Threat Intelligence and digital forensics

Dr. Samuel Liles

Associate Professor

Purdue Cyberforensics Laboratory

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

Who am I?

- Nobody special, Nobody important
  - Purdue Professor and Dr. of DFIR
  - Non-traditional career track (Marine, Cop, IT/IR, Higher Ed, next?)
- Blog: http://selil.com
- Twitter: @selil
- Goal I just want to have a conversation
  - What do I hear your bosses want to hear?

PURDUE UNIVERSITY
CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

Definitions because words matter when you might end up in court

- In this context **threats** are actors, entities, environmentals that can have negative consequence on the information technology enterprise
- **Intelligence** is the gathering of information for countermeasure development and analysis for impact mitigation.

PURDUE UNIVERSITY
CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

Attribution

- **Political** attribution based on the actors motives and goals
- **Technical** attribution based on tactics, techniques and means of an entity
- **Forensic** attribution based on the evidence of behaviors and facts

PURDUE UNIVERSITY
CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

The three meanings of intelligence

- Intelligence as in knowledge, “What intelligence have you about ISIL?”
- Intelligence as an organization “What does the Central Intelligence Agency think about that?”
- Intelligence as an activity “The intelligence behind that operation must have been difficult.”

Sherman Kent, Strategic Intelligence for American World Policy

PURDUE UNIVERSITY
CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

The father of modern intelligence analysis

Whatever the complexities of the puzzles we strive to solve, and whatever the sophisticated techniques we may use to collect the pieces and store them, there can never be a time when the thoughtful man can be supplanted as the intelligence device supreme.

Sherman Kent, Strategic Intelligence for American World Policy

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

The intelligence activity

- Surveillance operation
- Research operation
- Acquisition
- Delivery
- Acceptance
- Interpretation
- Implementation

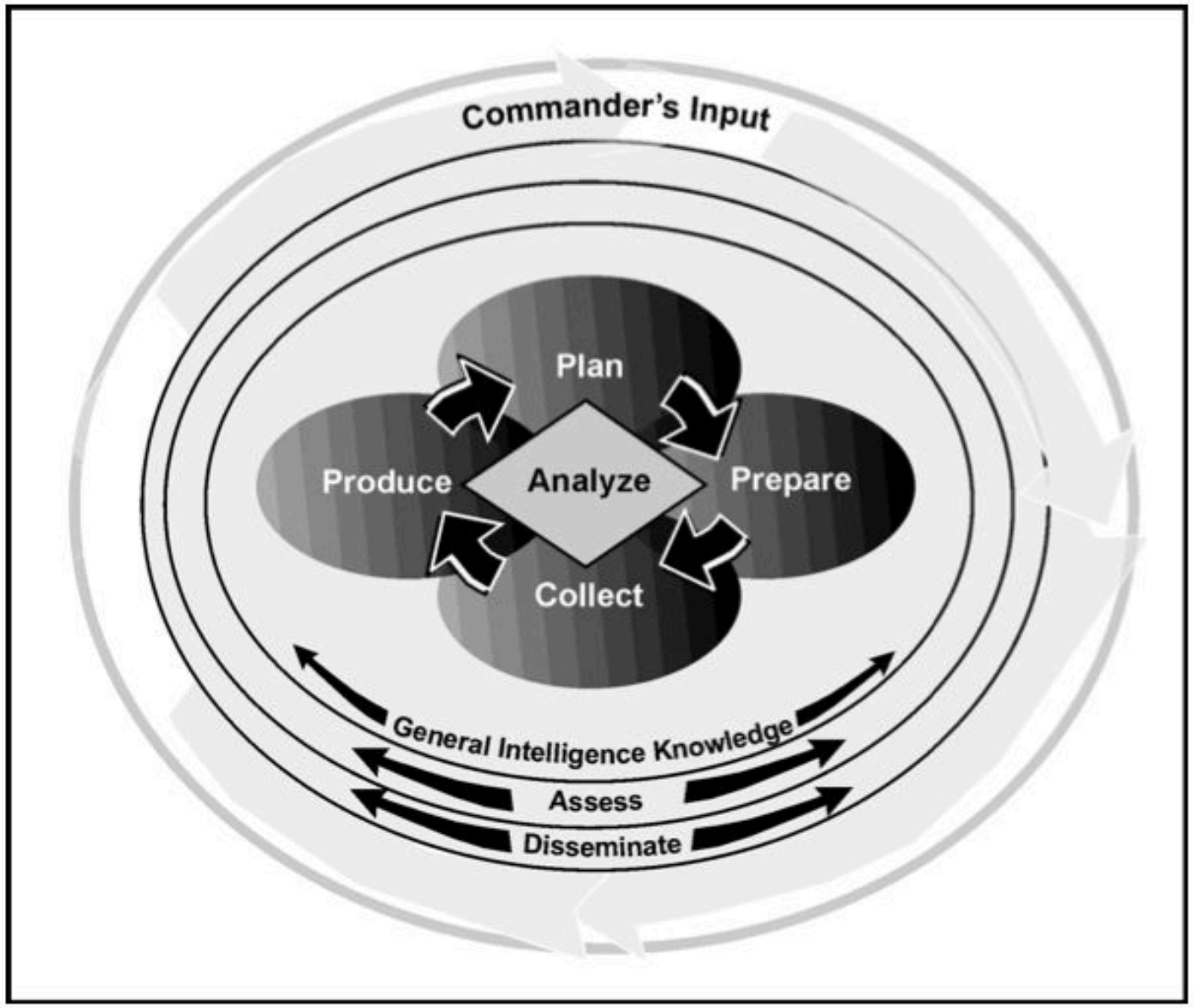
Keegan, J., (2003) "Intelligence in War: Knowledge of the enemy from Napoleon to Al-Qaeda"

