



HUNTING FOR THREATS IN THE ICS ENVIRONMENT

MARC SEITZ | INDUSTRIAL HUNTER
AMY BEJTICH | ADVERSARY HUNTER



MARC SEITZ

THREAT HUNTER
THREAT OPERATIONS



AMY BEJTlich

ADVERSARY HUNTER
THREAT INTELLIGENCE

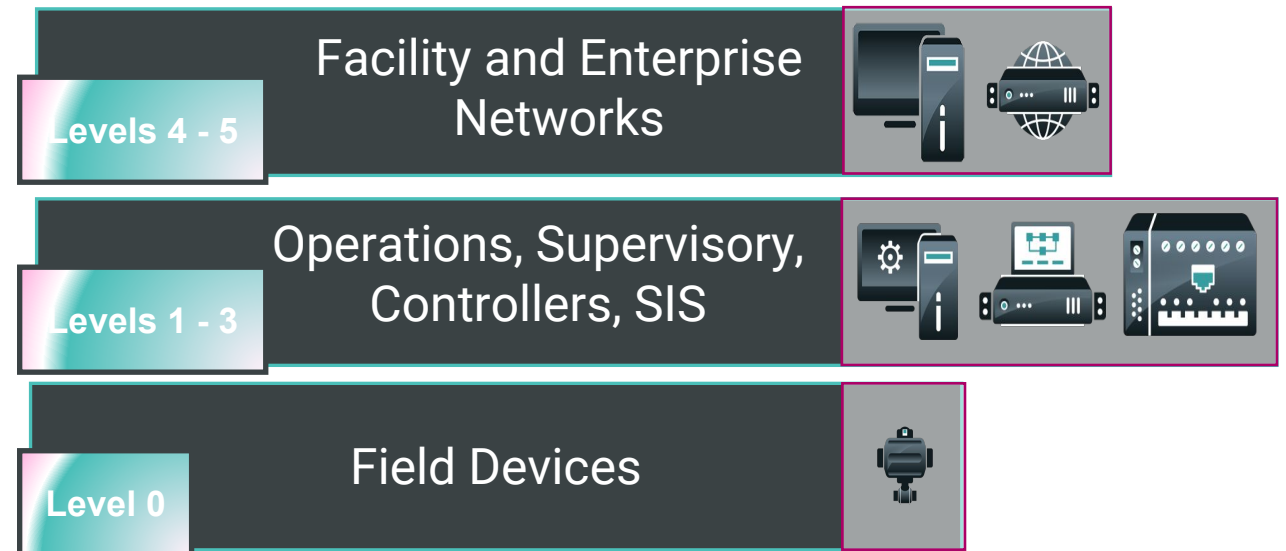
AGENDA

- **ICS LANDSCAPE**
 - **IT/OT PERSPECTIVE**
- **ACTIVITY GROUPS**
 - **DEEP DIVE**
- **HUNTING**
 - **THREAT MODEL**
- **CONCLUSION**
 - **Q&A**

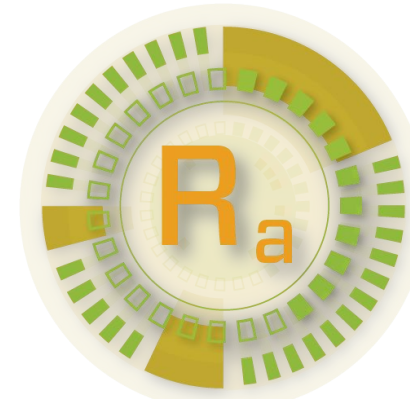
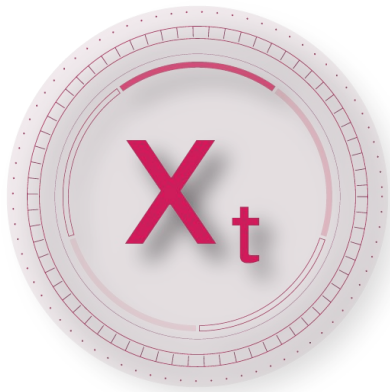
THE ICS ENVIRONMENT

INDUSTRIAL CONTROL SYSTEMS (ICS) IS A GENERAL TERM THAT DESCRIBES THE **NETWORK-CONNECTED** INTEGRATION OF **HARDWARE AND SOFTWARE** THAT CAN AFFECT OR INFLUENCE THE SAFE, SECURE, AND RELIABLE OPERATION OF **INDUSTRIAL PROCESSES**.

