Pack Hunting

OPERATIONAL THREAT HUNTING AS A TEAM

BUT FIRST

What is threat hunting?

TO US

"It's a proactive hypothesis lead investigation that goes beyond your current automation footprint."
@RobertMLee

"Operating under the assumption that an organization has been breached, threat hunting is the process of proactively seeking out attacker activity that has evaded automated security tools."

MISCONCEPTIONS

"So… you are part of the red team?"

"You search through the alerts that don't go to the SOC analysts?"

"How do you find something you don't know is there?"

What value does a threat hunting program bring to an organization?

THE VALUE

Team Vision & Mission

Hunt brings peace-of-mind by leveraging a working knowledge of the threat landscape to hunt for and disrupt criminals and nation-state actors.

DETECT.

PROTECT.

CONNECT.

How do you maximize the value a threat hunting program brings to an organization?

MAXIMIZE THE VALUE

Pack Hunting

"A systematic and collaborative approach to hunting that allows a team to work together throughout all phases of hunt operations."

BENEFITS

- Multiple points-of-view on the same hypothesis
- Outcomes that immediately demonstrate value
- Huntresses can choose between breadth and depth for their career
- Increased knowledge sharing between the pack
- Increased documentation of hunter methodologies

MAXIMIZE THE VALUE

Roles of the Pack

LEAD

Keep the pack on target and on time.

Ensure quality deliverables.

HUNTRESS | HUNTER

Seeks evidence of attacker presence within the environment and documents analysis

TRACKER

Follows the leads identified by hunters and determines what to escalate to incident response

TELL THE BUSINESS WHAT YOU DO

Hunt Models

CROWN JEWEL

STARTING POINT

A high value target.

RESEARCH

Infrastructure-based

OUTCOME

Courses of action

BACKSTOP

STARTING POINT

A current deficiency.

RESEARCH

Exploit-based

OUTCOME

Boost Defense

ADVERSARY

STARTING POINT

A threat actor.

RESEARCH

TTP-based

OUTCOME

Courses of action

R&D

STARTING POINT

Curiosity.

