01

Introduction to Threat Hunting

Wednesday, May 27, 2020
2:00 - 3:00 PM PDT

Women CyberSecurity Society | Workshop

INSTRUCTOR

LISA KEARNEY

Founder & CEO

During the spring of 2018, Lisa founded the Women CyberSecurity Society (WCS2) to address the lack of support for women and minorities within the cybersecurity industry. WCS2 is a non-profit organization providing support, services and advocacy to women around the globe.

Consultant

For more than 2 decades, Ms. Kearney has been defending networks, systems and data by providing cybersecurity services to hundreds of companies globally while working with Canada's top service providers and independently on contracts.

03

Workshop Goals

- UNDERSTAND WHAT THREAT HUNTING IS AND HOW IT WORKS
- PROVIDE YOU A BASIS OF THE THREAT HUNTING FRAMEWORK AND METHODOLOGY
- LEARN NEW SKILLS TO ANALYZE THEATS AND LOOK FOR INDICATORS OF COMPROMISE
- INSTILL A PASSION FOR LEARNING ABOUT CYBERSECURITY

What You'll Learn

- DEFINATION OF THREAT HUNTING
- THE NEED FOR THREAT HUNTING
  - PROBLEM
  - SOLUTION
  - KEY FACTORS
- WHO, WHAT, WHEN , WHY, WHERE & HOW TO HUNT?
- THREAT HUNTING MATURITY MODEL
- TREAT HUNTING GOALS & DATA SOURCES
- THE BENEFITS OF THREAT HUNTING
- THREAT HUNTING TOOLS & RESOURCES
- DEMO OF WINDOWS TOOLS TO BEGIN THE HUNT

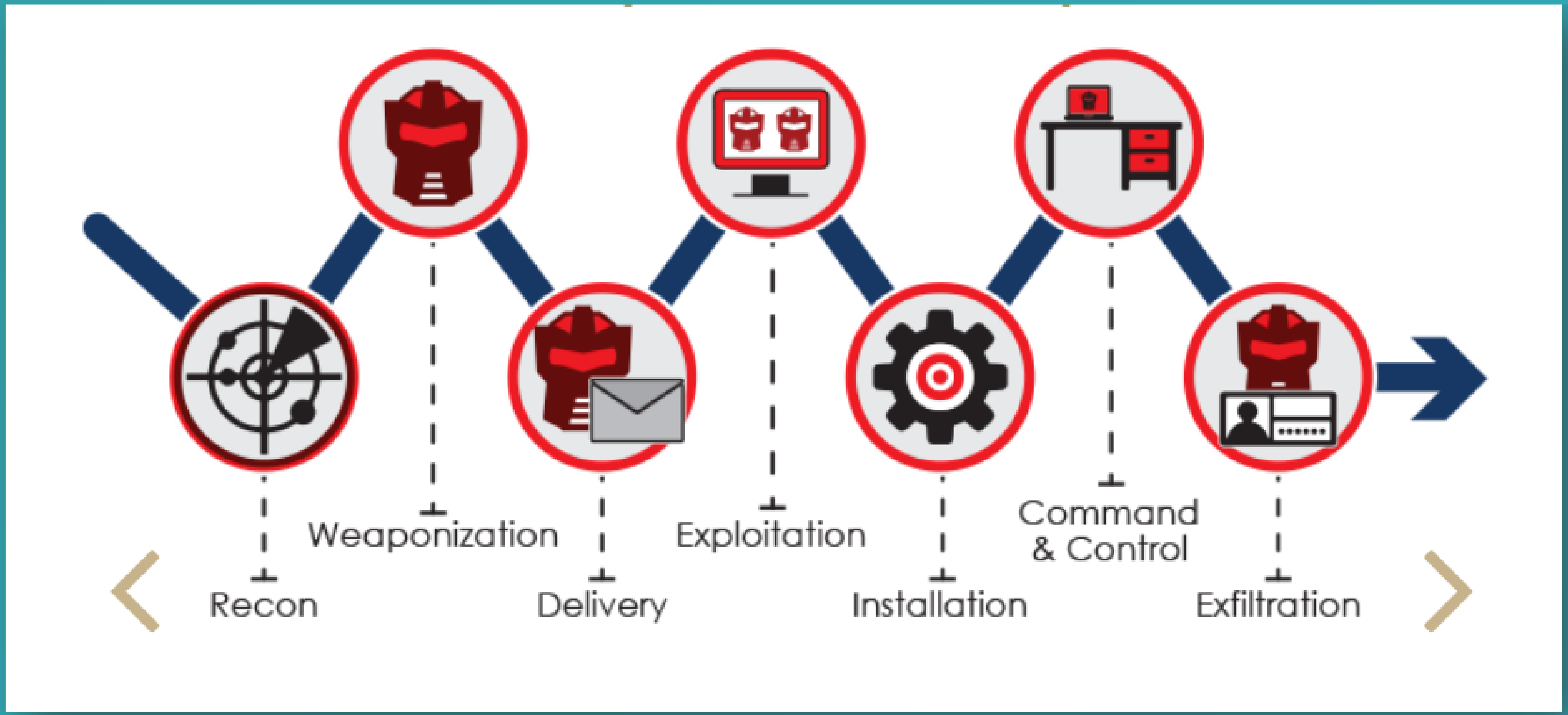
What is Threat Hunting?

