



ASMGi
ONEteam



Ransomware Reality: Dispelling the Myths

January 20, 2021

Ransomware Reality – Dispelling the Myths



Tim Smoot
Senior Presales Engineer
Arctic Wolf



Steve Roesing
President, CEO
ASMGi



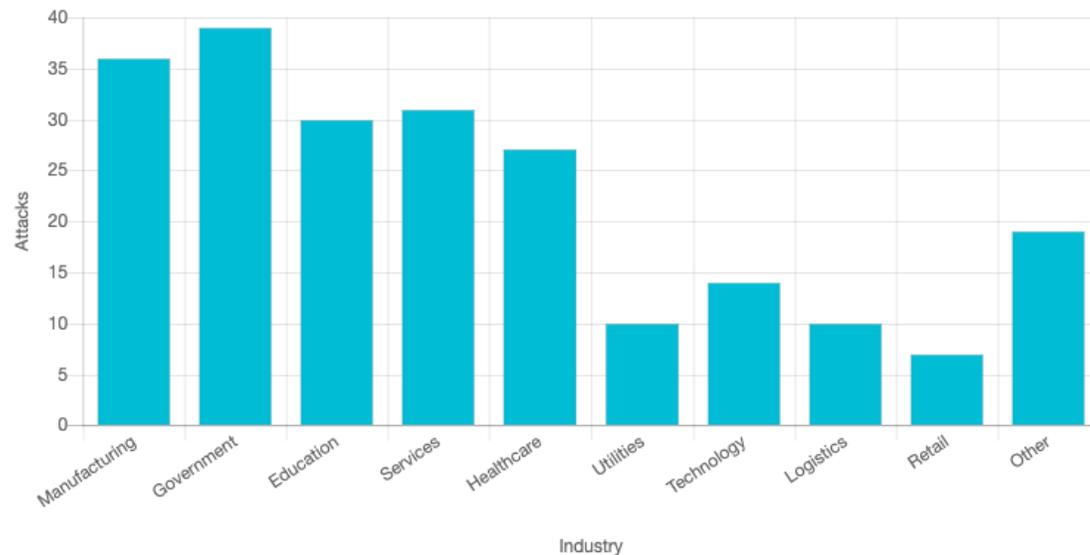
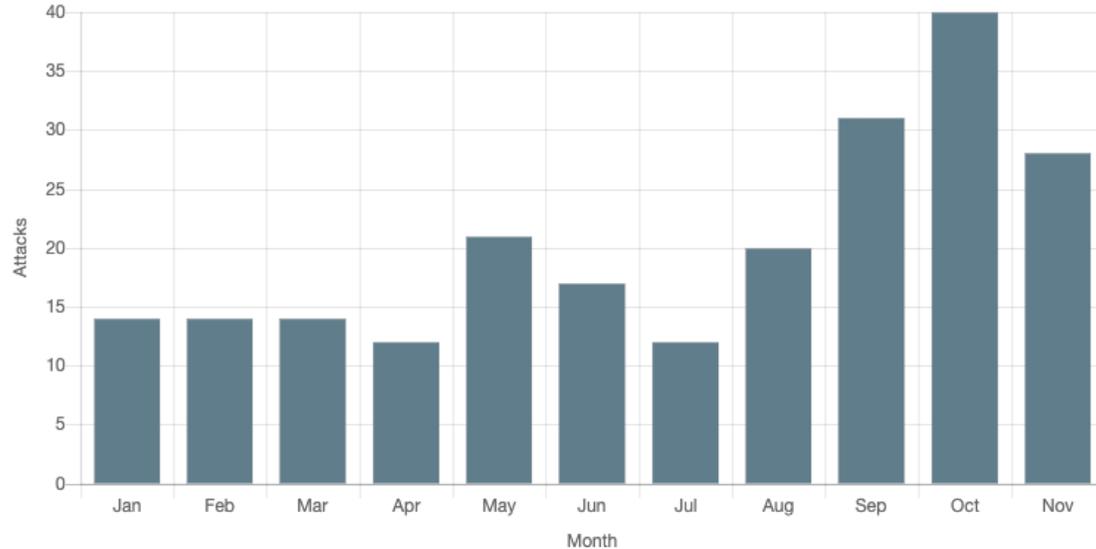
Agenda



- ◆ *Is Ransomware Still a Thing in 2021?*
- ◆ *What is Ransomware?*
- ◆ *What Does a Typical Attack Look Like?*
- ◆ *What are 3 Goals to fight Ransomware?*
- ◆ *What is **ONEteam** MDR/MSOC *plus* and how does it protect me?*
- ◆ *Key Takeaways*
- ◆ *Q & A*

Is Ransomware Still a Thing?

