So you want to build a Threat Hunting Program

by Bryan Bowie

PS> whoami

16+ years in Security Roles

Currently

- Sr. Incident Responder for Fortune Company
  - Hunt Lead and Program Organizer

Prior Experience

- Sr. Threat Hunter of Managed Services
  - Created and Managed EDR “recipes” for hunts and remediation
- Sr. Security Engineer, Application Security Engineer
  - Incident response & threat intelligence
  - Penetration testing & vulnerability assessments
  - Supported risk management & compliance
  - Auditing & internal control evaluations
- 8 years Army – Infantry & Intelligence

Bryan Bowie
CISSP, GCFE, CISM, CEH

Disclaimer

- The information expressed here are those of the author(s) and do not necessarily reflect the official policy or position of their employer or any customers of said employer.

Agenda

- Hunting Overview
- Mission Statement
- Unstructured versus Structured Hunting
- Pyramid of Pain
- Maturity Curve and Matrix
- Process Overview
- Resources
- Questions? Maybe some answers…

Overview of Threat Hunting

Every one has their own definition

- Security Vendors
- MSSPs
- Other Organizations

But what about program maturity?
How do I start one myself in my own org?
What resources are needed?
*Where do I start?

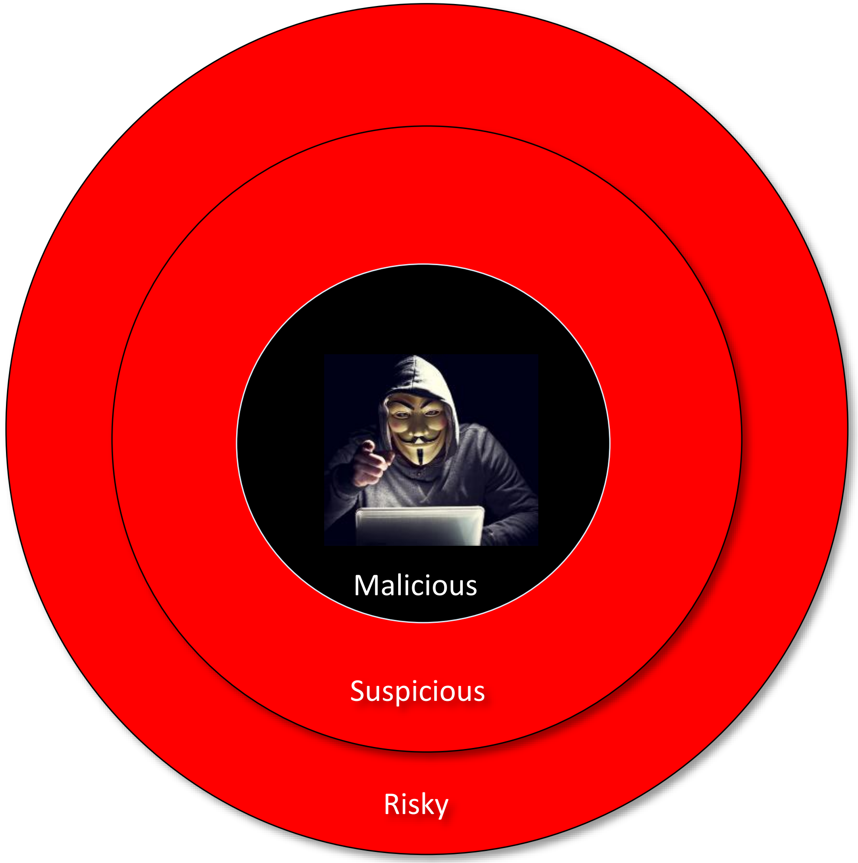
Threat Hunting Mission

Definition:

Threat hunting is the human-driven, proactive and iterative search through networks, endpoints, or datasets in order to detect malicious, suspicious, and/or risky activities that have evaded detection by existing automated tools.