DEFINATION

Threat hunting is a focused and iterative approach to seeking, identifying and understanding adversaries that have entered the defender’s networks.

These proactive tasks attempts to identify unknown adversaries on a network.

This is differs from incident response, which is reactive and based on an alert or security incident. Focused and funded adversaries will not be countered by security boxes on the network alone.



Credit: Cyber Kill Chain by Lockheed Martin

Cyber Kill Chain

RECON
WEAPONIZATION
DELIVERY
EXPLOITATION
INTRODUCTION
COMMAND & CONTROL
EXFILTRATION

Women CyberSecurity Society | Workshop

Problem

EMPLOYEES LACK SKILLS

Many organizations have limited resources and budget for training or to hire highly skilled resources. Therefore, more often than not, hackers penetrate an organization and go undetected due to lack of skills by internal employees and service providers.

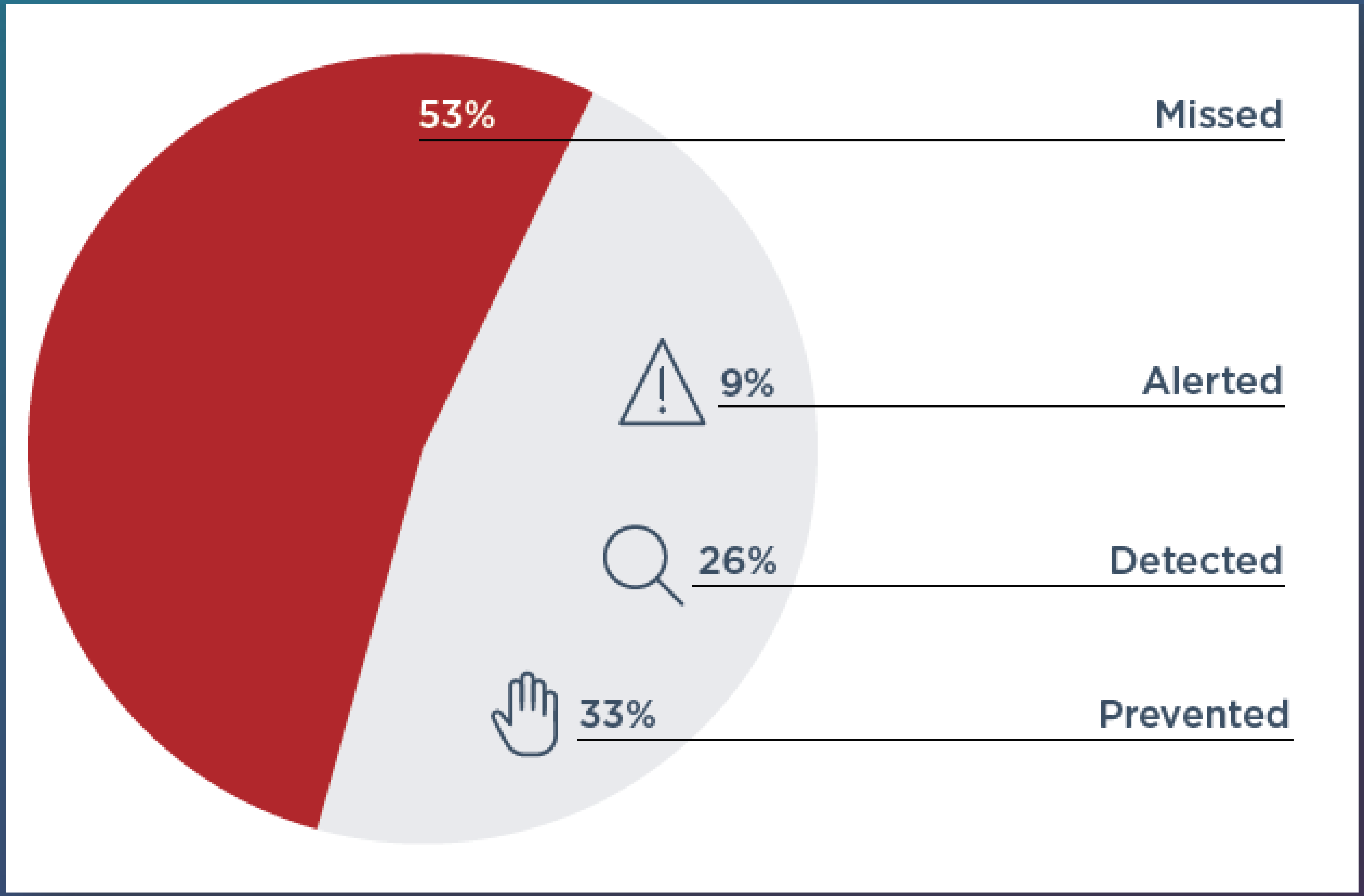
ENTERPRISES FAIL TO TAKE ACTION

Patching, remediating and threat hunting costs time and money. It requires a deligent and organized approach to do it right which results in lowering the risk to orgnaizations. However, many fail to do what is required to increase the security posture because they see security as a cost centre. This is changing.

HACKERS ARE STEALTHY

The modern hacker works to maintain persistance on a network in order to capture more confidential information which can be sold, barters or traded on the surface and dark web.

Mandiant Security Effectiveness Report 2020



53% Attacks Are Missed

DELVELOP A THREAT HUNTING PROGRAM

Take a strategic approach to developing your threat hunting program using a proven framework or methodology to meet your internal needs.

HIRE QUALIFIED PERSONNEL

Hire and engage trained personnel.

BE PROACTIVE AND ITERATIVE

Record your findings. Measure progress. Improve the program and continue building and uising machine learning to improve threat detection and response. Know when to hand it over to teh IR and DR teams..

SOLUTION

KEY FACTORS

SKILLS OF THE ANALYSTS

Presentations are communication tools that can be used as demonstrations, lectures.