Ransomware: Is It Still a Thing?



North American Industries Reporting Ransom Attacks in the Last Year



“There will be a ransomware attack on businesses every 14 seconds by the end of 2019, and every 11 seconds by 2021”

Steve Morgan
Editor-in-Chief, Cybercrime Magazine

What is Ransomware?

Ransomware

- ✓ Subcategory of “malware”, malicious software
- ✓ Encrypts valuable information
- ✓ Requests payment for decryption
- ✓ Often exfiltrating data and threatening to release for further leverage

Ransomware attack

- ✓ Typically penetrates via email phishing, software vulnerability, or configuration scanning (RDP)
- ✓ Can aim for wide lateral distribution before launch
- ✓ Can occur as a pure attack or as part of a more complex hack
- ✓ Pure ransomware: “spray and pray”, or targeted (e.g. Texas attack)



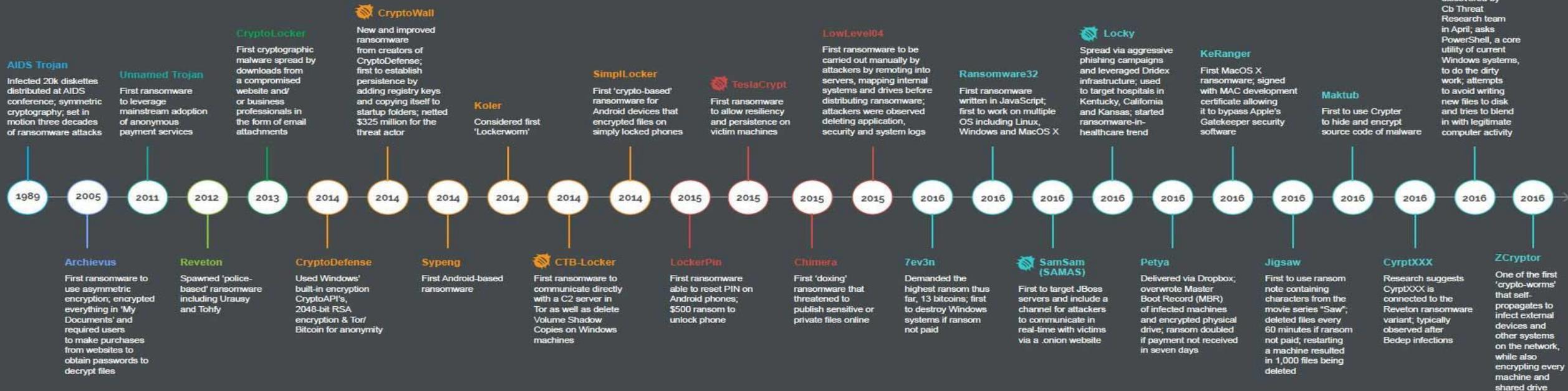
The screenshot shows the interface of the Wanna Decryptor 1.0 ransomware. The title bar reads "Wanna Decryptor 1.0". The main window has a dark red background with white and yellow text. At the top right, a banner says "Oops, your files have been encrypted!". Below this, there's a section titled "What Happened to My Computer?" with a paragraph explaining that files are encrypted and inaccessible. To the left, there's a large white padlock icon. Below the padlock, a yellow box says "Payment will be raised on" followed by the date "5/15/2017 16:25:02" and a "Time Left" counter showing "02:23:58:28". Below that, another yellow box says "Your files will be lost on" followed by the date "5/19/2017 16:25:02" and a "Time Left" counter showing "06:23:58:28". To the right of these boxes is a vertical progress bar. Below the "What Happened..." section, there's a section titled "Can I Recover My Files?" with a paragraph explaining that files can be recovered for free by clicking "<Decrypt>". Below that, there's a section titled "How Do I Pay?" with a paragraph explaining that payment must be made in 3 days, or the price will be doubled. At the bottom, there's a Bitcoin payment section with a "Send \$300 worth of bitcoin to this address:" label, a Bitcoin logo, and the address "15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1". There are also buttons for "Check Payment" and "Decrypt".

