ASMGi ONEteam

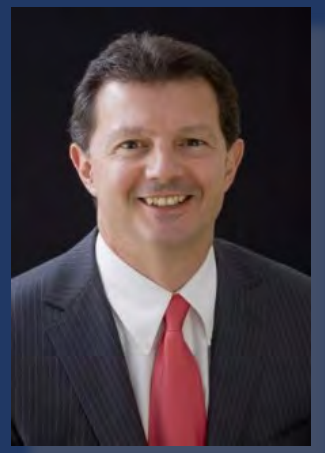
ARCTIC WOLF

Next-Gen Cybersecurity Through CMMC

May 20, 2021

Next-Gen Cybersecurity through CMMC

Brad Hanley
Systems Engineer
Arctic Wolf



Steve Roesing
President, CEO
ASMGi

ARCTIC WOLF

ASMGi
ONEteam

Agenda

- What is CMMC
- Some important definitions
- Breakdown of CMMC structure
- How do we help meet this Compliance Requirement?
- Some Announcements and Promotions
- Q & A

DIB Compliance Challenges

Securing the DIB has been challenging

Percent of the Defense Industry Base (DIB) that self reported not complying to DFARS 7012.

Summit7 survey- 2/2021

62%

Good example of what can happen …

ASMGi ONEteam

ARCTIC WOLF

VISSERPRECISION™

Small Subcontractor Breach

Visser Precision on April 10th, 2021, was hit with DoppelPaymer variant (ransomware). Visser is in the supply chain of Tesla, SpaceX, Boeing, Lockheed Martin, and others.

The threat actors stole all company files and have already released some of the data on the internet.

Some of the data already leaked:

- Specs for an antenna in an anti-mortar defense system
- Billing information
- Payment forms
- Data analysis reports
- Supplier information
- Legal paperwork
- Primes sensitive files

What is CMMC?

What is CMMC?

CMMC

Cybersecurity Maturity Model Certification

The framework used by the Department of Defense to further mature their supply chain

Some Definitions …

Federal Contract Information (FCI): FCI is information provided by or generated for the Government under contract not intended for public release.

Controlled Unclassified Information (CUI): CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.

Some Definitions …

The model encompasses the *basic safeguarding requirements* for specified in Federal Acquisition Regulation (FAR) Clause 52.204-21 and the *security requirements* for CUI specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 per Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204.7021.

When implementing CMMC, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for a particular segment(s) or enclave(s), depending upon where the information to be protected is handled and stored.

CMMC structure

The Cybersecurity Maturity Model Certification (CMMC) framework consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the Defense Industrial Base (DIB) and Department of Defense (DoD) stakeholders. The model framework (Figure 1) organizes these *processes* and *practices* into a set of *domains* and maps them across five *levels*. In order to provide additional structure, the framework also aligns the practices to a set of *capabilities* within each domain. The ensuing subsections provide additional information regarding each element of the model.

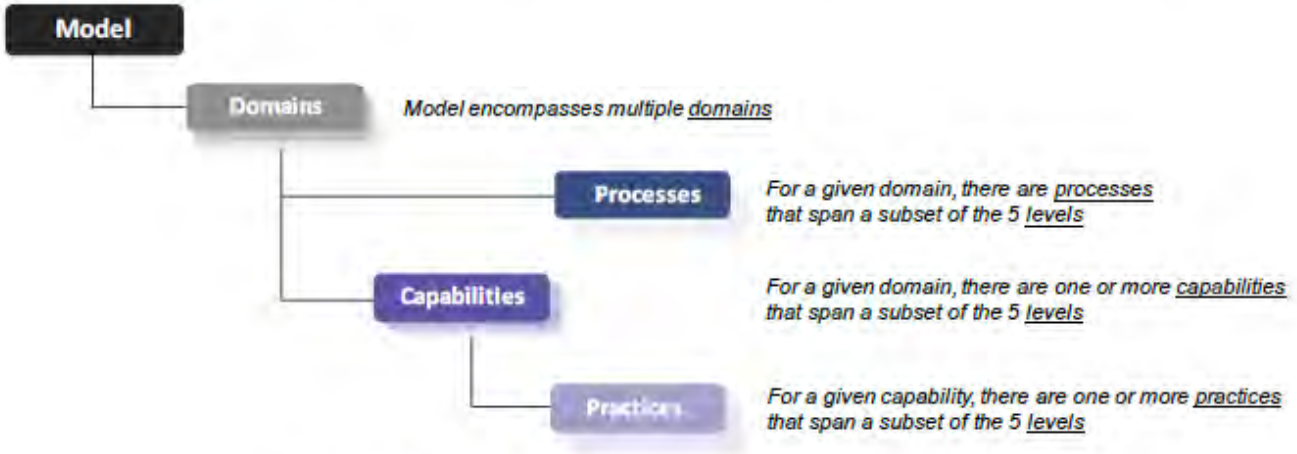


Figure 1. CMMC Model Framework (Simplified Hierarchical View)

