ASMGi ONEteam

ARCTIC WOLF

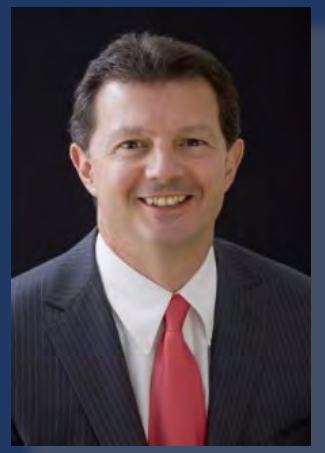
Cloud Security

Don't Let Your Cloud Security Fall Behind!

April 8, 2021

Cloud Security – *Don't Let Your Cloud Security Fall Behind!*

Dmitriy Sandler
Director of Presales Engineering
Arctic Wolf



Steve Roesing
President, CEO
ASMGi

ARCTIC WOLF

ASMGi
ONEteam

Webinar Series – ASMGi ONEteam MDR/MSOC *plus* (*powered by Arctic Wolf*)

1. Managed Detection and Response – *How to Stop Cyber Attacks with Modern MDR and Managed SOC, March 4*

2. Managing Cyber Risk - *Don’t be careless about your exposure to cyber-attacks, March 25*

3. Cloud Security - *Don't Let Your Cloud Security Fall Behind, April 8*

ASMGi

ARCTIC WOLF

Agenda

- The Big Move to the Cloud
- Risks in the Cloud
- What is Cloud Security Posture Management (CSPM) and How Does it Prevent Attacks
- Re-Cap of the Total Solution: MDR + Managed Risk + Managed Cloud Security = MDR/MSOC *plus*
- Q & A

The Big Move to the Cloud

The Big Move to the Cloud

Source: Cloud Computing: The New Plastics
Frederick Scholl, Ph.D., Cybersecurity Program Director, Quinnipiac University

TOP 5 INVESTMENTS FOR 2020 AND 2019

Technology	2020	2019
Cloud Computing (IaaS, PaaS, SaaS)	1	2
Analytics/Business Intelligence/Forecasting/Big Data	2	1
Security/Cybersecurity	3	3
Software Development/Maintenance	4	4
CRM (Customer Relationship Management)	5	5

CLOUD ARCHITECTURE TRENDS

Cloud Technology	Percent Organizations Using
Internal private	13%
Public multitenant	51%
External, single tenant dedicated	18%

From Society for Information Management (SIM) IT Trends Survey

Risks in the Cloud

Risks in the Cloud

Top 5 Cloud Security related Data Breaches!

Posted By **Naveen Goud**

The Year 2017 has so far witnessed some data slip-ups from the worlds top cloud storage providers and the details are as follows-

Accenture- World's first Cyber Resilience startup UpGuard discovered in its Cyber Risk survey that Accenture left at least 4 AWS S3 storage buckets unsecured.

Booz Allen Hamilton- In this year, technology consulting firm Booz Allen hired UpGuard to carry out security assessment on both its internal and external computer systems. To our surprise, the assessment discovered that 60,000 files were on a public access on AWS S3 bucket owned by an intelligence and defense contract of Booz Allen.