A Brief History of Ransomware



Ransomware Timeline

Top 5 ransomware variants in U.S.



Ransomware Today

◆ Time and Cost Impacts:

- 9.6 days of average downtime
- Average ransom payment of \$36,295

◆ Costs aren't just \$\$\$:

- Recovery impacts to operations/business
- Legal ramifications

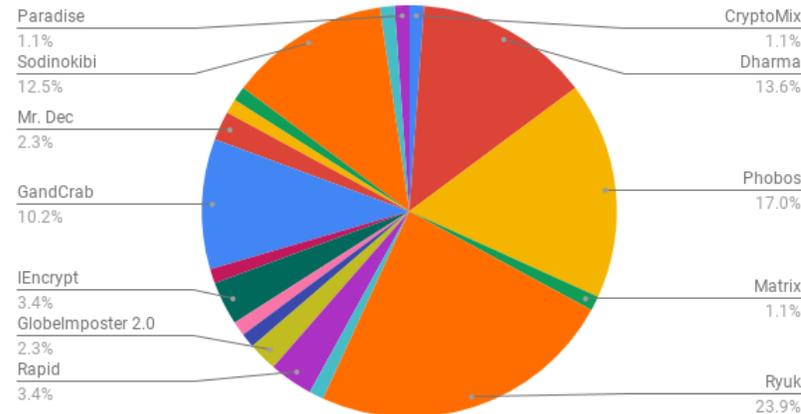
◆ ...and sometimes the most costly

- Reputation costs customers/partners

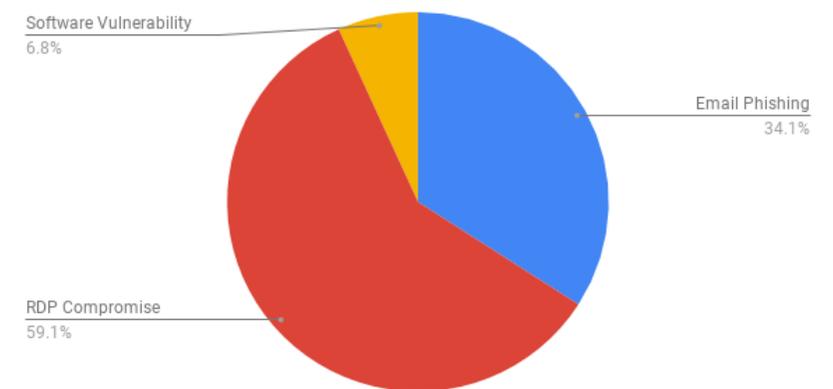
◆ State of Ransomware

- Wide range of ransomware strains in the market today. Ryuk highest at under 25%
- All industries under attack, from software services (20.5%) to public sector (3.4%)
- Attack vectors: RDP compromise and email phishing lead, followed software vulnerability