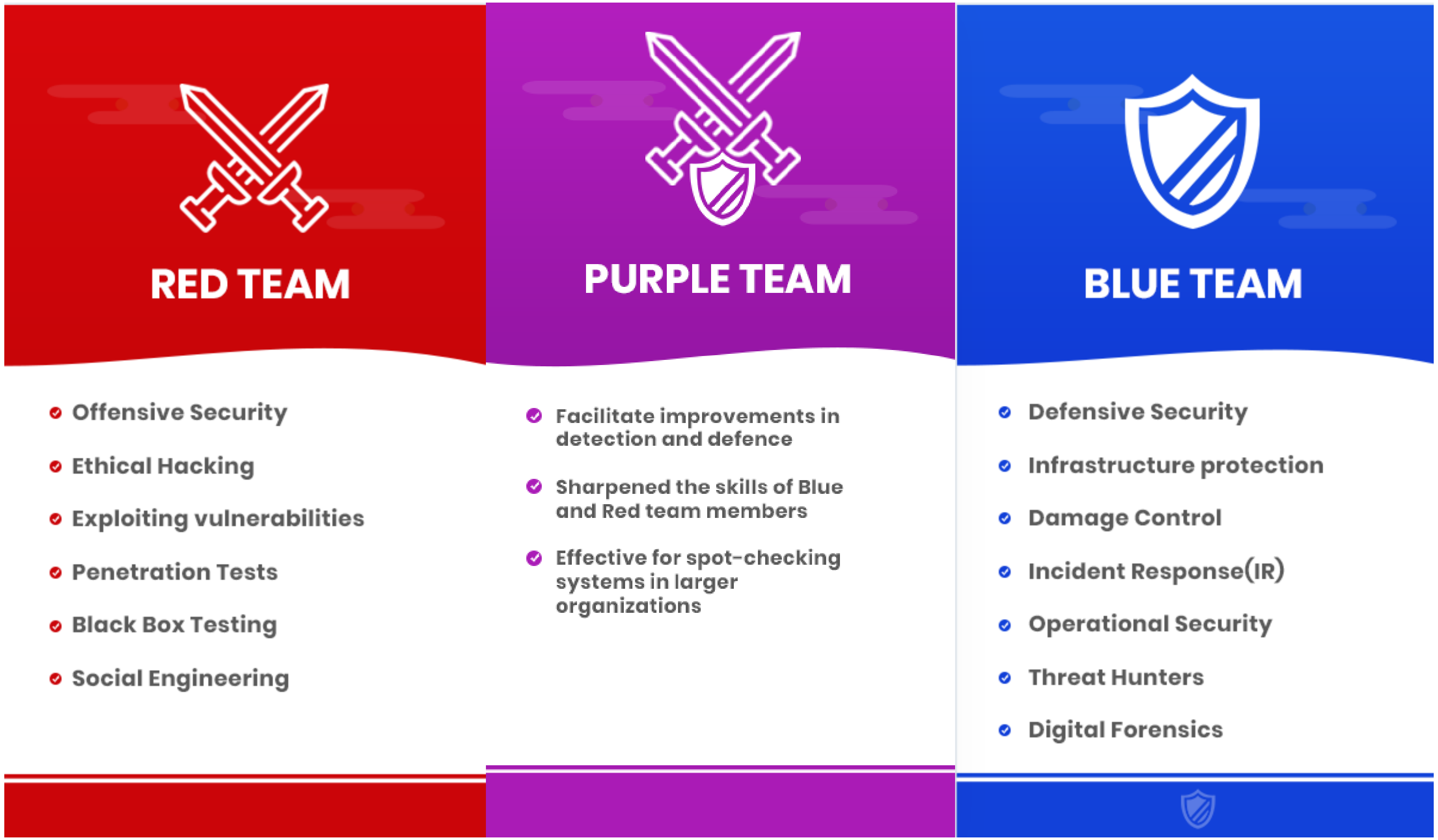
We are not out to just catch evil

"…detect malicious, suspicious, and/or risky activities that have evaded detection…"



What Threat Hunting Is and Is NOT…

- Red Team
- “Purple” Team
- Incident Response
- Automatic or Static
- Results not guaranteed



RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering

PURPLE TEAM

- Facilitate improvements in detection and defence
- Sharpened the skills of Blue and Red team members
- Effective for spot-checking systems in larger organizations

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

Unstructured versus Structured

Unstructured

- Agile
- Flexible Scope
- No dedicated team

However

- Normally Undocumented
- Success and Failure is unknown
- (Level of effort cannot be measured)