CMMC structure

Figure 2. CMMC Levels and Descriptions

CMMC structure

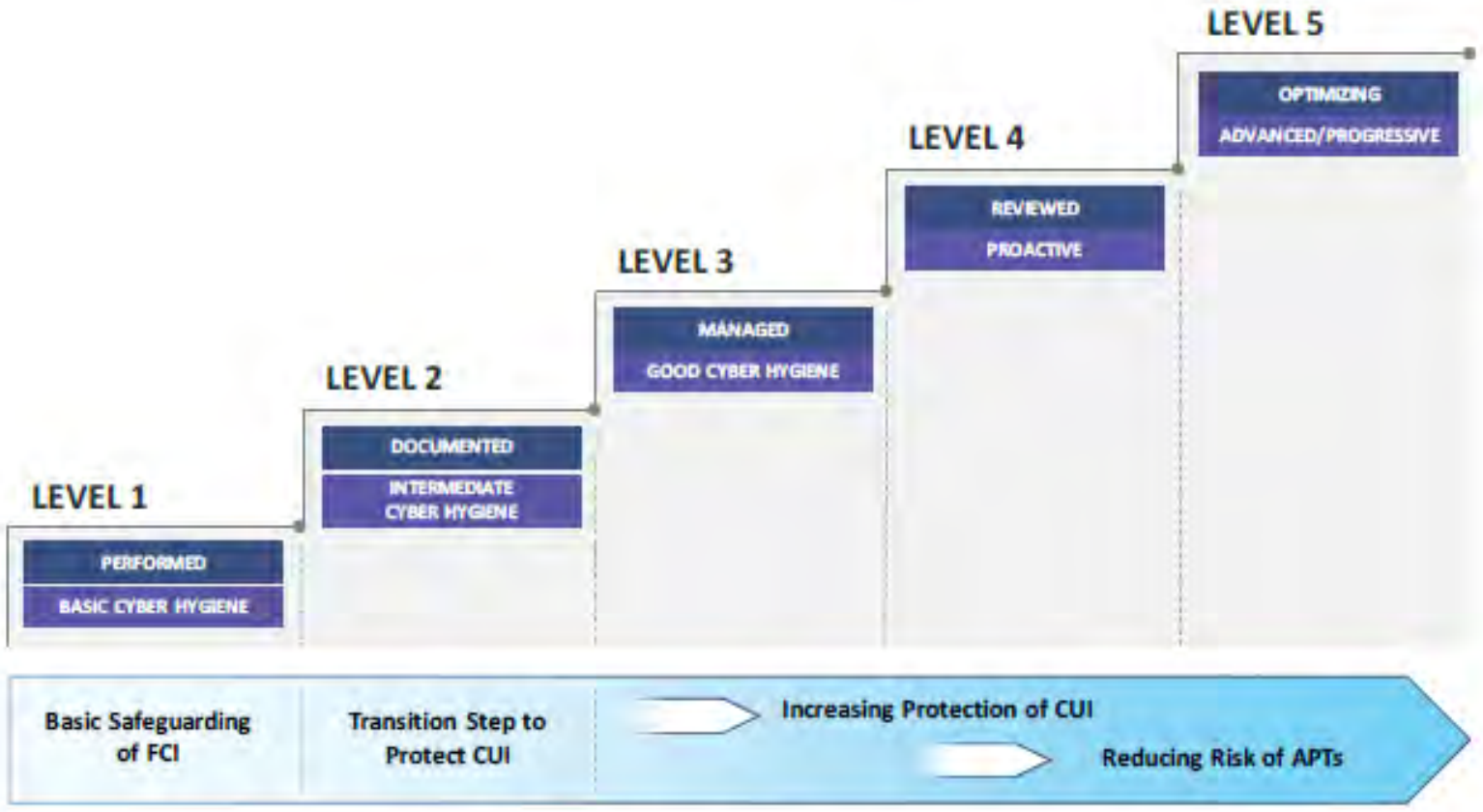


Figure 3. CMMC Levels and Associated Focus

CMMC structure

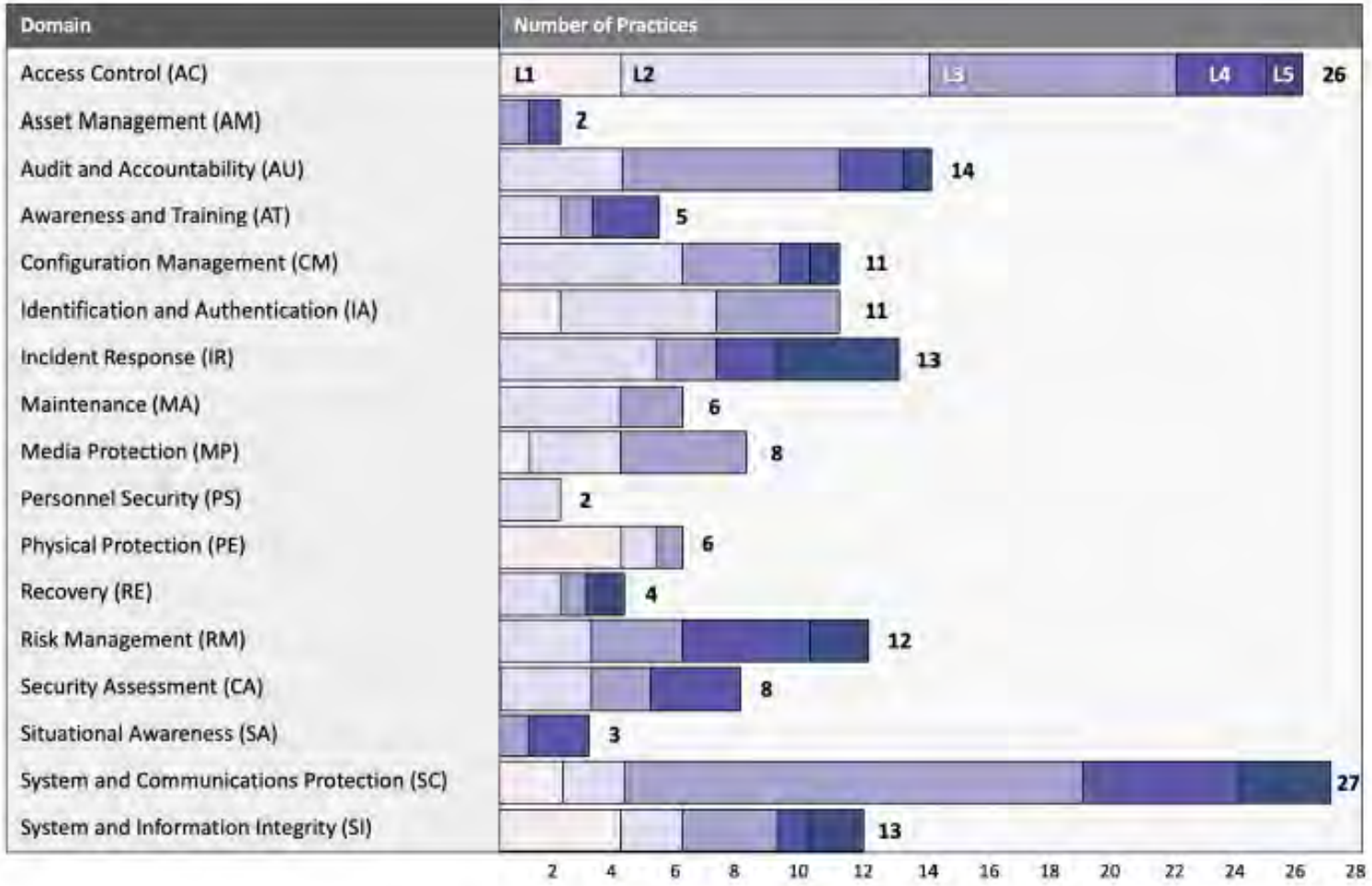


Figure 6. CMMC Practices Across Domains Per Level

Certification

Meet the CMMC
Accreditation Body

Non-Profit Accreditation Organization

The CMMC AB is contracted with the Department of Defense to train companies that will audit, assess, and guide the DIB into compliance with their respective CMMC Level.

CMMC
ACCREDITATION BODY
Cybersecurity Maturity Model Certification

C3PAO

C3PAO

Certified 3rd Party Assessor Organization
In charge of auditing and certifying DoD contractors are compliant with their CMMC Level

RPO

Registered Provider Organization

Registered Provider Organization
Provide advice, consulting, and recommendations to DoD contractors

