578.6
Capstone

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

FOR578.6 | Cyber Threat Intelligence

Day 6 Capstone

Robert M. Lee (Lead Author)

Robert M. Lee is the CEO and Co-Founder of the industrial (ICS/OT/IIoT) cybersecurity company Dragos, Inc. which creates and delivers technology, services, and cyber threat intelligence to the industrial community. He is a SANS Senior Instructor and the course author of SANS ICS515: ICS Active Defense and Incident Response and the lead author of SANS FOR578, Cyber Threat Intelligence. Robert is also a Department of Energy employee serving on the Electric Advisory Committee and the Vice-Chair of the Grid Security Committee. He also serves on the World Economic Forum's Oil and Gas and Electricity Subcommittees focusing on the cybersecurity of global infrastructure.

Robert obtained his start in cybersecurity in the U.S. Air Force, where he served as a Cyber Warfare Operations Officer tasked to the National Security Agency. He has performed defense, intelligence, and attack missions in various government organizations, including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Routinely sought for his expertise, he has keynoted and spoken at major conferences such as RSA, BlackHat, and DEFCON, and has testified to the U.S. Senate Energy and Natural Resources Committee. Robert is also the author of the books *SCADA and Me*, *Cyber Threat Intelligence and Me*, and *Santa and Me: The SCADA before Christmas* as well as the weekly webcomic LittleBobbyComic.com. Robert may be found on Twitter @RobertMLee or contacted via email at RLee@Dragos.com.

Rebekah Brown (co-author)

Rebekah is a cybersecurity and intelligence analysis professional specializing in threat intelligence, network warfare analysis, systems analysis, and threat modeling. Rebekah spent over a decade on active duty as a cryptologic linguist, network warfare analyst, and cyber operations chief in the U.S. Marine Corps before moving to the private sector, where she has developed threat intelligence programs at multiple Fortune 500 companies. She received degrees in International Relations from Hawaii Pacific University, and Homeland Security with a cybersecurity focus, and a graduate certificate in Intelligence Analysis from American Military University. She is a published author, instructor, and public speaker on intelligence-driven incident response and adversary tactics.

Capstone: The Goals

- Expose you to technical and non-technical datasets for you to satisfy a set of intelligence requirements that match real-world expectations
- Provide a fun exercise to have various components of the class come together for you to reinforce the lessons

This page intentionally left blank.

Capstone: What to Know To Have Fun

- There is no one right answer
  - In making the scenario, there was obviously an intent to some of the paths you may take, but it is up to your creativity and analysis to find the path that fits best for you
- None of the data related to adversary capabilities (TLS certs, IPs, hashes, etc.) correlate with anything in the real world; searching OSINT for them will be a distraction
- The theming of the scenario, Star Wars, is based on correct Star Wars lore with a little creativity on the "cyber" components. Therefore, any understanding of Star Wars lore prior to the class or searching you may do using OSINT is completely appropriate

This page intentionally left blank.

Capstone: How to "Win"

- Present your findings at the end of the capstone, following guidance you've learned throughout the course as if the instructor is the individual asking you for the intelligence requirements; do this before exposing your methods
  - Present first as an intel analyst
  - Present after the "official" presentation your methods, process, etc.
- Where you didn't know something or had to make assessments, note what those were and expose how you worked through the process
- Points are awarded for:
  - Satisfying the intelligence requirements
  - Using concepts and tools from the class
  - Working as an effective team (if playing as a team)
  - Presentation skills and ability to convey the topics to a wide audience

This page intentionally left blank.

Scenario Background

This page intentionally left blank.

You

- You are a Mandalorian
  - An elite cyber threat intelligence analyst
- You and your crew have been called in analyze the breach of the Sullust Space Exploration company to satisfy the client's intelligence requirements
- You also have intrusions that have not been analyzed that will be useful

This page intentionally left blank.

The State Actors

- In scope for our analysis, there are a few state actors (planets and their governments) that you must be aware of

- Tatooine
  - Desert planet home to the Hutt Clan, Jawa, Tusken Raiders, and others
- Sullust
  - Volcanic planet with advanced R&D along major trade routes
- Corellia
  - One of oldest civilizations and early star voyagers
- Bespin
  - Gas planet home with the galaxy's provider of Tibanna gas

This page intentionally left blank.