TOOLS TO ACCESS & ANALYZE DATA

Presentations are communication tools that can be used as demonstrations, lectures.

QUALITY & QUANTITY OF THE DATA

Presentations are communication tools that can be used as demonstrations, lectures.

ALL HUNTS WILL NOT RESULT IN FINDINGS

Just because you didn't find anything doesn't mean your enviroment is clean. In fact, most organizastions are breached to one degree or another and don't know it. It's all about lowering risk.

Threat Hunting Considerations

NEXT STEP IN THE EVOLUTION OF THREAT DETECTION & RESPONSE

1. Who should conduct the hunt?
2. What should you hunt for?
3. When should this activity take place?
4. Where to conduct the hunt
5. How to conduct a hunt
6. What data should you collect?

#1

WHO SHOULD HUNT?

- Activity should be limited on a business need only.
- Access granted based on role with assigned responsibilities. (RACI Chart)
- Qualified members of your security team.
- Security management should have access to threat hunting dashboards.
- Executives should receive weekly/monthly reports on threat hunting findings and activities.
- Security consultants hired to lead the team or investigate threats.
- incident response and digital forensic team should conduct investigations & triage.

#2

WHAT SHOULD YOU HUNT FOR?

SET A GOAL

0-Day
Attacker tools in use
C2
Data Hiding
Exploits
Malware
Phishing
Privildege Escalation

#3

WHEN TO HUNT?

Threat hunting can take place anytime using manual , machine asssisted and or automated processes. Automation, combined with machine learning, should assist hunters and help them prioritize their efforts.

As you build out and mature your threat hunting program, you'll develop advanced techniques for threat detection based on the needs of your enviroment, leadership, budget, available tools, resources and qualified personnel.

#4

WHERE TO HUNT?

MOST HUNTING ACTIVITY **TAKES PLACE INTERNALLY** BUT CAN TAKE PLACE ANYWHERE WHERE YOU HAVE ACCESS TO AN ORGANIZATIONAL DATA. INCLUDING **EXTERNAL SOURCES.** OFTEN REFERRED TO AS **OPEN SOURCE INTELLIGENCE** (OSINT) & PARTICULARLY **DARK WEB** ACTIVITY RELATED TO YOUR COMPANY CAN UNCOVER PREVIOUSLY UNKNOWN THREATS.