Biggest Changes …

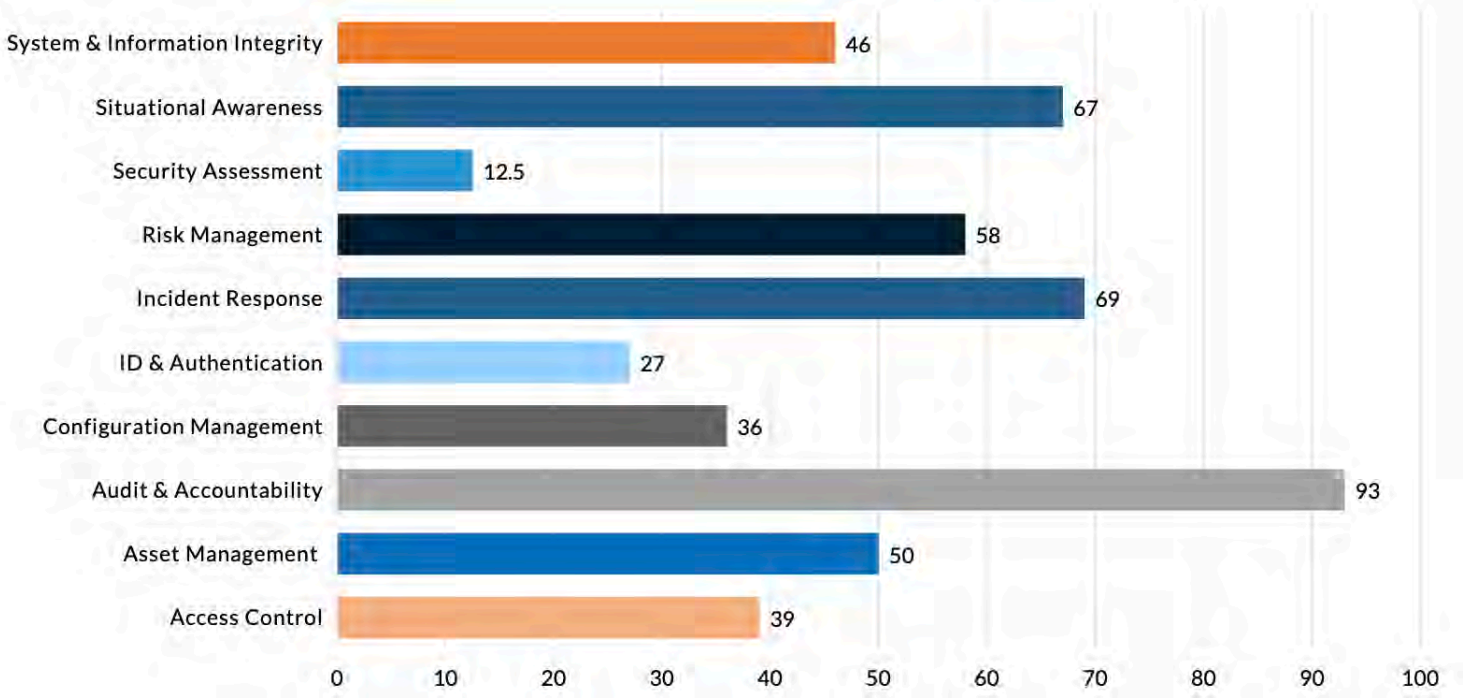
ASMGi ONEteam

ARCTIC WOLF

- 3rd Party Audits
- Trickle Down to Subs
- Pass or Fail
- POAM's are Not Used
- Built in Costs for Added Expenses
- Maturity Based
- Part of the Contract
- Certifications are Valid for 3 Years

How can we help meet these requirements?

How do we help meet these requirements?



Domain Coverage (Percentage)

How We Align

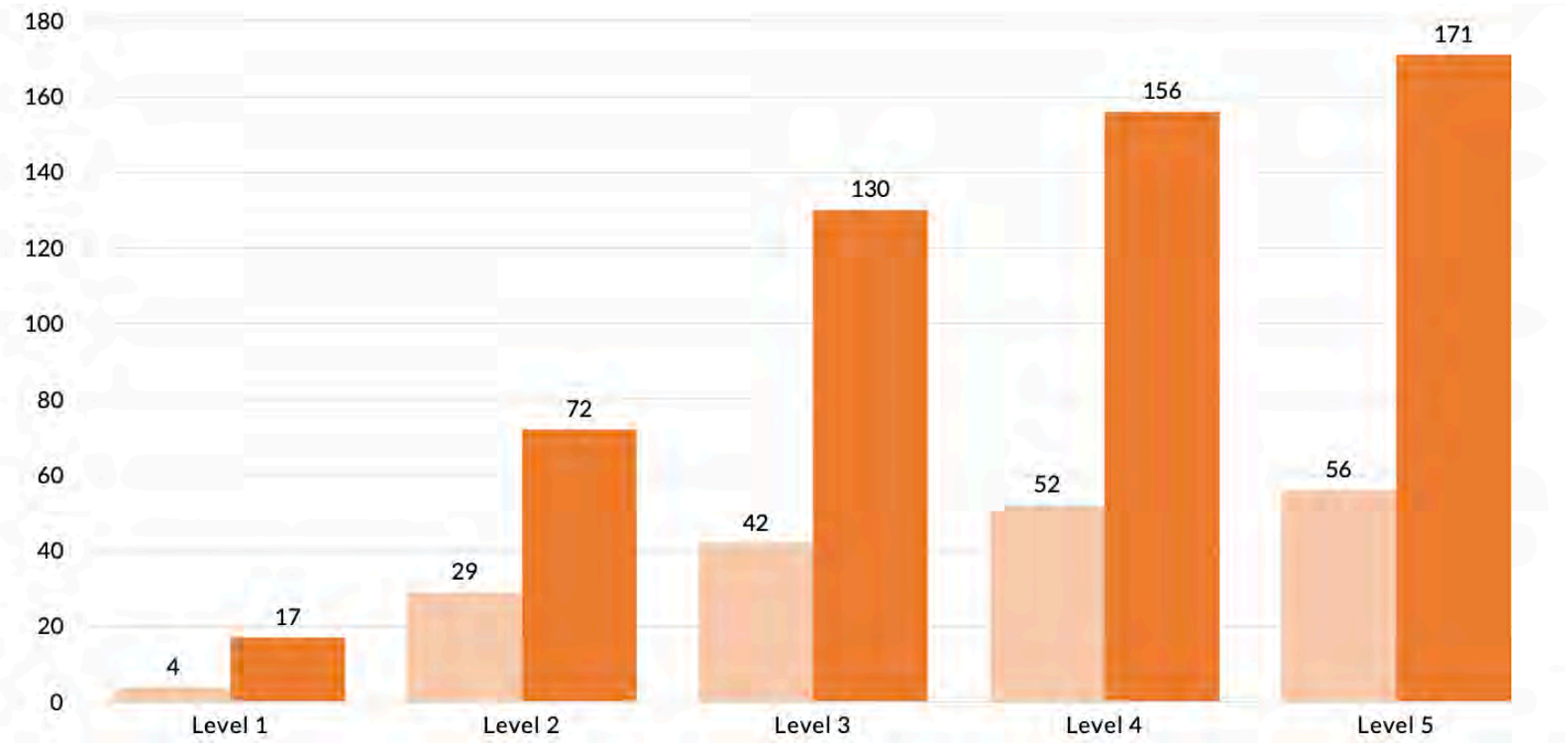
With MDR and Managed Risk, we help you meet some of the hardest practices in CMMC

How do we help meet these requirements?

ASMGi ONEteam

ARCTIC WOLF

This is our coverage of practices that we play a part in helping to fulfil broken out by the 5 Levels.



Here's the solution that will help you meet these requirement AND ***Lower your Risk****!*

What is ONEteam MDR/MSOC *plus*?

