ARCTIC WOLF

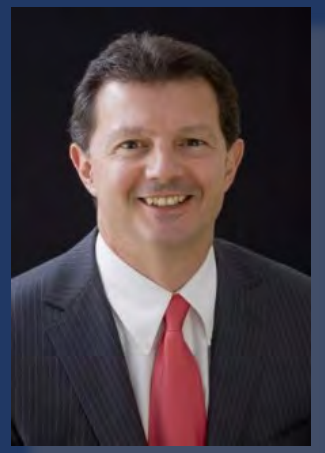
ASMGi ONEteam

How to Stop Cyber Attacks with Modern MDR and Managed SOC

March 4, 2021

How to Stop Cyber Attacks with Modern MDR and Managed SOC

Dmitriy Sandler
Director of Presales Engineering
Arctic Wolf



Steve Roesing
President, CEO
ASMGi

ARCTIC WOLF

ASMGi
ONEteam

Upcoming ASMGi Cyber Security Webinars with Arctic Wolf

Managing Cyber Risk - Don’t be careless about your exposure to cyber-attacks!
presented by ASMGi and Arctic Wolf Networks
live webinar, ***March 25 at 1PM ET***

Don't Let Your Cloud Security Fall Behind
presented by ASMGi and Arctic Wolf Networks
live webinar, ***April 8 at 1PM ET***

*Reply “**YES**” in the Question Box and we will preregister you for both of these webinars*

ASMGi

ARCTIC WOLF

Agenda

- *Cyber Security has a Problem!*
- *Some Quick Facts About Attacks*
- *Can't do MDR without a SOC!*
- *What is Special About Arctic Wolf?*
- *What is ASMGi's* ONEteam MDR/MSOC *plus and how does it protect me?*
- *Key Takeaways*
- *Q & A*

CYBER SECURITY SOLUTIONS

IS There a Problem with Security?

Is There a Problem?

ARCTIC WOLF

ASMGi
ONEteam

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.

Finding The Right Approach

1990s

Antivirus + Firewall

2000s

Next Gen Tools

2010s

Security Platforms

Now

Security Operations

Why are Cyber Security Operations critical?

ARCTIC WOLF

ASMGi ONEteam

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

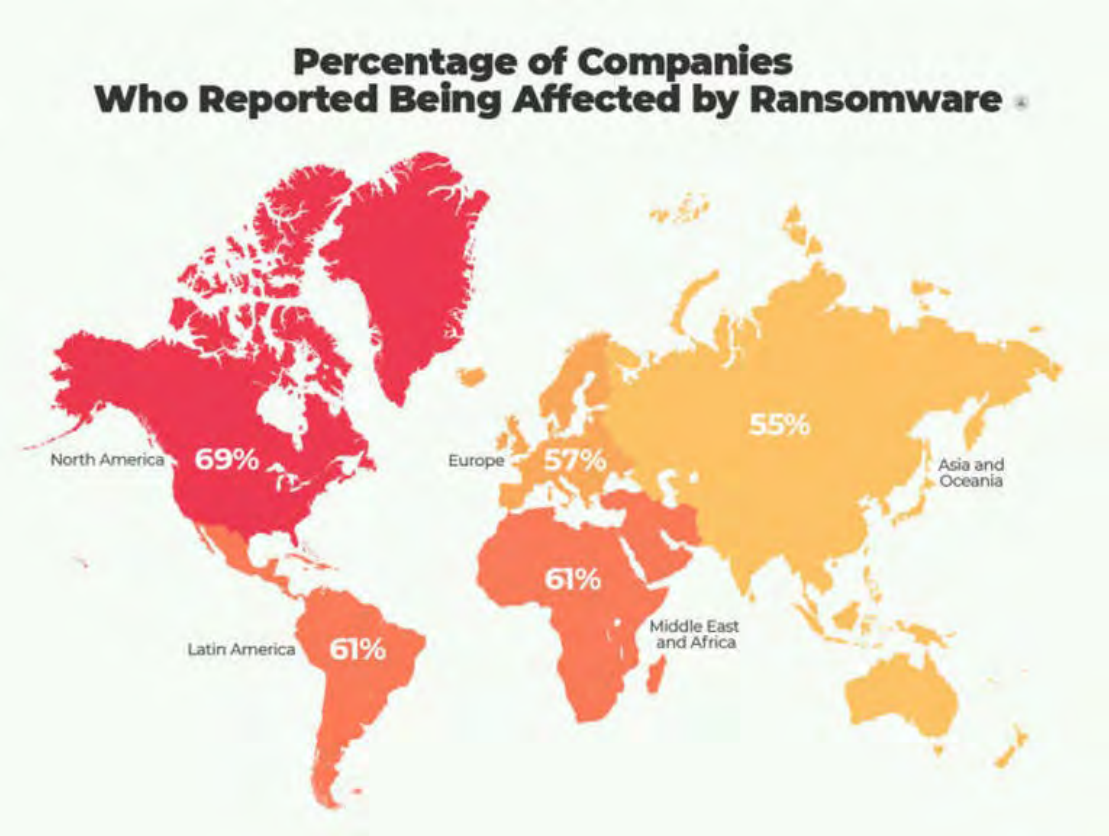
Misconfiguration in cloud service went unnoticed despite availability of monitoring products.