Structured

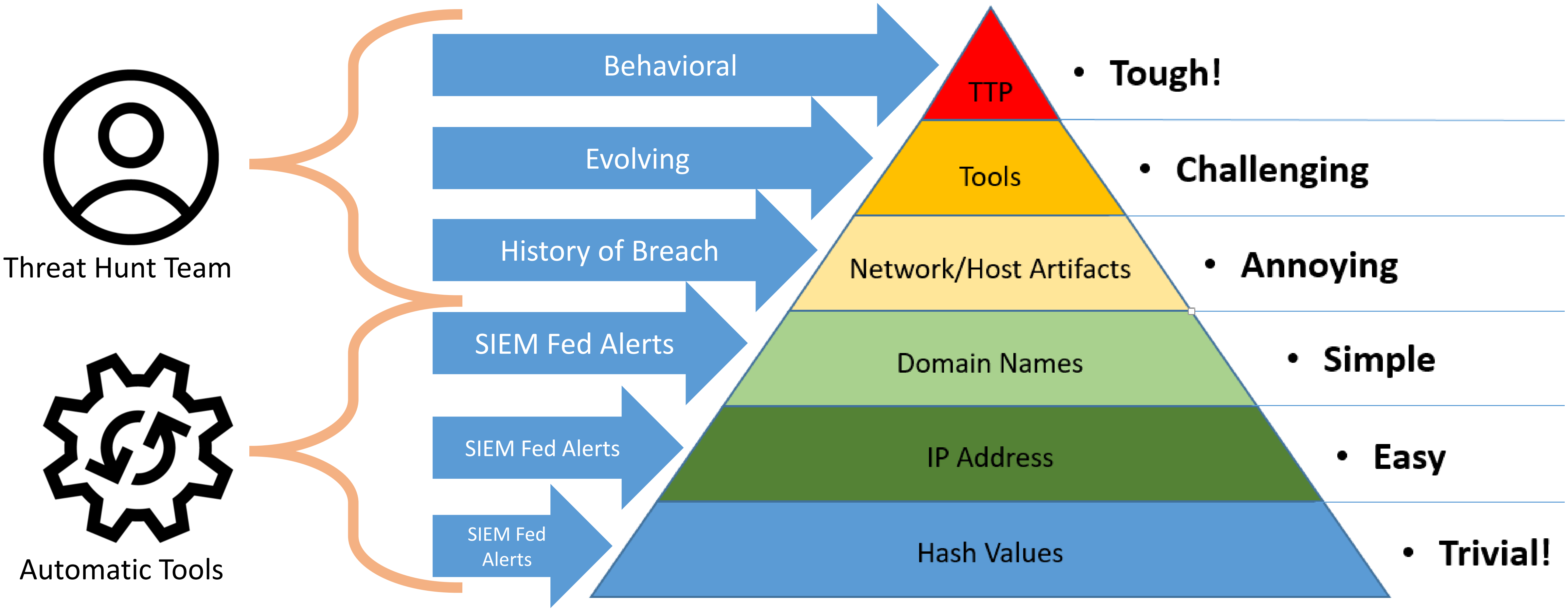
- Cross functional team
- Task / ticket driven
- Repeatable process
- Focused Scope
- Solid metrics

However

- Takes a lot of effort
- Needs management backing to be successful

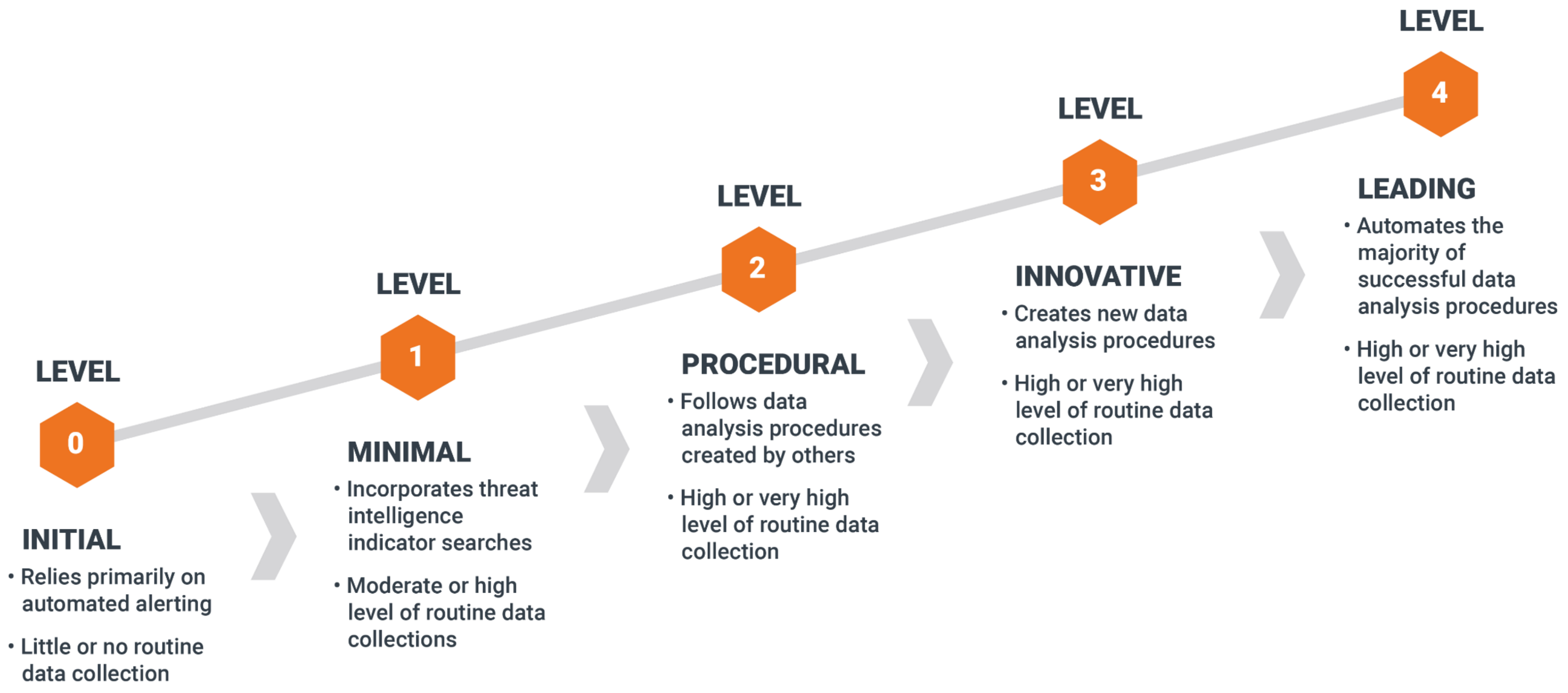
NOTE: Having a structured hunt team should NEVER dissuade someone from hunting in an unstructured manner