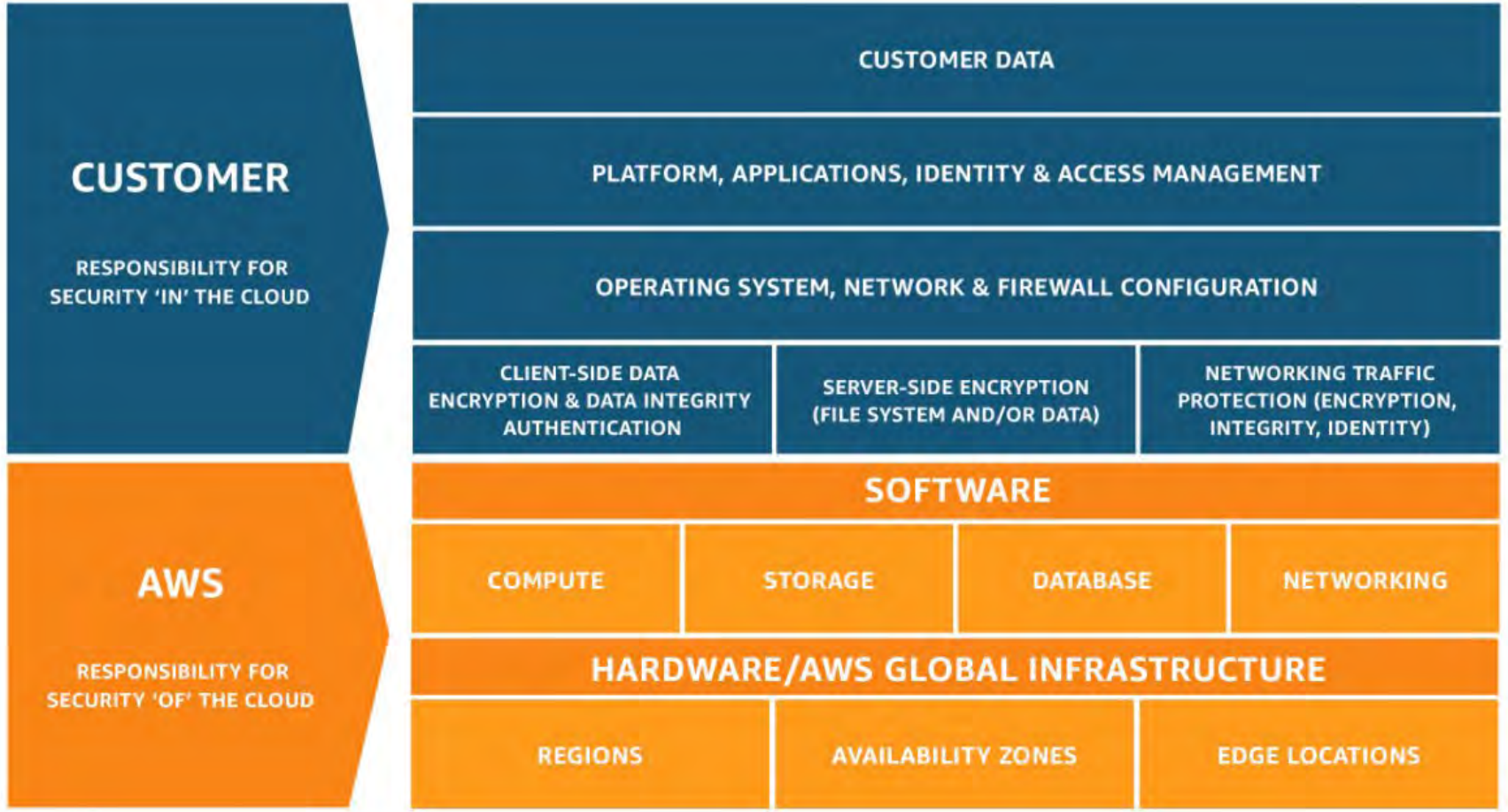
Risks in the Cloud

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

We're all moving workloads to the Cloud, and fast! Avoiding misconfigurations should be top of mind for everyone!

Is anyone checking your Cloud configurations?

Shared Responsibility Model



What is Cloud Security Posture Management (CSPM)?

What Is CSPM?

CSPM is a continuous process of cloud configuration monitoring and adaptation to reduce the likelihood of a successful attack. It includes use cases for compliance monitoring, DevOps integration, incident response, risk assessment, and risk visualization.

"Through 2024, organizations implementing a cloud security posture management (CSPM) and extending this into development will reduce cloud-related security incidents due to misconfiguration by 80%."

— Gartner

Innovation Insight for Cloud Security Posture Management

Summary

Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement and mistakes. Security and risk management leaders should invest in cloud security posture management processes and tools to proactively and reactively identify and remediate these risks.

- Gartner

THE WALL STREET JOURNAL.