June 2020

Control Systems Targeted Shutting Down Production In Honda Breach

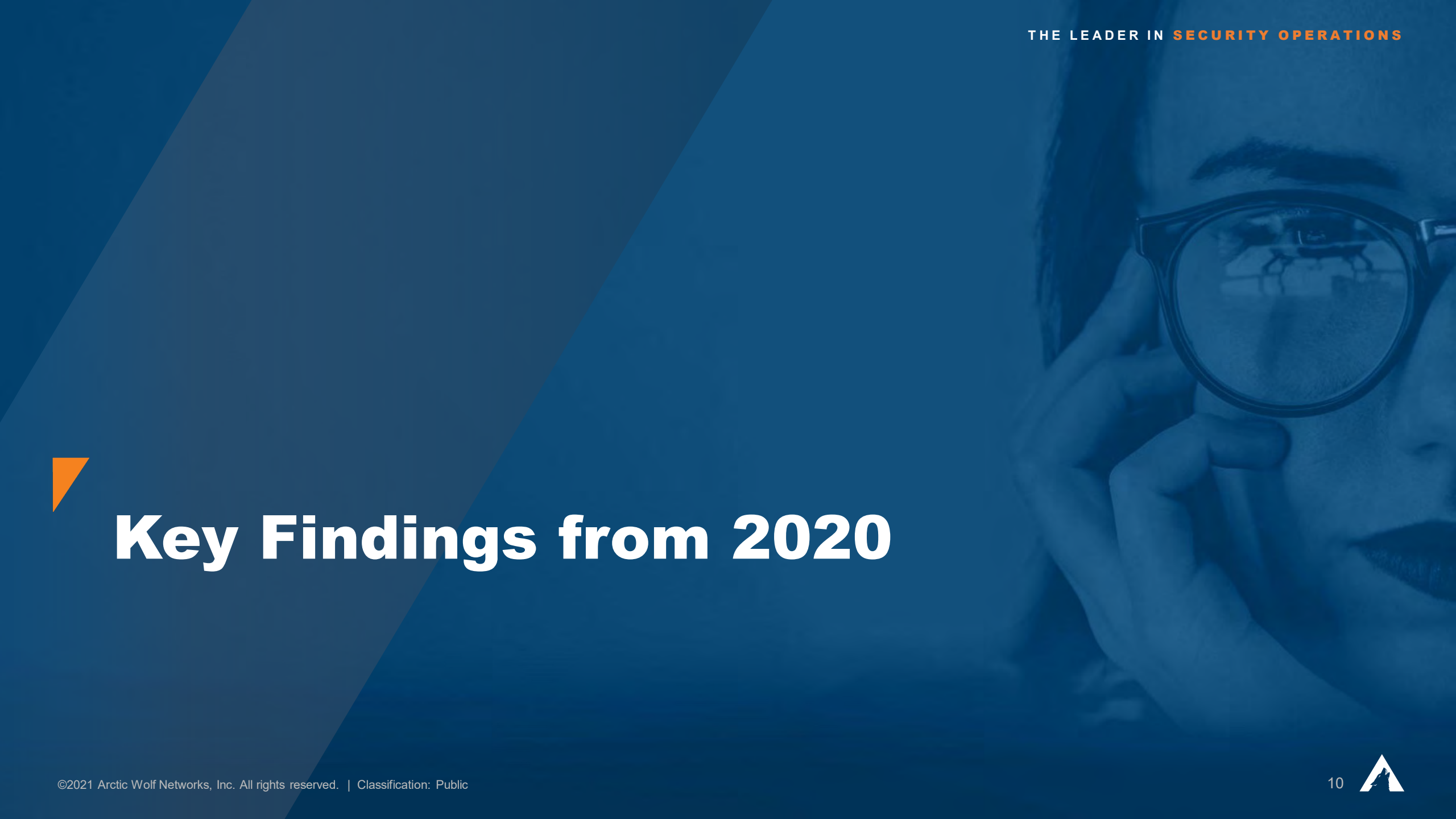
Attack focused on control systems, in the production line

Ransomware: Is It Still a Thing?



"By 2021, a ransomware attack is expected to take place every 11 seconds .."

That's 7,855 attacks per day!

