



[Click here to view the recording of Effective Vulnerability Management Webinar](#)

EFFECTIVE VULNERABILITY
MANAGEMENT

KEVIN HAYES, CISSP, CISM
CHIEF INFORMATION SECURITY OFFICER
MERIT NETWORK, INC.





EFFECTIVE VULNERABILITY
MANAGEMENT

KEVIN HAYES, CISSP, CISM
CHIEF INFORMATION SECURITY OFFICER
MERIT NETWORK, INC.





AGENDA

- **Introductions**
- **Risk Management**
Concepts overview
- **Threat Landscape**
With Exploit Demo
- **Vulnerability Scanning Basics**
- **Managing Vulnerabilities** with the
Merit CISO Scanner

INTRODUCTION

KEVIN HAYES

- Chief Information Security Officer
- 20 years in security industry for education and nonprofit
- Passion for cybersecurity education

CISSP – Information Systems Security Professional

CISM – Information Security Manager

GCIH, GCFA, GCCC – SANS Incident Handling, Forensics Analysis, Top 20 Security Controls

CIHE, CPTe, CISSO – Mile2 Incident Handling, Penetration Testing, Security Officer






IT ALL STARTS WITH RISK

Risk: It's what's for dinner!

Every single thing we do in our lives is governed by some form of risk management.

Naturally, this applies to cyberspace as well.

How do we best manage risk in a complex, technical, and constantly changing environment?



Risk is the chance that a **threat** will **exploit** a **vulnerability** on an **asset** causing damage or **loss**.

Decrease **any** of the above terms and you reduce your risk.

The caveat is that you **must understand** how each of those terms truly impact your environment.

Sticking your head in the sand **does not affect** the equation.



ALL ABOUT THE **VULNERABILITIES**

Vulnerabilities are the ways that an attacker can get in to your environment and give you a **really, really bad time**.

Outdated software and **misconfigured services** are the technical vectors that an attacker will exploit to gain access and do damage.

You **must** be aware of these vulnerabilities and work to address them.



OF COURSE, RANSOMWARE

The risk of ransomware is typically the most **visible concern** of organizations.

Ransomware is “only” the **monetization** of exploited vulnerabilities.

Efforts placed into reducing the risk of ransomware will **directly translate** into a better overall security program.



SADLY, IT
WORKS

Of sites infected with ransomware:

- **70%** pay the ransom
- **20%** pay more than \$40k
- **Median** payout is around \$10k
- **85%** will be hit more than 3 times
- **25%** pay but do not recover data
- **Hospitals** have been the most likely to pay, followed by law offices

OH,
ATLANTA!

OUTAGE ALERT

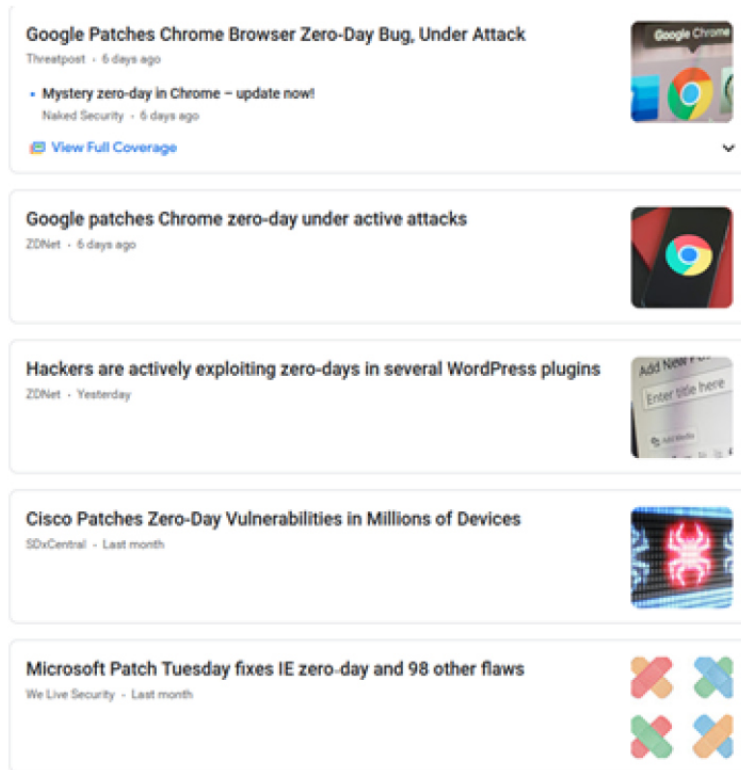


The City of Atlanta is currently experiencing outages on various customer facing applications, including some that customers may use to pay bills or access court-related information. Our @ATL_AIM team is working diligently with support from Microsoft to resolve this issue. Atlantaga.gov remains accessible. We will post any updates as we receive them. Thank you for your patience.