PRO CYBER NEWS

Human Error Often the Culprit in Cloud Data Breaches

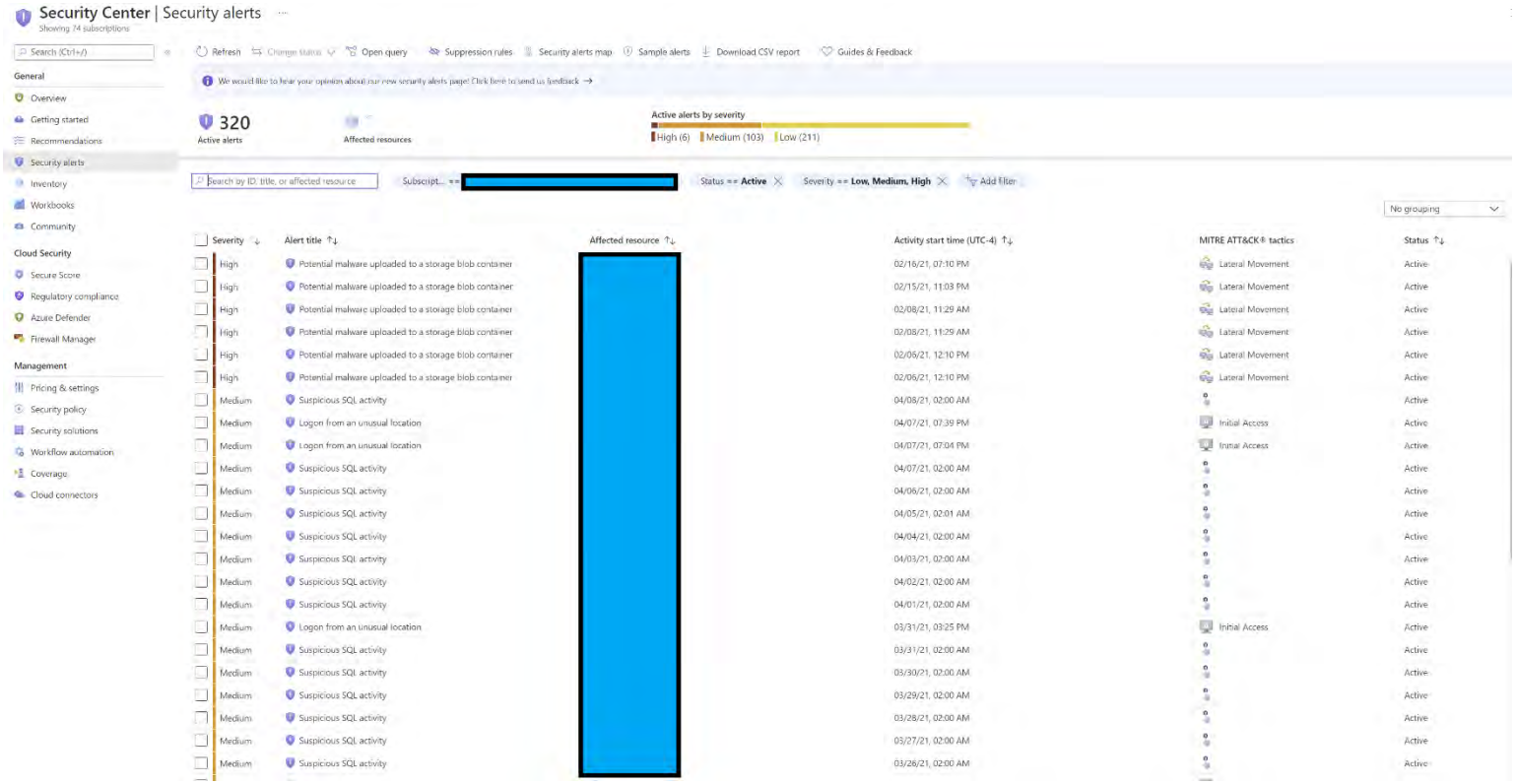
Mistakes made by customers can often lead to the finger being pointed at cloud providers

The process of setting up and securing a server on AWS's popular S3 storage system, for instance, is complicated, said Teresa Walsh, global head of intelligence at the Financial Services Information Sharing and Analysis Center, while speaking at a conference held by WSJ Pro Cybersecurity in London in June. She pointed to AWS's 130-page instruction guide for how to operate its S3 service.

"You just need to miss one [security] item, and that opens the door to any bad actor," said Nico Fischbach, global chief technology officer at security firm Forcepoint Inc. Even minor oversights can have disastrous consequences, he said. In the Verizon breach, for instance, the company estimated that six million customer records, including addresses and identification numbers, were compromised.

