Andrew Kozma

- InfoSec professional that used to work in healthcare
- A big fan of Bruce Lee, Ninjas and Samurai films
- 1 of 5 Directors of ATLSECCON
  - www.atlseccon.com
- 1 of 5 organizers for the HASK
  - www.thehask.com
- A husband, a father, nerd with a lab in my basement…

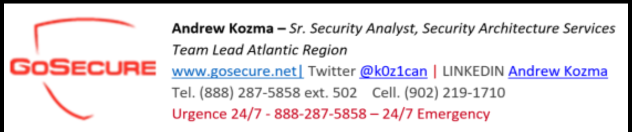
Practical Threat Hunting

A Field Guide

ISACA 2017

Atlantic Provinces Chapter
Information Security & Risk Conference

November 7-8, 2017
Halifax, Nova Scotia



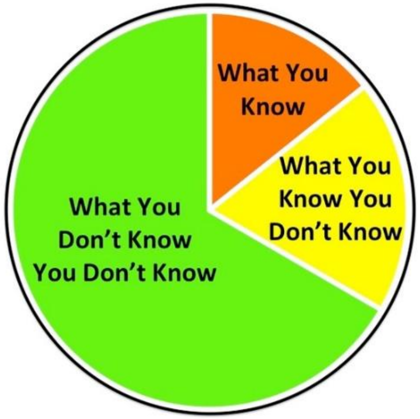
GOSECURE

Andrew Kozma – *Sr. Security Analyst, Security Architecture Services*
Team Lead Atlantic Region
www.gosecure.net | Twitter @k0z1can | LINKEDIN Andrew Kozma
Tel. (888) 287-5858 ext. 502 Cell. (902) 219-1710
Urgence 24/7 - 888-287-5858 – 24/7 Emergency

Threat Hunting

Objectives

- Minimize the frequency of attacks
- Minimize impact
- Earliest possible detection
- Reduce adversary dwell time