Pyramid of Pain



Maturity Curve

- “Its seeing where you are going in your mind. Knowing where you are - by knowing where you been.”
- -Maui, Shapeshifter, Demigod of the Wind and Sea, Hero to All



LEVEL 0

INITIAL

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

LEVEL 1

MINIMAL

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

LEVEL 2

PROCEDURAL

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

LEVEL 3

INNOVATIVE

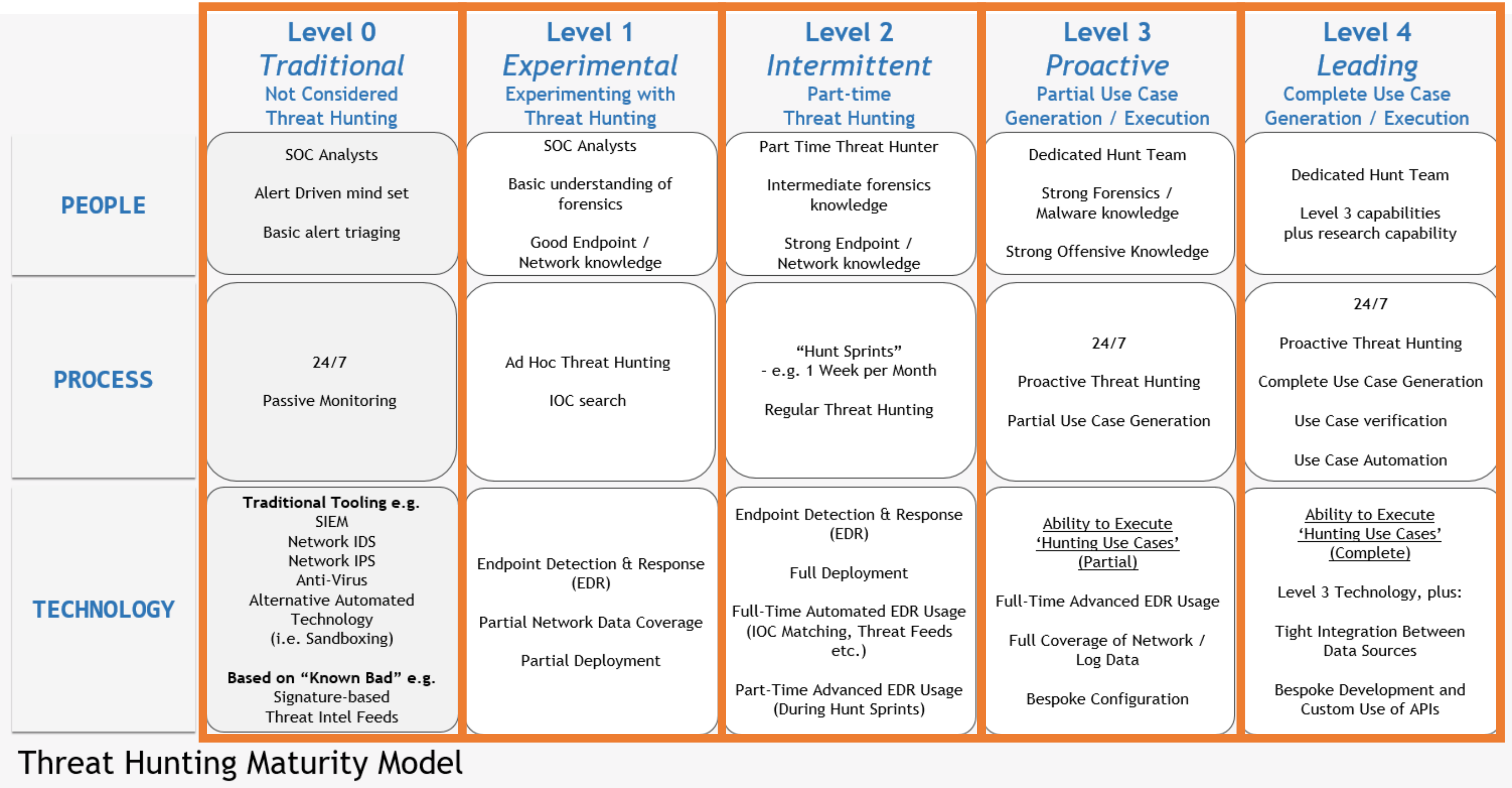
- Creates new data analysis procedures
- High or very high level of routine data collection

