THE WEBINAR WILL BEGIN SHORTLY

Please feel free to leave questions in our Q&A box

Airiam

June 14, 2023

Actively Monitor Threats

Are You Cybersecurity Ready? Webinar Series

Your Presenters

Art Ocain | Field CISO and CIO | Airiam

Alan Villaseñor | SOC Manager | Airiam

Airiam

Company Overview

Your Dedicated Team

About Airiam

Mission

Airiam's mission consists of three interconnected and bold ambitions:

- Offer the best IT management products and services.
- Build the best-in-class cybersecurity platform.
- Create more value for businesses through resilience.

As Featured In

FORTUNE eWEEK WSJ yahoo! finance

Born from the Fusion of Five Amazing Companies

Airiam's mission is to become a trusted partner to businesses everywhere—offering products and services that help businesses safely and strategically adapt as technology and security needs evolve.

Frontline Experience to Inform Protection

50,000+

hours of experience responding to ransomware and other cybersecurity incidents, which inform our strategy.

100+

ransomware incidents responded to per year ranging from SMB to Fortune 100 companies.

25,000+

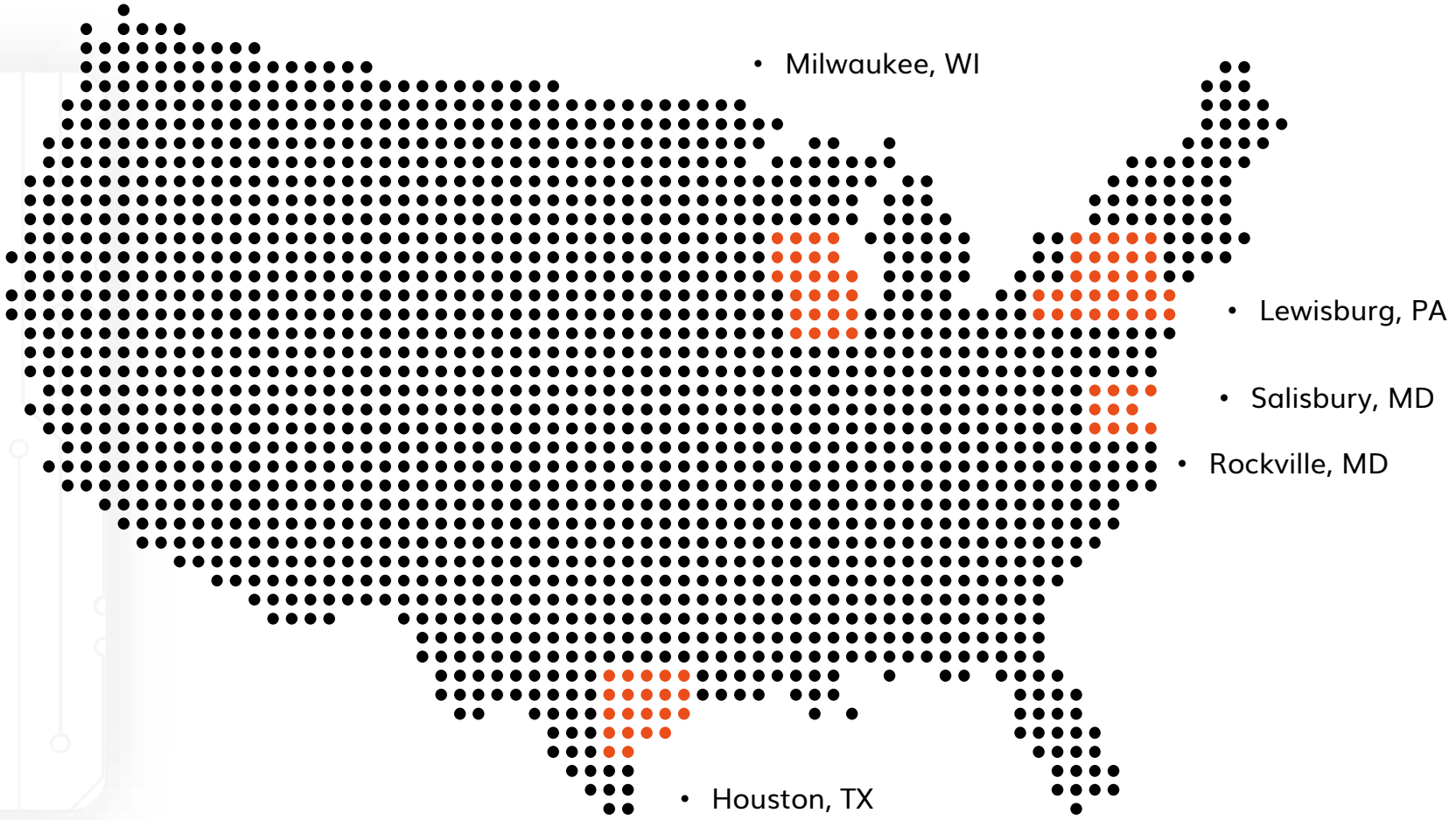
servers, workstations & networks recovered, rebuilt and restored.