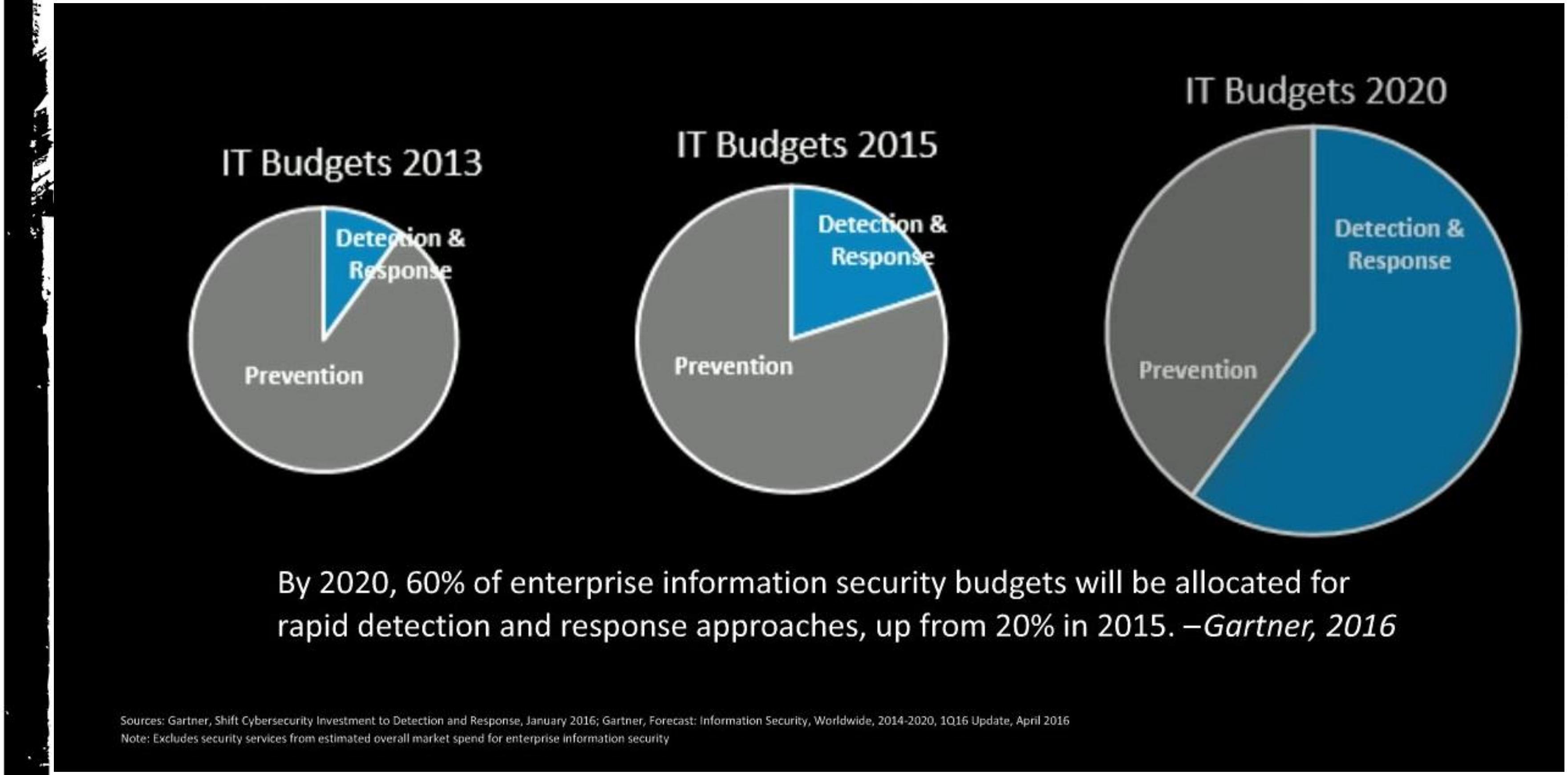

What You Know
What You Know You Don't Know
What You Don't Know You Don't Know

Q: What percent of emerging and advanced threats are missed by automation security tools?

threats go undetected by automated security tools

Source: 2017 Threat Hunting Report
http://www.cybersecurity-insiders.com/wp-content/uploads/2017/02/2017-Threat-Hunting-Report.pdf

Threat Hunting



By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from 20% in 2015. –*Gartner, 2016*

Sources: Gartner, Shift Cybersecurity Investment to Detection and Response, January 2016; Gartner, Forecast: Information Security, Worldwide, 2014-2020, 1Q16 Update, April 2016
Note: Excludes security services from estimated overall market spend for enterprise information security

