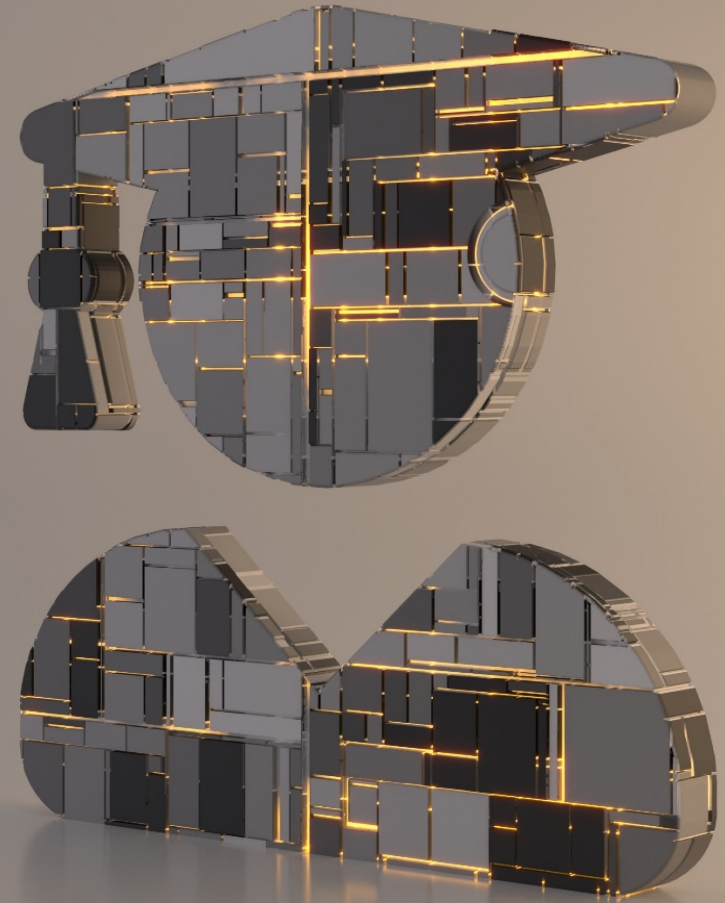




A Risk-Based Information Security & Cyber Strategy for Higher Education

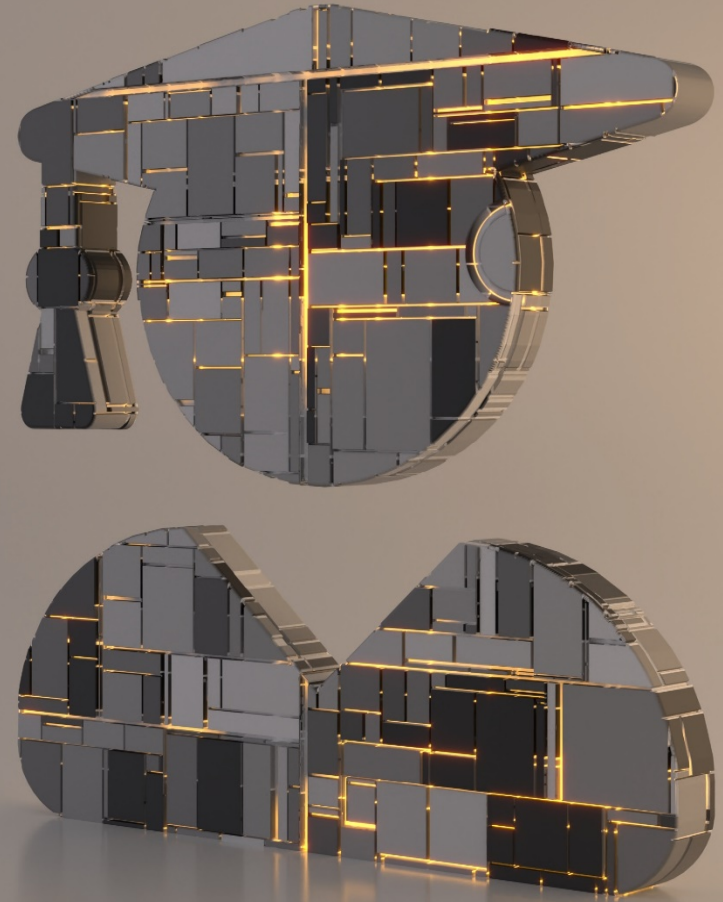
April 21, 2020





A Risk-Based Information Security & Cyber Strategy for Higher Education

April 21, 2020



A Risk-Based Information Security & Cyber Strategy for Higher Education



Frank Yako
CIO, Director of Strategic Initiatives
ASMGi



Steve Roesing
President, CEO
ASMGi

ASMGi is full-stack technology company headquartered in Cleveland, OH. Our expertise across the full spectrum of IT Services, GRC & Cyber Services and SDLC Services provides value to our customers.

Higher Education leverages our ONETeam turn-key solutions to achieve relevant, cost effective outcomes combining Programs, Technology and Operations.



ONETeam

- ◆ *Cyber Security Landscape in Higher Education*
- ◆ *Discussion Topic #1 – Security Strategy & Assessments*
- ◆ *Discussion Topic #2 – Cyber Security Solutions*
- ◆ *Conclusion + Key Points*
- ◆ *Questions + Closing Remarks*