- Between March and April of 2018, 5 of 13 city departments were **shut down**.
- There was a direct impact on **revenue collection** and there was no plan in place.
- Atlanta spent \$2.7 million instead of paying a \$50,000 ransom.
- January 2018 audit identified **over 1500** vulnerabilities.
- Ransomware **brute-forced** passwords.

ZERO-DAYS HAVE ZERO LOVE



- A **zero-day vulnerability** allows an attacker to exploit a vulnerability with no warning or advance notice to the community.
- Defenses are almost non-existent and involve deploying **emergency fixes** or **compensating controls**.
- Your teams must be extremely **responsive** and **understand their environment**.



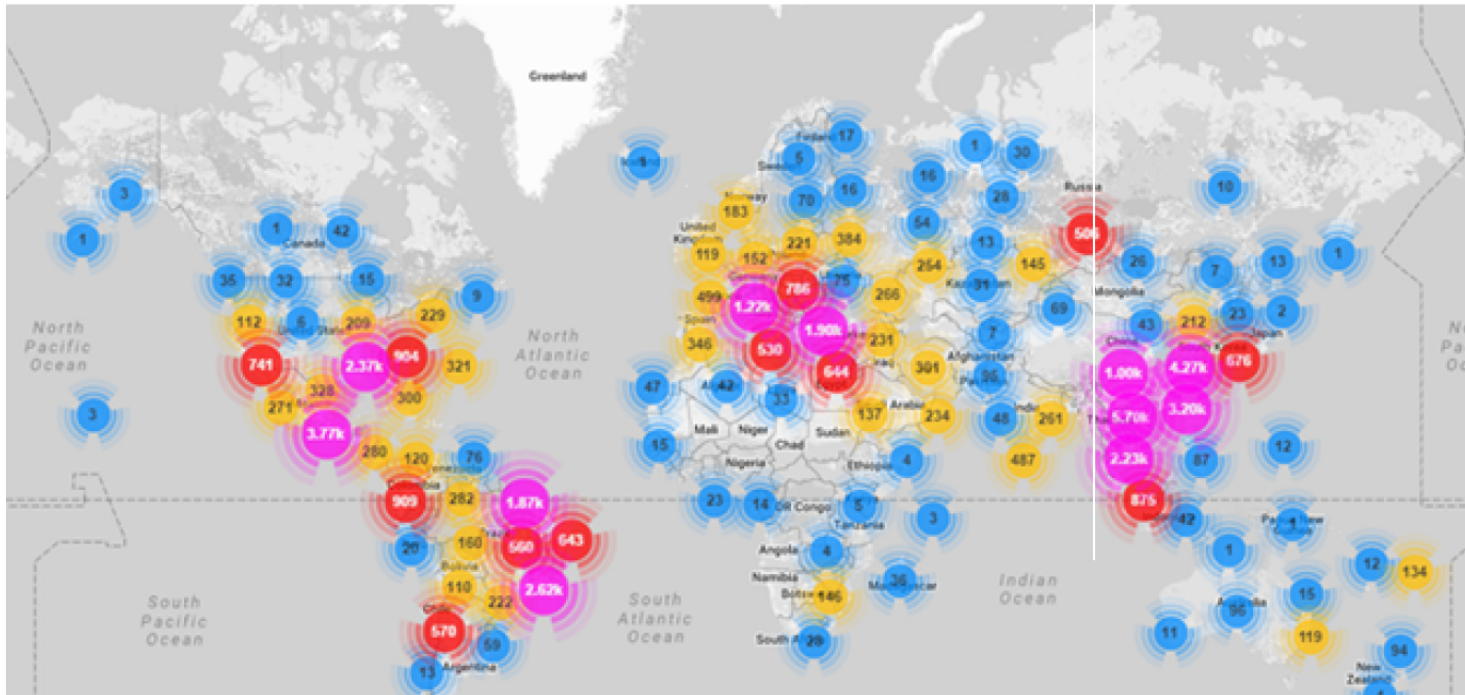
AND DON'T
GET ME
STARTED...