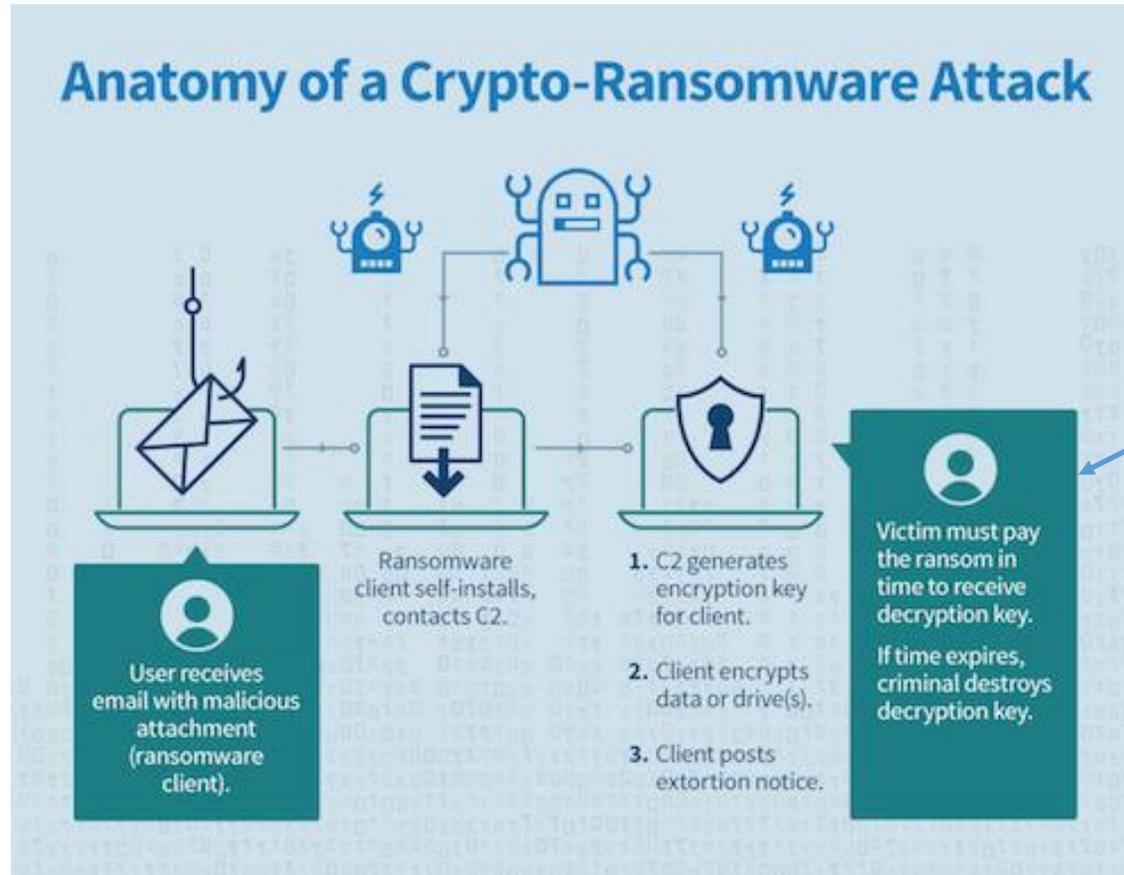
Ransomware Market Share by Type: Q2 2019



Attack Vectors Commonly Used in Ransomware Incidents: Q2 2019



A Typical Ransomware Attack



Today, Victim also risks data being stolen and released on the Internet!

Should I pay the Ransom?



My philosophy has changed. I used to be opposed to paying ransoms in general. Now I think of it more as a business decision – could be yes, could be no. Our job, as a trusted partner is to make NOT paying the ransom the best “business decision”.

Steve Roesing, ASMGi

3 Goals to Fight Ransomware



1. Prevent Ransomware Attacks
2. Minimize impact if you are attacked
3. Have a structured, rehearsed Incident Response Plan.

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.