RESEARCH

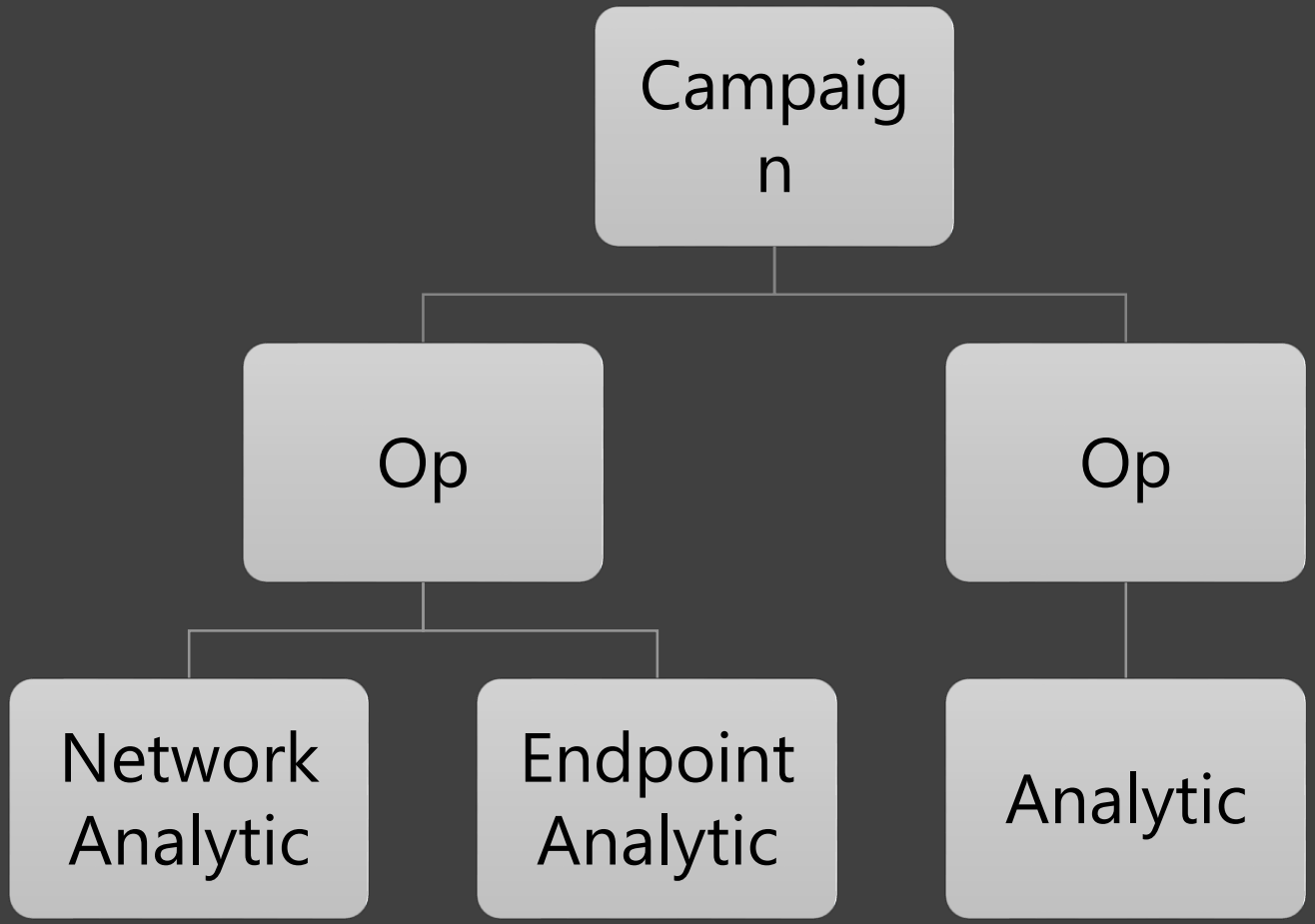
Variable

OUTCOME

Validated analytic

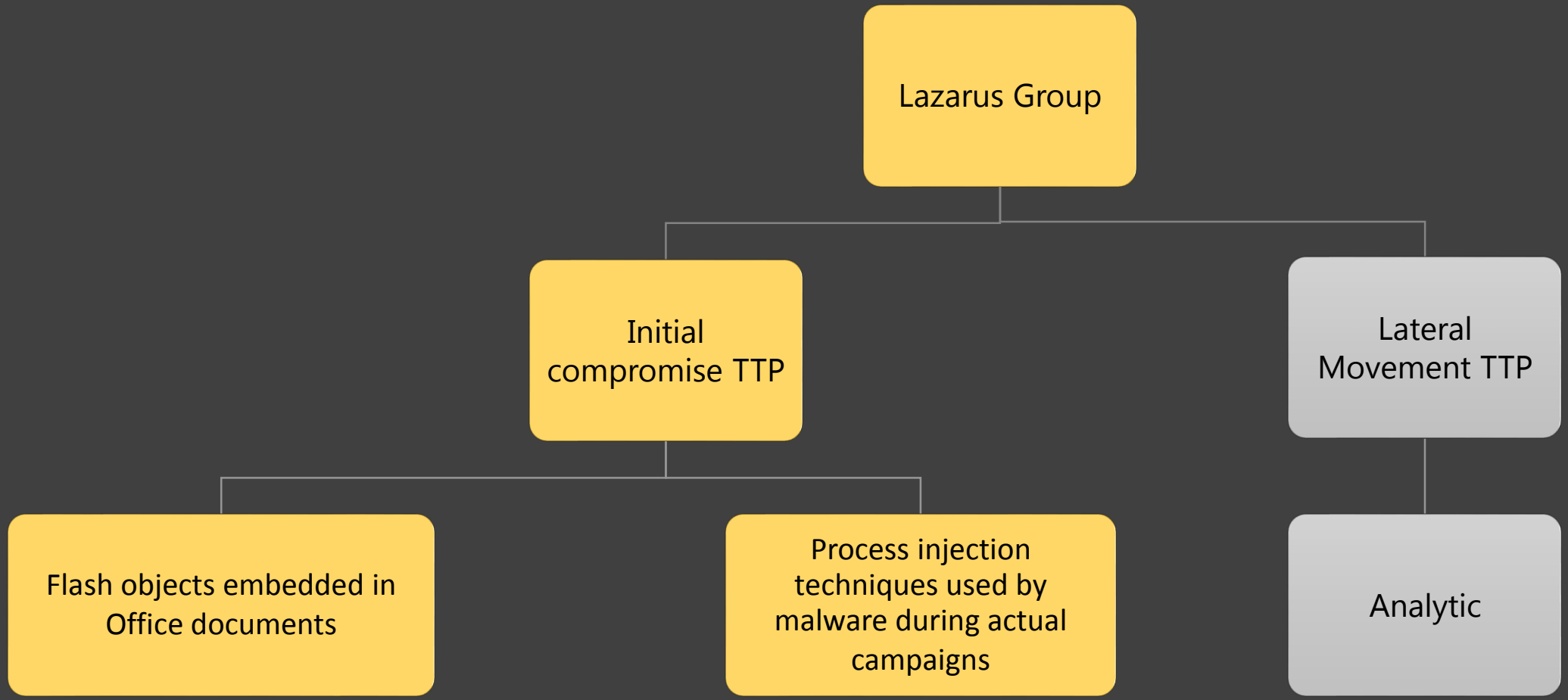
ORGANIZE WHAT YOU DO

Hunt Topology



ORGANIZE WHAT YOU DO

Adversary Hunt Topology



THREAT HUNTING FRAMEWORK

Planning

- Create hypothesis
- Model the threat
- Research infrastructure and current alerting
- Identify data sources
- Develop analytics
- Engage stakeholders

HYPOTHESIS

Malicious actors used a weaponized Microsoft Office document to deliver a payload leveraging a 0-day vulnerability in Adobe Flash.

RESEARCH

- Analyze the tactical intelligence & malware samples provided by Intel team
- Create a baseline of normal behavior
- Review current security control configurations

DEVELOP ANALYTICS

Analytics developed to target:

- Flash objects embedded in Office documents
- Process injection techniques used by malware during actual campaigns

THREAT HUNTING FRAMEWORK

Hunting

- Systematically apply analytics to the data
- Evaluate current analytics and develop new ones based on analysis
- Investigate leads generated from hunting
- Escalate malicious activity to SOC

NOTE OBSERVATIONS

- Suspicious Activity – *"We found evil!"*
- Red Team – *"We found evil, but it was self-inflicted."*
- Signature Development – *"We found a way to automate finding evil."*
- Gaps – *"We couldn't possibly find evil, here's why."*

TEST THE HYPOTHESIS

Perform analytics to try to disprove your hypothesis.

- Analytics applied to Sysmon data available in SIEM
- Multiple suspicious events escalated for further investigation

PULL THE THREAD