LEVEL 4

LEADING

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

Maturity Model Matrix



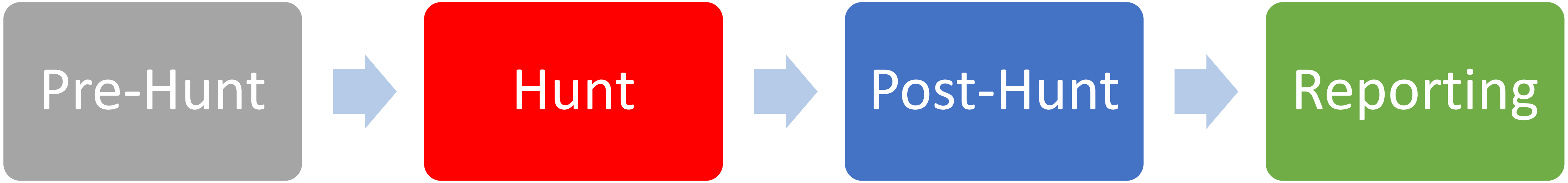
	Level 0 *Traditional* Not Considered Threat Hunting	Level 1 *Experimental* Experimenting with Threat Hunting	Level 2 *Intermittent* Part-time Threat Hunting	Level 3 *Proactive* Partial Use Case Generation / Execution	Level 4 *Leading* Complete Use Case Generation / Execution
PEOPLE	SOC Analysts Alert Driven mind set Basic alert triaging	SOC Analysts Basic understanding of forensics Good Endpoint / Network knowledge	Part Time Threat Hunter Intermediate forensics knowledge Strong Endpoint / Network knowledge	Dedicated Hunt Team Strong Forensics / Malware knowledge Strong Offensive Knowledge	Dedicated Hunt Team Level 3 capabilities plus research capability
PROCESS	24/7 Passive Monitoring	Ad Hoc Threat Hunting IOC search	"Hunt Sprints" - e.g. 1 Week per Month Regular Threat Hunting	24/7 Proactive Threat Hunting Partial Use Case Generation	24/7 Proactive Threat Hunting Complete Use Case Generation Use Case verification Use Case Automation
TECHNOLOGY	**Traditional Tooling e.g.** SIEM Network IDS Network IPS Anti-Virus Alternative Automated Technology (i.e. Sandboxing) **Based on "Known Bad" e.g.** Signature-based Threat Intel Feeds	Endpoint Detection & Response (EDR) Partial Network Data Coverage Partial Deployment	Endpoint Detection & Response (EDR) Full Deployment Full-Time Automated EDR Usage (IOC Matching, Threat Feeds etc.) Part-Time Advanced EDR Usage (During Hunt Sprints)	Ability to Execute 'Hunting Use Cases' (Partial) Full-Time Advanced EDR Usage Full Coverage of Network / Log Data Bespoke Configuration	Ability to Execute 'Hunting Use Cases' (Complete) Level 3 Technology, plus: Tight Integration Between Data Sources Bespoke Development and Custom Use of APIs