Threat Hunting

Adversaries

Means – Highly capable, have proven methodologies and have the upper hand

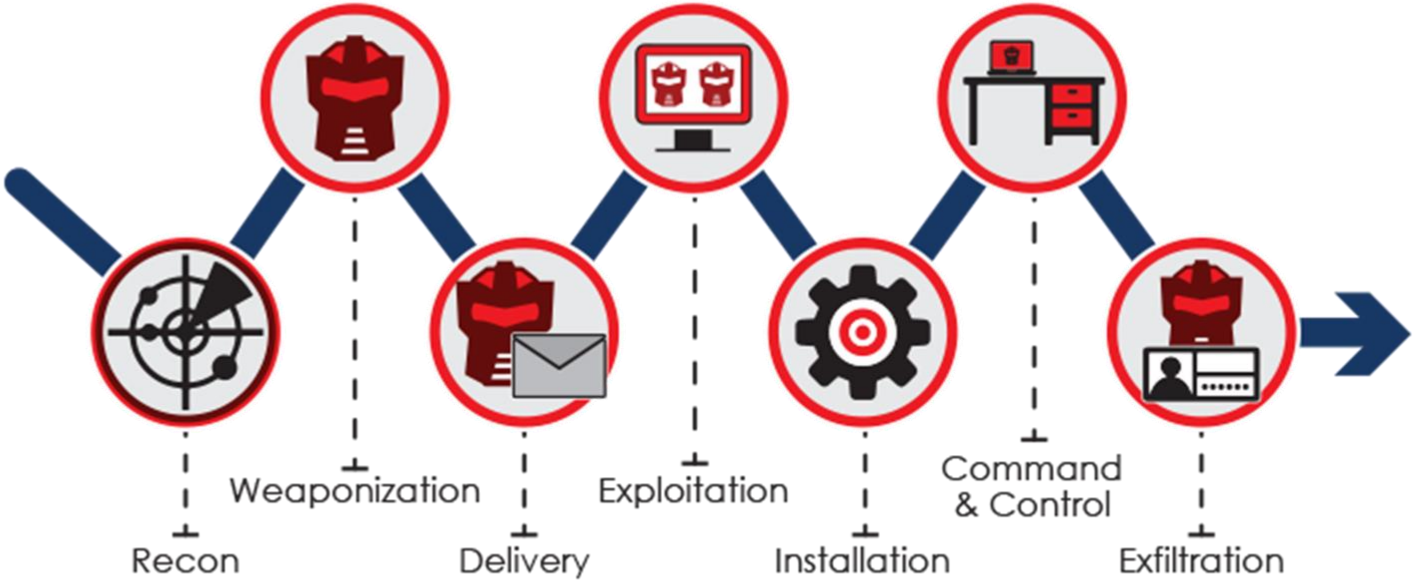
Motive – Financially or politically driven

Opportunity – Will exploit your weaknesses

Objective – Maintain foothold, exfiltrate data, disrupt operations

Threat Hunting

Cyber Kill Chain



Threat Hunting

Adversary TTP

- Majority of attacks do not appear abnormal
- Today’s adversaries are more sophisticated
- Breaches mostly occur due to poor IT Hygiene
    - If a simple exploit works an adversary will use it

Threat Hunting

Shellcode Injection

- Shell Code Injection – most basic been around the longest has 4 stages
    - Open Target Process
    - Allocate Memory
    - Write shellcode payload to memory
    - Create thread in remote process to execute shellcode
- An oldie but worth mentioning - Poison IVY RAT

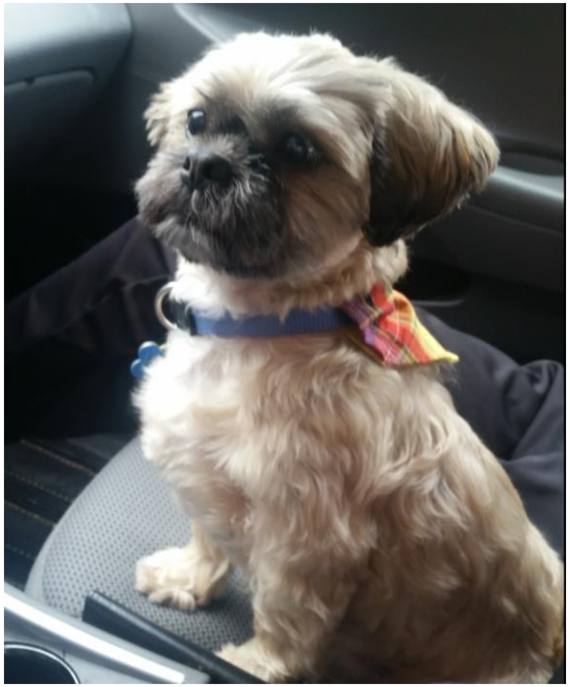
Threat Hunting

Injection and Persistence via Registry Modification

- Appinit_DLL, AppCertDlls, and IFEO (Image File Execution Options) are registry keys that malware has used for both injection and persistence
- Malware can insert the location of their malicious library under the Appinit_Dlls registry key to have another process load their library.
- Every library under this registry key is loaded into every process that loads User32.dll.
- User32.dll is a very common library used for storing graphical elements such as dialog boxes.
- When a malware modifies this subkey, the majority of processes will load the malicious library