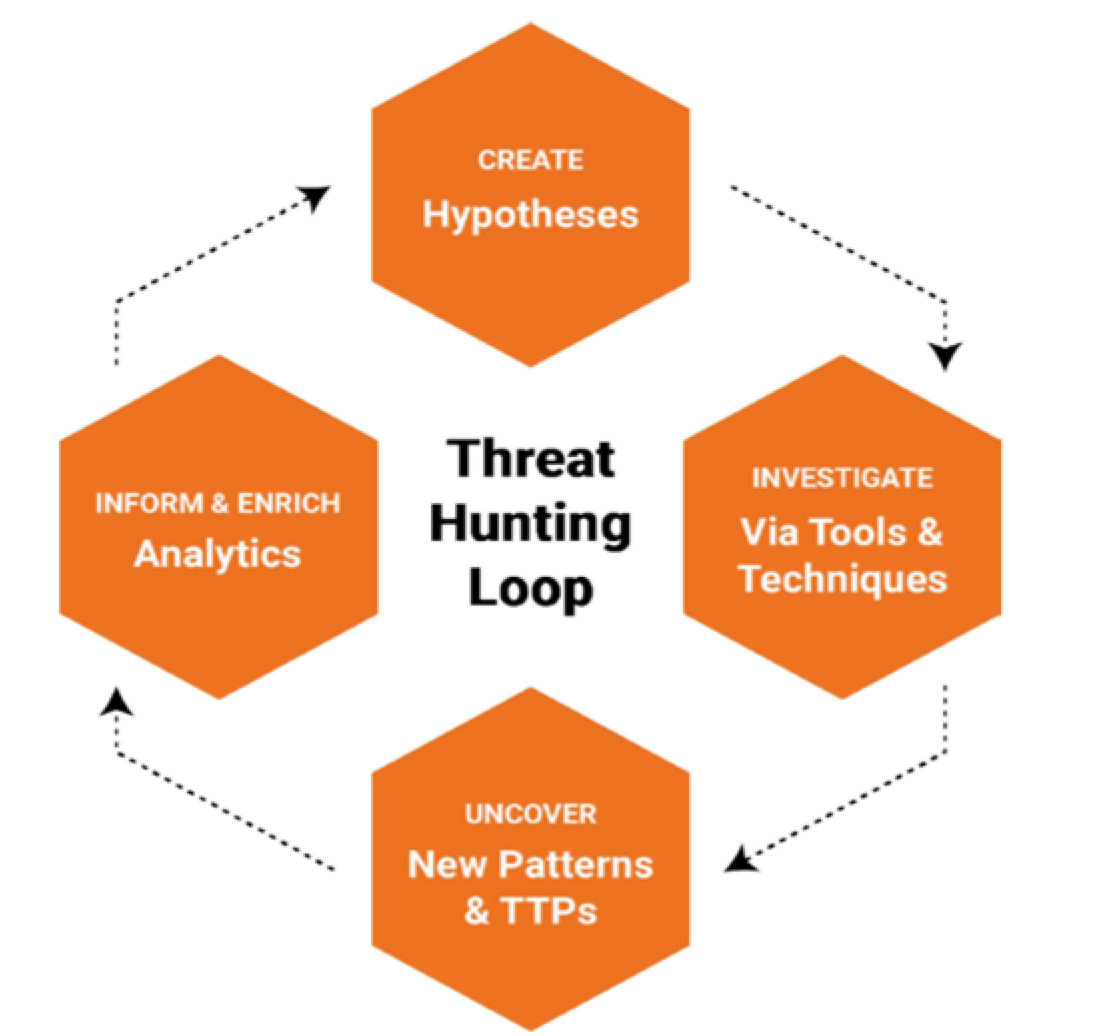


Fig. 1.2: the Threat Hunting Loop

#5

HOW TO CONDUCT A HUNT?

Have a plan
Set goals and targets
Collect your tools based on your goals and targets
Analyse, research, and record you findings
Hand off when required for triage to IR and Forensics
Follow an iterative process
Report

#6

WHAT DATA TO COLLECT?

Remeber the hunt results are only as good as the data your collect and examine. That's why it's important to work with other key stakeholders such as your security operations, incident responders, digital forencis to ensure you are collecting, storing and backing up the data you need to perform a successful hunting activities.

DATA SOURCES

SIEM
Syslog
AV Logs
Firewall logs
DNS Query Logs
SMTP or similar logs
FTP/Telnet/RDP/SSH
Memory Dumps

TCP Dumps
Filesystem
Registry
Processes
Proxy
Server
Bandwidth logs
Windows Event Logs
(Security, System, Application)

HOW IT BEGINS

SUSPICION OR CONFIRMED CASE OF AN INCIDENT

A hunt starts with creating a hypothesis, or an educated guess, about some type of activity that might be going on in your IT environment.

An example of a hypothesis could be that users who have recently traveled abroad are at elevated risk of being targeted by state-sponsored threat actors, so you might begin your hunt by planning to look for signs of compromise on their laptops or assuming that their accounts are being misused around your network.

Each of these subhypotheses would be tested individually. Analysts can develop hypotheses manually based on this type of intelligence.