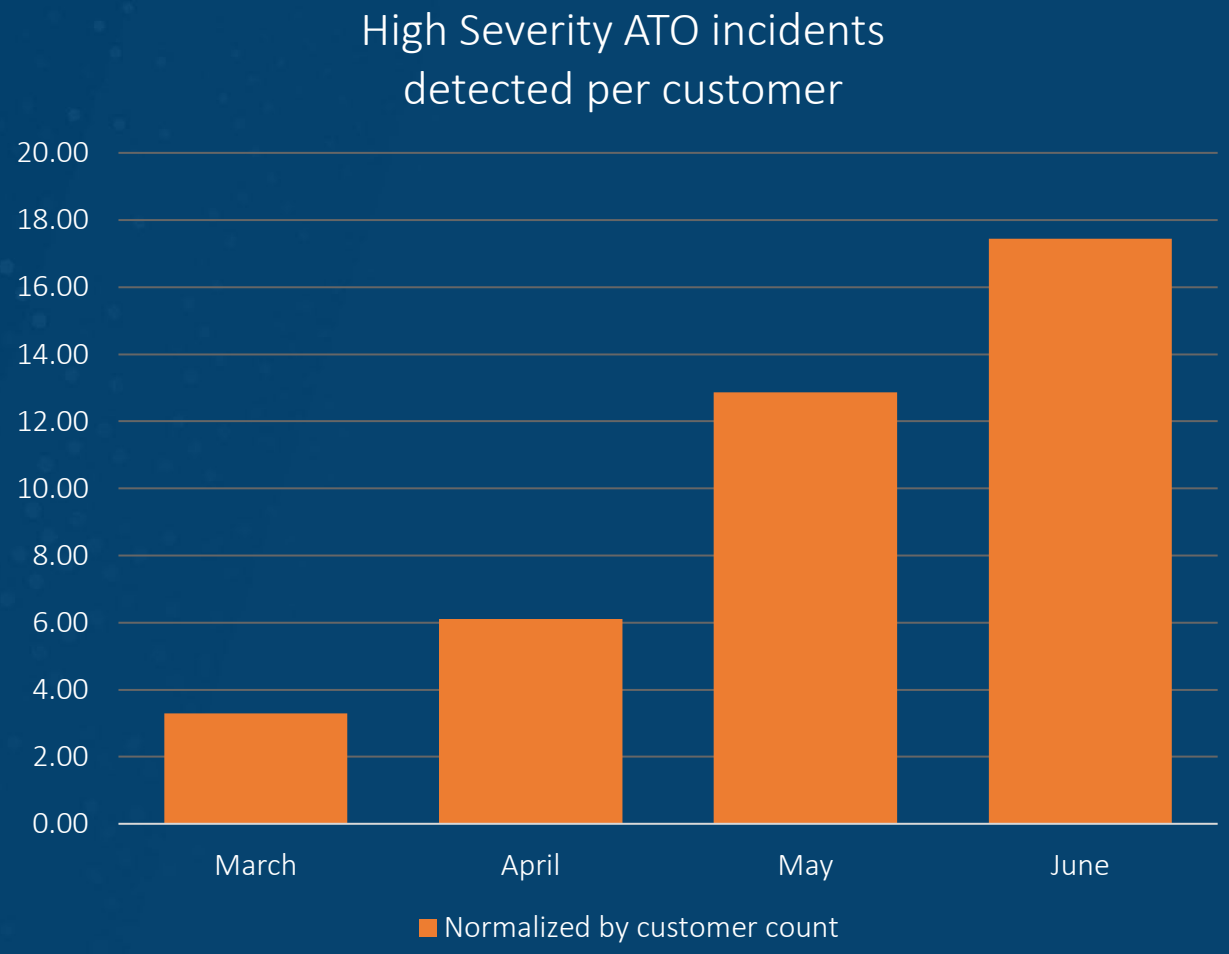


Key Findings from 2020

Shining a Spotlight On The Dark Web

429%

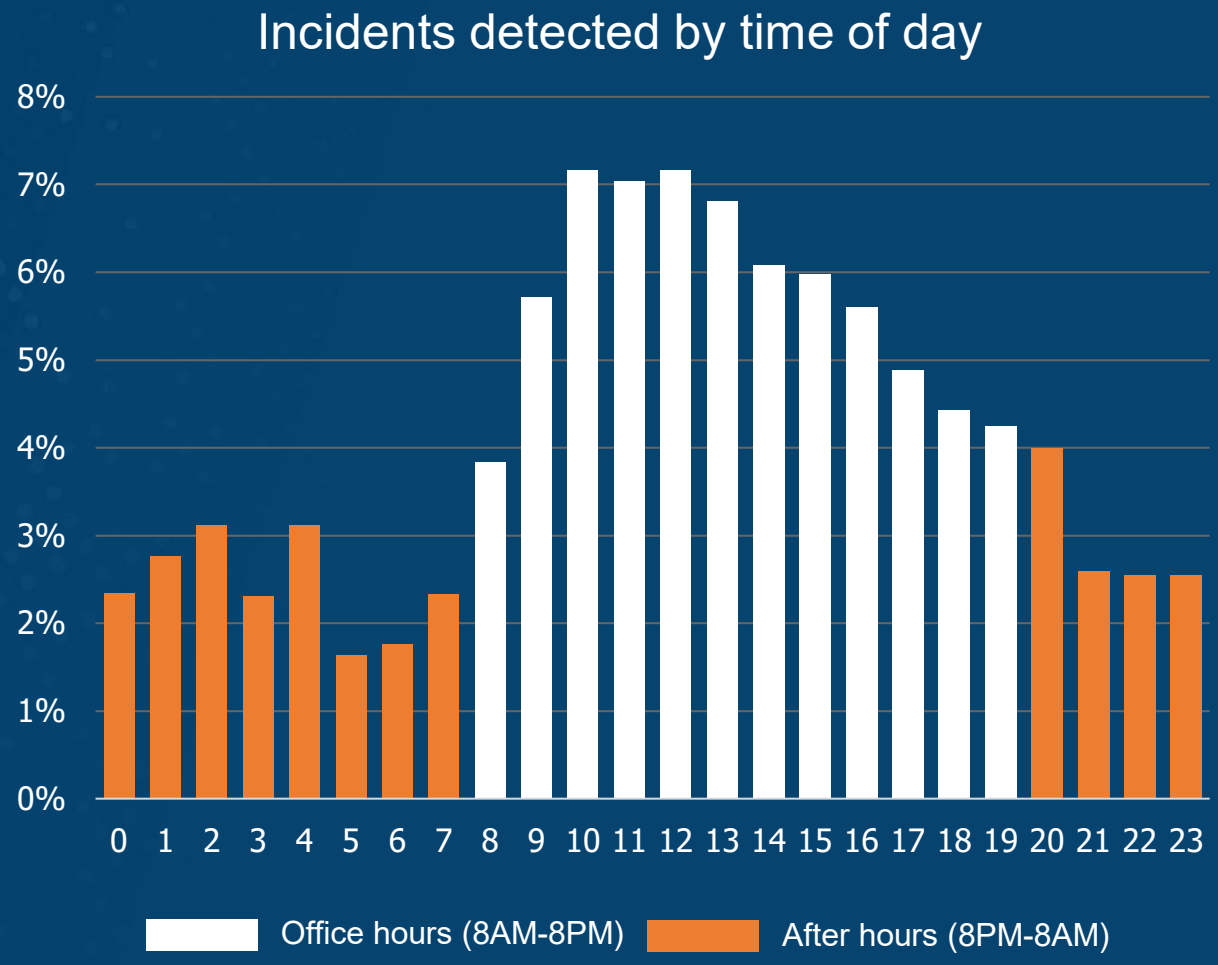
- Account takeover incidents detected (Where PII has found exposed on the dark web) have increased by 429% since March.



Nocturnal Attackers

8PM to 8AM

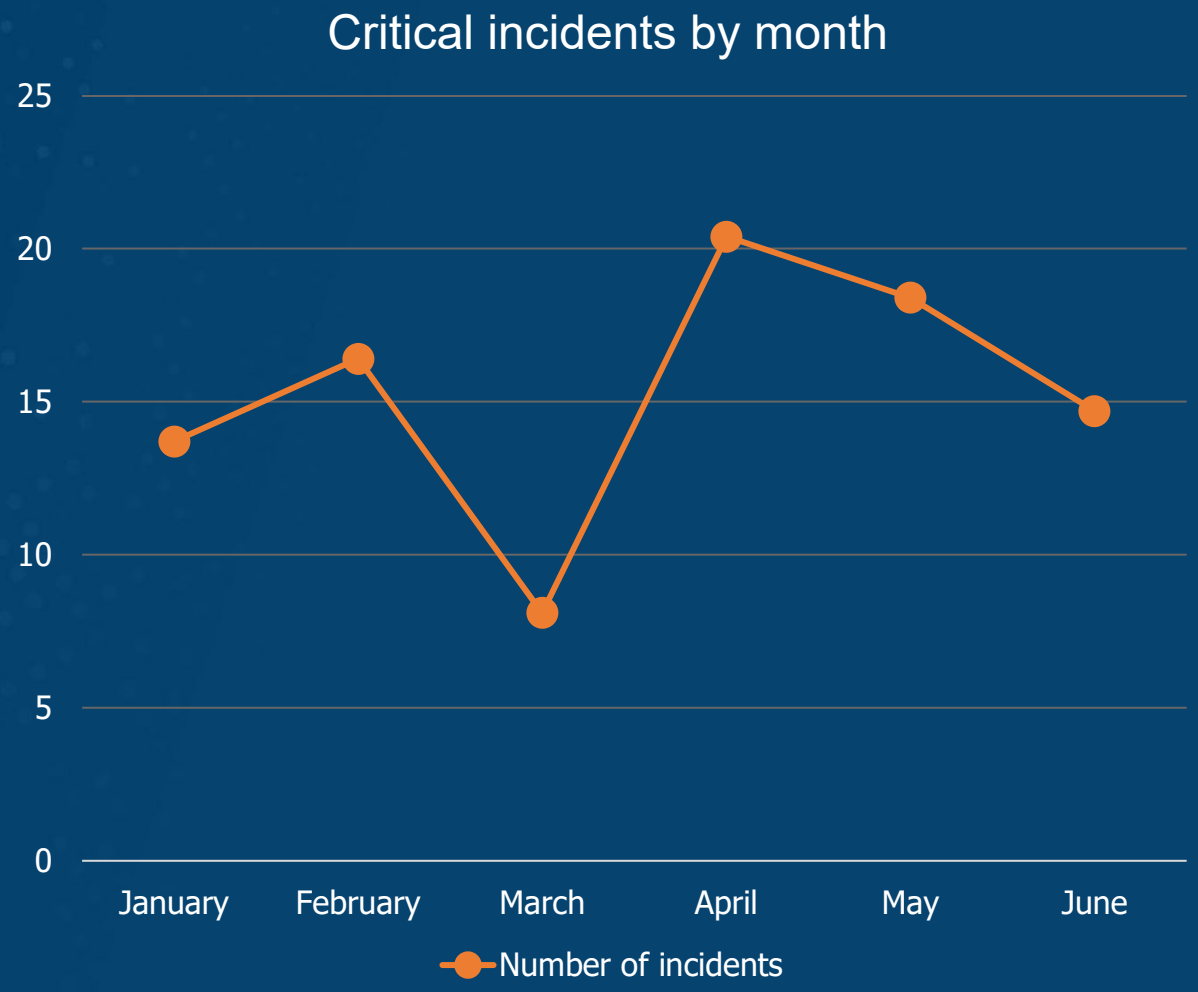
- In Q2, 2020, of all the threats detected by our Concierge Security Team, 35 percent of them happened between the hours of 8 PM and 8 AM.