Educause Top 10 IT Issues

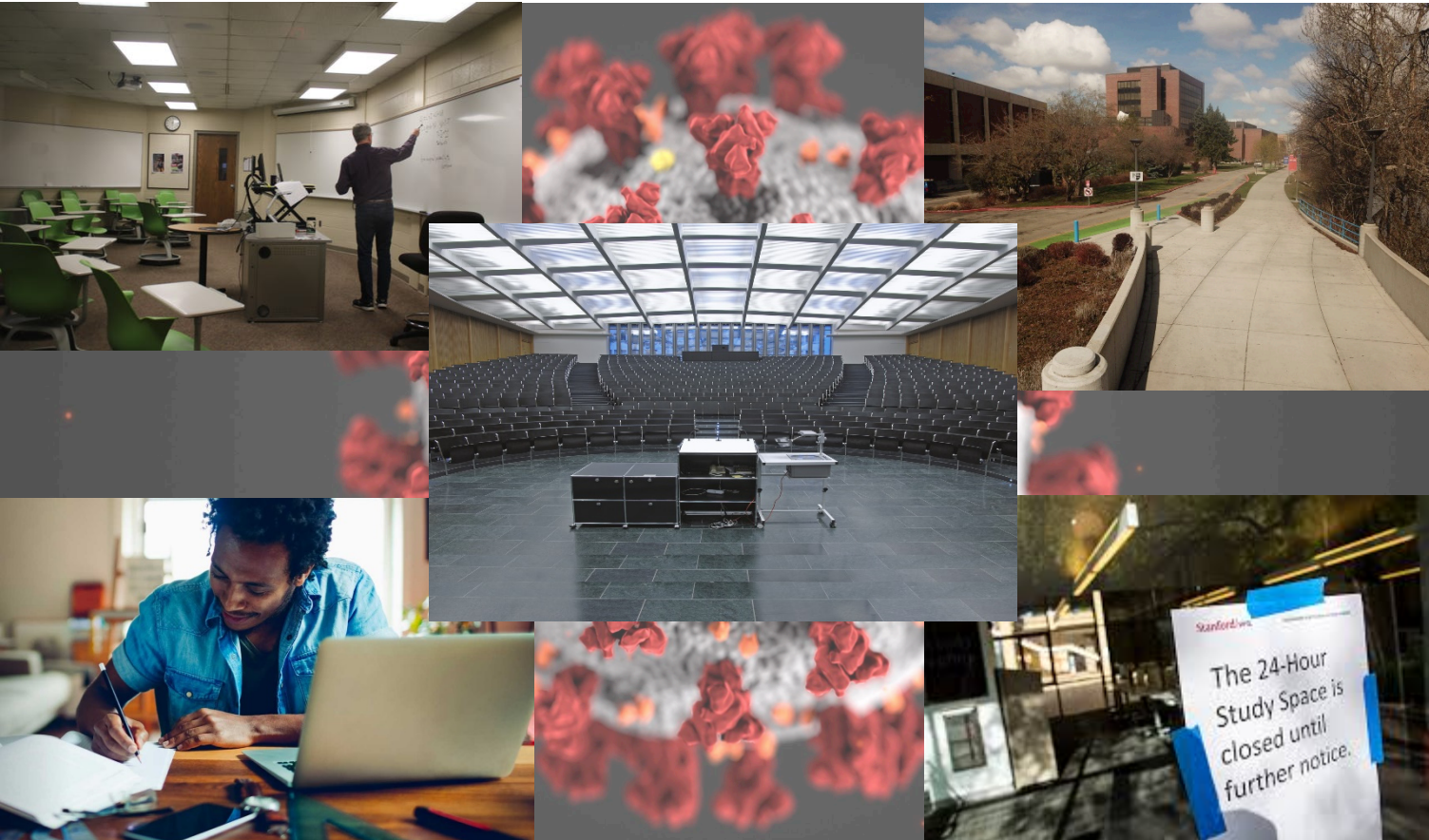


2020 Top 10 IT Issues

- ✓ **1. Information Security Strategy:** Developing a risk-based security strategy that effectively detects, responds to, and prevents security threats and challenges
- ✓ **2. Privacy:** Safeguarding institutional constituents' privacy rights and maintaining accountability for protecting all types of restricted data
- 3. Sustainable Funding:** Developing funding models that can maintain quality and accommodate both new needs and the growing use of IT services in an era of increasing budget constraints
- ✓ **4. Digital Integrations:** Ensuring system interoperability, scalability, and extensibility, as well as data integrity, security, standards, and governance, across multiple applications and platforms
- 5. Student-Centric Higher Education:** Creating a student-services ecosystem to support the entire student life cycle, from prospecting to enrollment, learning, job placement, alumni engagement, and continuing education
- 6. Student Retention and Completion:** Developing the capabilities and systems to incorporate artificial intelligence into student services to provide personalized, timely support
- 7. Improved Enrollment:** Using technology, data, and analytics to develop an inclusive and financially sustainable enrollment strategy to serve more and new learners by personalizing recruitment, enrollment, and learning experiences
- ✓ **8. Higher Education Affordability:** Aligning IT organizations, priorities, and resources with institutional priorities and resources to achieve a sustainable future
- ✓ **9. Administrative Simplification:** Applying user-centered design, process improvement, and system reengineering to reduce redundant or unnecessary efforts and improve end-user experiences
- ✓ **10. The Integrative CIO:** Repositioning or reinforcing the role of IT leadership as an integral strategic partner of institutional leadership in supporting institutional missions

Source: Educause Website, 2020, <https://www.educause.edu/research-and-publications/research/top-10-it-issues-technologies-and-trends/2020>

Has Coronavirus impacted your Top 10 IT Issues?



- ◆ An Information Security Strategy, including Data Privacy & Protection is more critical now than ever

What about WFH and Remote Learning security – is it currently in your program?

- ◆ Affordability is a heightened concern as economic models are disrupted

Are you faced with cutting costs even more than before?

- ◆ Digital Transformation is expedited to accommodate remote learning requirements

Did Digital Transformation initiatives such as remote learning become your highest priority?

SECURITY STRATEGY & ASSESSMENTS

*Does your Information Security Strategy Lower
your Risk and Improve your Security Posture?*

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

The ONEteam Strategic Plan

What if there was a way to ...



Get more from your existing security



Minimize security exposure



Ensure you are meeting compliance requirements



Test your Incident Response Plan



Prioritize initiatives based on actual Risk



Rationalize your cyber investments and demonstrate performance

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

ASSESSMENTS

How many assessments do you do per year to meet your Compliance and Privacy requirements?