The Internet of Things (IoT) is a network of Internet-connected computing devices embedded in everyday objects, enabling them to send and receive data via various communications protocols, **often with little or no security.**

Dangers include:

- Hardcoded and publicly available passwords
- No passwords
- Unsecure protocols and ports
- Inability to upgrade software or firmware
- Complete lack of knowledge that they exist

WEAPONIZING IOT



The Mirai botnet uses security cameras and other IoT devices to launch volumetric attacks.

DDoS attacks can be up to 1 Terabyte per second and last as long as 54 hours.

Source code has been made public so additional functionality can be added.



LOW HANGING FRUIT

There is an extraordinarily large amount of **background scanning** on the Internet. Cloud services such as **shodan.io** and **censys.io** have already cataloged your Internet footprint.

Low-effort attackers can use this information to cause **significant problems** if you are not prepared.

LOW HANGING FRUIT

92.80.89.232 [View Raw Data](#)

City	Bucharest
Country	Romania
Organization	Telekom Romania
ISP	Telekom Romania
Last Update	2020-02-10T22:57:24.218492
ASN	AS9050

Ports

81 82

Services

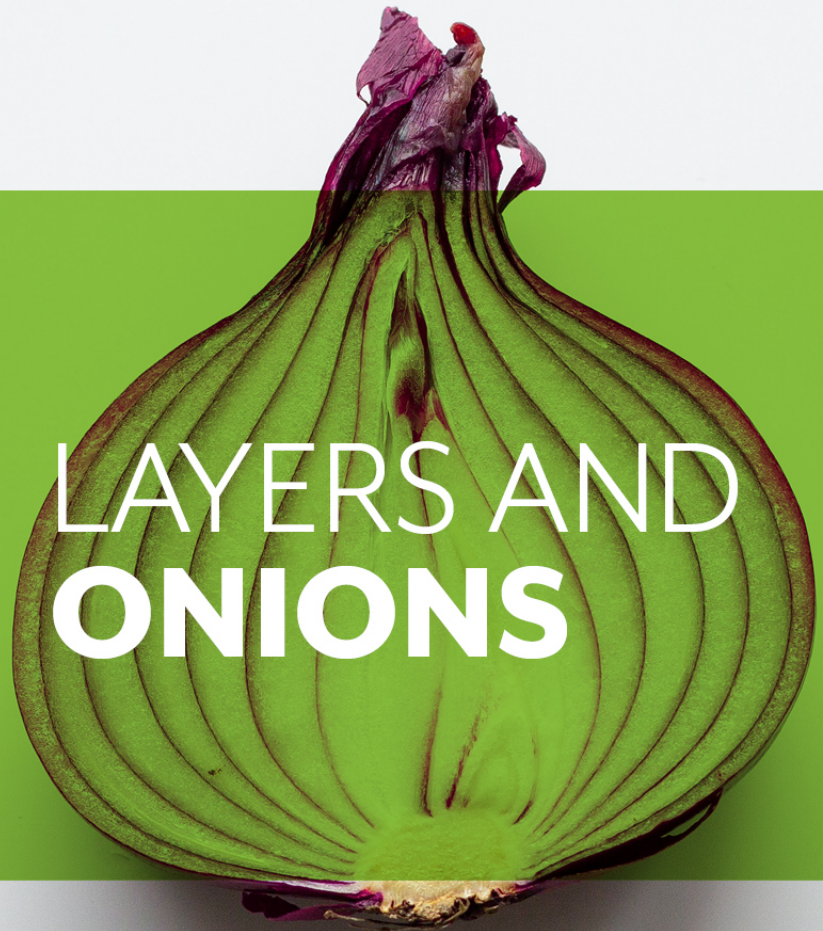
81
81p
http-simple-new
dvr1614n web-cam httpd
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:1002

82
82p
http-simple-new
Netwave IP camera http config
HTTP/1.1 200 OK
Server: Netwave IP Camera
Date: Mon, 10 Feb 2020 20:37:52 GMT
Content-Type: text/html
Content-Length: 7244
Cache-Control: private
Connection: close

Understanding what is exposed to the Internet is **extremely important**.