Phishing With Ransomware

64%

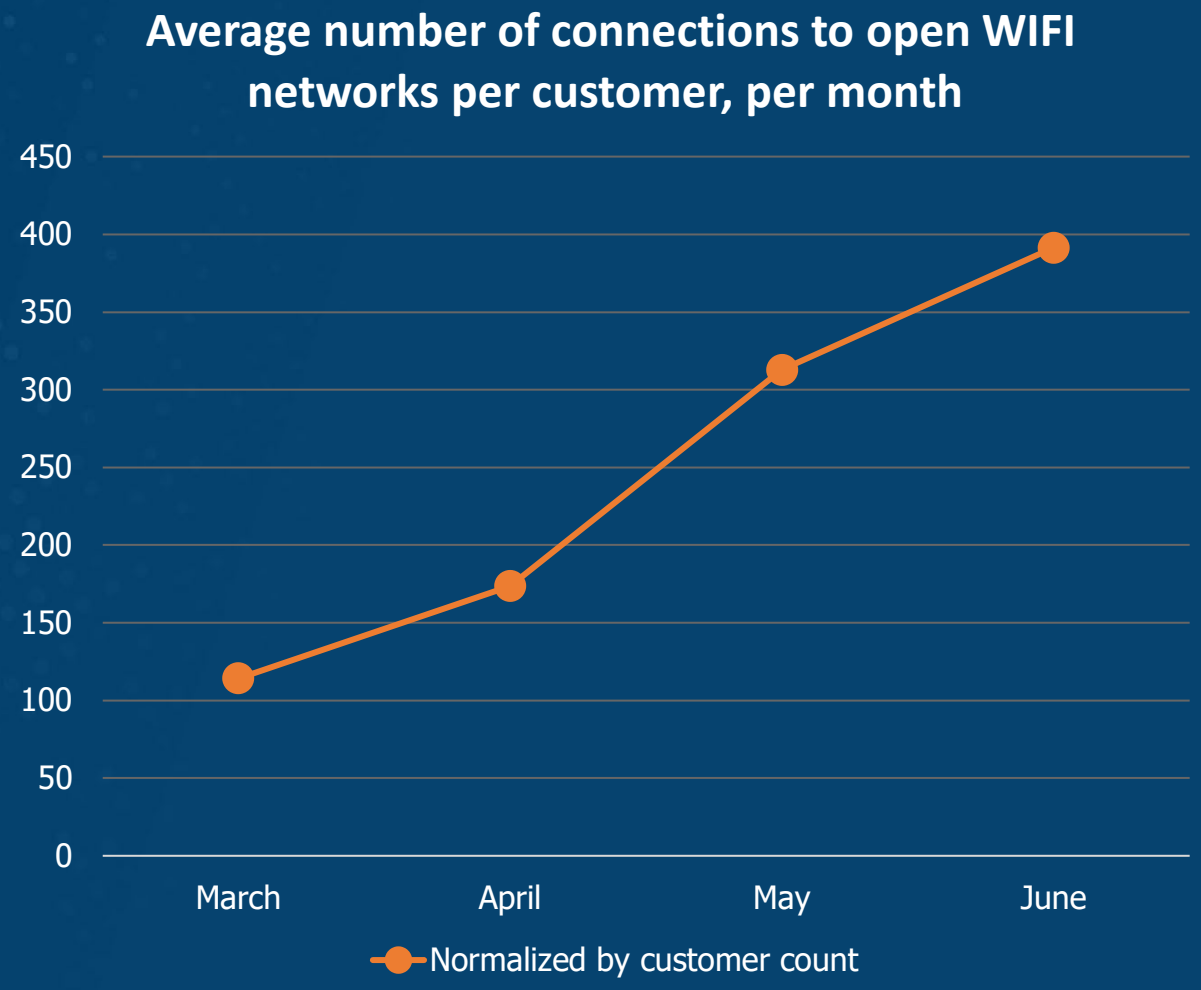
- In Q2, 2020, critical threats such as ransomware and phishing attempts increased by 64% over Q1, 2020.



Unsecured WIFI Networks Leave The Door Open

243% ⬆

- The total number of connections to open and unsecured WIFI networks has increased by 243% since March.



SIM? SEM? SIEM? HUH?

ARCTIC WOLF

ASMGi ONEteam

Some Definitions:

- **Security Information Management (SIM) – Long-term storage as well as analysis and reporting of log data**
- **Security Event Manager (SEM) – Real-time monitoring, correlation of events, notifications and console views.**
- **Security information and event management (SIEM) – Combines SIM and SEM and provides real-time analysis of security alerts generated by network hardware and applications.**

What do socks have to do with anything?

ARCTIC WOLF

ASMGi ONEteam

Security Operations Center (SOC) – A centralized function within an organization employing *people, processes, and technology* to *continuously* monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

A SOC acts like the hub or central command post, taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside. The proliferation of advanced threats places a premium on collecting context from diverse sources. Essentially, the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and acted upon.

Lots of Acronyms!