Common Controls Framework (CCF)



Compliance

PCI-DSS

HIPAA

FERPA

GLBA

FISMA

Global and State Privacy Laws

Frameworks

NIST

ISO/IEC 27001,2

CIS

	CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4*	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	
1	Inventory of Authorized & Unauthorized Devices	CA-7 CM-8 SA-4 SC-17	IA-5 IA-5-3 PM-5 PL-DS-3	• HWNM: Hardware Asset Management	A.8.1.1 A.9.1.2 A.13.1.1	A.7.1.1 A.10.4.2 A.11.4.6	• Map Your N • Baseline Ma • Document N
2	Inventory of Authorized & Unauthorized Software	CA-7 CM-2 CM-8 CM-11 SC-18 SC-34	IA-5 IA-5-3 PM-5 PL-DS-4	• HWNM: Hardware Asset Management • SWNM: Software Asset Management	A.12.5.1 A.12.6.2		• Baseline Ma • Executable I • Configuration
3	Secure Configurations for Hardware & Software	CA-7 CM-2 CM-3 CM-5 CM-8 CM-9 CM-11 MA-4 MA-5 SC-15 SC-24 SC-34	PL-IP-1	• CDM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.1	A.15.2.2	• Patch Mana • Baseline Ma • Data-on-Net • Configuration
4	Continuous Vulnerability Assessment & Remediation	CA-2 CA-7 CM-5 CM-14 SC-14 SC-17	IA-5 IA-5-3 DE-DS-8 DE-DS-9 PM-3 PL-IP-12	• VUL: Vulnerability Management	A.12.6.1 A.14.2.8	A.12.6.1 A.13.1.2 A.15.2.2	• Patch Mana • Log Manage • Configuration
5	Controlled Use of Administrative Privileges	AC-2 AC-4 AC-17 AC-19 CA-7 SC-4 SC-14	PL-AC-4 PL-AC-2 PL-IP-3		A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	A.10.4.4 A.11.5.1 - A.11.5.3	• User Access • Baseline Ma • Log Manage
6	Maintenance, Monitoring, & Analysis of Audit Logs	AC-23 AC-24 AC-25 AC-26 AC-27 AC-28 AC-29 AC-30 AC-31 AC-32 AC-33 AC-34 AC-35 AC-36 AC-37 AC-38 AC-39 AC-40 AC-41 AC-42 AC-43 AC-44 AC-45 AC-46 AC-47 AC-48 AC-49 AC-50 AC-51 AC-52 AC-53 AC-54 AC-55 AC-56 AC-57 AC-58 AC-59 AC-60 AC-61 AC-62 AC-63 AC-64 AC-65 AC-66 AC-67 AC-68 AC-69 AC-70 AC-71 AC-72 AC-73 AC-74 AC-75 AC-76 AC-77 AC-78 AC-79 AC-80 AC-81 AC-82 AC-83 AC-84 AC-85 AC-86 AC-87 AC-88 AC-89 AC-90 AC-91 AC-92 AC-93 AC-94 AC-95 AC-96 AC-97 AC-98 AC-99 AC-100	PL-IP-1 PL-IP-2 PL-IP-3 PL-IP-4 PL-IP-5 PL-IP-6 PL-IP-7 PL-IP-8 PL-IP-9 PL-IP-10 PL-IP-11 PL-IP-12 PL-IP-13 PL-IP-14 PL-IP-15 PL-IP-16 PL-IP-17 PL-IP-18 PL-IP-19 PL-IP-20 PL-IP-21 PL-IP-22 PL-IP-23 PL-IP-24 PL-IP-25 PL-IP-26 PL-IP-27 PL-IP-28 PL-IP-29 PL-IP-30 PL-IP-31 PL-IP-32 PL-IP-33 PL-IP-34 PL-IP-35 PL-IP-36 PL-IP-37 PL-IP-38 PL-IP-39 PL-IP-40 PL-IP-41 PL-IP-42 PL-IP-43 PL-IP-44 PL-IP-45 PL-IP-46 PL-IP-47 PL-IP-48 PL-IP-49 PL-IP-50 PL-IP-51 PL-IP-52 PL-IP-53 PL-IP-54 PL-IP-55 PL-IP-56 PL-IP-57 PL-IP-58 PL-IP-59 PL-IP-60 PL-IP-61 PL-IP-62 PL-IP-63 PL-IP-64 PL-IP-65 PL-IP-66 PL-IP-67 PL-IP-68 PL-IP-69 PL-IP-70 PL-IP-71 PL-IP-72 PL-IP-73 PL-IP-74 PL-IP-75 PL-IP-76 PL-IP-77 PL-IP-78 PL-IP-79 PL-IP-80 PL-IP-81 PL-IP-82 PL-IP-83 PL-IP-84 PL-IP-85 PL-IP-86 PL-IP-87 PL-IP-88 PL-IP-89 PL-IP-90 PL-IP-91 PL-IP-92 PL-IP-93 PL-IP-94 PL-IP-95 PL-IP-96 PL-IP-97 PL-IP-98 PL-IP-99 PL-IP-100	• Generic Audit Monitoring	A.12.4.1 - A.12.4.4 A.12.7.1	A.10.10.1 - A.10.10.3 A.10.10.4	• Log Manage
7	Email & Web Browser Protections	CA-7 CM-2 CM-3 CM-5 CM-8 CM-9 CM-11 MA-4 MA-5 SC-15 SC-24 SC-34	PL-IP-1	• CDM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.1	A.15.2.2	• Patch Mana • Baseline Ma • Data-on-Net • Configuration
8	Malware Defenses	CA-7 CM-2 CM-3 CM-5 CM-8 CM-9 CM-11 MA-4 MA-5 SC-15 SC-24 SC-34	PL-IP-2 DE-DS-8 DE-DS-9 DE-DS-10		A.8.2.1 A.12.2.1 A.13.2.1	A.10.4.1 - A.10.4.2 A.10.7.1	• Device Accn • Virus Scans • Prevention I • Security Gnt • Firewalls
9	Limitation & Control of Network Ports	AC-1 AC-2 AC-3 AC-4 AC-5 AC-6 AC-7 AC-8 AC-9 AC-10 AC-11 AC-12 AC-13 AC-14 AC-15 AC-16 AC-17 AC-18 AC-19 AC-20 AC-21 AC-22 AC-23 AC-24 AC-25 AC-26 AC-27 AC-28 AC-29 AC-30 AC-31 AC-32 AC-33 AC-34 AC-35 AC-36 AC-37 AC-38 AC-39 AC-40 AC-41 AC-42 AC-43 AC-44 AC-45 AC-46 AC-47 AC-48 AC-49 AC-50 AC-51 AC-52 AC-53 AC-54 AC-55 AC-56 AC-57 AC-58 AC-59 AC-60 AC-61 AC-62 AC-63 AC-64 AC-65 AC-66 AC-67 AC-68 AC-69 AC-70 AC-71 AC-72 AC-73 AC-74 AC-75 AC-76 AC-77 AC-78 AC-79 AC-80 AC-81 AC-82 AC-83 AC-84 AC-85 AC-86 AC-87 AC-88 AC-89 AC-90 AC-91 AC-92 AC-93 AC-94 AC-95 AC-96 AC-97 AC-98 AC-99 AC-100	PL-AC-5 DE-AC-1	• Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.2 A.14.3.2	A.10.6.1 - A.10.6.2 A.11.4.4	• Baseline Ma • Configuration
10	Data Recovery Capability	CP-9 CP-10 HP-4	PL-IP-4		A.10.1.1 A.12.3.1	A.10.5.1 A.10.8.3	• Backup Sns
11	Secure Configurations for Network Devices	AC-4 CA-3 CA-7 CM-2 CM-3 CM-5 CM-8 CM-9 CM-11 MA-4 MA-5 SC-15 SC-24 SC-34	PL-AC-5 PL-IP-1 PL-IP-4	• CDM: Configuration Settings Management • Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.2	A.10.6.1 - A.10.6.2 A.11.4.5 A.11.4.7 A.11.5.1 - A.11.5.3	• Map Your N • Patch Mana • Baseline Ma • Document N
12	Secure Configurations for Network Devices	AC-4 CA-3 CA-7 CM-2 CM-3 CM-5 CM-8 CM-9 CM-11 MA-4 MA-5 SC-15 SC-24 SC-34	PL-AC-5 PL-IP-1 PL-IP-4	• CDM: Configuration Settings Management • Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.2	A.10.6.1 - A.10.6.2 A.11.4.5 A.11.4.7 A.11.5.1 - A.11.5.3	• Map Your N • Patch Mana • Baseline Ma • Document N