Follow each lead to understand if the suspicious behavior identified was malicious, against policy, or possible due to insecure methodologies

- Identified multiple opportunities to improve Sysmon configuration
- Identified several gaps that made application of analytic more difficult at scale

THREAT HUNTING FRAMEWORK

Documenting

- Develop courses of action
- Summarize and trend the observations
- Evaluate metrics
- Create the final product(s)

TURN OBSERVATIONS INTO ACTIONS

- Requested changes to Sysmon configuration
- Engaged SOC and supporting teams to develop better alerting capabilities
- Documented cases that were initially suspicious but later explained

INFORM VARIOUS STAKEHOLDERS

- Share the courses of action with the stakeholders that can directly implement them
- Share an overview and metrics with leadership
- Share the technical analysis with the SOC and IR

SUMMARY

Implementing Pack Hunting

HUNT MODELS

- Create a high level description of what you do for business stakeholders
- Align final products with these models
- Define your terminology

HUNT ROLES

- Split roles that so you can bring a wide array of talent on the team
- Allow your team to seamlessly move between roles where they have demonstrated the ability

HUNT FRAMEWORK

- Take the time to research before you hunt, so you have a good understanding of what to expect
- Document as much as possible during and after the hunt
- Share it all

Align process to goals.

Use data to show value.

Scope is key to relevancy.

Never stop promoting the program.

Andrew Moore
@malwaresoup

Kristina Sisk
@kathayra
www.happythreathunting.com
www.linkedin.com/in/kristinasisk/

COLLABORATE WITH US