ARCTIC WOLF

ASMGi ONEteam

MDR

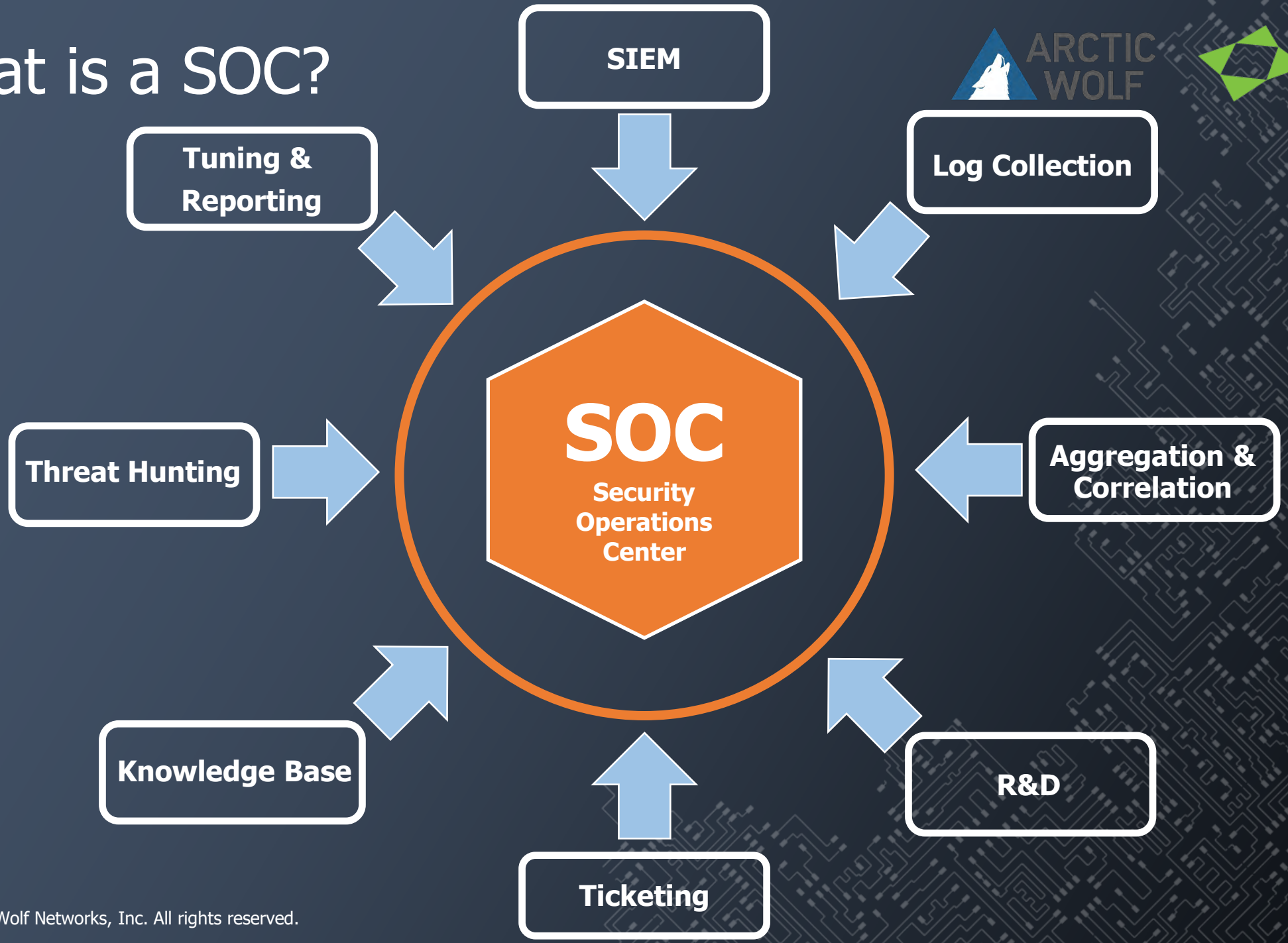
SIEM

SOC-as-a-Service

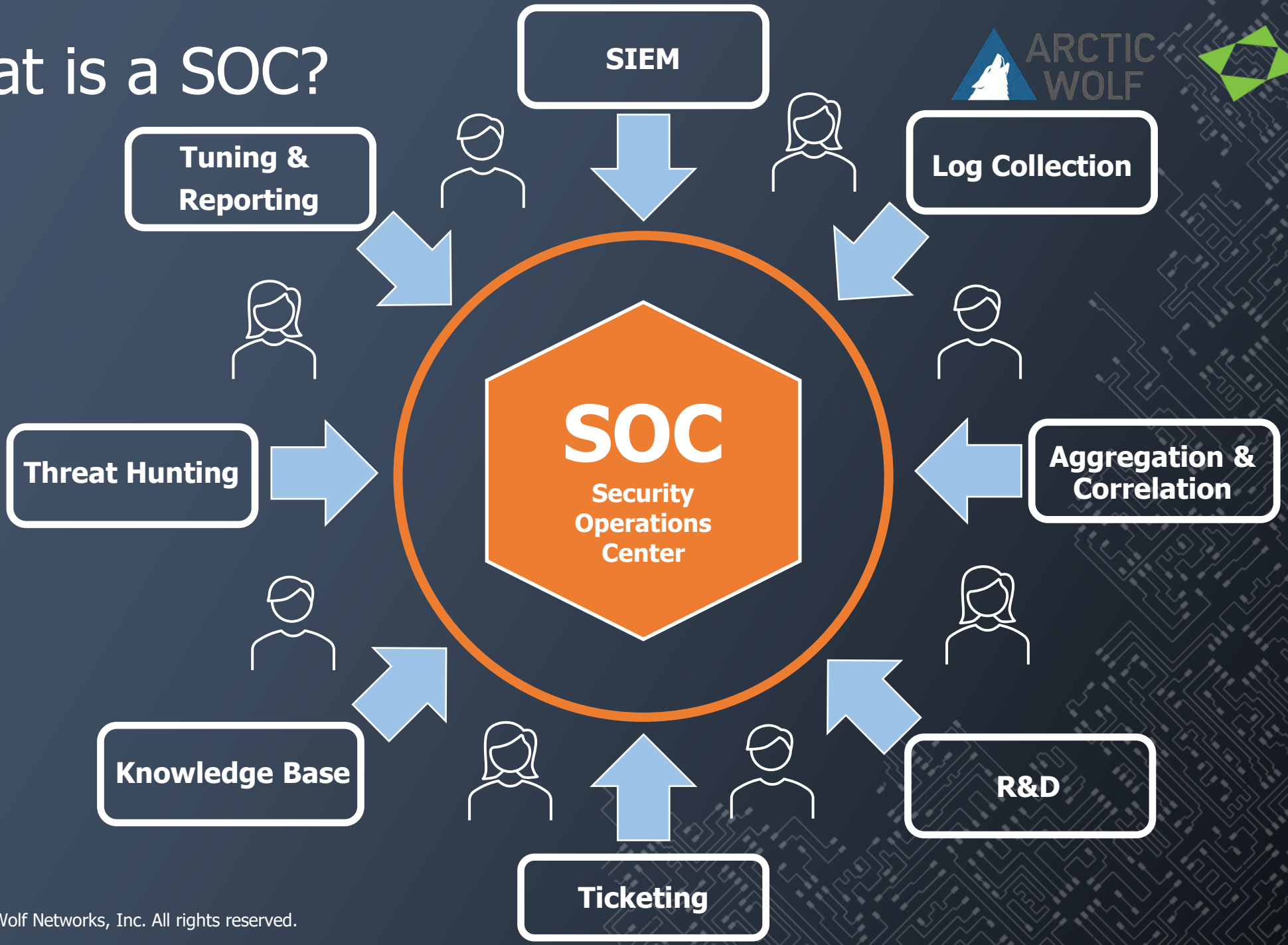
EDR

Managed SOC

What is a SOC?



What is a SOC?



Managed Detection and Response (MDR) - Architecture

Arctic Wolf Security Operations

- Internal Threat Intel and Ruleset
- Commercial Threat Feeds
- Gov't & Industry-specific Threat Intel
- IP Reputation and Geolocation data

Security Intelligence

Scalable Backend

Concierge Security Team (CST)

Personal Protection

- Alert Triage and Prioritization
- Guided Remediation
- Custom Rules and Reports
- Audit Support
- Strategic security posture reviews

Secure Transport

On-Premises Sensor Appliance

Network IDS and Log Aggregation

- Flow Data
- FW/UTM Logs
- AV/ EDR Alerts
- Active Directory
- DNS Logs
- Web Gateway
- Wireless Access
- Server Logs
- Email Gateway
- Other syslog

Endpoint Agent

Threat Detection for Windows, Mac, and Linux

- Managed Containment
- Asset Information
- USB Devices
- Process Tables
- Logs
- Network Information