How do you prioritize your initiatives?



**Breach
Attack
Simulation**

Gain Continuous Visibility
into Your Security Posture

Prioritize Your Resources
and Responses

Remediate Your Security
Gaps



CYBER SECURITY SOLUTIONS

What problems are you trying to solve?

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.**”



A Holistic Approach to Cyber Security



ONEteam = TOTAL SOLUTION

Program + Technology + Operations



SOC as a Service / Managed Security Services

Core Security Services

- ◆ Managed Detect and Response (MDR) – *Included*
- ◆ Cyber Incident Response (CIR) / Forensics - *Included*
- ◆ Vulnerability Management–as-a–Service – *Included**
- ◆ Custom Reporting - *included*
- ◆ User Behavior Analysis (UBA) - *Light included / Enterprise Optional*
- ◆ Attack Simulation as a Service – *Included / Optional**

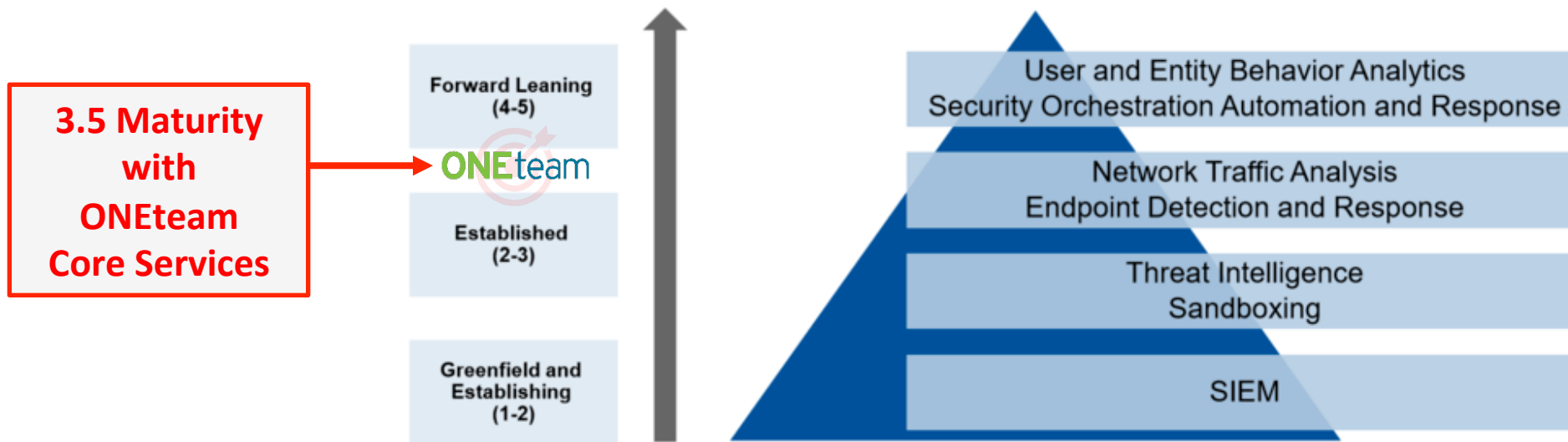
Add-On Services

- ◆ Security Awareness & Phishing as a Service – *Optional*
 - Facilitated / Automated Training
 - Facilitated / Automated Phishing
- ◆ Third Party Risk as a Service (TPRMaaS) – *Optional*
- ◆ Virtual Desktop Infrastructure (VDI) / Desktop as a Service - *Optional*
- ◆ Other Services depending on outcome of prioritized roadmap



Gartner Maturity Model

Modern SOC Analytics Tooling and Stage of Maturity



Remember: The maturity of the security analytics program does not correlate with the number of tools.

10 © 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Key to a Successful MDR/MSOC



24x7, Real-Time Threat Detection

Cybercriminals don't keep office hours. A security incident can unfold at any time. You need a 24x7 team of security analysts and engineers who monitor and triage alerts, and actively respond to indicators of compromise when they occur. You can't afford to wait for a report delivered to you hours or days later.



Threat Intelligence Integration

To reduce the risk of advanced threats, you need the latest threat intelligence from multiple sources. MDR solutions that integrate threat intelligence, as well as behavior analytics, are much better positioned to analyze data in the right context and to detect advanced, unknown threats.