THEORY VS. PRACTICE



ICS-TARGETING ACTIVITY GROUPS



LANDSCAPE

ACTIVITY GROUPS

HUNTING

CONCLUSION

DEFINING “ACTIVITY GROUPS”

- COLLECTION OF OBSERVABLE ELEMENTS
- FOCUS ON *HOW* A TRACKED ADVERSARY OPERATES
- LESS EMPHASIS ON *WHO* THEY ARE
- BUILT OFF DIAMOND MODEL OF INTRUSION ANALYSIS

ICS CYBER KILL CHAIN



LANDSCAPE

ACTIVITY GROUPS

HUNTING

CONCLUSION

ACTIVITY GROUPS

- ELECTRUM
- ALLANITE
- XENOTIME
- DYMALLOY



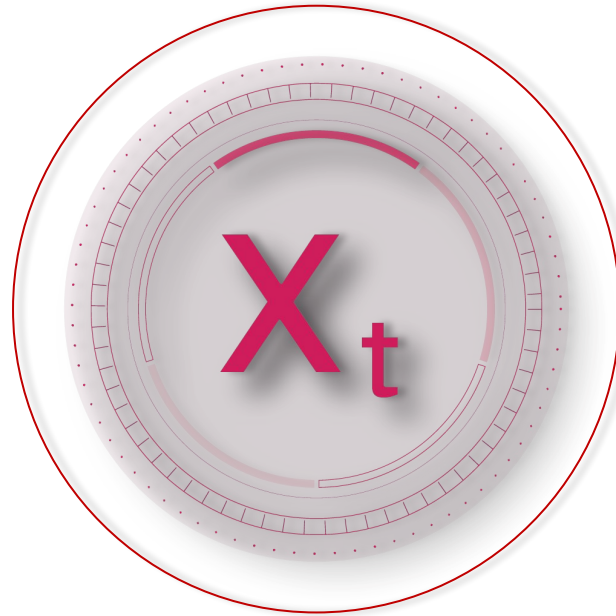
XENOTIME

ADVERSARY

UNIQUE TOOL DEVELOPMENT SINCE AT
LEAST 2014

INFRASTRUCTURE

- SPECIFIC WEB HOSTING PROVIDERS
- LEGITIMATE BUT COMPROMISED INFRASTRUCTURE
- ASIAN SHIPPING COMPANY




CAPABILITY / TRADECRAFT

- TRISIS
- CUSTOM CREDENTIAL HARVESTING
- OFF THE SHELF TOOLS

VICTIM/TARGET

- OIL & GAS, ELECTRIC
- MIDDLE EAST, NORTH AMERICA, APAC, EUROPE
- OEMs, SIS

XENOTIME BEHAVIORS



ENUMERATES PUBLIC-FACING ACCESS AND AUTHENTICATION PORTALS; SEARCHES FOR EXTERNALLY-ACCESSIBLE TCP 445 (SMB) SERVICES.

RELIES ON CREDENTIAL CAPTURE AND REPLAY TO MOVE Laterally WITHIN NETWORKS AND BETWEEN IT AND ICS NETWORKS.

USES NATIVE WINDOWS COMMANDS AND STANDARD SYSTEM TOOLS SUCH AS PSEXEC, AND CUSTOM-BUILT TOOLS FOR OPERATIONS ON VICTIM HOSTS.

USES NON-PUBLIC MALWARE VARIANTS AND PEN TESTING TOOLS FOCUSED ON C2.

How do I find them?

Where do I find them?

What if I don't find anything?

How can I be more efficient?

How many people do I need?

What technologies do I need?

How long is this going to take?