Cloud Connectors

API-based monitoring for misconfigurations and attacks

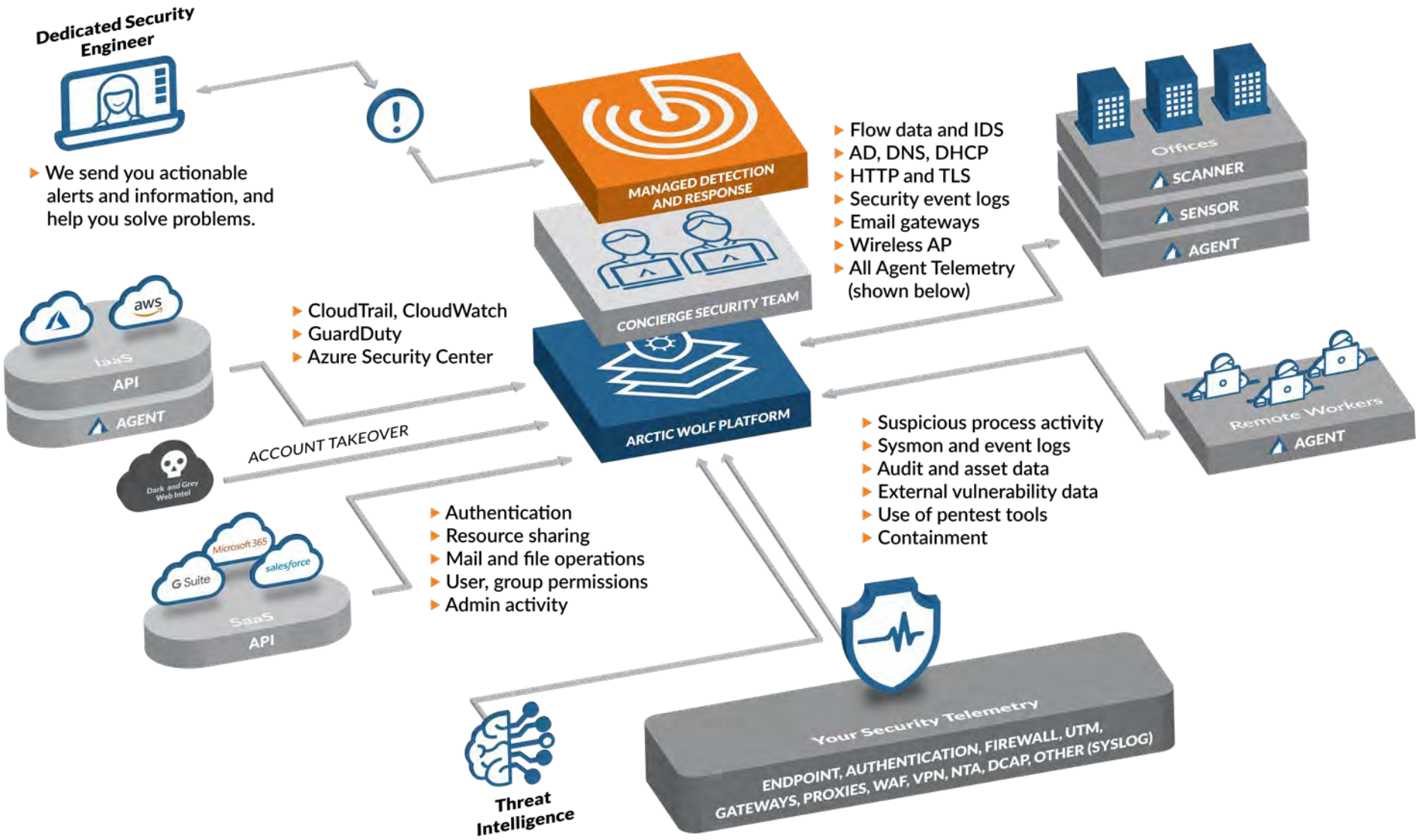
Cloud Logs: WEBROOT an opentext company, CYLANCE, CROWDSTRIKE, Cisco Umbrella, okta

IaaS: Azure, aws

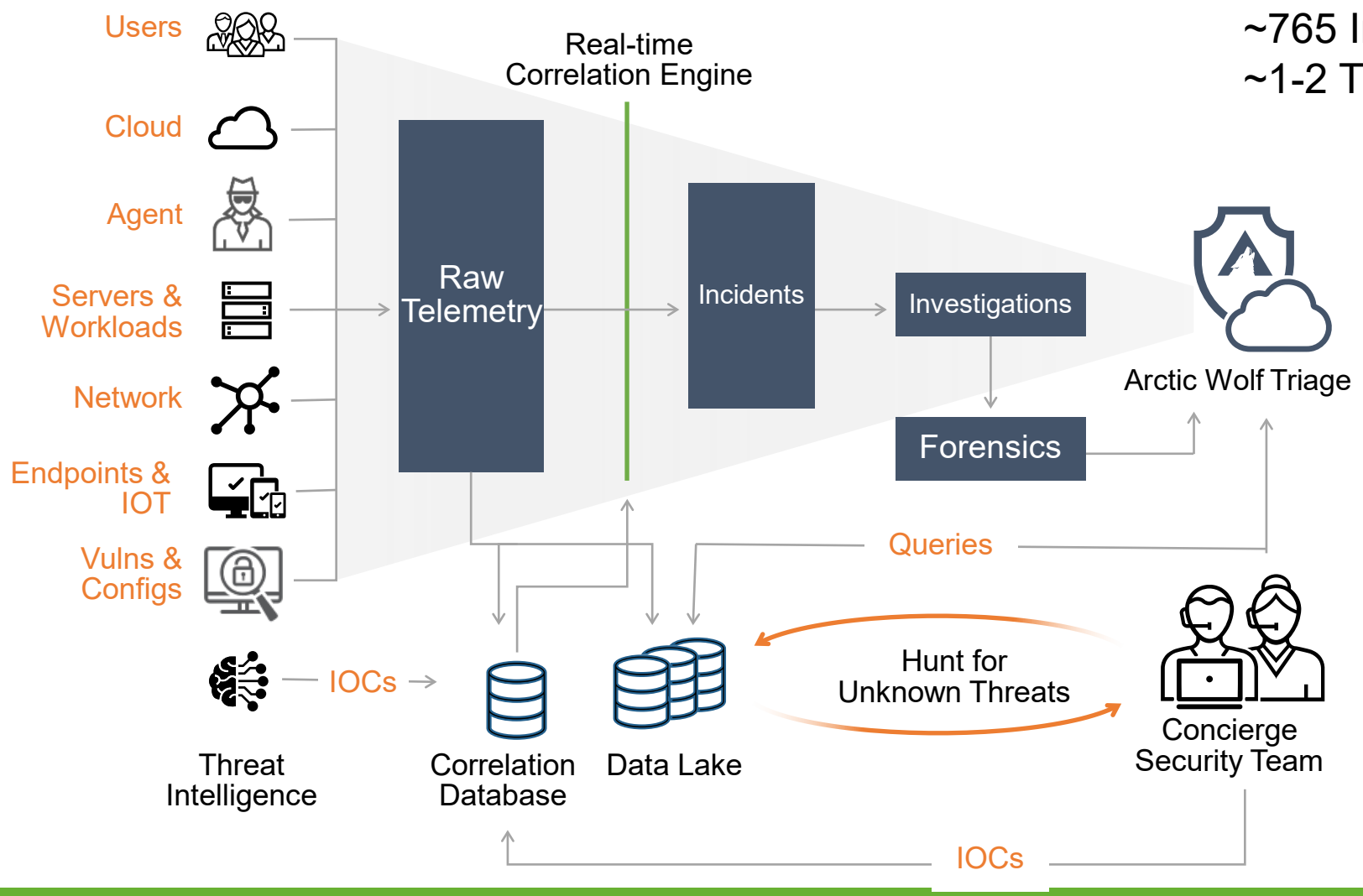
SaaS: Office 365, box, G Suite, salesforce