Incident Response

The longer your dwell time, the more expensive your remediation becomes. The mean time to identify (MTTI) a breach is 197 days — but companies that identify a breach in fewer than 100 days can save \$1 million³. MDR providers include different degrees of incident response as part of their base fee, along with crisis support.



Threat Hunting

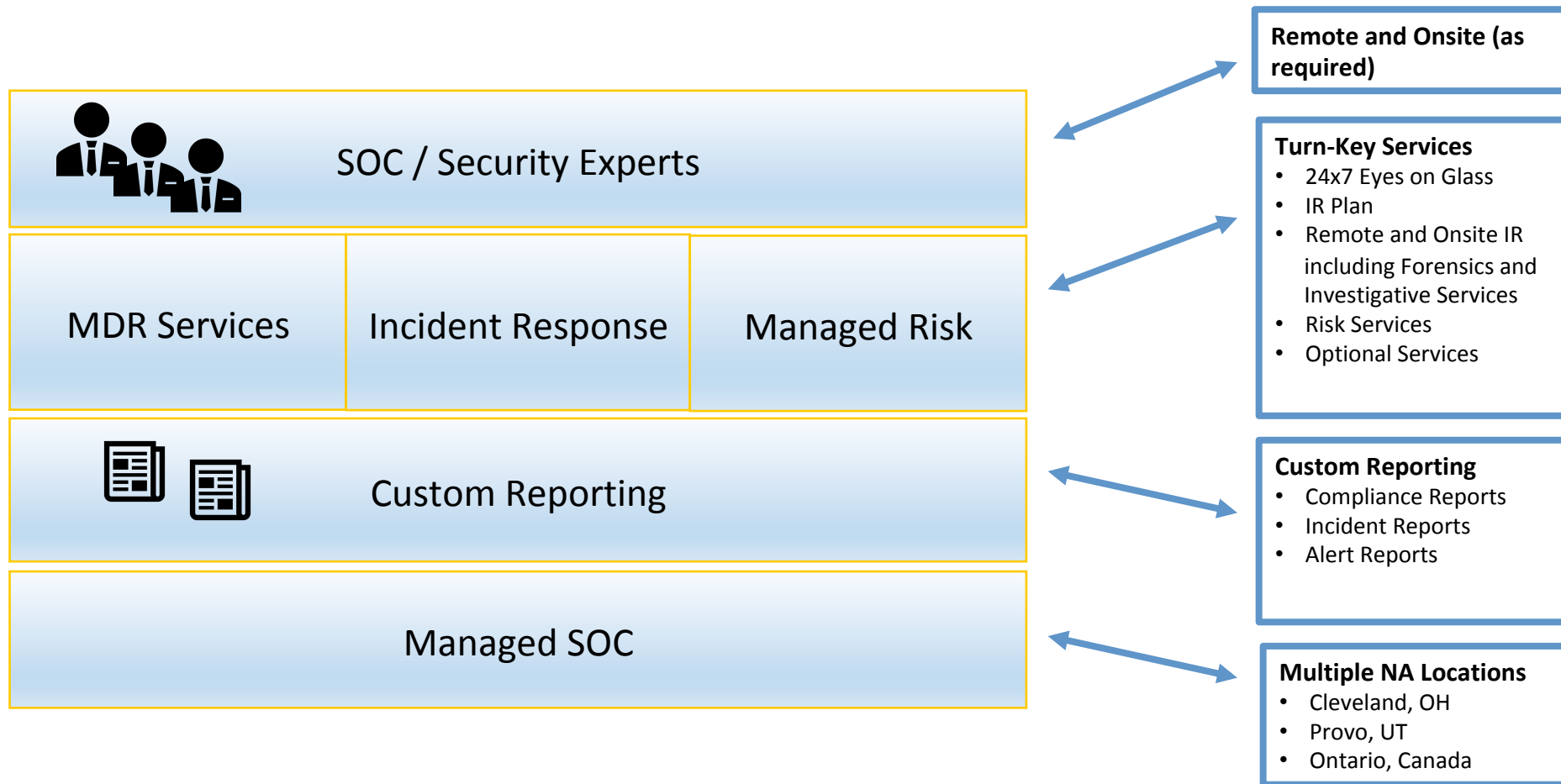
Defenses based on point-in-time scanning or signatures can no longer keep up with today's stealthy threats like fileless malware. Proactive threat hunting goes beyond scanning files when they enter your environment. Instead, it relies on a combination of automated tools and human analysts to track activity and identify suspicious behavior even as a threat evades perimeter or endpoint controls.



Advanced Analytics

Through leveraging machine learning, threat intelligence, and big data, advanced analytics is a critical MDR component that enables real-time threat detection. Top providers invest heavily in analytics platforms and other tools to analyze data in context, as well as correlate events across the entire environment.