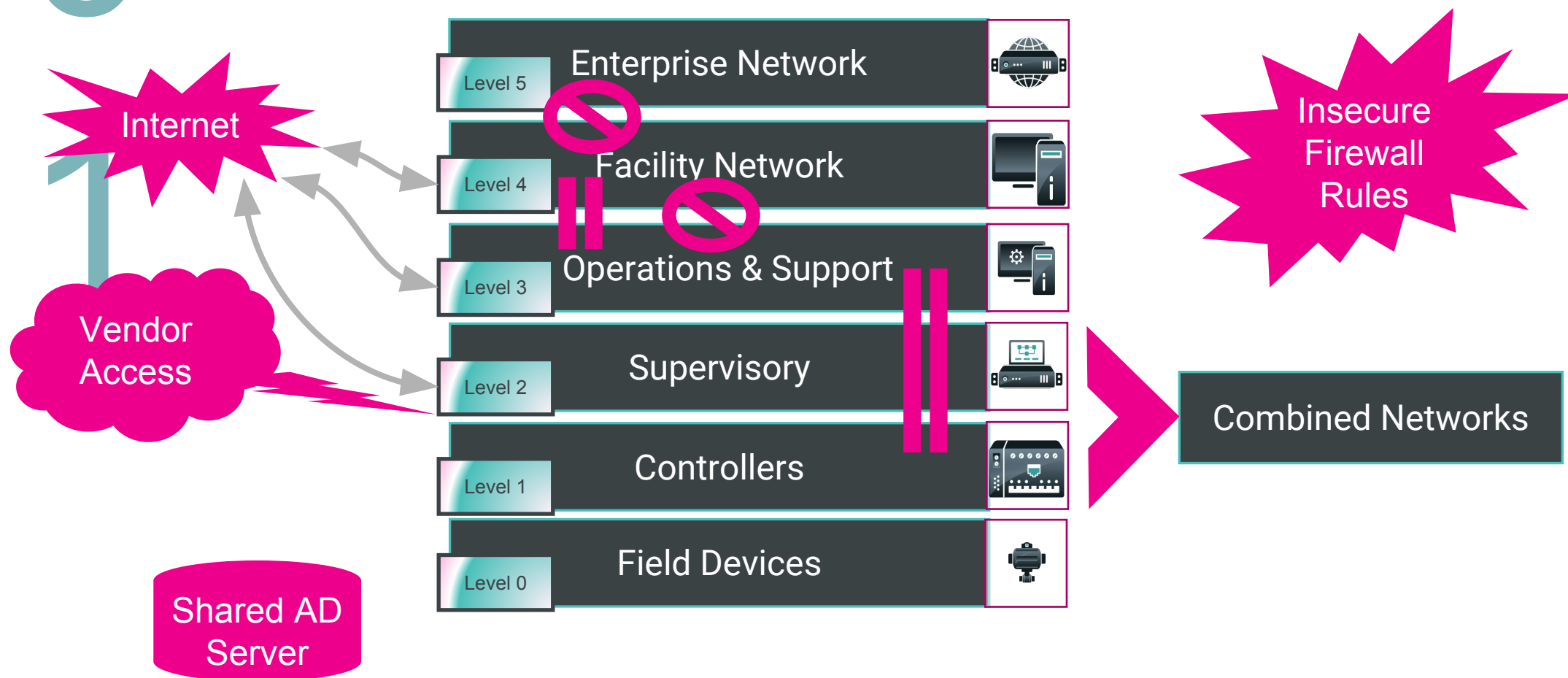


NO SECRET SAUCE

1. Do YOUR HOMEWORK
2. COLLECT RELEVANT DATA
3. ASK QUESTIONS

0

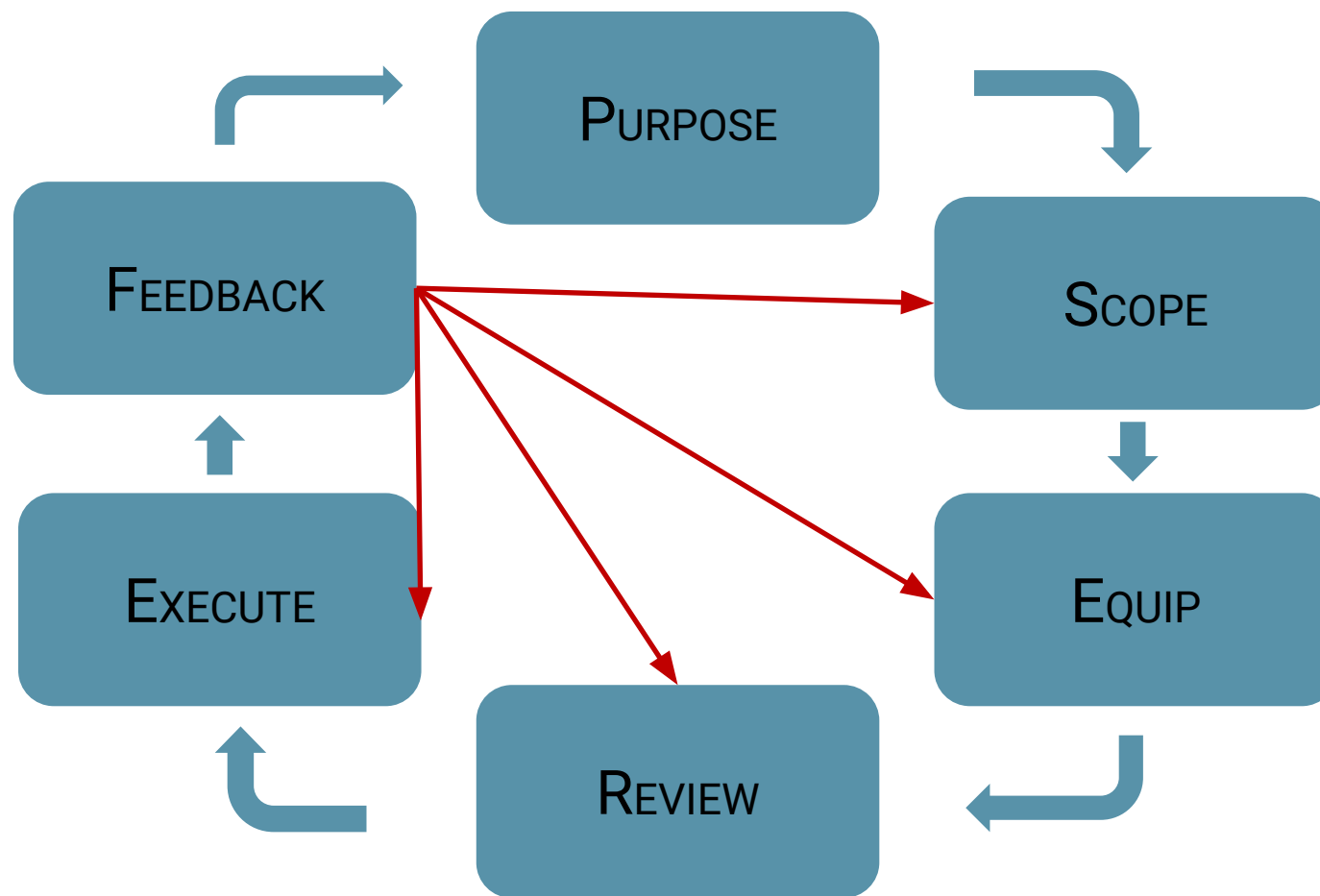
DO YOUR HOMEWORK



0

2

DEFINE A METHODOLOGY/PROCESS AND DOCUMENT FINDINGS



LANDSCAPE

ACTIVITY GROUPS