Gartner Inc. estimates that up to 95% of cloud breaches occur due to human errors such as configuration mistakes, and the research firm expects this trend to continue.

Public Clouds try to make it easier …



Someone needs to investigate all of these!

ASMGi ONEteam

ARCTIC WOLF

How does CSPM enable Cloud Security?

Cloud Security Posture Management

47%

Of the incidents we detect include a cloud component

CSPM is the process of cloud configuration monitoring and adaptation to **reduce the likelihood of a successful attack**

- Cloud Environment Benchmarking
  - Cloud configuration best practices
  - Quantified risk score
- Posture Hardening Recommendations
  - Remediation recommendations by your Concierge Security Team
  - Detailed documentation on configuration changes
- Incorporated into Managed Risk
  - Results available in EVA and through reports
  - Standard risk workflow process (open, accept, mitigate, etc.)

Vulnerabilities Identified by CSPM

ASMGi ONEteam

ARCTIC WOLF

Examples of misconfigurations we check for:

- Services exposed publicly to the internet
- Unencrypted data storage
- Lack of least-privilege policies
- Poor password policies or missing MFA
- Misconfigured backup and restore settings
- Data exposure and privilege escalation

ONEteam
MDR/MSOC *plus*

AWS

AWS Data Collection

- Simplified setup via Cloud Formation
- Comprehensive CloudTrail, CloudWatch, and GuardDuty monitoring
- Instance visibility via Arctic Wolf Agent
- No data volume limits

AWS Events/Alerts Detected:

- 120+ alerting rules
- Customizable threat detection logic
- CIS Security Controls benchmarking
- Sample AWS alerts
  - Unauthorized authentication and access
  - Suspicious administrative actions
  - Brute-force login attacks

Comprehensive AWS Visibility

CloudTrail	AWS account activity
CloudWatch	AWS resources, OS, and apps monitoring
GuardDuty	Curated GuardDuty findings
AWS WAF	AWS WAF logs

Microsoft Azure

Azure Data Collection

- Simplified setup to monitor Azure resource creation, deletion and modification
- Log capture via APIs to capture activity logs and Active Directory events
- No data volume limits

Azure Events/Alerts Detected:

- 250+ alerting rules purpose built for Azure
- Detect administrative actions and user activity in Azure Resource Manager
- Sample Azure alerts
  - Unauthorized authentication and access
  - Suspicious administrative actions
  - Anomalous resource usage

Leverages Azure APIs

Activity Logs	Monitors actions performed on resources by subscribers using Azure Resource Manager
Active Directory Events	Login activity, user and service settings

G-Suite

Deep G Suite Visibility & Alerting

- 230+ alerting rules at setup, plus CST customizations
- Detailed usage reporting
- Sample Alerts:
  - Brute-force attacks; Multi-geo logins
  - Anomalous admin settings changes
  - Suspicious file and folder activity

Comprehensive G Suite Monitoring

- Monitor activity in Google Drive, Gmail, Calendar, Groups, and Hangouts
- No data volume limits

Office 365

Office 365 Data Collection

- Monitors activity in Active Directory, SharePoint, OneDrive, Exchange admin and mailbox
- No data volume limits

Office 365 Events/Alerts

- 50+ altering rules at setup, plus CST customizations
- Sample Alerts:
  - Brute-force logins
  - Concurrent access from multiple geos
  - Login from blacklisted IP addresses