ASMGi SOC as a Service = MDR / MSOC / MSSP



MDR / MSOC Services



Network Monitoring

Managed IDS, flow creation,
network security monitoring



Log Analysis & Search

Aggregation and correlation



Threat Intelligence

Multiple sources leveraged to
identify potential IOC or IOA



Cloud Monitoring

IaaS/SaaS configuration,
user/admin anomalies



Endpoint Visibility

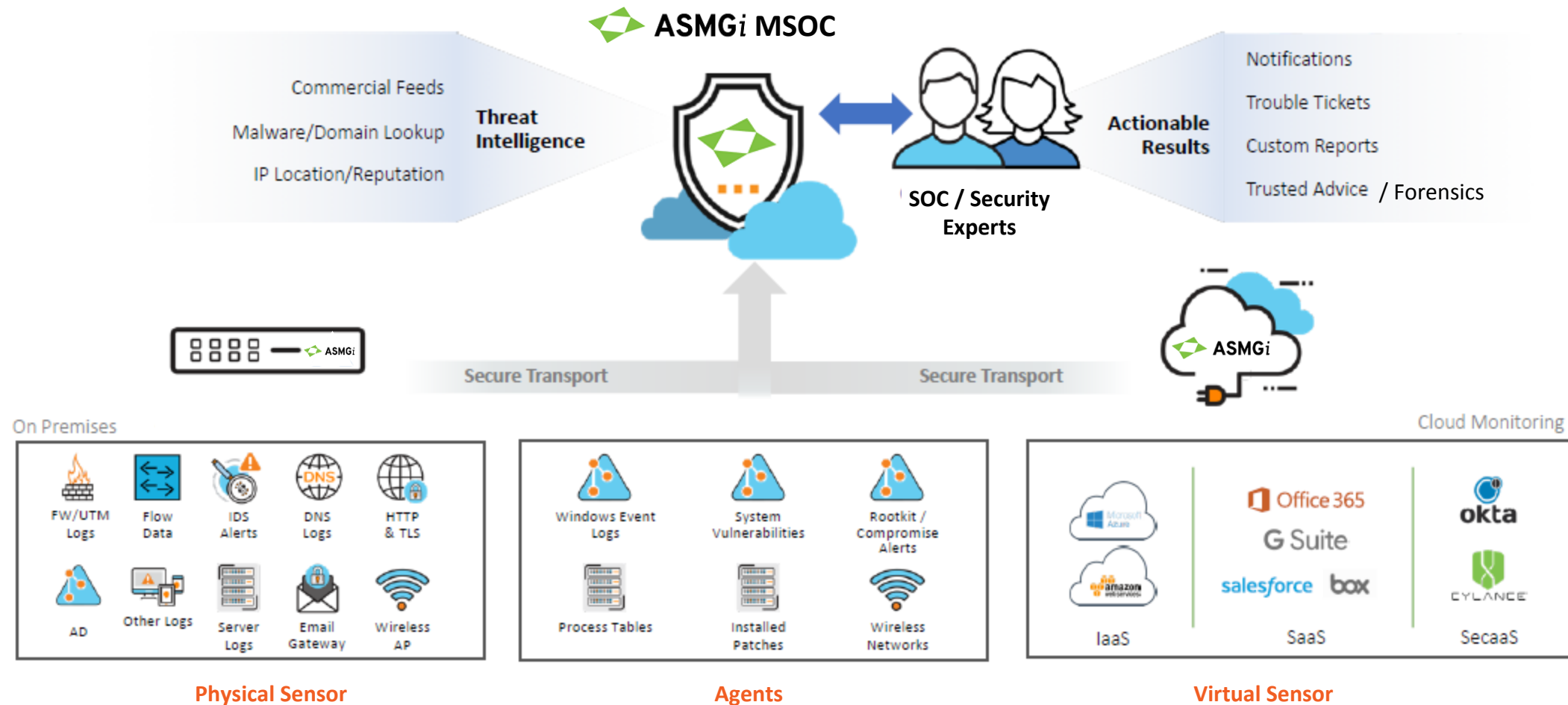
Asset data, EDR lite



Compliance

Reports and audit support

MDR / MSOC Architecture



List of Log Sources *

✓ Active Directory

- ▶ ADFS via NXLog
- ▶ NXLog
- ▶ NXLog-DNS

✓ Authentication

- ▶ Cisco RADIUS
- ▶ Okta

✓ Endpoint

- ▶ Arctic Wolf Agent
- ▶ Bit9
- ▶ Carbon Black Defense
- ▶ CylanceOPTICS
- ▶ CylancePROTECT
- ▶ Kaspersky
- ▶ OSSEC
- ▶ Palo Alto Networks Traps
- ▶ SentinelOne
- ▶ Sophos
- ▶ Symantec
- ▶ Trend Micro Control Manager
- ▶ Webroot

✓ Firewalls

- ▶ Barracuda CloudGen Firewall
- ▶ Check Point
- ▶ Cisco-ASA
- ▶ FireEye
- ▶ Fortinet FortiGate
- ▶ Juniper
- ▶ Meraki
- ▶ NeScreen
- ▶ Palo Alto Networks
- ▶ pfSense
- ▶ SonicWall
- ▶ Sophos XG
- ▶ Sorcefire
- ▶ Untangle
- ▶ Versa Networks
- ▶ WatchGuard Firefox

✓ IDS/IPS

- ▶ FireEye
- ▶ Sentinel

✓ Mail Servers

- ▶ Barracuda
- ▶ CommuniGate Pro
- ▶ McAfee

SaaS/IaaS

- ✓
 - ▶ AWS
 - ▶ Azure AD
 - ▶ Box
 - ▶ G Suite
 - ▶ Office 365
 - ▶ Microsoft Azure
 - ▶ Salesforce

✓ SSL-VPN

- ▶ Barracuda

✓ UTM

- ▶ Cisco WSA
- ▶ Sophos

✓ WAP

- ▶ Meraki
- ▶ Ubiquiti
- ▶ UniFi

✓ Web Gateways

- ▶ Barracuda
- ▶ Cisco Ironport
- ▶ Cisco Umbrella
- ▶ Citrix Netscaler
- ▶ EdgeWave iPrism
- ▶ Symantec ProxySG
- ▶ Websense
- ▶ Zscaler

✓ Others

- ▶ Darktrace
- ▶ Digital Guardian
- ▶ Microsoft Advanced Threat Analytics
- ▶ Microsoft Cloud App Security
- ▶ Microsoft SQL Server
- ▶ Pixier Scrutinizer
- ▶ Sailpoint
- ▶ Veronis

Cloud Services Monitoring



Virtual Sensors for Cloud Monitoring

Users, Apps, Data, Infrastructure Activity

IaaS	SaaS
Supported Platforms	Supported Platforms
AWS	Office 365
Azure	Salesforce
	Box
	G Suite
Supported Alerts	Supported Alerts
Suspicious resource usage, access, and deletions	Modified administrator settings
Changes to profiles and access	Administrator privilege escalation
Brute-force logins	Resources accessed or altered
Concurrent access	OAuth token and API access changes
Blacklisted IP sign-in	Group privacy or domain changes
Hijacked admin accounts	SSO configuration changes
	Anomalous login activity
	Brute-force logins
	Concurrent access across geos
	Compromised mobile device activity
	DLP violations
	Changes to file and folder permissions