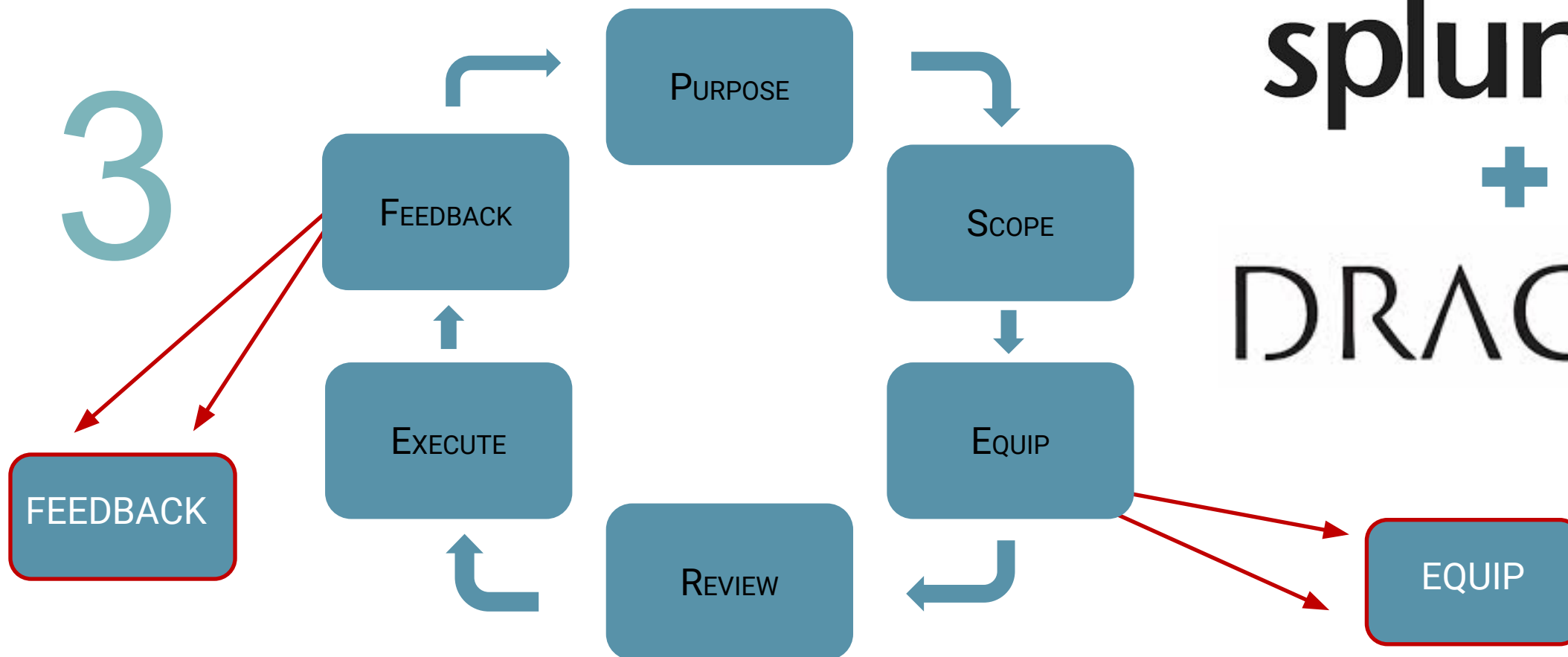
HUNTING

CONCLUSION

0

ENABLE THE HUNT AND CODIFY KNOWLEDGE

3



splunk>

+

DRAGO

LANDSCAPEA

ACTIVITY GROUPS

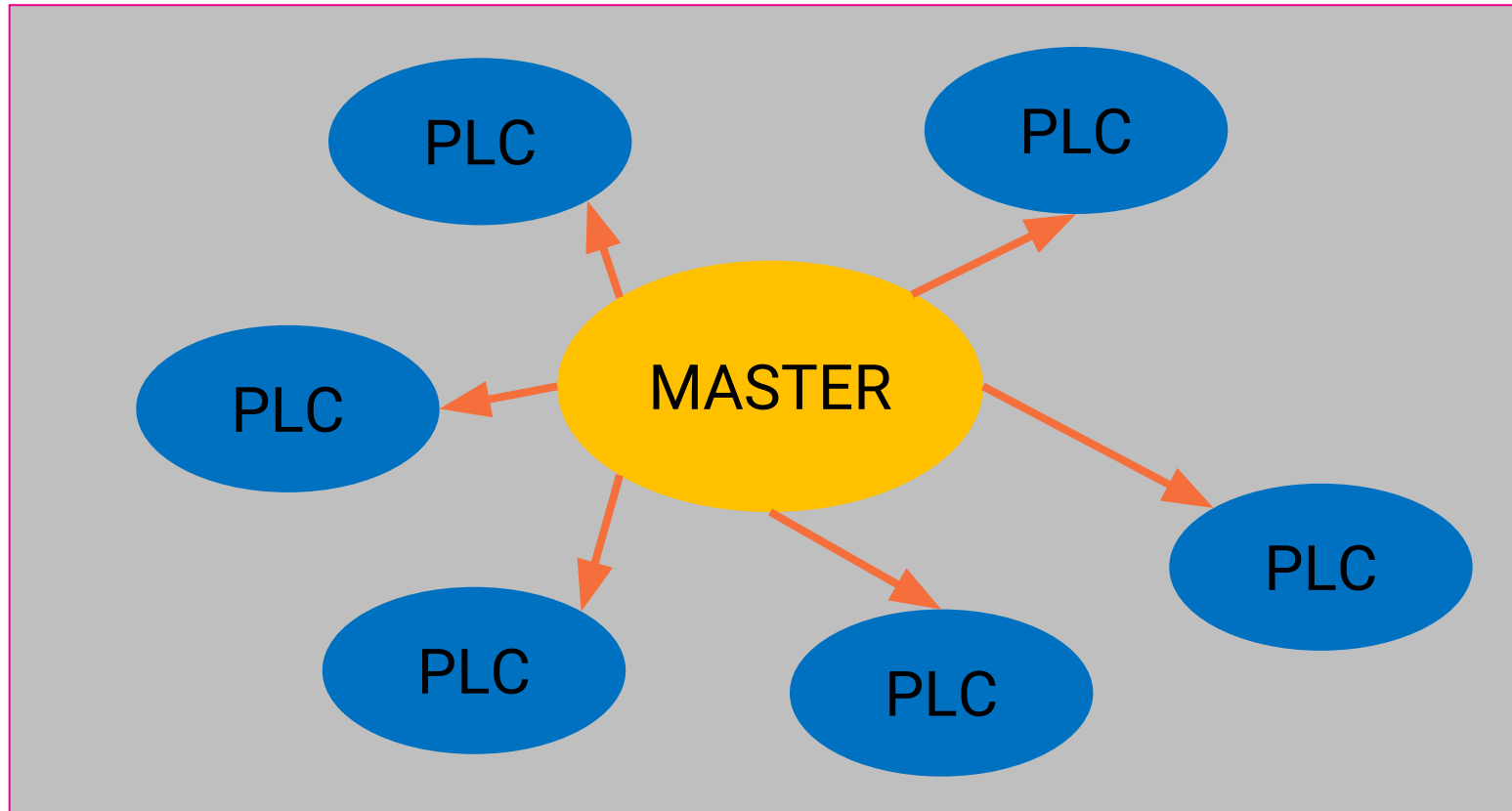
HUNTING

CONCLUSION

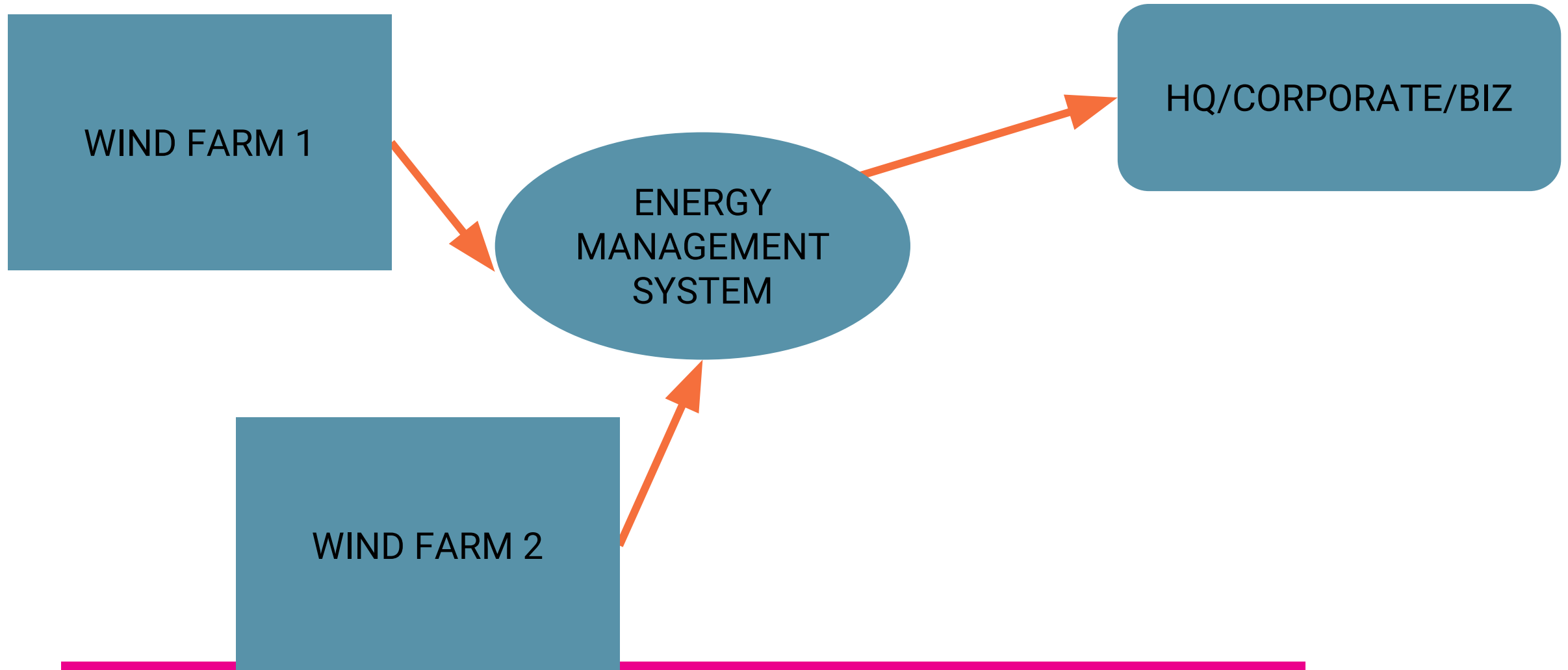
splunk> .conf19

CASE STUDY: WIND FARM