Threat Hunting Maturity Model

Maturity Model Matrix Continued

	HM0 Traditional Not considered Threat Hunting	HM1 Experimental Experimenting with Hunting	HM2 Intermittent Part-Time Threat Hunting	HM3 Proactive Partial Use Case Generation / Execution	HM4 Leading Complete Use Case Generation / Execution
People	**SOC Analysts** **Alert Driven Mind Set** **Basic Alert Triaging**	**SOC Analysts** **Basic Understanding of Forensics** **Good Endpoint / Network Knowledge**	Part Time Threat Hunters **Intermediate Forensics Knowledge** Strong Endpoint / Network Knowledge	Dedicated Threat Hunters Strong Forensics / Malware Knowledge Strong Offensive Knowledge	High collection of many types of data throughout IT environment
Process	**24 / 7** **Passive Monitoring**	Ad Hoc Threat Hunting **IOC Search**	"Hunt Sprints" i.e. 2 Week per Month, etc Regular Threat Hunting	24 / 7 Proactive Threat Hunting Partial Use Case Generation	Review threat intelligence and "friendly intel", and manual cyber risk scoring (i.e. "crown jewel analysis) to develop new hypothesis
Technology	**Traditional Tooling e.g.** **SIEM** **Network IDS** **Network IPS** **Anti-Virus** **Alternative Automated Technology (i.e. Sandboxing)** **Based on "Known Bad" e.g.** **Signature-based** **Threat Intel Feeds**	Endpoint Detection and Response (EDR) **Partial Network Data Coverage** **Partial Deployment**	Endpoint Detection and Response (EDR) Full Deployment Full-Time Automated EDR Usage (IOC Matching, Threat Feeds, etc) Part-Time Advanced EDR Usage (During Hunt Sprints)	Leverage visualizations and graph searches. Develop new hunting procedures	Advanced visualizations and graph searches. Publish, and automate new hunting procedures.

Process Overview (10K View)