$2M

recovery guarantee for your organization if an incident happens while you are fully protected by Airiam.

Select Customers

Offices Throughout the United States



Airiam

Airiam

Agenda

1. Different Types of & Most Common Threats
2. Importance of Active Monitoring
3. How To Actively Monitor Threats
4. Tool & Techniques
5. Respond & Improve

Airiam

1. Different Types of & Most Common Threats

You need to know the threat to protect against it.

Airiam

Poll Question

How many types of threats do you think exist?

Your answer will be anonymous.

10-100

101-500

501-1000

1001-5000

MORE

What Are The Most Common Threats Businesses Face?

Phishing Attacks

Malware

Data Breaches

What Are The Most Common Threats Businesses Face?

APWG detected 64,696 unique phishing email subject lines in July, 430,141 unique phishing websites in August and 637 phishing campaigns targeted toward organizations in September 2022.

According to the AV-TEST Institute, an independent research institute for IT security from Germany, more than 450,000 new malicious programs (malware) and potentially unwanted applications (PUA) are registered daily.

According to Spanning's Tech Trends & Insights 2022 Survey Report, 14% of SMBs and 27% of MMEs experienced a data breach incident in 2022. Of these, 60% of the attacks against SMBs and 35% against MMEs occurred during the second half of 2022.

Different Types of Threats

Phishing Attacks

- Technique used by cybercriminals to trick individuals into revealing sensitive information and can occur via email, social media, instant messaging, or even phone calls.

Malware

- Malicious software, such as viruses, worms, ransomware, and spyware, poses a significant threat to businesses

Data Breaches

- Unauthorized access to sensitive data can occur due to weak passwords, unpatched software vulnerabilities, insider threats, or targeted attacks.

Social Engineering

- Manipulating people, include impersonation, baiting, pretexting, or eliciting information through psychological manipulation.

Airiam

Different Types of Threats

Insider Threats

- Risks posed by individuals within an organization who misuse their access privilege, including disgruntled employees, negligent insiders, or those targeted by external attackers.

Distributed Denial of Service (DDoS) Attacks

- Overload a network or website with a massive volume of traffic, rendering it inaccessible to legitimate users.

Advanced Persistent Threats (APTs)

- Sophisticated, long-term cyber attacks targeting specific organizations. involving a persistent and stealthy approach to compromise networks, exfiltrate data, or establish unauthorized access.

Zero-day Exploits

- Target vulnerabilities in software or hardware that are unknown to the vendor or have not been patched yet.

Airiam

Different Types of Threats

Data Leakage and Loss

- Data loss refers to the accidental or intentional loss of data due to system failures, human error, or cyberattacks.

Cloud Security Risks

- Threats from using the Cloud from shared responsibility model between the cloud provider and the business.

Mobile Device Security

- Security threats posed by mobile device usage

Internet of Things (IoT) Vulnerabilities

- Insecurely configured or unpatched IoT devices can become entry points for attackers.