Amazon Web Services Checked

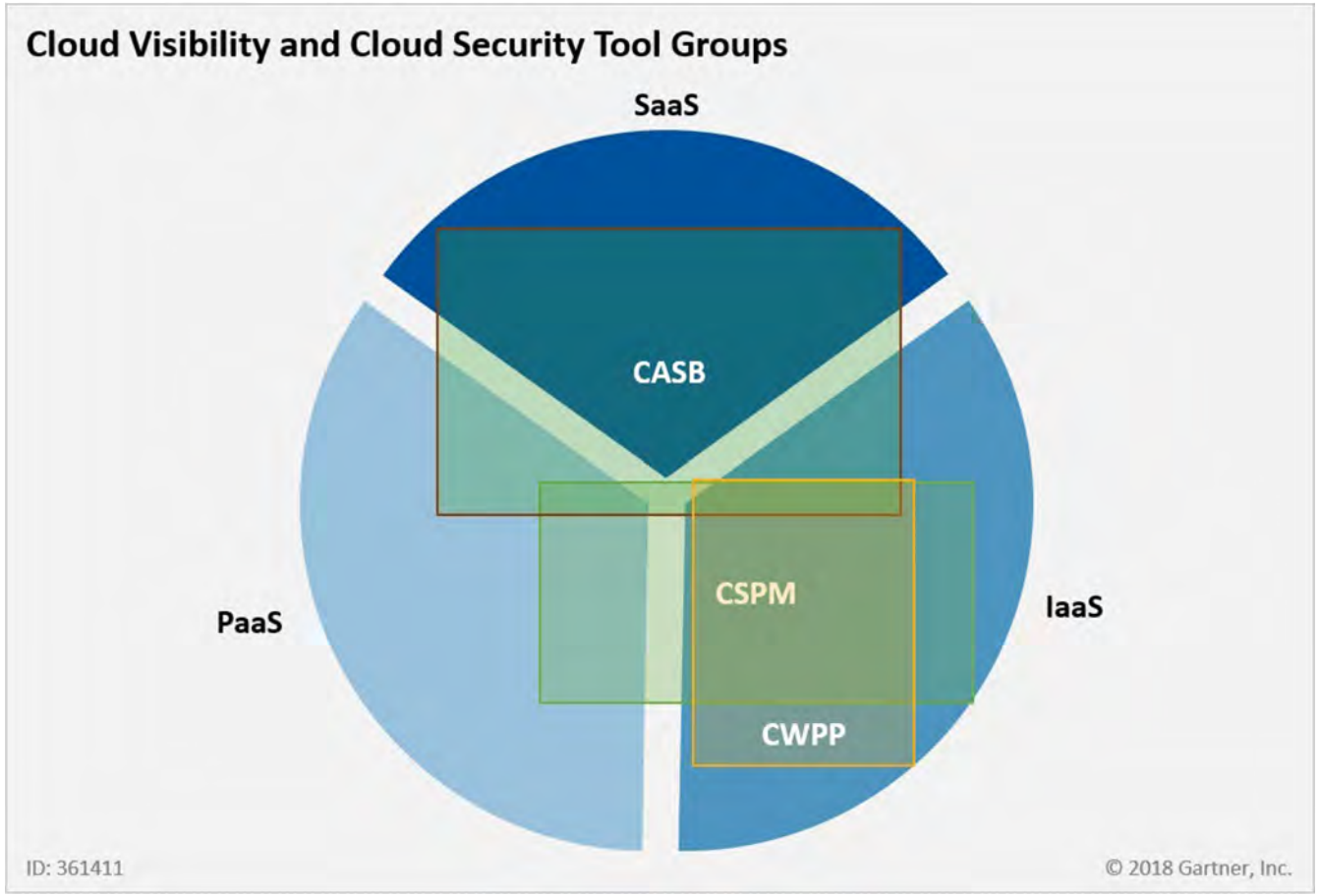
- Certificate Manager (ACM)
- Athena
- Auto Scaling
- CloudFront
- CloudTrail
- CloudWatch
- Config
- Database Migration Service (DMS)
- DynamoDB
- Elastic Cloud Compute (EC2)
- Elastic Container Registry (ECR)
- Elastic File System (EFS)
- Elastic Kubernetes Service (EKS)
- Elastic Load Balancing (ELB)
- Elasticsearch Service (ES)
- Kinesis Data Firehose
- Identity & Access Management (IAM)
- Kinesis
- Key Management Service (KMS)
- Lambda
- Organizations
- Relational Database Service (RDS)
- Redshift
- Route 53
- Simple Storage Service (S3)
- SageMaker
- Shield
- Simple Email Service (SES)
- Simple Notification Service (SNS)
- Simple Queue Service (SQS)
- Systems Manager Agent (SSM)
- Transfer Family
- X-Ray

