn't matter. We work with small enterprises as well as very large global enterprises. This service is a good fit for any company, in any vertical, that needs the "outcome" achieved with this solution.
- Especially companies that have compliance requirements – *regulatory or contractual*. Are they doing all they can to protect their customers' data?

Gartner Maturity Model

3.5 Maturity with ONEteam MDR/MSOC*plus*



Summary – Key Takeaways

- There is a 2.93 million person gap in the cybersecurity talent pool (ISC2)
- Security professionals identify understaffing as their biggest challenge, and nearly a quarter says that the inability to keep up with the workload is a root cause of security incidents (ESG/ISSA)
- Almost three-quarters of organizations say they're impacted by the talent shortage and of those that are impacted, 66% increase the workload on existing staff (ESG/ISSA)
- Almost 40% of organizations say that less than 2% of their IT personnel has a dedicated security focus (EY)
- Nearly 60% of organizations say they face extreme or moderate risk due to the security talent shortage (ISC2)
- Only 35% of CISOs say that determining the scope of a compromise, containing it, and remediating the damage from exploits is easy (Cisco).
- More than 40% of organizations receive more than 10,000 security alerts every day. Additionally, organizations only respond to about half of the alerts and fix only 43% of those that turn out to be legitimate (Cisco).

Summary – Key Takeaways

- A Total Solution = Program + Technology + Operations. If you are missing any piece you are vulnerable!
- Leverage the information you have
- Focus on foundational elements of security to improve right now
- You don't have to get caught in the "buy security" frenzy. Security happens when you do the basics well.
- If you only do one thing to improve your security – Do This!

Q & A

Reference Slides

Reality of Enterprise Security

97%
of breaches are at companies which have already deployed the right controls

99%
of attacks are known and have been for years

95%
of firewall breaches are due to misconfiguration

Source: SafeBreach

Average of almost 7 months to detect a compromise!

On average, it takes businesses 206 days to detect infections, and a further 73 days to resolve them

The Fundamental Problem with Strategy

Many Enterprises …

- Implement security tools / technologies based on Frameworks (HIPAA, PCI, ISO 2700x, NIST, etc. = Controls-based)
- Don’t validate their controls - are the tools and techniques working?
- Don’t prioritize initiatives based on greatest risk to the organization
- Are not able to demonstrate return on investment AND reduction in risk

Wouldn't it be great if you could …

ASMGi ONEteam

ARCTIC WOLF

Get more from your existing security

Minimize security exposure

Ensure you are meeting compliance requirements

Prioritize initiatives based on actual Risk

Rationalize your cyber investments AND reduce risk

ASMGi
ONEteam

ARCTIC WOLF

For more information:

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Email: sales@asmgi.com

www.asmgi.com