DO YOUR HOMEWORK: WIND FARM LAYOUT

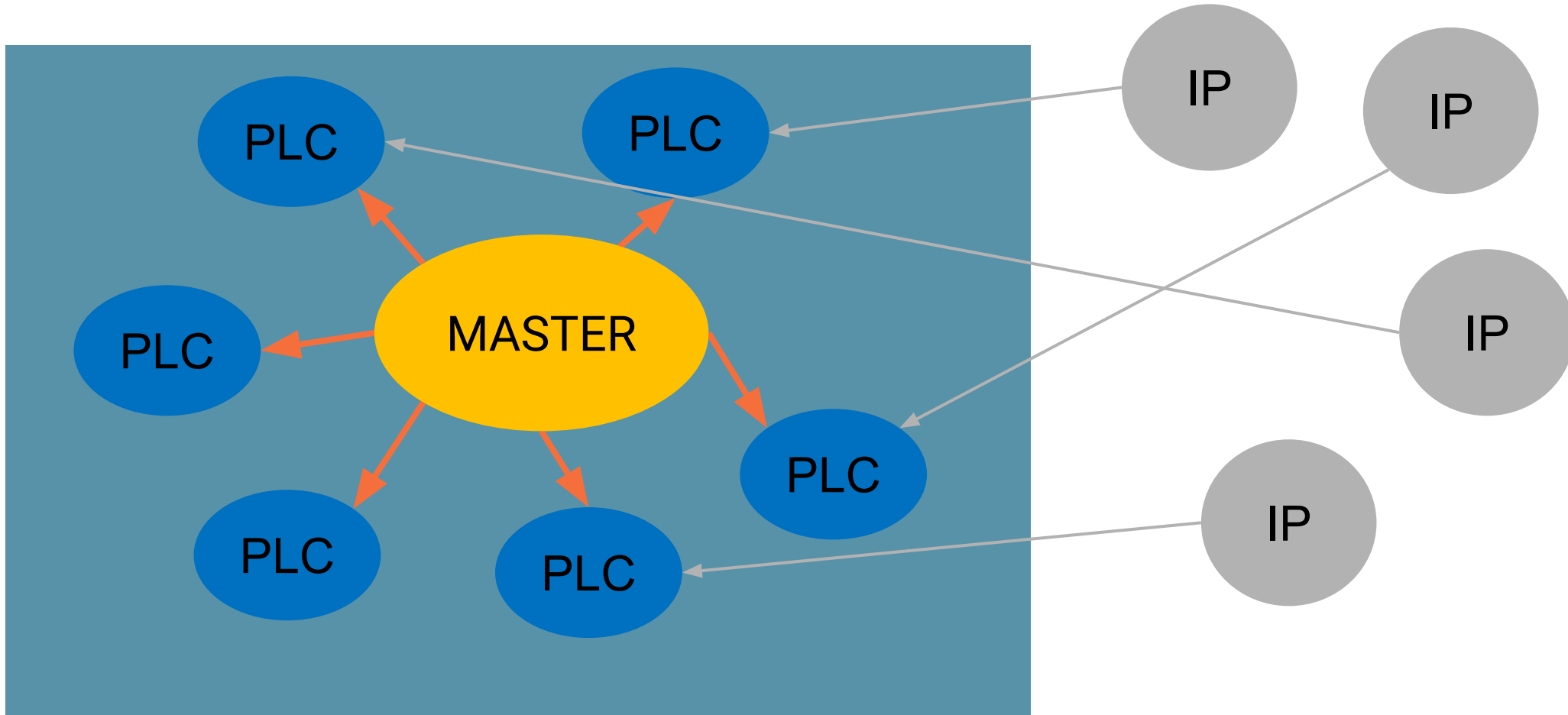


DO YOUR HOMEWORK: NETWORK LAYOUT



METHODOLOGY/PROCESS, DOCUMENT FINDINGS

NEW COMMUNICATIONS DIRECT TO PLCS



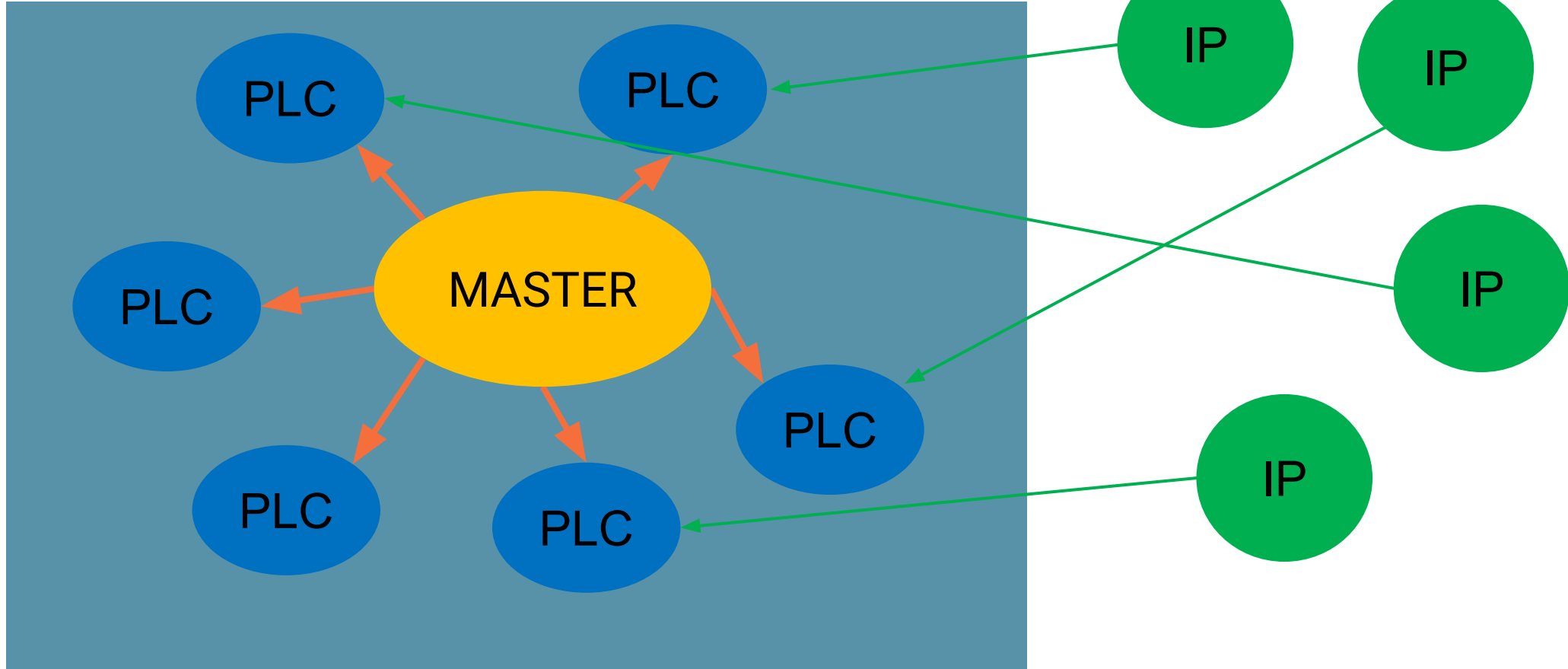
LANDSCAPE

ACTIVITY GROUPS

HUNTING

CONCLUSION