ASMGi ONEteam

ARCTIC WOLF

ONEteam MDR/MSOC *plus* =

RISK = *Likelihood* x *Impact*

We Lower "Likelihood" by:

- Remediating Vulnerabilities makes "Likelihood = 0" and prevents an attack.

- Identifying Vulnerabilities continuously and across all modes - Account Takeovers, External, Network-based, Host-based, and Cloud helps reduce Likelihood, and if the Vulnerabilities are remediated, makes "Likelihood = 0".

We Lower "Impact" by:

- Identifying intruders quickly, anywhere on your network and assets, reduces the Impact of an incident. The longer an intruder spends on your network (dwell time), the larger the Impact. If the intruder is detected quickly, Impact may even be eliminated completely.

- Identification of Configuration issues in Cloud environments enables you to quickly fix them.

- Containment of the incident reduces the Impact of an incident. We contain incidents both manually and using automation.

- Structured, rehearsed Incident Response Program (including table-top exercises)

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

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

Key

- Arctic Wolf + ASMGi
- ASMGi

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.

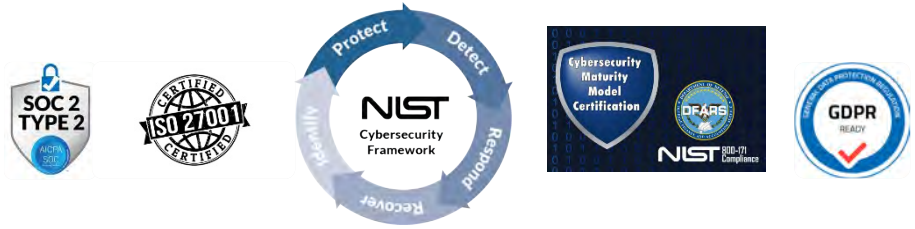
Table 3-5. Incident Handling Checklist

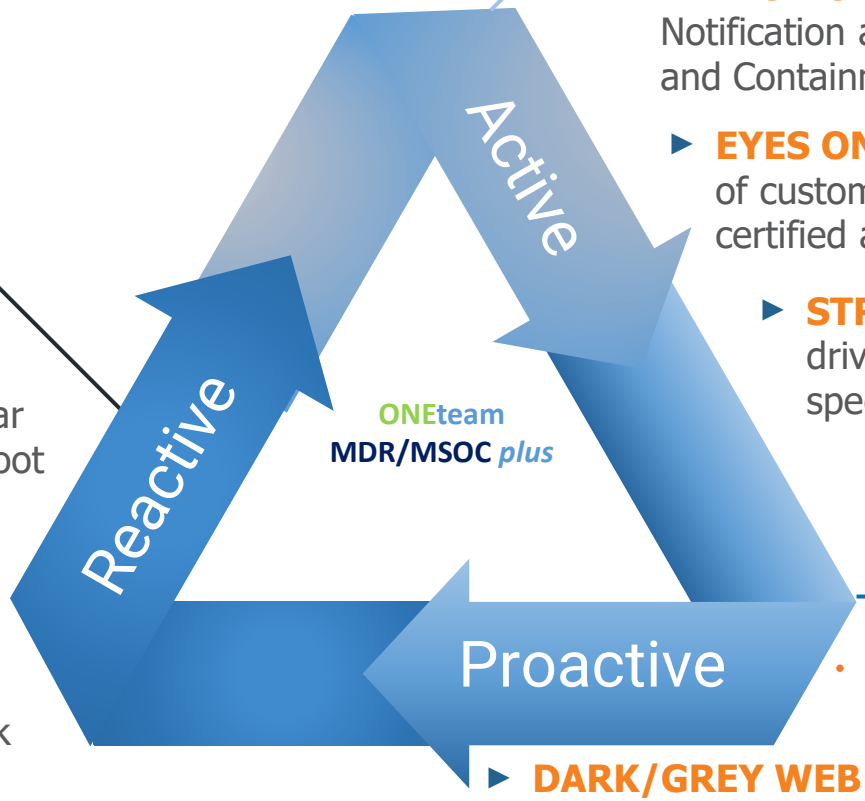
	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting 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)	

The Complete Cybersecurity Operations Platform

Managed Detection & Response

- **PROACTIVELY** provides IDS, Dark Web Scanning, and Endpoint Intelligence
- **REMEDIATION** Including detailed steps, War Room Assistance, Required Reporting, and Root Cause Analysis Detail
- **ACTIVE** monitoring of Cloud assets and resources for misconfigurations and vulnerabilities
- **ACTIVE** scanning of customer entire network environment to achieve and maintain broad visibility of assets agent or agentless