Managed Risk Services



Asset Identification

Dynamic asset identification and classification



Comprehensive Risk Assessment

Identify vulnerabilities and provide a risk roll-up



Comprehensive Risk Profiling

Risk write-ups and recommendations



Monthly Risk Review

Discuss and validate progress tracking on vulnerabilities and asset classification



Incident Creation

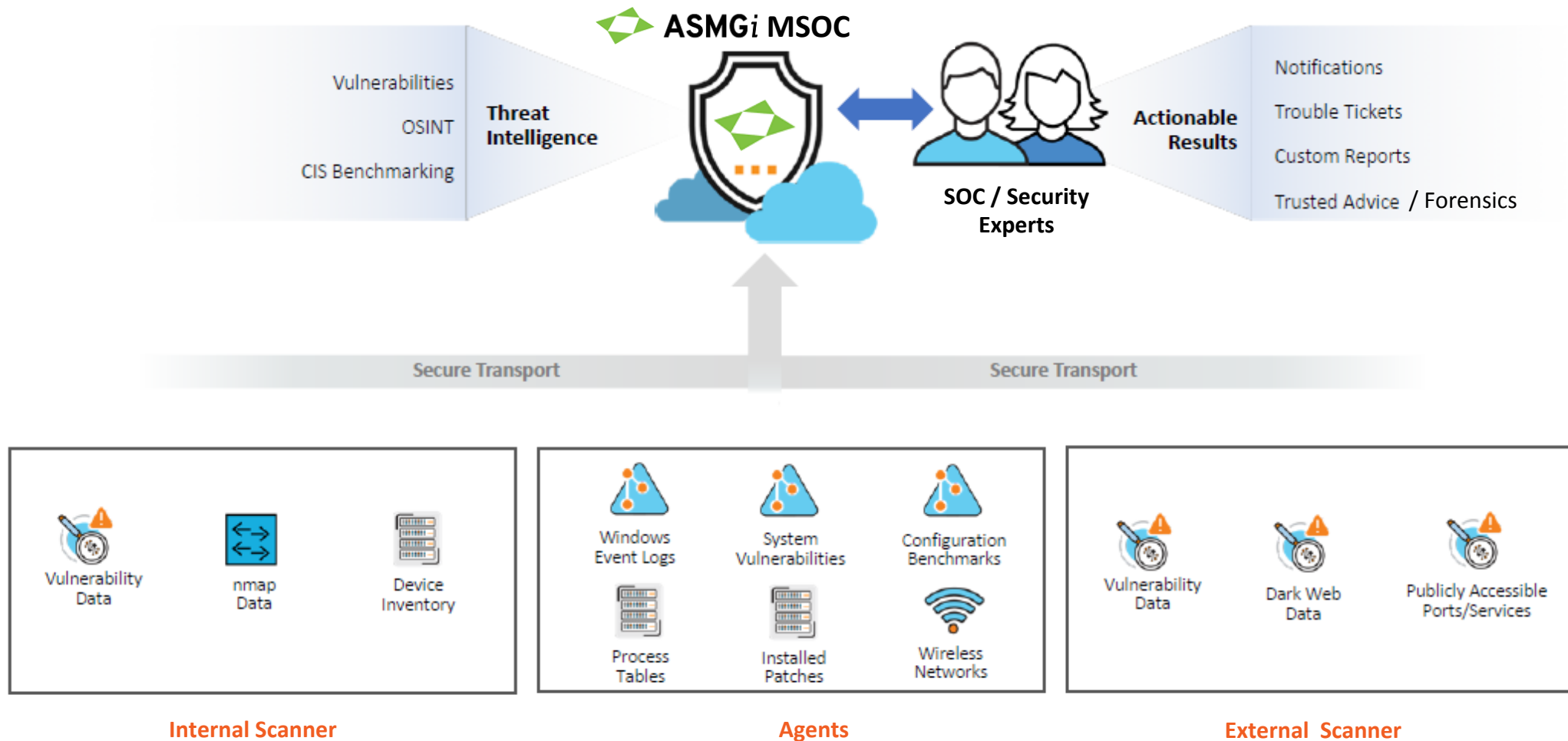
Generate incidents for critical vulnerabilities



Configuration and Monitoring

Scanner setup and monitoring to validate vulnerability scans are happening successfully

Managed Risk Architecture




Standard Reports

- Monthly Assessment
- Bi-Annual External Scan Report
- Weekly Security Review
- Weekly Summary of Events
- Weekly SaaS standard reports: O365, Salesforce, Box, Gsuite
- 12 Active Directory Reports