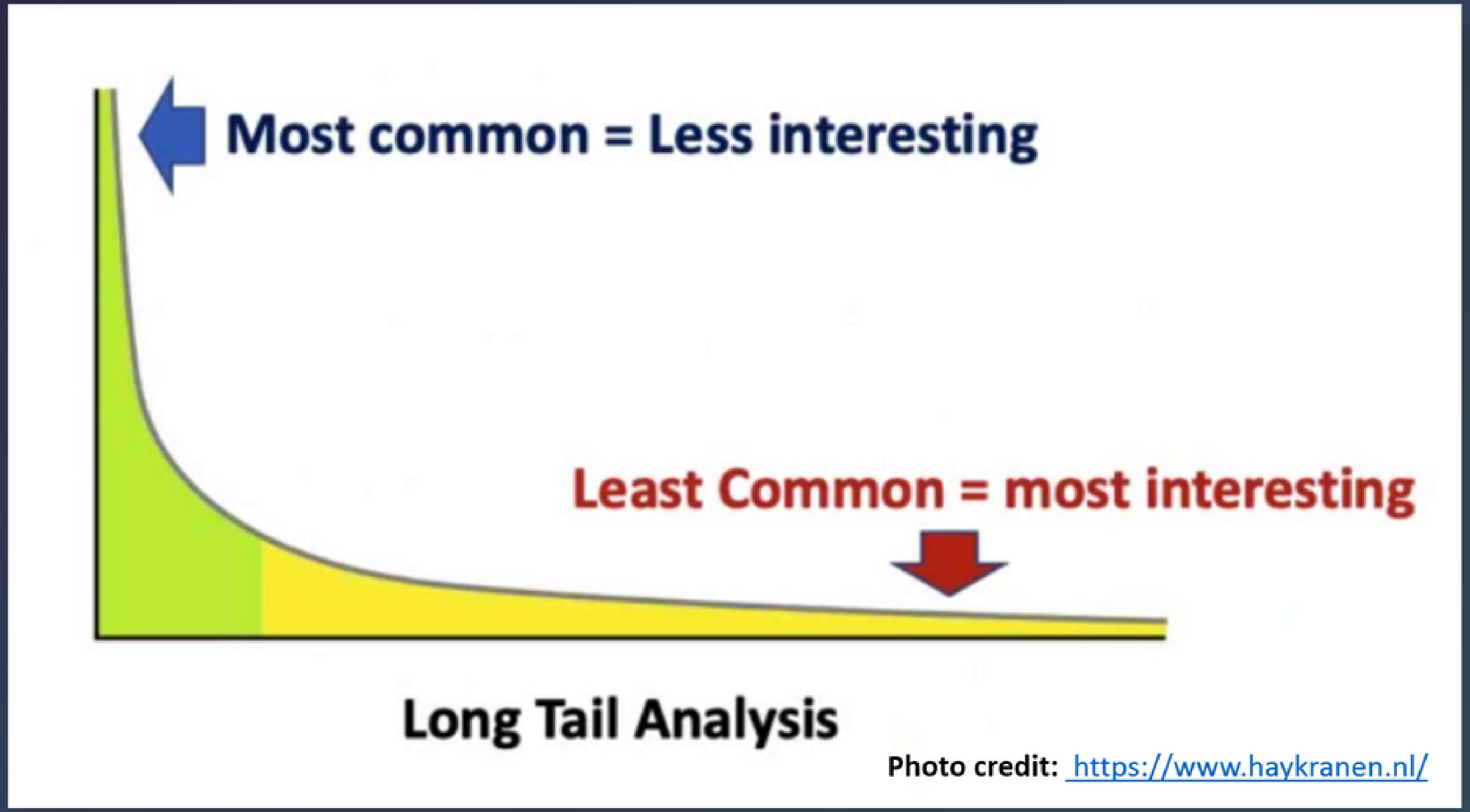


Photo credit: https://www.haykranen.nl/

Remeber the hunt results are only as good as the data your collect and examine. That's why it's important to work with other key stakeholders such as your security operations, incident responders, digital forencis to ensure you are collecting, storing and backing up the data you need to perform a successful hunting activities.

Benefits

IMPROVING SECURITY POSTURE

Employees who perform threat hunting activities work with other key security stakeholders and share information to improve monitoring and alerting, and build baseline known good traffic.