Threat Hunting

Hunters



Threat Hunting

01

Human Driven

02

Proactive Search

03

Detect Evaded

Human intelligence and effort required for threat hunting

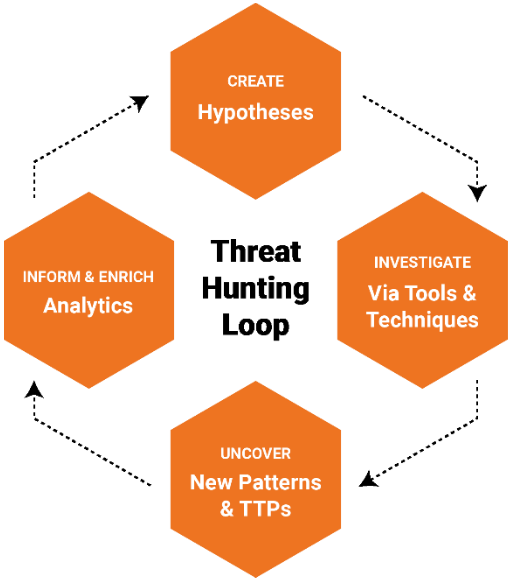
Proactive and iterative search through networks, endpoints or datasets

To detect malicious, suspicious, or risky activities that have evaded automated tools