Azure Services Checked

- Active Directory
- App Service
- Azure Policy
- Blob Storage
- Content Delivery Network (CDN)
- Container Registry
- File Service
- Key Vaults
- Kubernetes Service
- Load Balancer
- Log Alerts
- Monitor
- MySQL Database
- Network Security Group
- PostgreSQL Database
- Queue Service
- Resource Manager
- Security Center
- SQL Database
- SQL Servers
- Azure Storage
- Table Storage
- Virtual Machines
- Virtual Networks

Cloud Security Posture Management

Approaches to securing the cloud



Protect the 3 major cloud environments with CSPM

The CSPM capability provides you with (for Azure, AWS and GCP):

Cloud Inventory Reporting:

Returns a complete inventory and categorization of all assets found within the cloud environment for auditing, monitoring, and executive reporting purposes.

Cloud Environment Benchmarking:

Assigns a cloud environment risk score to quantify how your environment compares to generally accepted cloud configuration benchmarks.

Posture Hardening:

Our experts work with you and provide rich context and remediation / recommendations to close cloud vulnerability gaps and harden your security posture.

Key Features

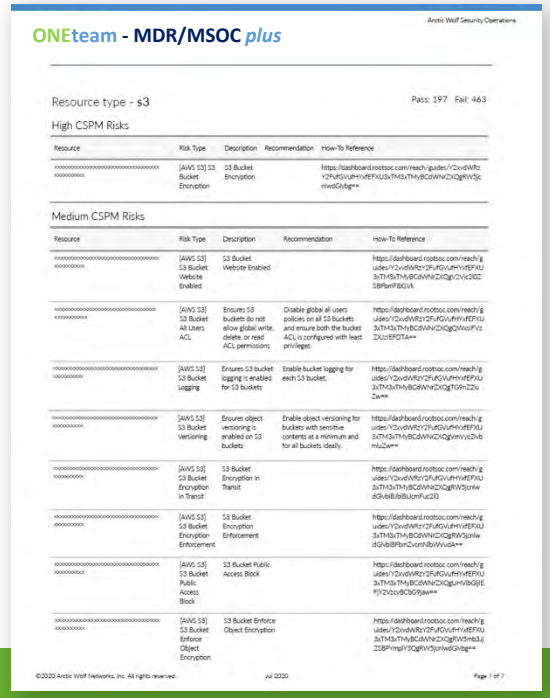
Cloud providers have hundreds of services with thousands of configuration options. Our Experts work closely with you to identify and close security gaps within your cloud infrastructure, such as:

- Servers that are publicly exposed to the internet
- Unencrypted databases and data storage
- Lack of least-privilege policies

- Misconfigured backup and restore settings
- Data exposure and privilege escalation
- Poor password policies or missing multifactor authentication (MFA)

Cloud Security Posture Management

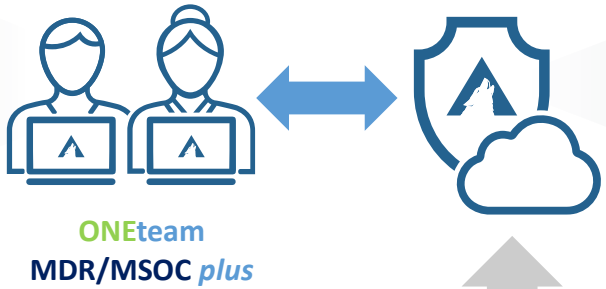
Part of Managed Risk; Cloud Security Posture Management (CSPM) performs security and configuration scans on your cloud infrastructure environments (such as AWS) to detect thousands of potential threats. This insight is used to produce detailed cloud inventory, as well as a quantified view of your cloud infrastructure misconfiguration risks.



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

Re-Cap

What is ONEteam MDR/MSOC *plus*?

ASMGi ONEteam

ARCTIC WOLF

ONEteam MDR/MSOC *plus* =

ARCTIC WOLF + ASMGi

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.