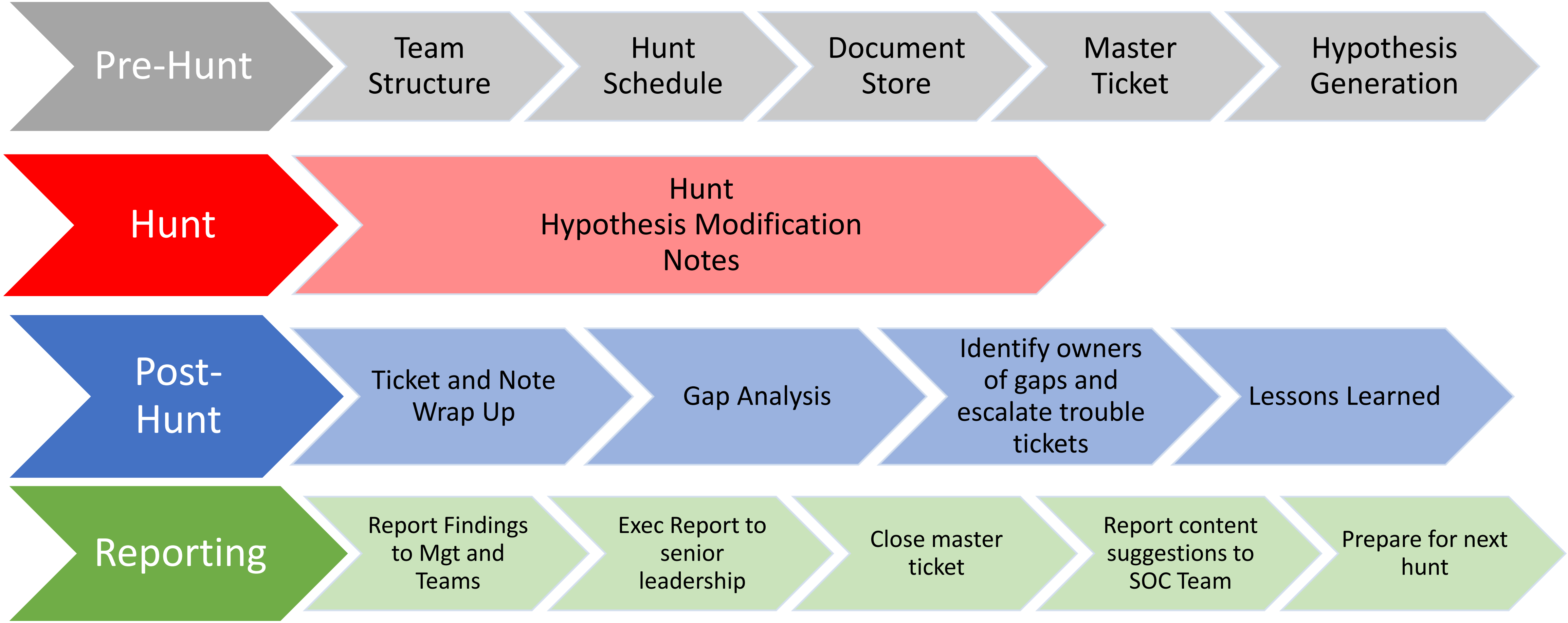
Pre-Hunt

Hunt

Post-Hunt

Reporting

Process Overview (10K View)



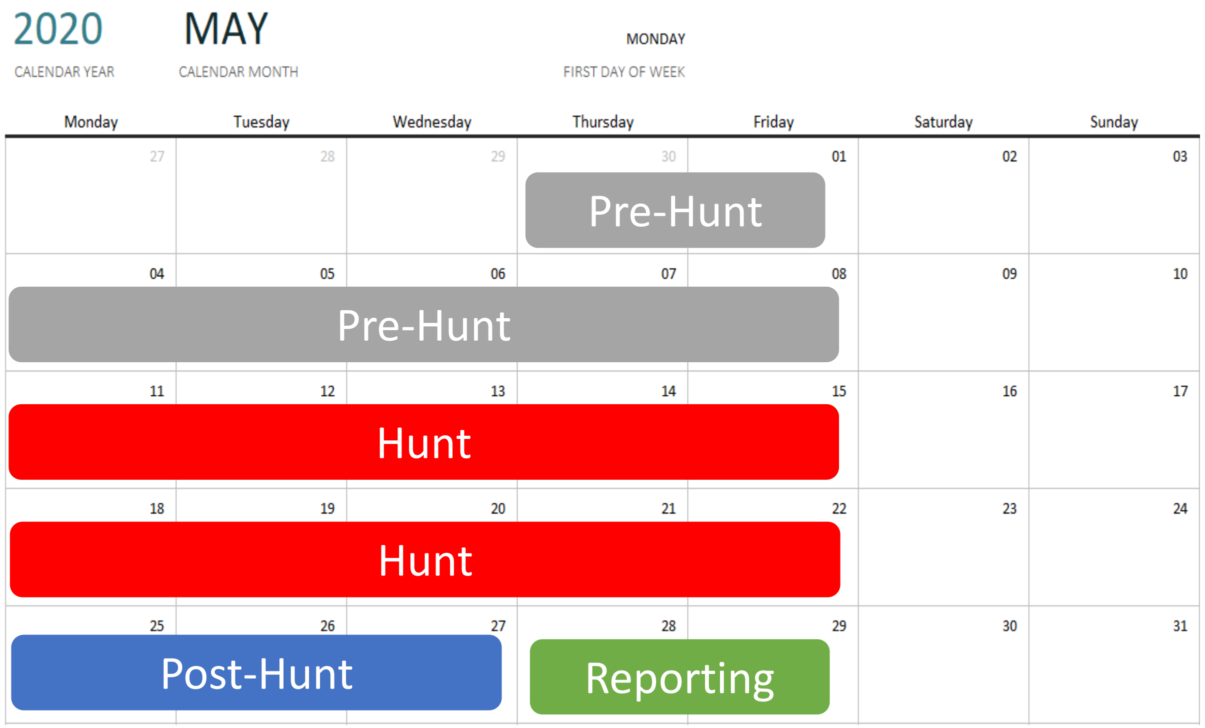
Pre-Hunt
- Team Structure
- Hunt Schedule
- Document Store
- Master Ticket
- Hypothesis Generation

Hunt
- Hunt
- Hypothesis Modification
- Notes

Post-Hunt
- Ticket and Note Wrap Up
- Gap Analysis
- Identify owners of gaps and escalate trouble tickets
- Lessons Learned

Reporting
- Report Findings to Mgt and Teams
- Exec Report to senior leadership
- Close master ticket
- Report content suggestions to SOC Team
- Prepare for next hunt