The Old Way: Point-Solution Mindset

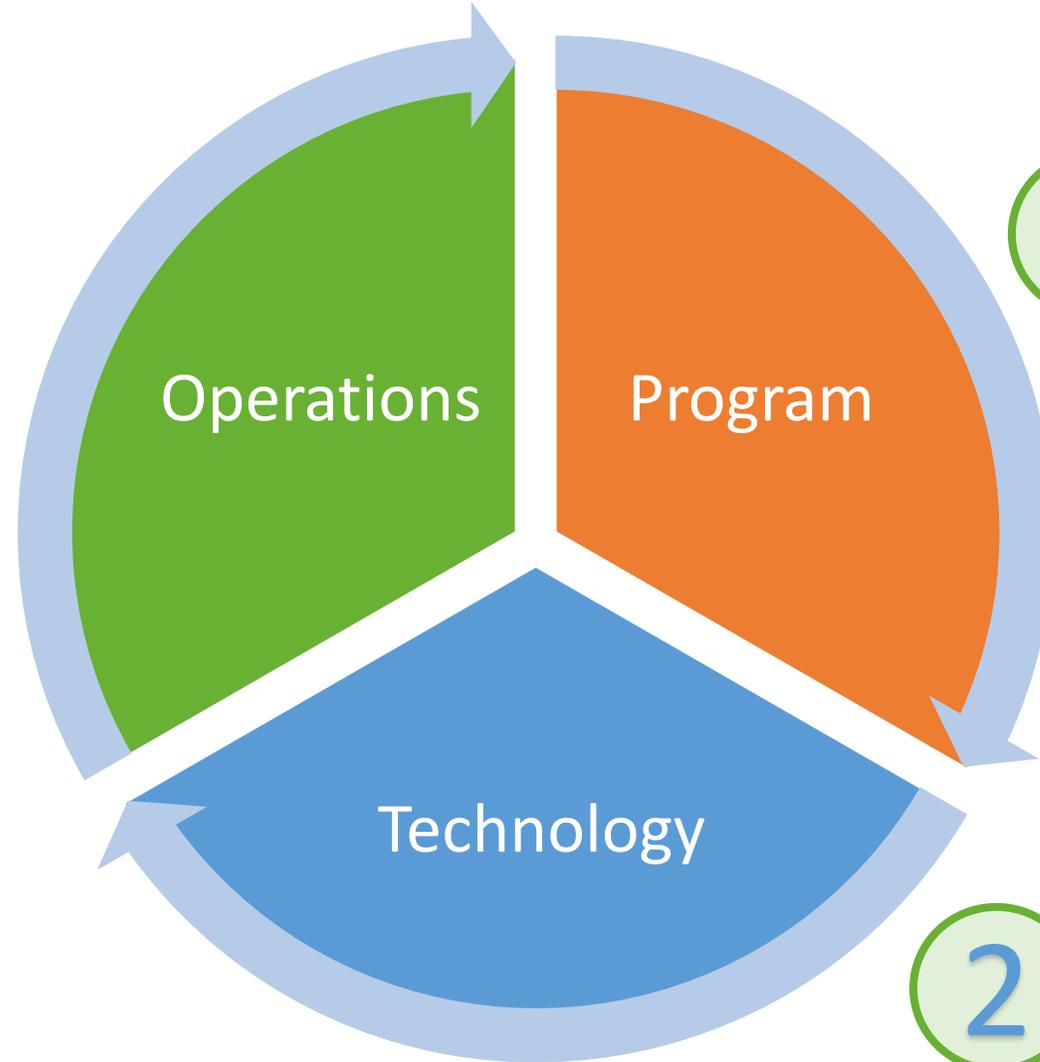
- ◆ Reactive
- ◆ Focus on Individual Controls
- ◆ Fragmented and inefficient
- ◆ Spend a lot and not necessarily improve security

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
 - ◆ Vulnerability Mgmt
 - ◆ Remediation
 - ◆ Incident Response

1 Program

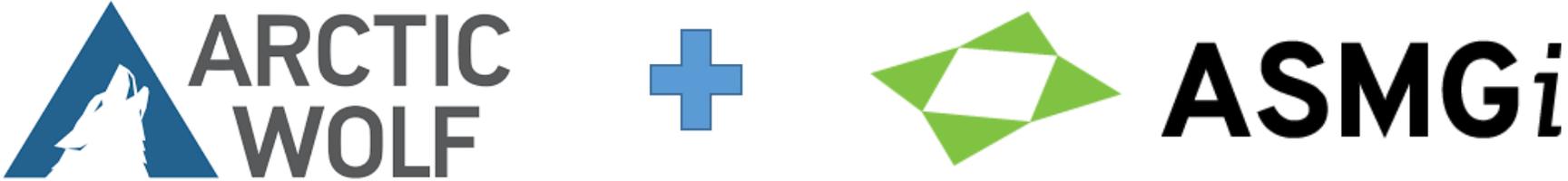
- ◆ Corporate Objectives
- ◆ SLOs / SLAs
- ◆ Strategic Goals (tech and operations must meet this requirements)

2 Technology Stack

- ◆ Tech Stack must meet strategic requirements and objectives

What is **ONEteam** MDR/MSOC *plus*?