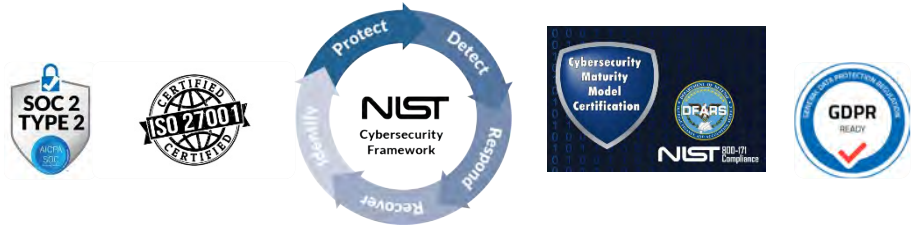
Table 3-5. Incident Handling Checklist

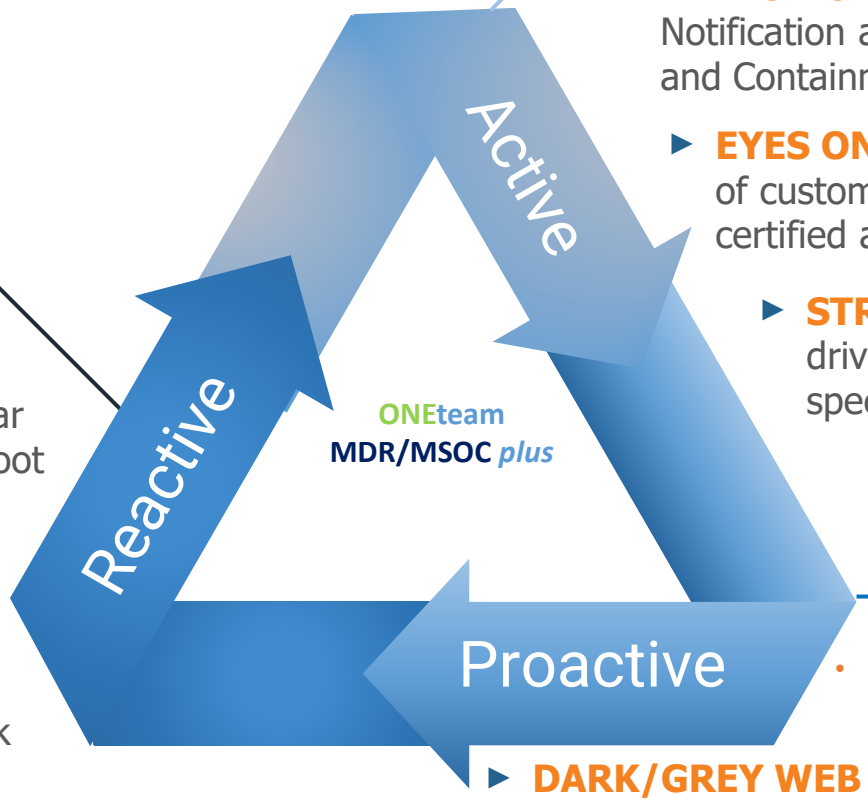
	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting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