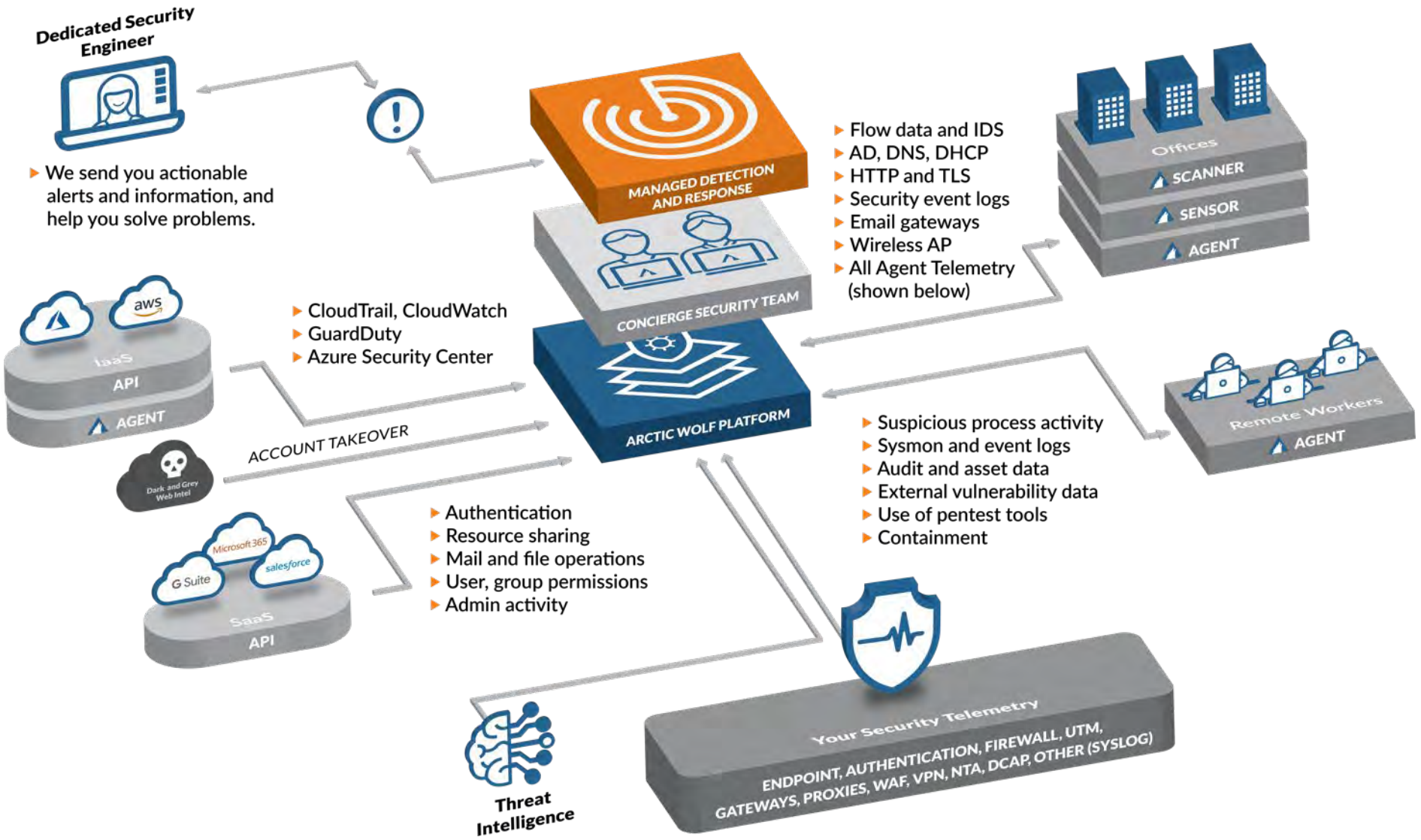
Security Operations

- **DETECTION** of in process attacks providing: Notification and Escalation, GEOIP Information, and Containment
  - **EYES ON GLASS** 24/7/365 Human monitoring of customer environments by experienced, certified and skilled security experts
    - **STRATEGIC** Security guidance and reporting driving continuous improvement tailored to the specific needs of each organization.