ENABLE HUNT, CODIFY KNOWLEDGE: VENDOR CONNECTIONS RESETTING TURBINES IN HIGH WIND



LANDSCAPE

ACTIVITY GROUPS

HUNTING

CONCLUSION

CASE STUDY BOTS: EVERYTHING YOU COULD ASK FOR

DATA/ANALYSIS COLLECTION:

- ZEEK LOGS
- RAW PCAP
- WINDOWS EVENT LOGS
- SYSMON
- SURICATA ALERTS
- NGUARD DEVICE LOGS

**SPLUNK DATA AGGREGATION*

**DRAGOS CONTEXTUAL ALERTS*

01

DO YOUR HOMEWORK

02

USE A METHODOLOGY/PROCESS AND
DOCUMENT FINDINGS

03

ENABLE THE HUNT.
CODIFY KNOWLEDGE

CONCLUSION: FINDING THREATS

01

DO YOUR HOMEWORK

02

USE A METHODOLOGY/PROCESS AND
DOCUMENT FINDINGS

03

ENABLE THE HUNT. CODIFY
KNOWLEDGE

QUESTIONS?

MARC SEITZ		AMY BEJTLICH	
Twitter: @SubtleThreat		Twitter: @_Silent_J	
Email: mseitz@dragos.com		Email: abejtlich@dragos.com	
Web: www.dragos.com			



**Thank
You!**

Go to the .conf19 mobile app to

**RATE THIS
SESSION**