The Non-State Actors

- In scope for our analysis, there are a few non-state actors (groups, clans, and criminals) that you must be aware of

- Black Sun
  - Criminal syndicate that takes every opportunity to make themselves richer
- Nightsisters
  - Magik-wielding cultists based on Dathomir
- Dragite Group
  - Unknown origin group that creates and leverages Dragite malware
- Kyberite Group
  - Unknown origin that makes the Kyberite malware
- Galactic Sentries
  - High-end incident response firm that also dabbles in intelligence

This page intentionally left blank.

Scenario Objectives

- A breach on Sullust has taken place and they suspect the technical specs of their latest engine for their prized starfighters was stolen

- The Mandalorian have been engaged to answer the following intelligence requirements:

- Who was responsible for the breach (Intrusion 1)?
- What is their potential motivation?
- What are some key indicators from this breach?
- Using your own judgment, determine what unique Activity Groups are worth tracking and being aware of for defenders. (Who would care and why?)
- What are key TTPs to prepare for defensive strategies against each Activity Group?

This page intentionally left blank.

Your Resources

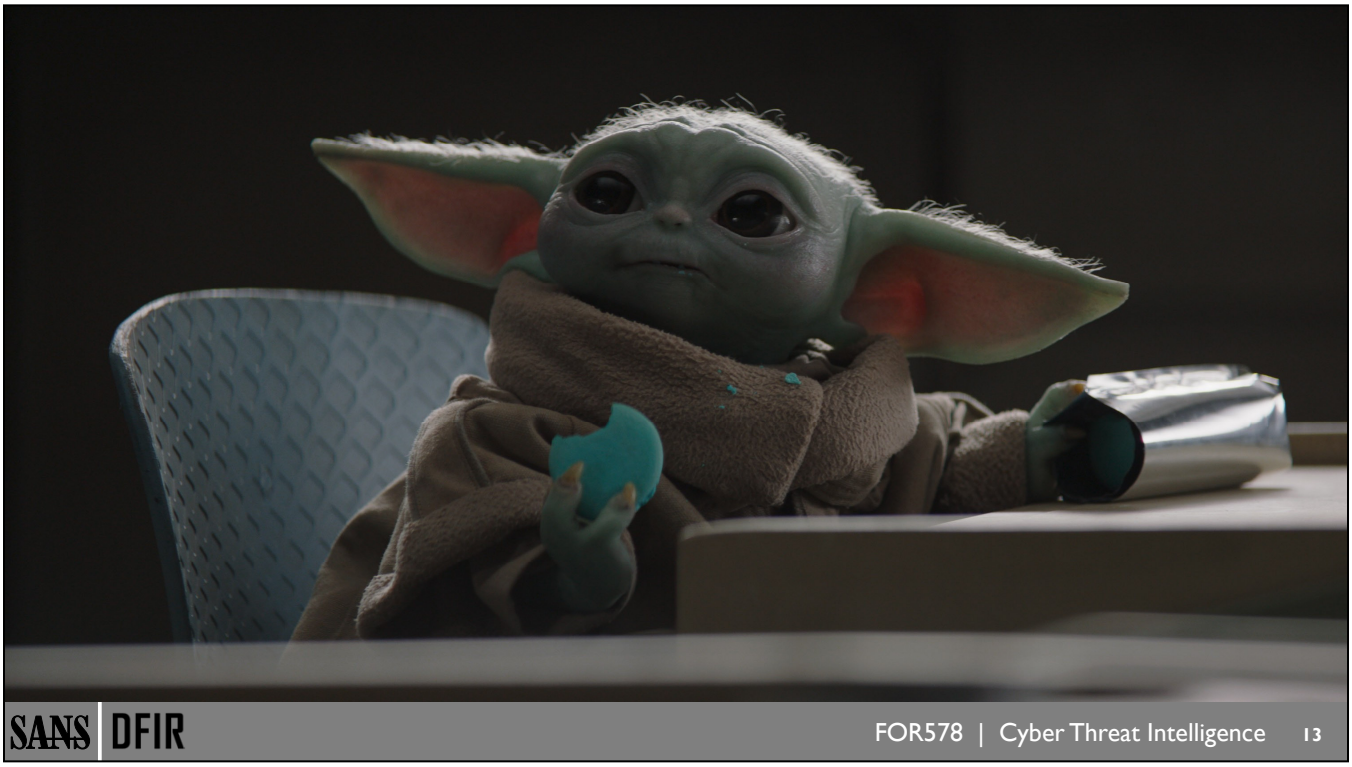
- In the Ex 6 folder in your media file, you have all the resources you will need for this exercise, including Dossiers on each State and Non-State actor as well as technical indicators and insights from intrusions
- Some of the technical data you are presented with is historical data from your previous adventures and shared with you from peers; everything is mixed in together and timing has no bearing
- You can use any tools you'd like but recognize that technical data from these scenarios is not at all relevant to any technical data publicly (i.e. an IP in the lab has nothing to do with real-world IPs)
  - Thus, tools like DomainTools, RecordedFuture, etc., are useless
  - Tools like Excel, Maltego, MISP, and probably Excel will be very useful