DISCOVER UNKNOWN THREATS

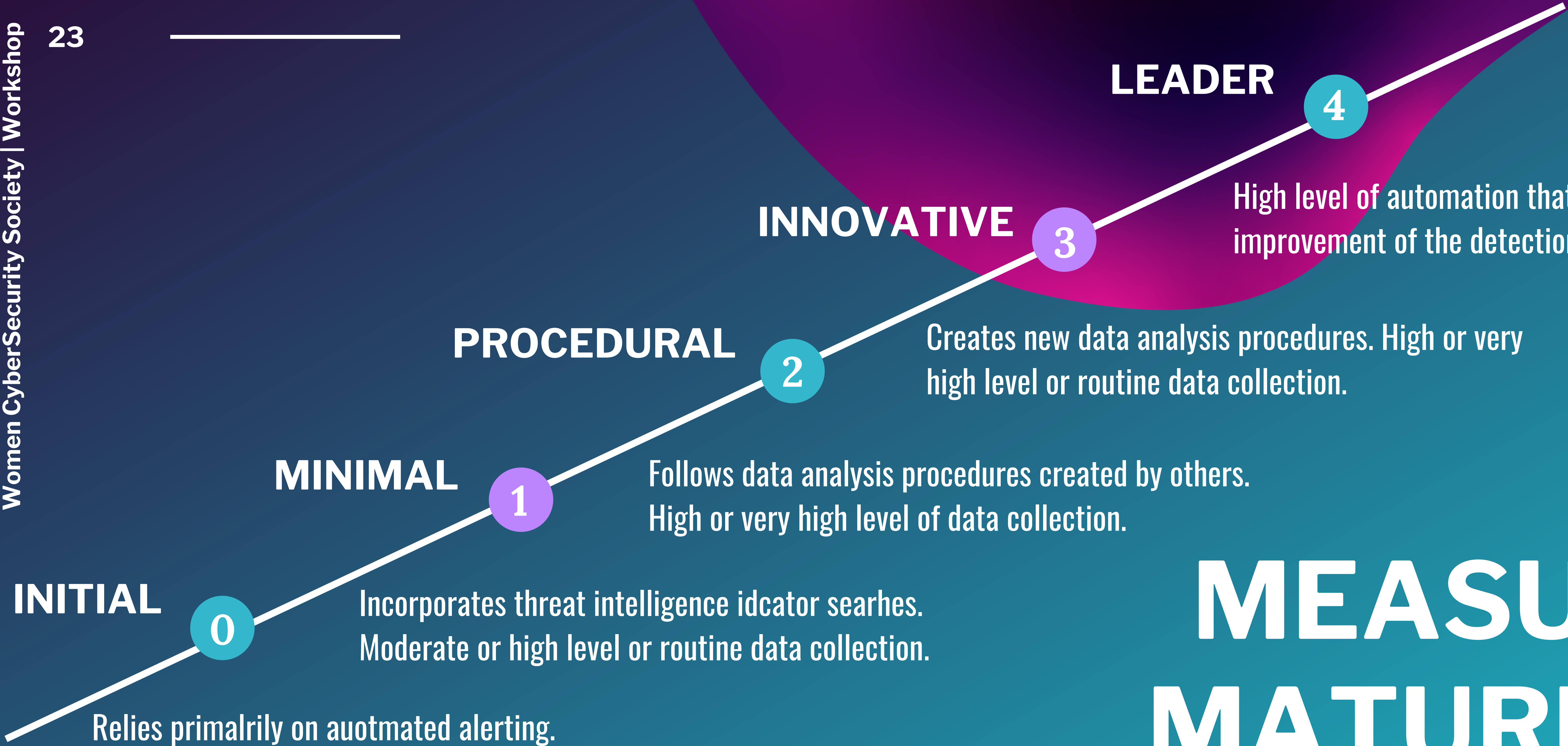
Threat hunting activities are investigations into unknown threats that have not been detected by existing technology, processes or people. Compromised devices ofen have threat detection software disabled by sophisticated malware so a hunter needs to use dig to discover compromised endpoints based on beahvior indicators.

LOWERING RISK

Discover of unknown threats lower risk to an organization catching the nefarious actor before data is exfiltrated, encrypted or destroyed resulting in savings of time, money and internal resources.

MEASURE MATURITY

THREAT HUNTING REFERENCE MODEL



INITIAL 0

Relies primalrily on auotmated alerting.
There is little to no routine data collection.

MINIMAL 1

Incorporates threat intelligence idcator searhes.
Moderate or high level or routine data collection.

PROCEDURAL 2

Follows data analysis procedures created by others.
High or very high level of data collection.

INNOVATIVE 3

Creates new data analysis procedures. High or very high level or routine data collection.

LEADER 4

High level of automation that results in constant improvement of the detection program.

Credit: David Bianco

Women CyberSecurity Society | Workshop

ON THE HUNT

Microsoft Network Monitor 3.4 (archive)

microsoft.com

PACKET CAPTURE

Using various tools to capture and examine packets is a key component of threat hunting activities. You can examine wired and wireless network traffic, Bluetooth, USB and other devices for incidcators of compromise.