Threat Hunting

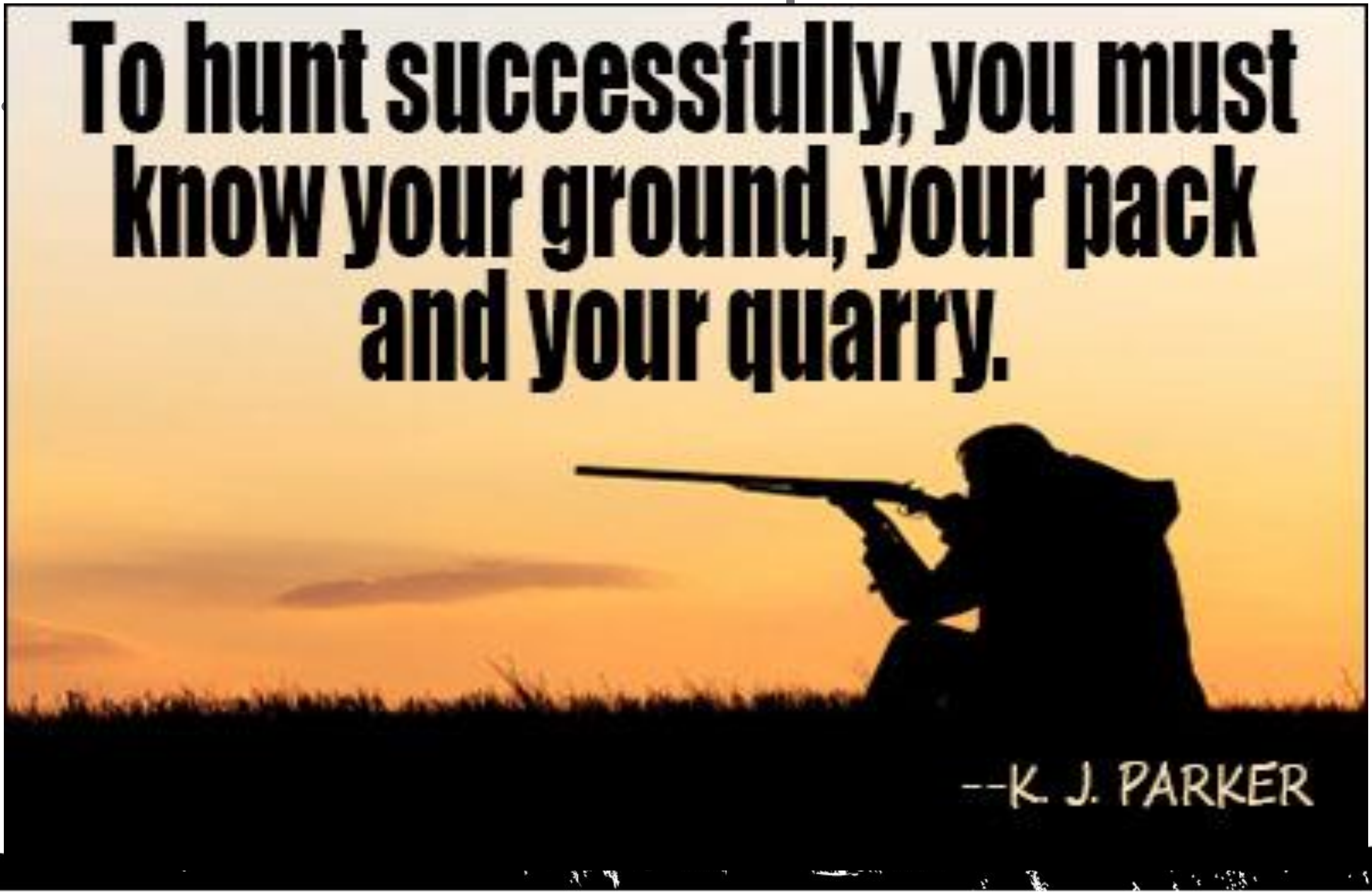
Overview

- A repeatable process of proactively and aggressively searching through networks and datasets to identify and isolate advanced threats that evade existing security controls



Threat Hunting

Foundational Requirements


To hunt successfully, you must know your ground, your pack and your quarry.
--K. J. PARKER

Threat Hunting

Understanding Threat

- What are the threats?
- What can an adversary do?
- Need to understand how adversaries operate
- This supports the 1st step in hunt loop - hypothesis

Threat Hunting

Threat Intelligence

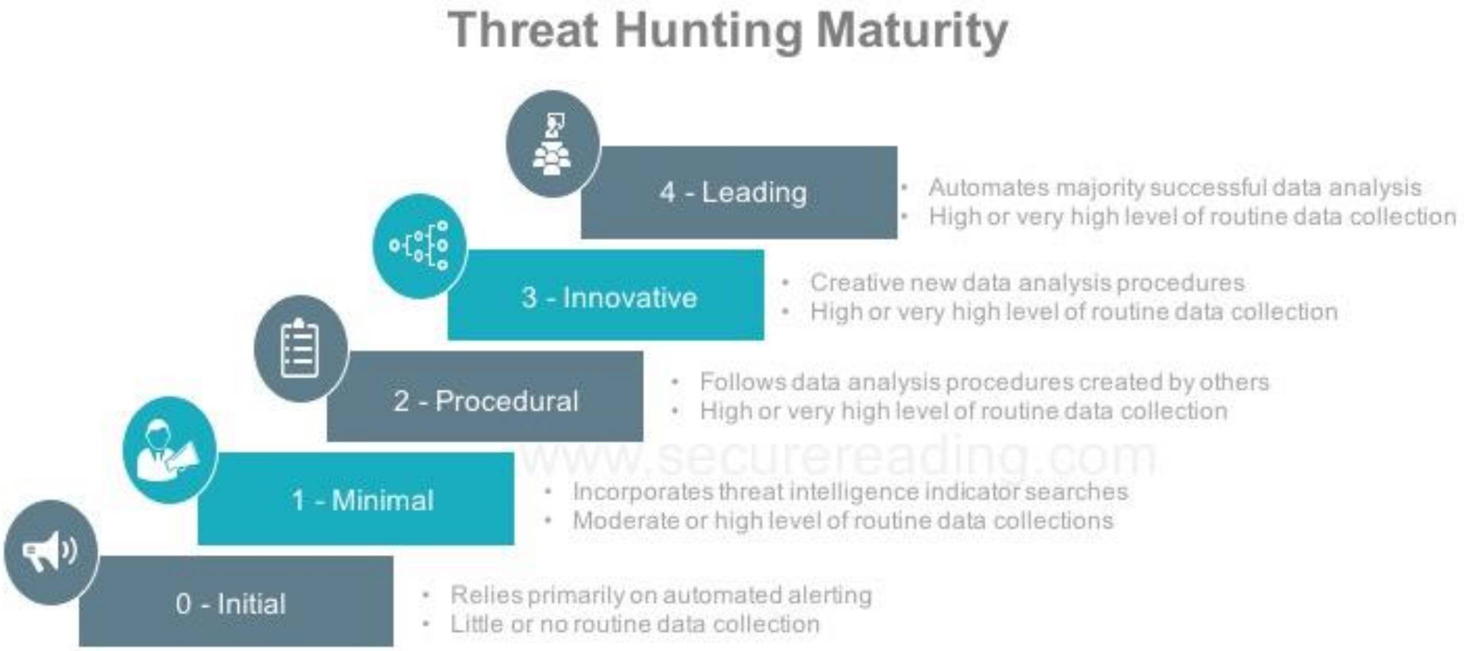
- Many sources and many tools that can incorporate intel
- Required to mature hunting process/procedures
- Can help detect adversaries earlier in the attack lifecycle
- Can reduce resource usage - Win/Win
- Nothing beats your own intel! Baseline of “normal”