This page intentionally left blank.

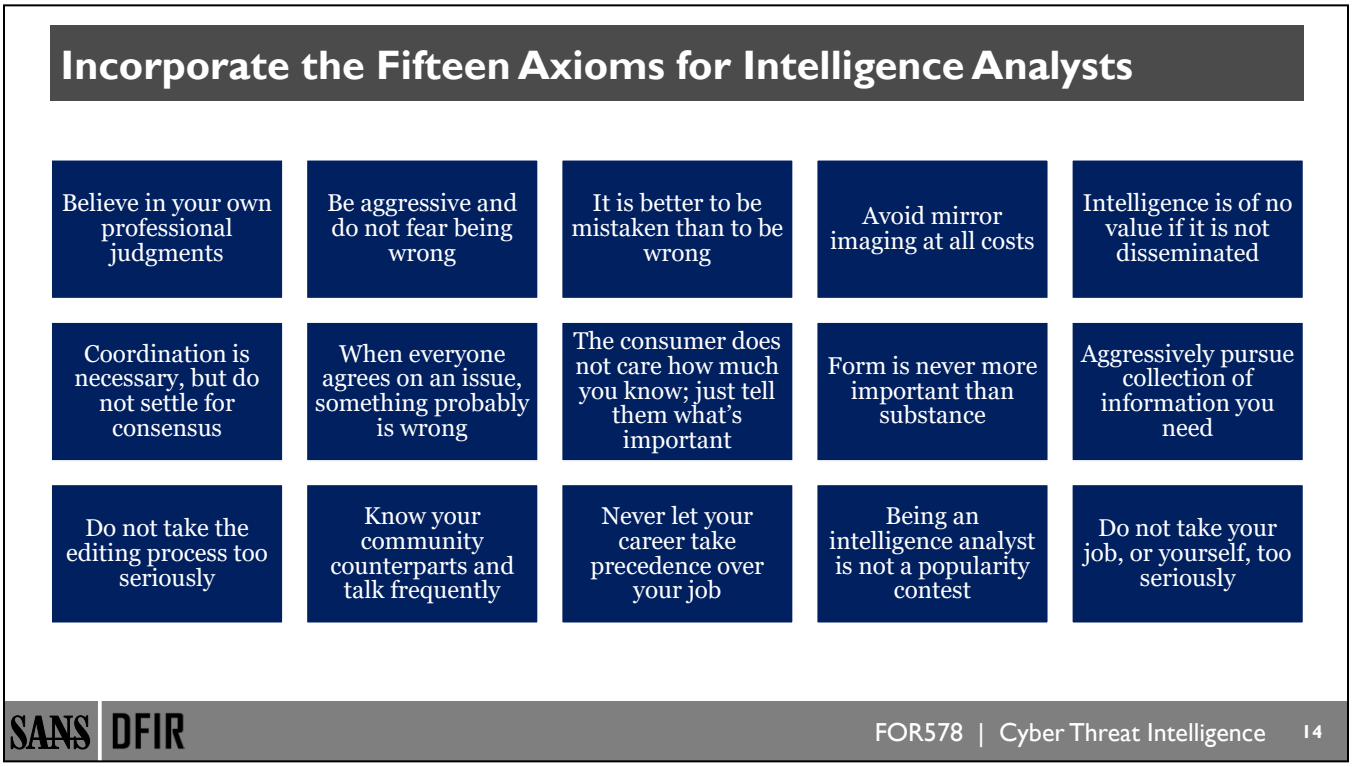
Capstone

Exercise 6

This page intentionally left blank.