WINDOWS TOOLS

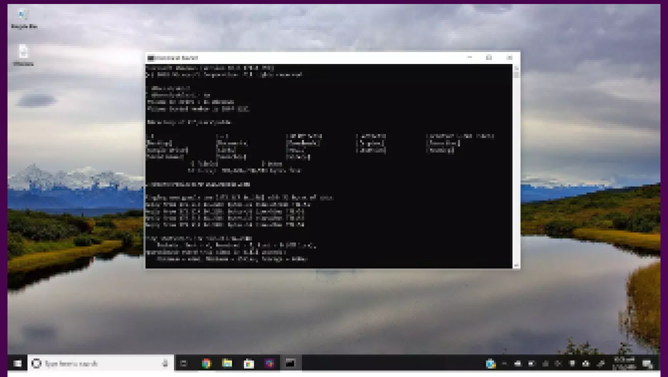
Hunting for threats often involves examining event logs and other data sets to look for threats. Today, we'll explore common Windows tools you can utilize to begin your threat hunting exercises from home.

Women CyberSecurity Society | Workshop

Lab Exercise

Using command line, we'll perform a few exercises to demonstrate access to running processes, ports, protocols and IP addresses.

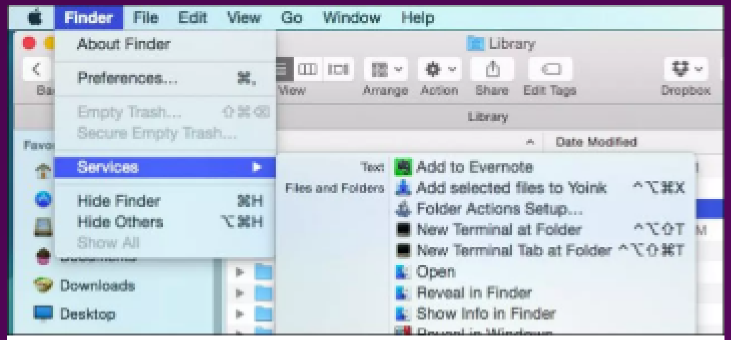
WINDOWS



How to Open Command Prompt in All Versions of Windows

Here's how to open Command Prompt in Windows 10, 8, 7, Vista, and XP. You have to open the Command Prompt in Windows before executing a command.

MAC OS



How to Open Terminal in the Current OS X Finder Location

Have you ever been working in OS X's Finder and wanted to open the Terminal in that exact location? There's an easy way to do this, and then there's an...

https://www.wireshark.org/

WIRESHARK

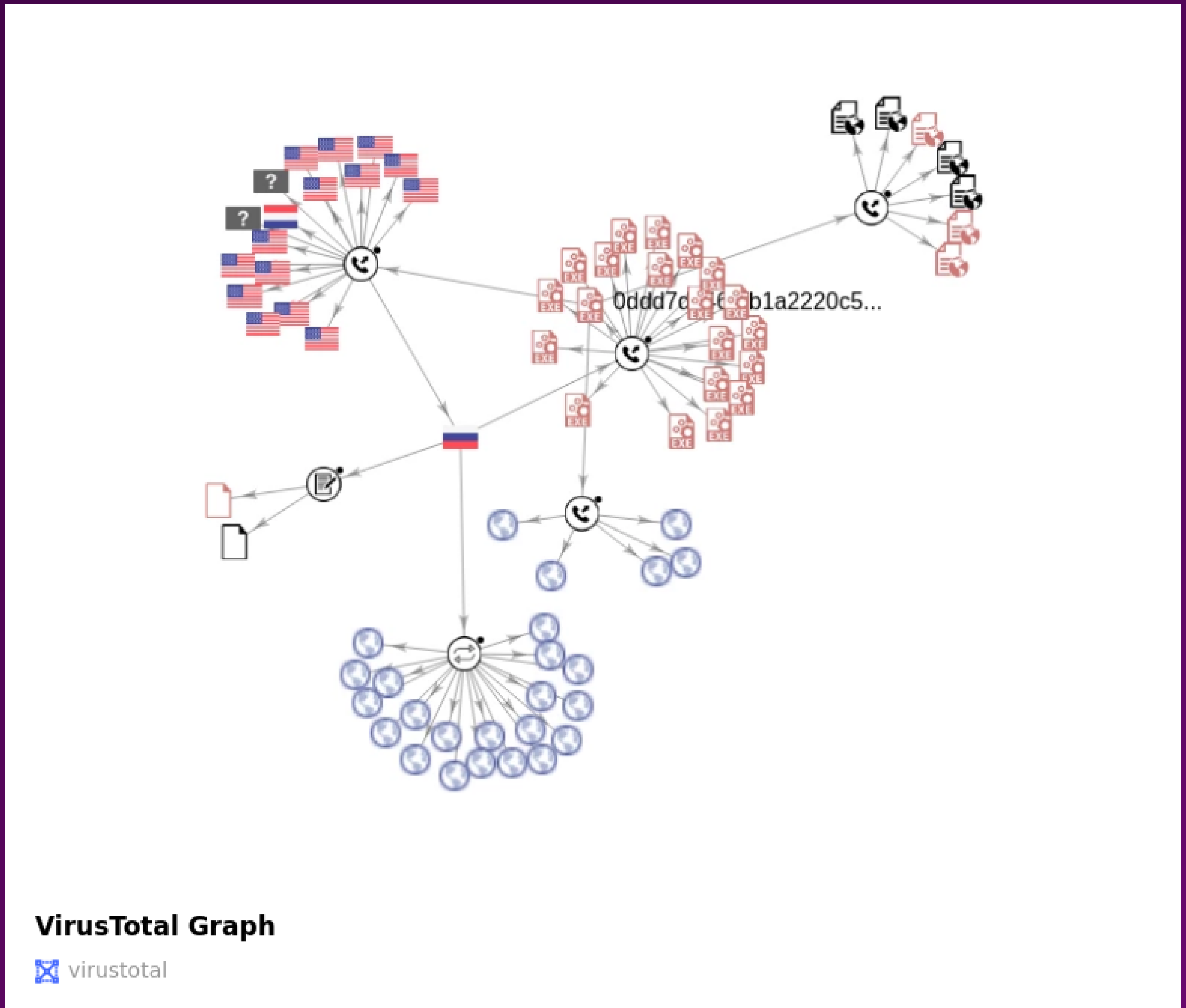
Wireshark is an open source tools that allows you to capture data traveling over your network and filter based on specific data or values.