Threat Hunting

Efficient versus Effective?

- Threat modelling
- Binary Risk Analysis weigh threats against critical assets
  - What threat is most likely
  - What threat could cause the most damage
- Remember adversaries change tactics and are persistent
- Threat hunting can scale from very basic to advanced

Threat Hunting



Threat Hunting Maturity

4 - Leading

- Automates majority successful data analysis
- High or very high level of routine data collection

3 - Innovative

- Creative new data analysis procedures
- High or very high level of routine data collection

2 - Procedural

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

1 - Minimal

- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collections

0 - Initial

- Relies primarily on automated alerting
- Little or no routine data collection

Threat Hunting

Recap

- Understand goal and value of threat hunting
    - Earliest possible detection
    - Minimal impact by controlling damage
- We know where our critical assets and data resides
- We know what the threats are and how adversaries operate

Threat Hunting

Practical Approach

- We know an adversary at a minimum requires 2 things
  - A compromised endpoint
  - A covert communication channel for CnC

- At its most basic this equals 2 components
  - Endpoint Based Hunting
  - Network Based Hunting

Threat Hunting

Network Based Hunting

- The objective is to identify lateral movement and CnC traffic
  - Lateral movement – Systems that send traffic that scans, probes or attempts to exploit other systems, typically inbound
  - CnC traffic – Typically encrypted traffic destined for unusual IP addresses

- *Blue Team tip – Use a proxy for all outbound traffic

Threat Hunting

Network Based Hunting – Tactical Approach

- List top “X” systems with most outbound connections
- List of top “X” systems with longest connections
- List of top “X” systems transferring the most data out
- Separate servers from workstations to increase fidelity

Threat Hunting

Host Based Hunting

- Host-based hunting involves analyzing an individual computer, looking at both what is installed on the computer and what is running on the systems, with the goal of finding indicators of compromise i.e. new files, new services, new registry keys, files that run on reboot.

Threat Hunting

Host Based Hunting – Tactical Approach

- Adversary - To achieve persistence changes to the system are required
  - **Upload files**
    - Know what files are on the system
  - **Run processes**
    - Look for changes, additions or subtractions
  - **Survive a reboot**
    - Know what runs at startup
  - **Modify Registry**
    - Changes in general
    - Review Run and Run Once keys

Threat Hunting

Hunt Metrics

- **Dwell Time –** How long adversary was there
  - Reduced time from infection to detection
  - Reduced time from detection to investigation
  - Reduced time from investigation and remediation

- **Lateral Movement –** How much damage
  - Number of systems compromised

- **Recurrence –Number of times adversary able to return**
  - Number of incidents associated with adversary

Threat Hunting

“ABSORB WHAT IS USEFUL, REJECT WHAT IS USELESS, ADD WHAT IS SPECIFICALLY YOUR OWN.”
– BRUCE LEE