Airiam

Airiam

2. Importance of Active Monitoring

What do all these threats do?

What Each Threat Does

Phishing Attacks

- Cybercriminals to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or login credentials

Malware

- Can be used to gain unauthorized access, steal sensitive information, disrupt operations, or extort money.

Data Breaches

- Can lead to theft, exposure, or compromise

Social Engineering

- Can manipulate people into divulging confidential information or performing actions that may compromise security

Airiam

What Each Threat Does

Insider Threats

- Risks include stealing data, causing damage, or disrupting operations.

Distributed Denial of Service (DDoS) Attacks

- Can disrupt business operations, impact customer experience, and cause financial losses.

Advanced Persistent Threats (APTs)

- Sophisticated, long-term cyber attacks targeting specific organizations. involving a persistent and stealthy approach to compromise networks, exfiltrate data, or establish unauthorized access.

Zero-day Exploits

- Cybercriminals exploit these vulnerabilities before they can be mitigated, making them highly dangerous.

Airiam

What Each Threat Does

Data Leakage and Loss

- Sensitive information is unintentionally or maliciously disclosed to unauthorized parties.

Cloud Security Risks

- Includes unauthorized access to data, insecure APIs, data breaches, and account hijacking.

Mobile Device Security

- Threats include mobile malware, unsecured Wi-Fi networks, data leakage through lost or stolen devices, and malicious apps.

Internet of Things (IoT) Vulnerabilities

- Attackers can gain access to networks, extract data, or disrupt operations.

Airiam

Airiam

Poll Question

How do you actively monitor your threats?

(This is a multiple-choice answer)

Your answer will be anonymous.

Security Information and Event Management (SIEM) System

Intrusion Detection and Prevention Systems (IDS/IPS)

Log Monitoring and Analysis

Vulnerability Scanning and Penetration Testing

Employee Awareness and Reporting

Security Operations Center (SOC)

Other

I don’t know

Airiam

3. How to Actively Monitor Threats

What routines can I start to introduce?

Threat Intelligence Gathering	Subscribe to services that provide information about the latest threats, vulnerabilities, and attack techniques. They also stay updated on emerging risks that could affect their industry and the technology they use.
Security Information and Event Management (SIEM) System	Use SIEM to collect and analyze information about security events and logs from different sources, such as network devices, servers, and endpoints. This system helps monitor security in real-time, find connections between events, and send alerts if something suspicious is happening.
Intrusion Detection and Prevention Systems (IDS/IPS)	Install systems that can monitor the network traffic coming in and out of systems. These systems look for signs of potential intrusions or malicious activities. They can identify known attack patterns, detect unusual behavior, and block suspicious network traffic.
Log Monitoring and Analysis	Regularly review and analyze logs. By looking for patterns, anomalies, and suspicious activities in these logs, you can spot any signs of a security incident or breach.
Endpoint Detection and Response (EDR)	Use EDR to monitor and detect suspicious behavior on individual devices like computers and smartphones. These tools can find things like unauthorized access attempts, unusual changes to files, or strange actions taken by users.
Network Traffic Monitoring	Implement tools to monitor data flowing through networks. By inspecting this network traffic, you can identify any communication that looks malicious, such as attempts to steal data or connect to their systems without permission. If they detect something suspicious, they can actively block it.

Vulnerability Scanning and Patch Management	Regularly scan systems, applications, and network infrastructure to find weaknesses that hackers could exploit. When weaknesses are found, fix them by installing security updates and patches to make their systems stronger.
User Behavior Analytics (UBA)	Deploy UBA tools to learn how people typically behave on their computer networks. If someone starts behaving strangely, these tools can detect it and raise an alarm.
Dark Web Monitoring	Engage specialized services or tools to monitor the dark web for mentions of your organization's sensitive information, such as stolen credentials or leaked data. This helps identify potential data breaches or cyber threats targeting your organization.
Incident Response Team	Establish an incident response team or leverage the services of a managed security provider. This team should be responsible for monitoring security events, investigating incidents, and responding promptly and effectively to mitigate the impact.
Security Awareness and Reporting	Train employees to be aware of security risks and to report any suspicious activities or incidents they notice. Provide training on things like recognizing fake emails, avoiding tricks used by hackers, and best practices for handling sensitive information.
Red Teaming and Penetration Testing	Conduct periodic red teaming exercises or hire third-party experts to simulate real-world attacks and assess the effectiveness of existing security controls. Penetration testing helps identify vulnerabilities and provides insights into potential weaknesses.