Women CyberSecurity Society | Workshop

VIRUS TOTAL

We'll examine a new variant of a Trojan Horse.

ttps://www.virustotal.com/graph/g01b311708ad740dcb54e903a58871f18c64337d9c9e1494c866cc1af93b8d6d1



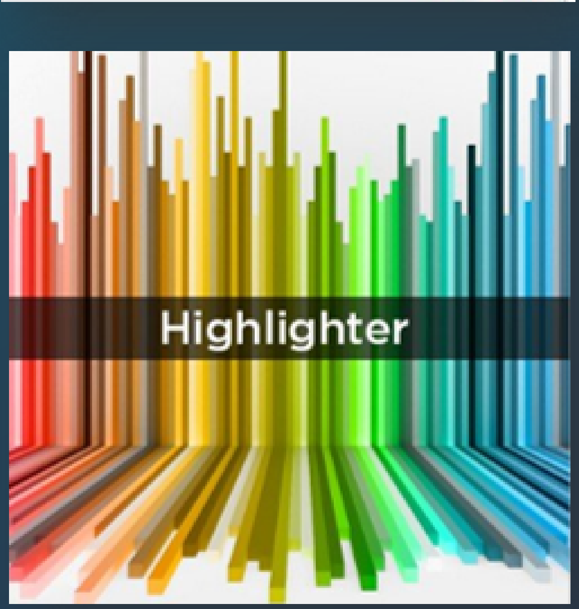
VirusTotal Graph

virustotal

Women CyberSecurity Society | Workshop

Analysis TOOLS

CHALLENGE YOURSELF



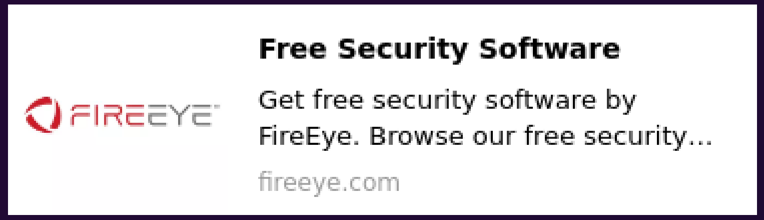
Resources

EXPAND YOUR KNOWLEDGE

Microsoft Network Monitor 3.4 (archive)
microsoft.com

Critical Log Review Checklist for Security Incidents
This cheat sheet presents a...
zeltser.com

A free Linux Toolkit for Reverse-Engineering and...
REMnux is a free Linux toolkit for...
remnux.org


Free Security Software
Get free security software by FireEye. Browse our free security...
fireeye.com

https://www.threathunting.net/
http://detect-respond.blogspot.com/
https://remnux.org/docs/distro/tools
https://docs.umbrella.com/investigate-api/docs/top-million-domains
https://slidelegend.com/a-framework-for-cyber-threat-hunting-sqrrl_5ad06d5c7f8b9a378c8b456a.html
https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center
https://haveibeenpwned.com/
https://www.fireeye.com/services/freeware.html
https://zeltser.com/malicious-software/
https://www.malwarebytes.com/pdf/white-papers/SANS_Report-The_Hunter_Strikes_Back_2017.pdf
https://tools.kali.org/forensics/volatility

Women CyberSecurity Society | Workshop

Social Media

LIKE & FOLLOW US

TWITTER

@womencssociety

WEBSITE

womencybersecuritysociety.org

FACEBOOK

https://www.facebook.com/WomenCSSocietyInc/

LINKEDIN

linkedin.com/company/women-cybersecurity-society-wcs2