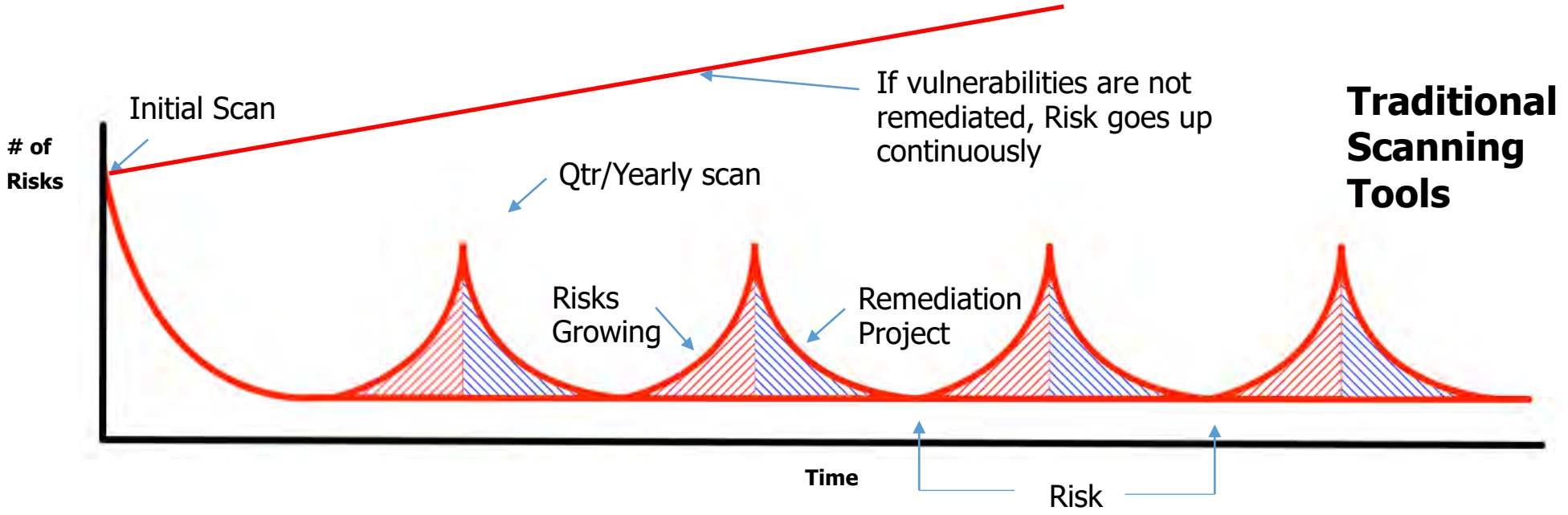
- **PREVENTION** of known attacks before they occur by limiting known attack surfaces
- **DARK/GREY WEB SCANNING** for customer accounts that may have been compromised
- **CONTINUOUS** vulnerability scanning of networks and endpoints
- **RISK QUANTIFICATION** from external and internal networks assets,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

Continuous Cyber Risk Assessment

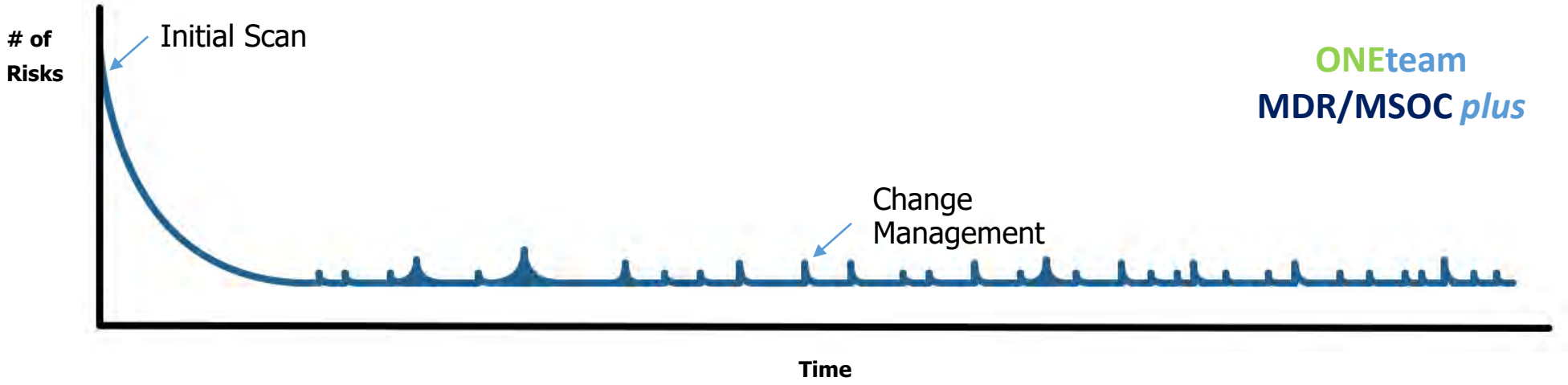
ASMGi ONEteam

ARCTIC WOLF

Point In Time Scans



Continuous Scans



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)

Key Takeaways

- Breadth of visibility is critical
  - External
  - Agent/Host-based (includes VMs (IaaS) on any Cloud platform)
  - Network Traffic Analysis
  - Cloud (All major public clouds)
- To lower risk, you must remediate vulnerabilities!
- 24x7 Eyes on Glass is Critical
- Single pane of Glass for all Cyber Risks
- Practice Cyber Incident Response (CIR) so you know what to do if something bad happens! (Tabletop Exercise)

ASMGi ONEteam

ARCTIC WOLF

Q & A

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