Airiam

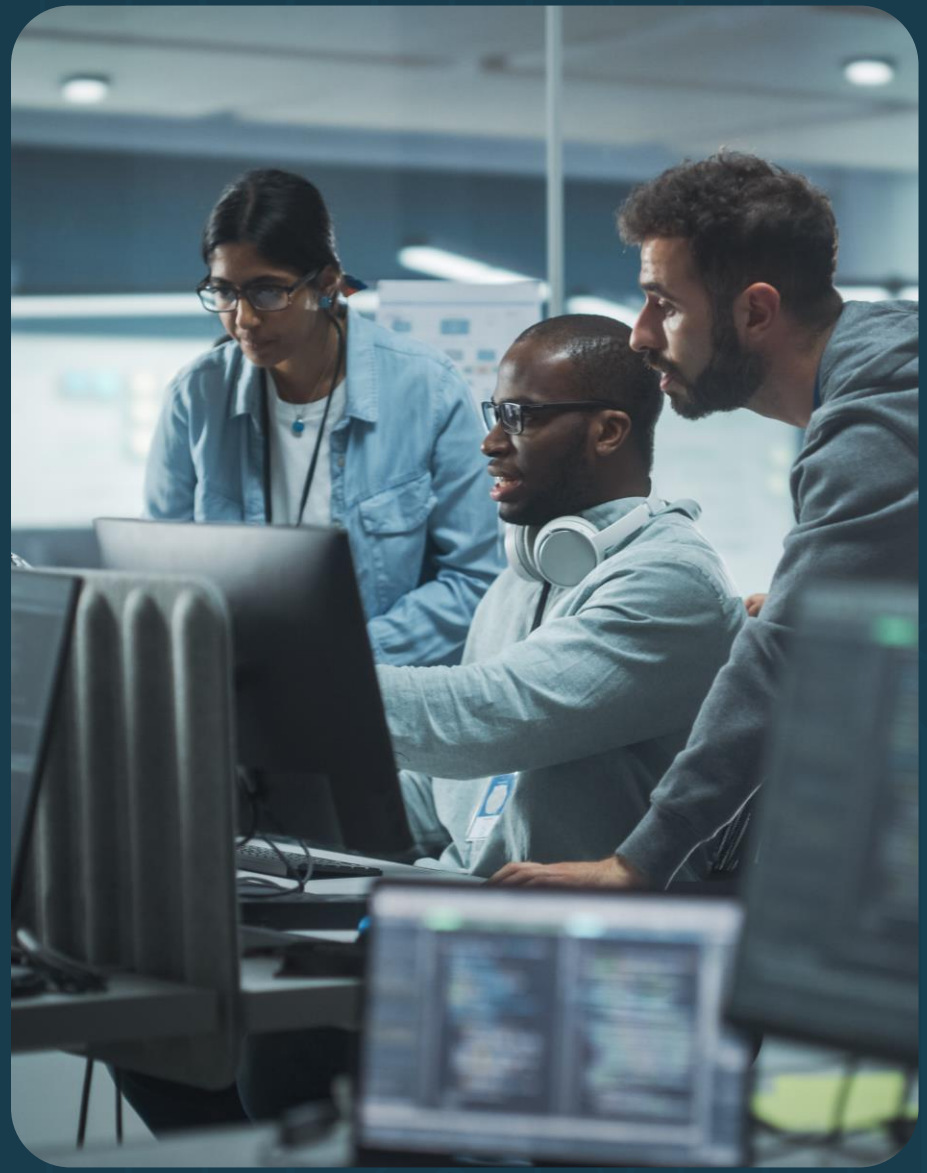
4. Tools & Techniques

Easy steps to get started.