Classification: Public

Managed Detection and Response Architecture



Arctic Wolf 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

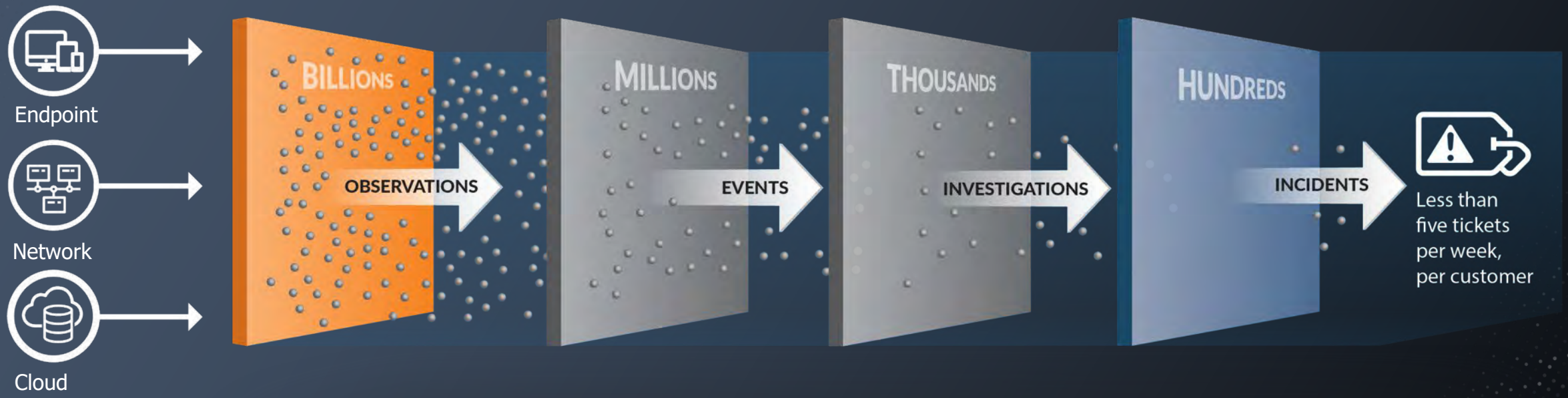
- Hunt for Advanced threats across endpoints, network and Cloud with deep analytics and human expertise
- Security Journey program to improve overall security posture

The End of Alert Fatigue

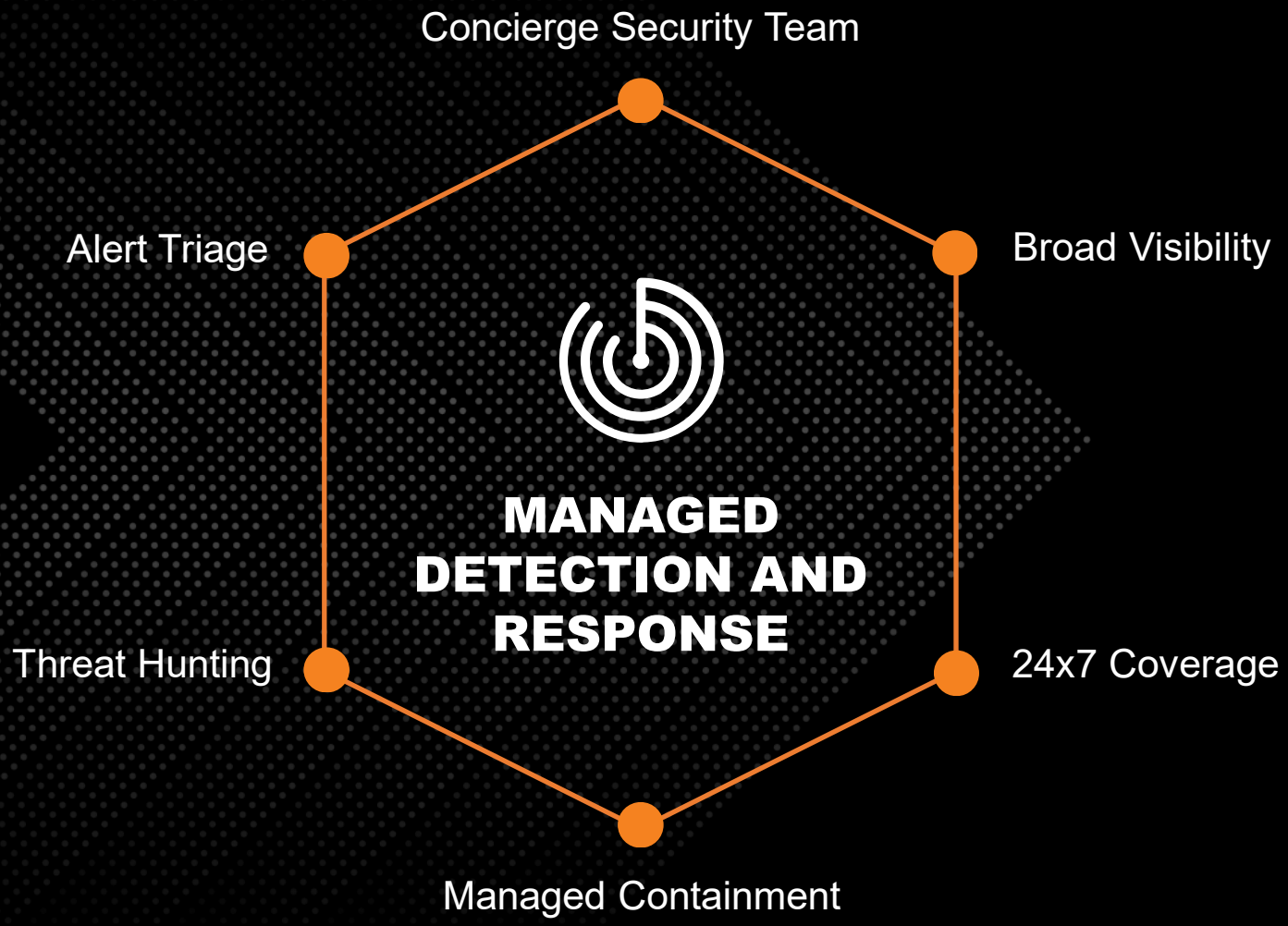
ARCTIC WOLF

ASMGi ONEteam

Observation of more than 100 billion events per day yields an average of <5 validated incidents with precise remediation per week.



Arctic Wolf Solutions



ARCTIC WOLF

ASMGi ONEteam

Detect

Leverage your existing tech stack to identify advanced network, endpoint, and cloud threats

Respond

24x7 coverage and guided response stops threats before they can do harm

Recover

Find root cause, validate remediation, and collaborate to continuously improve your overall security posture

70%

Of new customer environments have latent threats

Better Protection Against All Attack Types

Dwell Time

0:30

Industry average time to identify an intrusion is 206 days. Arctic Wolf does it in 30 minutes or less.