This page intentionally left blank.



Incorporate the Fifteen Axioms for Intelligence Analysts

In the CIA's Center for the Study of Intelligence is a document by Frank Watanabe related to Kent's intelligence doctrine. Frank laid out fifteen axioms for intelligence analysts that are useful, especially as we try to refine our intelligence and make it through the intelligence process fully, but before we start the process again.

His fifteen axioms are:

1. Believe in your own professional judgments
    a. You should always be willing to listen to alternate points of view, but you should be invested in your assessments
2. Be aggressive and do not fear being wrong
    a. Analysis paralysis is a real issue for analysts; you'll never have all the data, but you still need to make assessments and act on them
3. It is better to be mistaken than to be wrong
    a. That being said, do not refuse to be wrong; it's okay to make mistakes
4. Avoid mirror imaging at all costs
    a. You should be very careful not to project your thought process, values, background, etc., onto the adversary
5. Intelligence is of no value if it is not disseminated
    a. Sometimes, your requirements were just too lofty; you still need to get intelligence out for people to make decisions on

6. Coordination is necessary, but do not settle for the least common denominator
    a. Analytic differences will occur and it's okay; do not just buy into the most-agreed-upon assessment
7. When everyone agrees on an issue, something probably is wrong
    a. There are very few cases when the answer to complex scenarios is easy and gains mass traction
8. The consumer does not care how much you know; just tell them what is important
    a. Short and to the point for the actions they need to make
9. Form is never more important than substance
    a. We need to do well to be professional, but don't spend so much time and money on graphics and copy editing that you miss the requirement
10. Aggressively pursue collection of information you need
    a. Do not be okay simply assessing the available and easy information
11. Do not take the editing process too seriously
    a. In other words, edits are okay. We are all personal about our writing, but if it doesn't change the meaning, then just accept it and say thank you
12. Know your community counterparts and talk to them frequently
    a. This one was more applied to the NSA and DIA (Intelligence Community used broadly), but it should apply to our respective communities
    b. "If you cannot recognize their voices over the phone, then you probably are not talking to them often enough"
13. Never let your career take precedence over your job
    a. You have a responsibility as a professional analyst; do not let your career supersede that
14. Being an intelligence analyst is not a popularity contest
    a. Actually, most people don't really like intelligence analysts
15. Do not take your job, or yourself, too seriously
    a. There's always more work to be done

Reference:

https://www.cia.gov/static/d0626fb44a97e2d8734ef69c66a8fb7e/Fifteen-Axioms-for-Analysts.pdf

Thanks for Coming

- Our field is a growing one at the merger between intelligence and cybersecurity
- Be prepared for change and drive change

- Stay in touch and join us at the annual SANS Cyber Threat Intelligence Summit
  https://www.sans.org/intel

Remember, most people use intelligence analysts like drunkards use light poles: for stability, not illumination. Strive to be the illumination in your organizations.

Thanks for Coming

Take care and see you around. Thanks for coming and stay in touch. Join us at the annual SANS Cyber Threat Intelligence Summit to keep in touch.

This page intentionally left blank.

COURSE RESOURCES AND CONTACT INFORMATION

Here is my lens. You know my methods. —Sherlock Holmes

AUTHOR CONTACT
Robert M. Lee: @robertmlee
RLee@Dragos.com
Rebekah Brown: @PDXbek
pdxbek@gmail.com

SANS INSTITUTE
11200 Rockville Pike., Suite 200
N. Bethesda, MD 20852
301.654.SANS(7267)

DFIR RESOURCES
digital-forensics.sans.org
Twitter: @sansforensics

SANS EMAIL
GENERAL INQUIRIES: info@sans.org
REGISTRATION: registration@sans.org
TUITION: tuition@sans.org
PRESS/PR: press@sans.org

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Y