Exposed systems inherently have a **larger likelihood** of being exploited.

These systems **typically** can cause greater impact as well.



Applying **Defense in Depth**

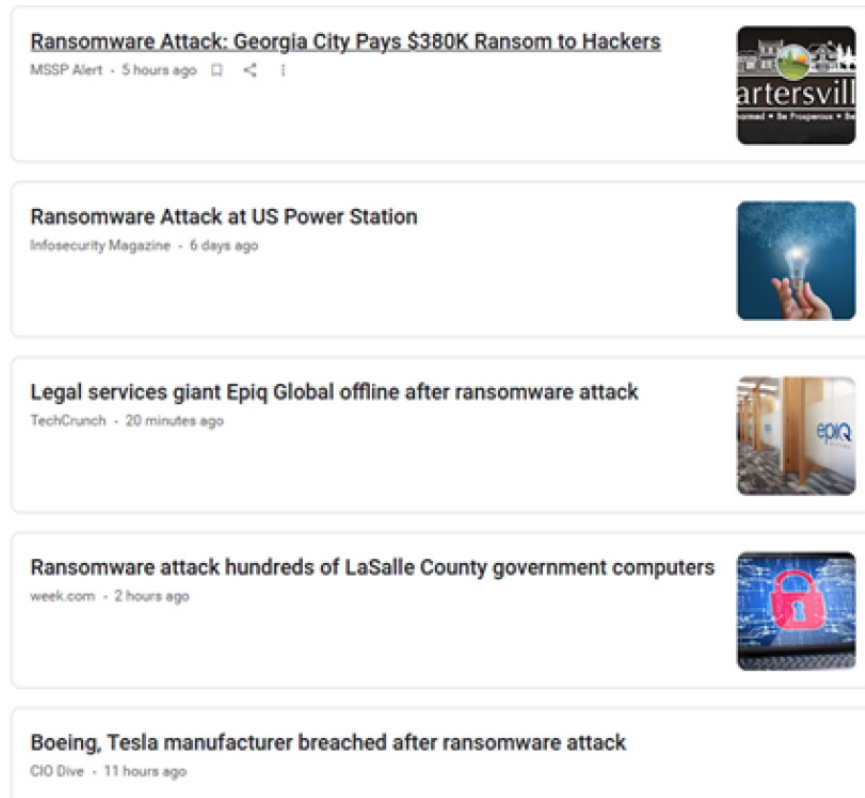
is critical as we ensure there are multiple controls protecting our information systems.

The failure of one layer should not cause disclosure, alteration, or destruction.

Additional layers can be used as **compensating controls** when we cannot perform our ideal actions.



I WISH THIS WAS A FAD



Not understanding, treating, and accepting risks leads to loss in an **extremely public way**.

While phishing is a common entrance point for ransomware and malware, **any vulnerability** can be used.

Humans just tend to be the easiest.



FIGHT FIRE WITH FIRE

Subscribe your ticketing system email address to the following bulletin sources at a minimum:

US-CERT

<https://www.us-cert.gov/ncas/bulletins>

MS-ISAC

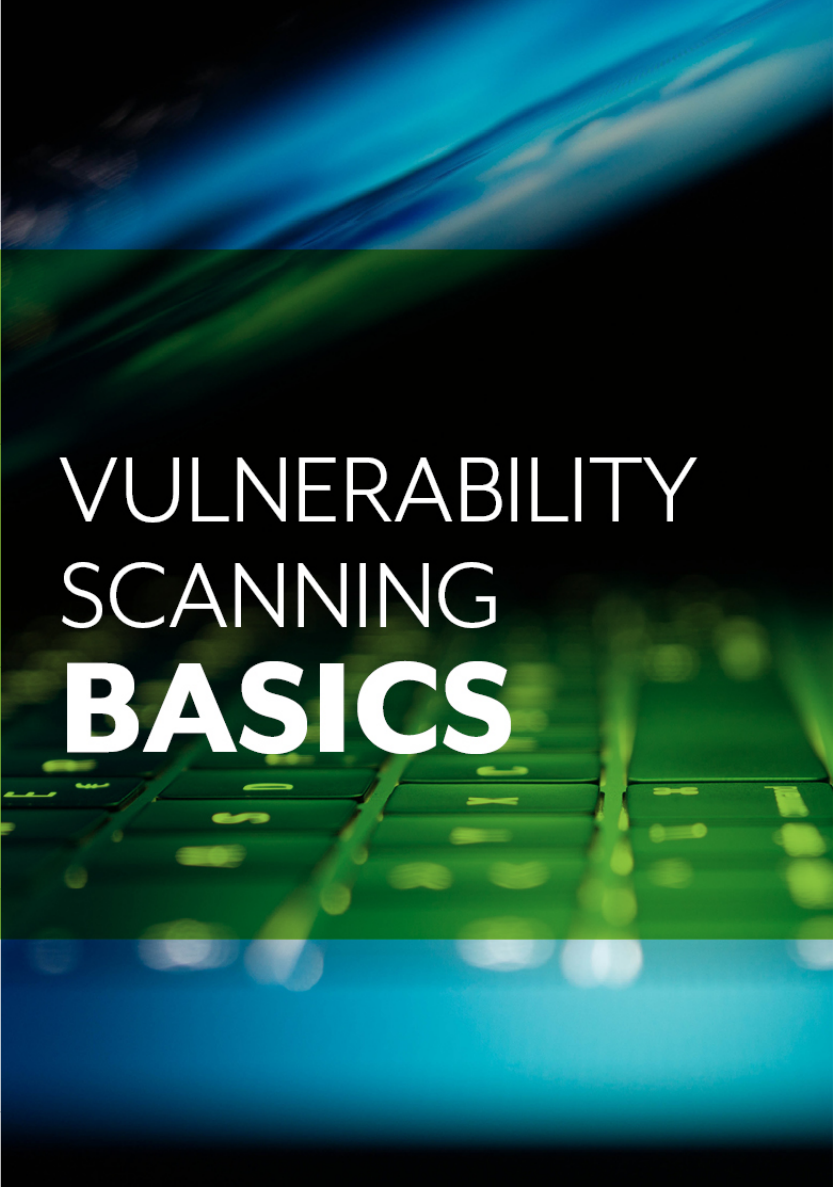
<https://www.cisecurity.org/resources/advisory/>

Microsoft

<https://www.microsoft.com/en-us/msrc/technical-security-notifications>



VULNERABILITY EXPLOIT **DEMONSTRATION**



VULNERABILITY SCANNING BASICS

Vulnerability scanners sit on the network and **assess your environment**, identifying sensitive areas where you may be vulnerable to technical attack.

Reports can **prioritize** the things you need to fix in your environment.

We need to **reduce the attack surface** that requires protection via more extensive and expensive means.



VULNERABILITY SCANNING BASICS

Scanners typically actively poll the **online machines** on your network.

You should ensure that there are **no firewall rules or restrictions** coming from the vulnerability scanner.

Basic fingerprinting is performed and then a selection of tests is executed based on what the scanner thinks of remote host.

This is **not** an overall test of your security controls. This **is** a test of your active vulnerabilities.



THIS IS NOT A PENETRATION TEST

Vulnerability scans are mostly **automated tools** used to give you an accurate report from the **defender** perspective.

A penetration test is mainly **manual work** by a skilled human to test your entire configuration of security controls as they appear from the **attacker** perspective.

Penetration tests are **much more expensive** and should be performed **only after** you have a regular vulnerability management program.



KEEPING THINGS COMMON: CVSS

The **Common Vulnerability Scoring System (CVSS)** is used to rate vulnerabilities on a scale of 0.0 to 10.0.

Inputs into the formula include complexity of the attack, what access is needed, and what the result of the attack is.

Critical vulnerabilities are rated above 9.0 and should be the **first priority**.

High vulnerabilities are between 7.0 and 8.9 and **come next**.

Review other vulnerabilities as **time permits**.