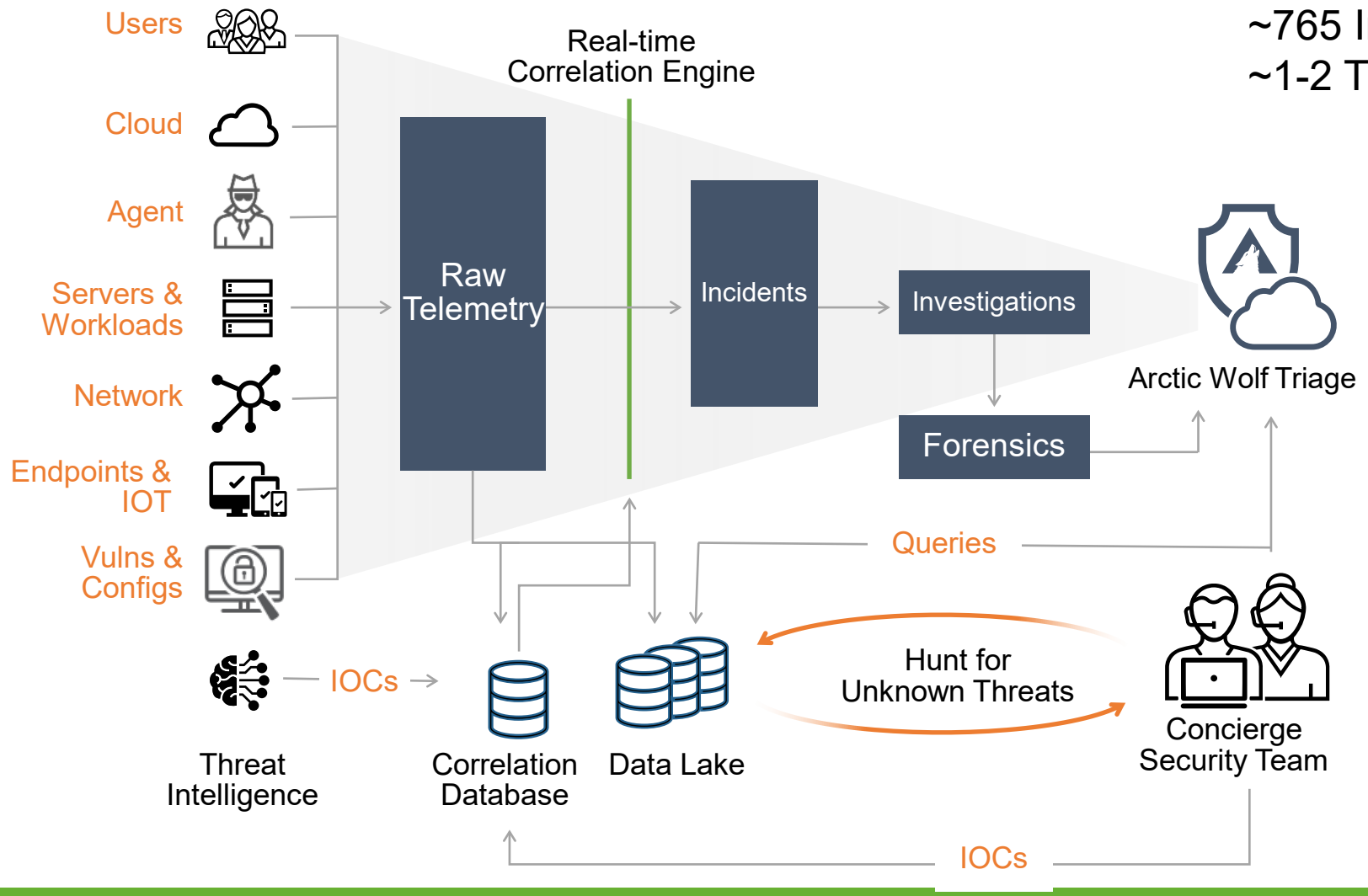
Managed Risk

- **PREVENTION** of known attacks before they occur by limiting known attack surfaces
- **DARK/GREY WEB SCANNING** for customer accounts that may have been compromised
- **CONTINUOUS** vulnerability scanning of networks and endpoints
- **RISK QUANTIFICATION** from external and internal networks assets, regardless of Arctic Wolf Agent installation capability
- **REMEDIATION PRIORITIZATION** Detailed correlation of risks

Managed Detection and Response Architecture



Security Operations



~165M Observations/Week
~765 Investigations/Week
~1-2 Tickets/Week

450 Users
150 Servers
4 Sensors

Identify

- Detect threats across network, endpoint, and cloud.
- Expert analysis of IOCs across entire attack surface using a purpose-built cloud platform
- Discover vulnerabilities and misconfigurations

Act

- Guidance and prioritization for remediating threats, vulnerabilities, and risks.
- Detailed recovery and hardening recommendations with closed-loop follow-up

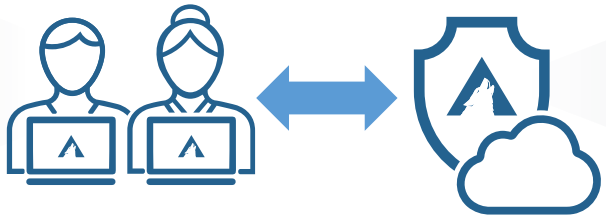
Improve

- Hunt for Advanced threats across endpoints, network and Cloud with deep analytics and human expertise
- Security Journey program to improve overall security posture

Managed Risk Architecture

- Customizes service to your needs
- Continuously scans your environment for digital risks
- Performs monthly risk posture reviews
- Provides actionable remediation guidance
- Delivers a customized risk management plan

ONEteam Security Operations



ONEteam
MDR/MSOC *plus*

Digital risk data sources

- IaaS Configurations
- Vulnerabilities (CVEs)
- CIS Benchmarking
- Account Takeover data

Managed Risk Dashboard

Managed Risk Scanner

Secure Transport

Agent

Secure Transport

Network Scanning

Vulnerability Data
Nmap Data
Network Inventory

Internal

Vulnerability Data
Dark and grey web intel
DNS
OWASP top-10 scanning
Publicly Accessible Ports / Services

External

Cloud Scanning

Cloud Security Posture Management (CSPM)