ONEteam
MDR/MSOC *plus*



3 Goals Of ONEteam MDR/MSOC plus



1. Prevent Ransomware Attacks
2. Minimize impact if you are attacked
3. Have a structured, rehearsed Incident Response Plan.

ONEteam MDR/MSOC *plus*



ONEteam MDR/MSOC *plus*

- ◆ 24 x 7 Security Operations Centers (SOCs)
- ◆ Continuous Managed Detect and Response
- ◆ Continuous Managed Risk Services
- ◆ Continuous Managed Cloud Monitoring
- ◆ Vulnerability Management and Remediation
- ◆ Cyber Incident Response / Forensics



PREVENT: 24 x 7 MDR/SOC catches intruders quickly!

PREVENT: Vulnerability Management includes your Program and Remediation!

Minimize: MDR includes isolating a system if IOC is detected!

Maturity: Incident Response includes your Program, a Table-Top Exercise and Incident Response (per NIST 800-61). The information is already available because we'll know if an incident is occurring.

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.

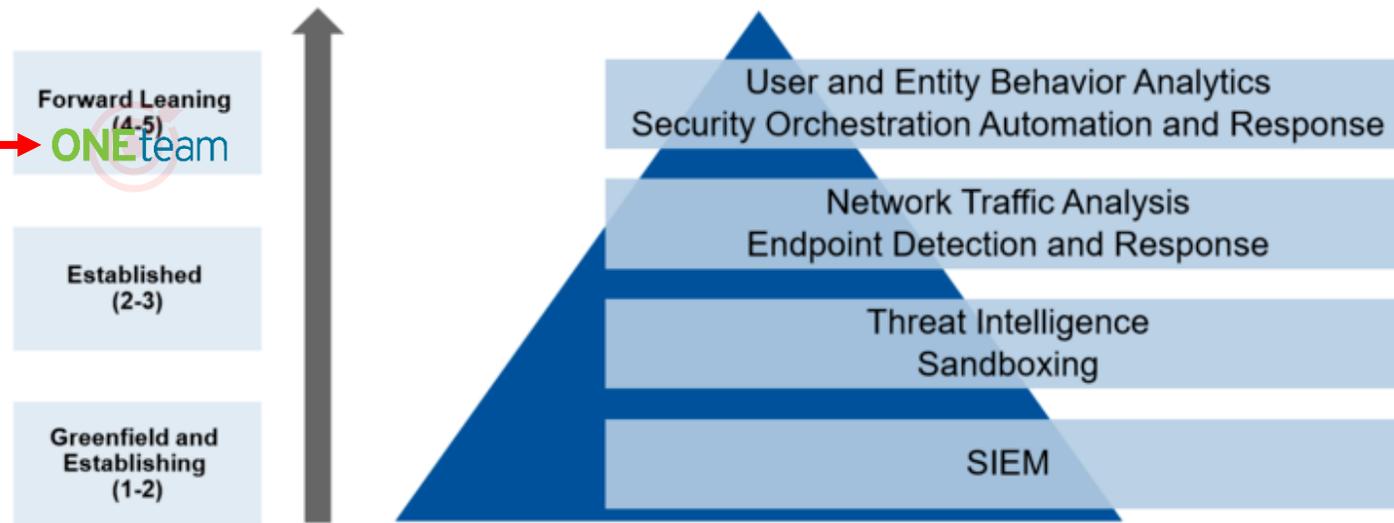
Table 3-5. Incident Handling Checklist

	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)	

Gartner Maturity Model

Modern SOC Analytics Tooling and Stage of Maturity

4+ Maturity with
ONEteam
MDR/MSOCplus



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

Some Key Points



- 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 and investments you already have
- ◆ Focus on foundational elements of security to improve right now
- ◆ You don't have to get caught in the security buying frenzy. Security Posture improves when you do the basics well!
- ◆ **If you only do one thing to improve your security – Do MDR/MSOC *plus!***

Q & A



For more information:

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Email: sales@asmgi.com

www.asmgi.com