AUTHENTICATED SCANS MATTER

Vulnerability scanners can perform their checks the easy way (with credentials) or the hard way (without).

Authenticated scans provide higher fidelity, are quicker, and cause less traffic on your network.

You do have to trust giving a scanner system **root** and/or **Administrator** level accounts.

Start with unauthenticated scans as a baseline, and **upgrade** to authenticated scans once you have a handle on your program.



THINK ABOUT **THE INSIDE**

Your external facing servers and systems will be have the most visibility, but your efforts **do not stop there.**

All internal assets **must** be assessed as well.

It only takes one infected internal computer to act as a pivot point and get attackers **around your border firewalls.**

Internal assets can be used as **pivot points** as well if compromised.



MUCH ADO ABOUT EVERYTHING

You will **never** be rid of vulnerabilities.

For issues your scanner identifies, you must decide what to do:

- You can **accept** the risk and call it a day
- You can **immediately** patch or resolve the issue
- You can put together a **plan** to patch or resolve the issue
- You can identify the issue as a **false positive**
- You can **eliminate** the server or service

All your actions and notes should be in either a **ticketing system** or a **spreadsheet**.



START
SMALL

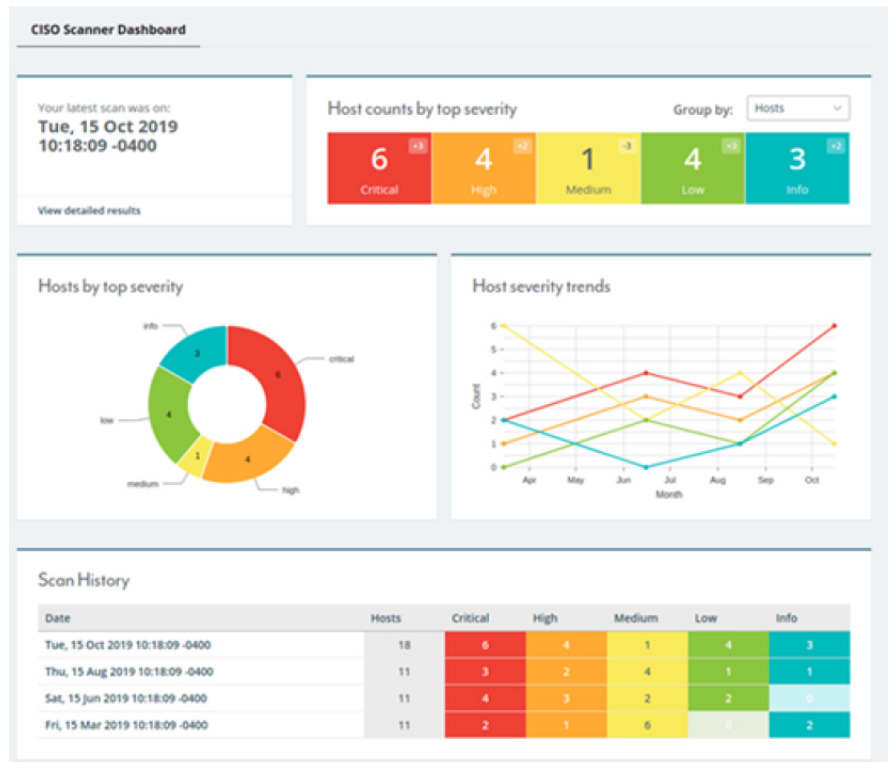
It is **extremely easy** to get overwhelmed with data once you begin vulnerability scanning.

Focus on **core systems or servers** first and build up your processes of confidence from there.

Start by scanning **monthly**. You can upgrade to weekly later.

Authenticated scans can really overload you, so upgrade to them **only** after everything else is well under wraps.

MERIT CISO SCANNER



- High-fidelity results at an affordable price
- Receive actionable information on how to secure your network without paying excessive per-host fees
- Track your efforts over time with ease
- Easily accept risk, denote false positives, and mark remediation work in process which carries over to any subsequent scans



EFFECTIVE VULNERABILITY
MANAGEMENT

KEVIN HAYES, CISSP, CISM

CHIEF INFORMATION SECURITY OFFICER

MERIT NETWORK, INC.

KRHAYES@MERIT.EDU