Quick Tips & Techniques

Easy things to implement in your business now

- Use strong passwords and security questions
- Keep software up to date
- Use, upgrade, and maintain firewalls
- Install antivirus and anti-malware software
- Be careful about what information you share online
- Educate employees about cyber threats through training



Quick Tips & Techniques

Easy things to implement in your business now

- Use security software
  - Identify and block threats, such as malware and phishing attacks.
- Monitor network traffic
  - Identify suspicious activity, such as large data transfers or unusual login attempts.
- Use threat intelligence
  - Identify emerging threats and provide insights into the tactics and techniques of attackers.
- Threat hunting
  - Proactive approach to security that involves actively searching for threats that may have evaded traditional security controls.

Airiam

Poll Question

How many of the 10 tips and techniques we discussed do you currently implement in your business?

1. Use strong passwords and security questions
2. Keep software up to date
3. Use, upgrade, and maintain firewalls
4. Install antivirus and anti-malware software
5. Be careful about what information you share online
6. Educate employees about cyber threats through training
7. Use security software
8. Monitor network traffic
9. Use threat intelligence
10. Threat hunting

Your answer will be anonymous.

1-3

4-6

7-9

All of them

Airiam Tools

AirGuard™

AirGuard is the only managed security service you need.

AirGapd™

Stop Ransomware. Guaranteed.

AirCTRL™

Vulnerability Patching

Airiam Tools

Airiam

5. Respond & Improve

I found a vulnerability. What now?

Respond & Improve

Airiam

Respond

- Assess the threat
  - Gather as much information as possible about the nature and severity of the threat. Determine its impact on your systems, data, and overall security posture.
- Activate your incident response plan
  - Follow your organization's established incident response plan. This plan should outline the steps to be taken when responding to a security incident. It may involve notifying relevant stakeholders, such as IT personnel, security teams, and management.
- Isolate and contain
  - If possible, isolate the affected systems or devices from the network to prevent the threat from spreading. This can involve disconnecting affected devices or segmenting the network.

Respond

- Investigate and analyze
  - Conduct a thorough investigation to understand the source, scope, and extent of the threat. Analyze any available logs, system alerts, or forensic evidence to gain insights into the incident.
- Mitigate and remediate
  - Take appropriate actions to mitigate the threat and minimize its impact. This may involve applying patches, removing malware, changing passwords, or implementing additional security measures. Follow best practices and guidance from cybersecurity professionals.

Improve

- **Communicate and report**
  - Keep relevant stakeholders informed about the incident and its resolution. Document the details of the incident, actions taken, and lessons learned for future reference. If necessary, report the incident to appropriate authorities or regulatory bodies as required by applicable laws or regulations.
- **Learn and improve**
  - After the incident is resolved, conduct a post-incident review to identify areas for improvement in your security practices. Update your security controls, policies, and procedures based on the lessons learned.

Airiam

What's Next?

More to come!

Simplify Compliance

RAMP – Jun 26, 5:30PM EST

- What is RAMP?
- What RAMP covers
- Federal vs State

https://zoom.us/webinar/register/WN_bYY52-AlQdeO7AK0SxkA-A

SOC & ISO – Jun 27, 11:00AM EST

- What are SOC and ISO?
- What SOC and ISO cover
- Why you need to comply to SOC and ISO

https://zoom.us/webinar/register/WN_qNTSStwiQJOwccnPU_3NPw

NIST 800-171 – Jun 28, 1:30PM EST

- What is NIST 800-171?
- What NIST 800-171 covers
- What businesses need to comply to NIST 800-171

https://zoom.us/webinar/register/WN_bYY52-AlQdeO7AK0SxkA-A

Airiam

Airiam

Please enter any questions into the chat box.

Your Dedicated Team

Airiam

Thanks!

info@airiam.com

(570) 524-6894

linkedin.com/company/airiam

youtube.com/@airiamtech