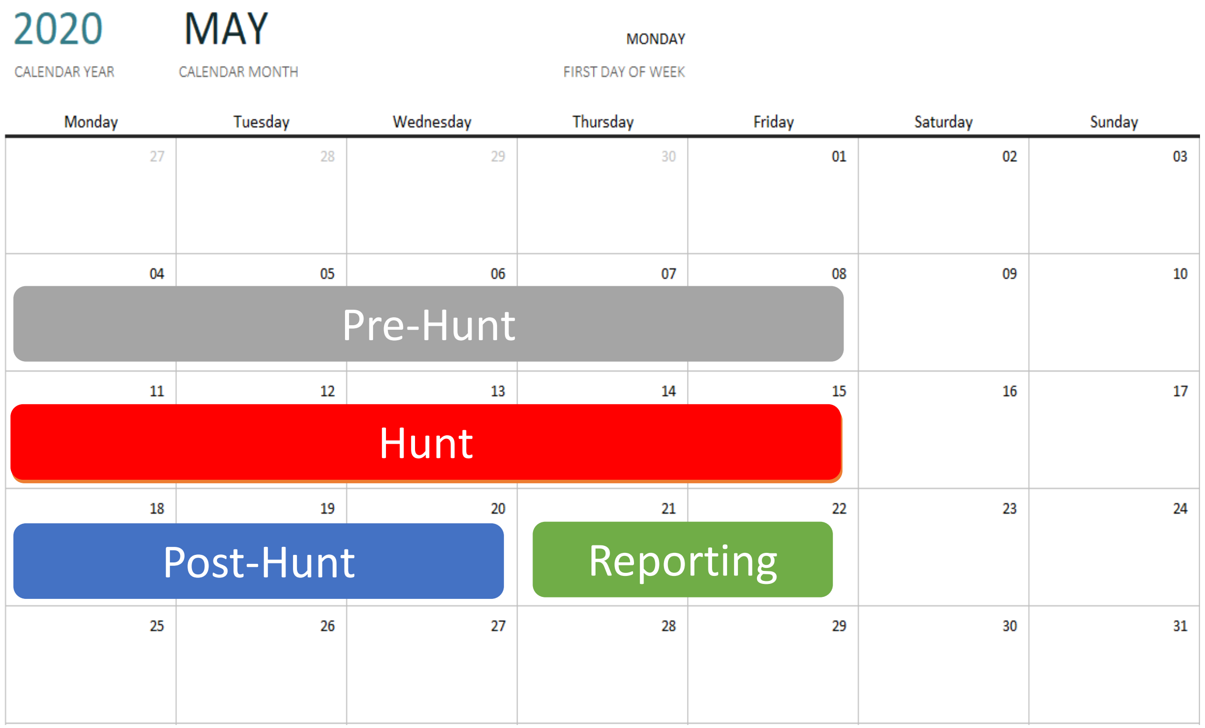
Time Schedule



2020 MAY MONDAY

CALENDAR YEAR CALENDAR MONTH FIRST DAY OF WEEK

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
27	28	29	30 Pre-Hunt	01	02	03
04 Pre-Hunt	05	06	07	08	09	10
11 Hunt	12	13	14	15	16	17
18 Hunt	19	20	21	22	23	24
25 Post-Hunt	26	27	28 Reporting	29	30	31



2020 MAY MONDAY

CALENDAR YEAR CALENDAR MONTH FIRST DAY OF WEEK

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
27	28	29	30	01	02	03
04 Pre-Hunt	05	06	07	08	09	10
11 Hunt	12	13	14	15	16	17
18 Post-Hunt	19	20	21 Reporting	22	23	24
25	26	27	28	29	30	31

Wrapping Up

- **Why** - Find malicious, suspicious, risky activities
- **Where** - Networks, endpoints, or datasets
- **What** – Network/Host Artifacts, Tools, and TTPs
- **Who** - Cross functional team
- **When** – 3 or 4 Week Hunts (or whatever your maturity is)
- **How** – List of Resources and Maturity Matrix

Check List of Resources

- **Documentation Store** – Confluence, Nuclino, Xwiki, Guru, Notepad
- **Ticketing System** – Jira, Hive, ServiceNow
- ***Chat Client** – Google Hangouts, Teams, Slack, Rocket.Chat
- **Document Processing** – MS Office, Gsuite, LibreOffice, OpenOffice
- **Event Logs** – Windows, *Nix, Mac, Applications, Netflows, NDR, etc…
- **Log Manager** – ELK, Splunk, GrayLog, Gravwell
- **System Logs (like EDR information**) – Sysmon, CrowdStrike, Carbon Black, Digital Guardian
- **Management Buy In**

Questions?