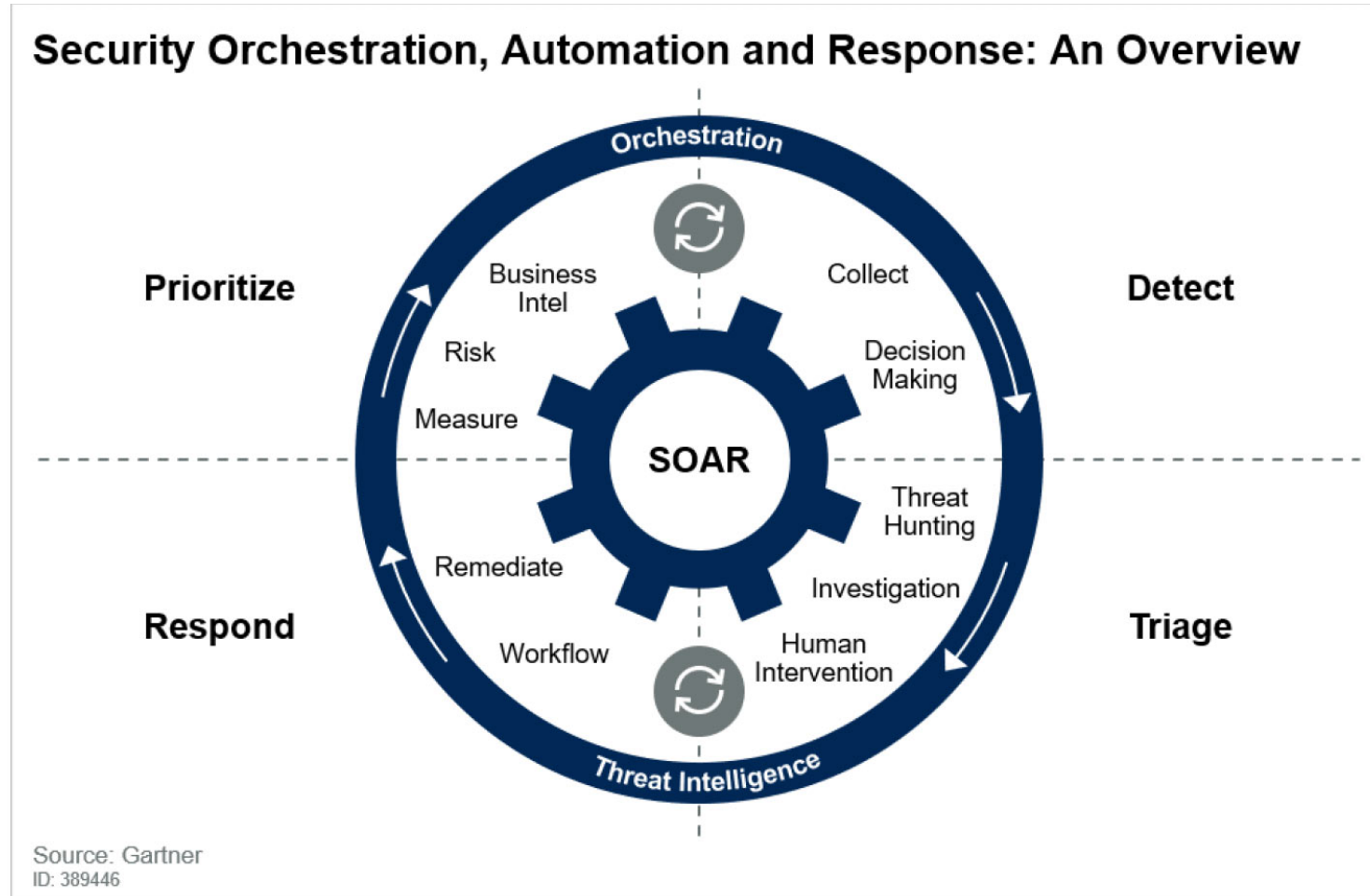
Active Directory Reports

- User Lock and Unlock
- User account creation & user account enabled
- User account termination
- Login Failures
- Login Success
- Member Add/Remove Global/Domain Group
- Member Add/Remove Local Group
- Event Log Cleared
- Account Policy Change
- Password Change
- Password Reset
- Directory Object Modification

 **ASMGi**
Active Directory
Active Directory Administrative Account Lockouts

Administrative accounts that have been locked out can be a sign of an attempted brute force attack against a privileged user or machines that have been left logged into with an administrative account for prolonged periods.

Last Seen	Account	Hostname	Domain	Attempts
2017-10-19 15:26:31Z	Administrator	DDO	W	2
2017-10-19 15:07:26Z	Administrator	DD	W	2
2017-10-18 11:32:39Z	Administrator	08-00000000	W	1
2017-10-16 18:05:19Z	Administrator	DD-L-CH	W	1
2017-10-22 05:37:15Z	Administrator	0000	W	1
2017-10-18 04:38:50Z	AdminU	0000ASP	W	1
2017-10-16 18:05:19Z	Administrator	41-CH	W	1
2017-10-16 19:04:58Z	Administrator	417-L-CH	W	1
2017-10-22 05:21:04Z	Administrator	SC0000	W	1



(SOAR)

- ◆ *Maximize Efficiency*
- ◆ *Economies of Scale*
- ◆ *Operational Excellence*
- ◆ *Built in Compliance*

Create an ecosystem with great Technology Partners



Conclusion + Key Points

- ◆ *Don't re-create the wheel –use what you already have*
- ◆ *Map controls to complete one assessment that meets all requirements*
- ◆ *Prioritize initiatives to improve security posture, lower risk and demonstrate return on investment*
- ◆ *There is strength in numbers! Let's work together to succeed!*

Key Value Delivered:

- ✓ Immediate Results - *Short time to value*
- ✓ Rationalized initiatives to lower risk and improve security posture
- ✓ Immediate maturity with Core Services
- ✓ No need for additional head count or expertise

ASMGi ONEteam Program – How to begin?



1

Assessment

- ◆ Controls mapping
- ◆ Simulation against controls
- ◆ Current State / Future State

2

Strategic Plan / Road Map

- ◆ 2-3 year plan (by year)
- ◆ Based on outcomes and priorities from Assessment
- ◆ Defines the program to be deployed and operationalized in Step

3

3

Tailored Program with a la carte components

- ◆ MDR/MSOC
- ◆ Attack Simulation
- ◆ TPRM
- ◆ Vulnerability Management
- ◆ MS Azure IaaS, PaaS, Security Suite, WVD

QUESTIONS / DISCUSSION

QUESTION: Upended The Model

- ◆ **Question:** Have you ever seen a change in program, technology or operations that ever substantially upended the model? Is that the value you can bring that if there is a technology change or a better technology that evolves you can operationalize it at a lower cost point and no disruption of services.
- ◆ **Answer:** Part of the world that we collectively live in requires the ability to adapt to changes based on changing business, organizational, technology, or security / threat profile changes. These changes can happen very quickly, most recently as exemplified by COVID-19, or over a longer period of time such as an adoption of technology like public clouds. The value of adopting a service like those proposed by ASMGi is the ability to evolve over time based on ASMGi's ability to anticipate change as its' client base evolves and interaction with our strategic business partners to be prepared for change whenever it happens. The ultimate goal is to prepare for these changes based on a plan and to optimize the value that is delivered in a cost effective but fully comprehensive manner.

QUESTION: Plug and Play

- ◆ **Question:** Can you plug and play if we already have specific tech in place into the architecture tools you are describing?
- ◆ **Answer:** Yes, the overall program and service offering has been structured to leverage the investment that may have already been made in hardware or software solutions if they are meeting the business and security requirements. The development of the specific solution and offering is based on assessing an organization's current state to determine what specific solutions exist today in your environment and to determine whether they can be leveraged and integrated into the ASMGi operating model.



ONETeam

Thank You!

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com