aws
Microsoft Azure
G Suite

Endpoint Scanning

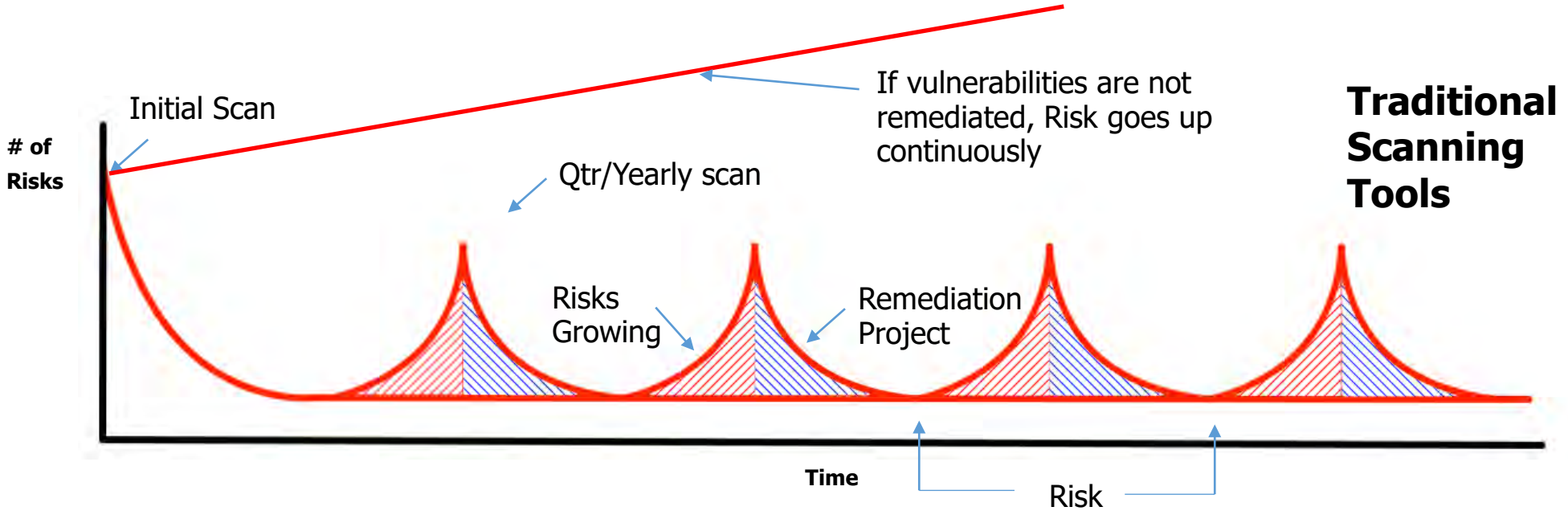
System Vulnerabilities
Configuration Benchmarks
Hardware / Software Inventory

Continuous Cyber Risk Assessment

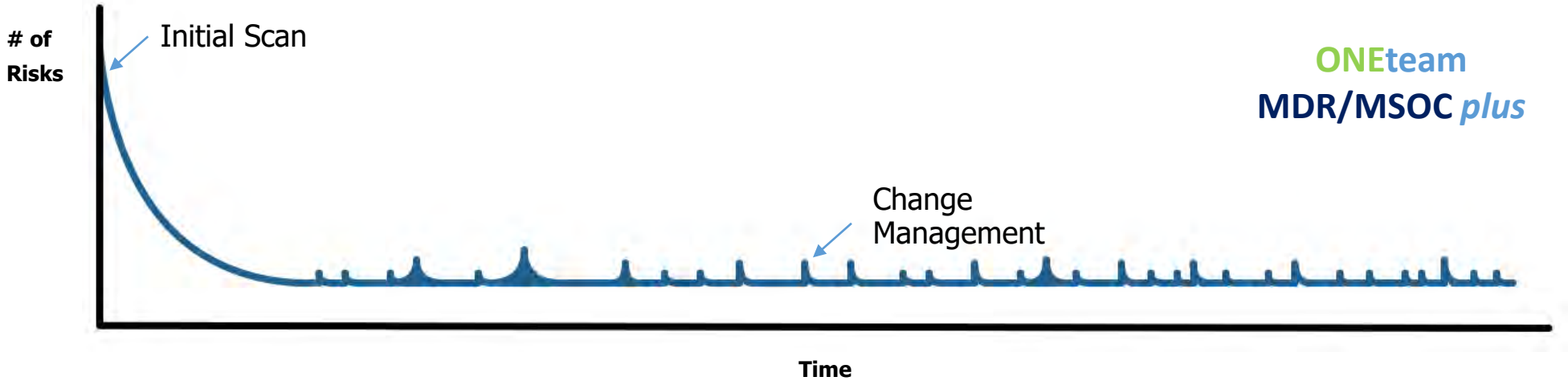
ASMGi ONEteam

ARCTIC WOLF

Point In Time Scans



Continuous Scans



Can Your YETI Stop Ransomware?

Sign Up for a 45-minute Zoom call with us and we'll show you!!!

The combination of Arctic Wolf and ASMGi Managed Detection & Response (MDR) / Managed Security Operations Center (MSOC) offers you a comprehensive and cost-effective end-to-end threat management and response strategy.

Register HERE and we'll send you a ***YETI RAMBLER***: **www.asmgi.com/Yeti/**

Or put your **name, title and business email** in the chat box and we'll set up the call.

TPRM Online Workshop | Our Next Event in our Compliance Series

Third-Party Risk – How to meet your Compliance Requirements and balance Risk, Cost and Resiliency

Thursday, June 3, 2021 - 1:00-2:30 PM ET

A live online interactive workshop
hosted by Linda Tuck Chapman of Third Party Risk Institute Ltd. and Steve Roesing of ASMGi

As attendees today we will automatically register you for this workshop

Resources

- https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

- https://arcticwolf.com/resources/blog/cmmc-certification-what-you-need-to-know
- ASMGi:
  - https://asmgi.com/resources/
  - https://asmgi.com/mdr-msoc/

ASMGi ONEteam

ARCTIC WOLF

Q & A

Can Your YETI Stop Ransomware?

Sign Up for a 45-minute Zoom call with us and we'll show you!!!

The combination of Arctic Wolf and ASMGi Managed Detection & Response (MDR) / Managed Security Operations Center (MSOC) offers you a comprehensive and cost-effective end-to-end threat management and response strategy.

Register HERE and we'll send you a ***YETI RAMBLER***: **www.asmgi.com/Yeti/**

Or put your **name, title and business email** in the chat box and we'll set up the call.

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