Phishing

18%

Of customers have phishing activity that is missed by email security but caught by Arctic Wolf

Advanced Threats

43%

Of customers have advanced threat activity being missed by security tools but caught by Arctic Wolf

Account Takeover

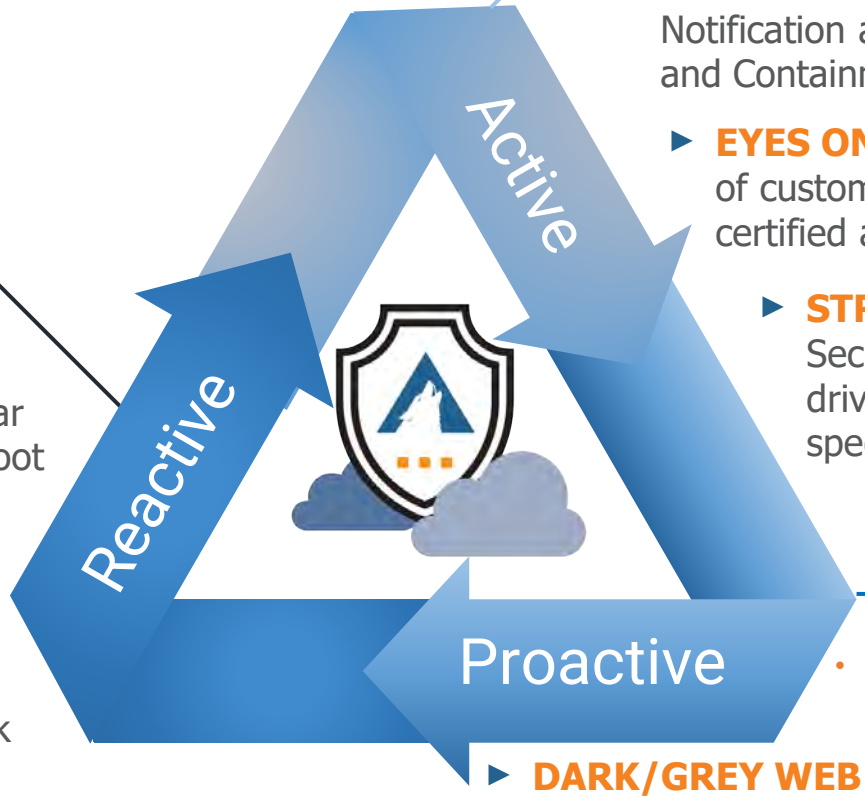
70%

Of customers have some PII exposure and 5.5% have plaintext passwords exposed online

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** 2 Person, Named Concierge Security Team providing Security guidance, 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

SOC 2 TYPE 2 · ISO 27001 · NIST Cybersecurity Framework (Protect, Detect, Respond, Recover, Identify) · Privacy Shield Compliant · GDPR READY

What is ONEteam MDR/MSOC *plus*?

ARCTIC WOLF + ASMGi

= ONEteam MDR/MSOC *plus*

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:

ARCTIC WOLF

ASMGi

ONEteam

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)	

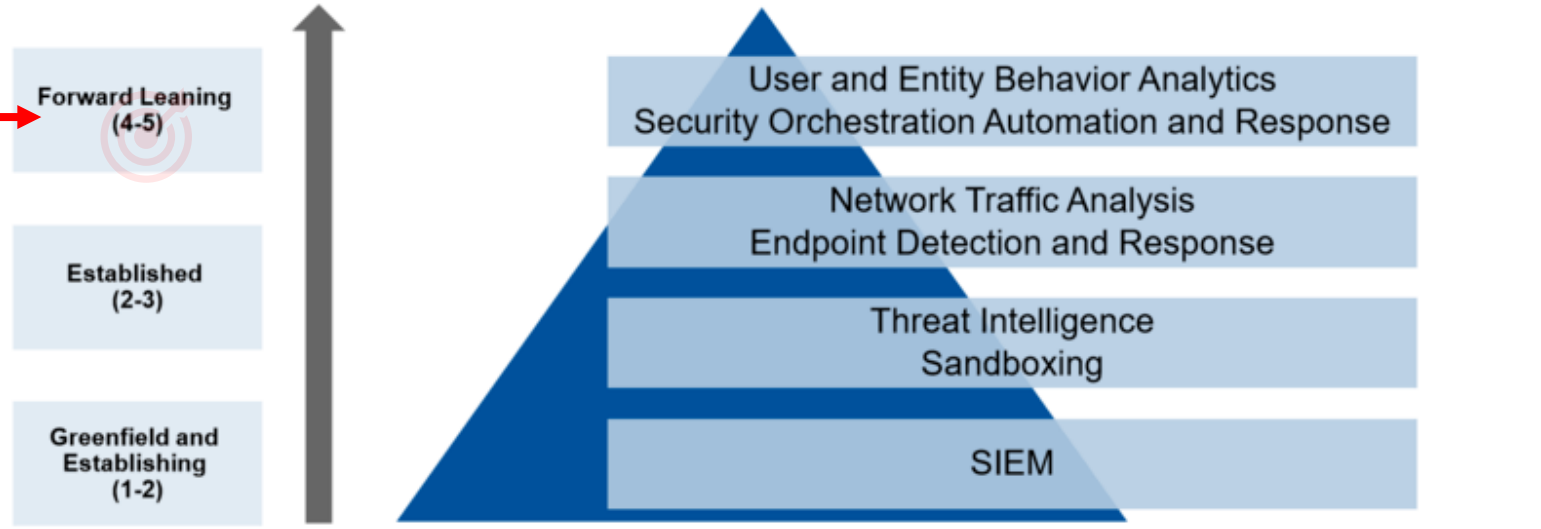
Key

- Arctic Wolf + ASMGi
- ASMGi

Gartner Maturity Model

4+ Maturity with ONEteam MDR/MSOC *plus*

Modern SOC Analytics Tooling and Stage of Maturity



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

Gartner

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

Summary – Key Takeaways

- A Total Solution = Program + Technology + Operations. If you are missing any piece, you are vulnerable!
- Leverage the investments you've already made and the information you already have
- Managed Detection and Response, will Stop Attacks that other methods miss!
- You don't have to get caught in the "buy security" frenzy. Security happens when you do the basics well.
- Dwell time – fast time to response is key to all Attacks!
- If you only do one thing to improve your security – Do This!

Upcoming ASMGi Cyber Security Webinars with Arctic Wolf

Managing Cyber Risk - Don’t be careless about your exposure to cyber-attacks!
presented by ASMGi and Arctic Wolf Networks
live webinar, ***March 25 at 1PM ET***

Don't Let Your Cloud Security Fall Behind
presented by ASMGi and Arctic Wolf Networks
live webinar, ***April 8 at 1PM ET***

*Reply “**YES**” in the Question Box and we will preregister you for both of these webinars*

ASMGi

ARCTIC WOLF

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