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

CERIAS

Slides located at http://selil.com



Open-Source Intelligence, ATP 2-22.9 (July 2012) Headquarters, Department of the Army

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

CERIAS

Slides located at http://selil.com

Intelligence is…

- Knowledge
  - Description, reporting, speculation
- Organization
  - Who, whom, how
- Activity
  - Methods, mechanisms, sensors, etc..

The goal of threat intelligence

- Early warning
- Discovery of trends
- Preparation of hostile actors
- Mitigation strategies for assessed risks

Intelligence types…

- HUMINT, SIGNIT, MASINT, OSINT, **TECHINT**, **CYBINT**, **DNINT**, FININT (Wikipedia !)
- Personalities, military, **political**, **economic**, **social**, moral, scientific and **technical**, **learning** and the arts (Sherman Kent)

Reliability v. Validity

A	***Reliable***	**No doubt** of authenticity, trustworthiness, or competency; has a history of complete reliability.
B	***Usually reliable***	**Minor doubt** about authenticity, trustworthiness, or competency; has a history of valid information most of the time.
C	***Fairly reliable***	**Doubt** of authenticity, trustworthiness, or competency, but has provided valid information in the past.
D	***Not usually reliable***	**Significant doubt** about authenticity, trustworthiness, or competency, but has provided valid information in the past.
E	***Unreliable***	**Lacking** authenticity, trustworthiness, and competency; history of invalid information.
F	***Cannot be judged***	**No basis** exists for evaluating the reliability of the source.

Open-Source Intelligence, ATP 2-22.9 (July 2012) Headquarters, Department of the Army

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

CERIAS

Slides located at http://selil.com

Reliability v. **Validity**

1	***Confirmed***	**Confirmed** by other independent sources; logical in itself; consistent with other information on the subject.
2	***Probably true***	**Not confirmed**; logical in itself; consistent with other information on the subject.
3	***Possibly true***	**Not confirmed**; reasonably logical in itself; agrees with some other information on the subject.
4	***Doubtfully true***	**Not confirmed**; possible but not logical; no other information on the subject.
5	***Improbable***	**Not confirmed**; not logical in itself; contradicted by other information on the subject.
6	***Misinformation***	**Unintentionally false**; not logical in itself; contradicted by other information on the subject; confirmed by other independent sources.
7	***Deception***	**Deliberately false**; contradicted by other information on the subject; confirmed by other independent sources.
8	***Cannot be judged***	**No basis** exists for evaluating the validity of the information.

Open-Source Intelligence, ATP 2-22.9 (July 2012) Headquarters, Department of the Army

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

CERIAS

Slides located at http://selil.com

Digital forensics knows AND REPORTS

- How the threat perceives an attack (success, failure, incremental)
- What the threat is operating against in the way of specific vulnerabilities
- What is the counter measure bypass mechanism utilized by the threat
- What is the flexibility and adaptability of the threat

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

Forensics provides technical intelligence

- Protocol
- Source and destination IP addresses
- Date/Time of attack
- Frequency of attack
- Number of events
- Targeted systems
- Associated IDS/IPS signatures
- Hashes of files
- Malicious code
- Known or unknown vulnerabilities

Symantec Cyber Threat Analysis Program: Program Overview, White paper

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

CERIAS

Slides located at http://selil.com

Why u no like computer science?

- **Technology**, the study of the art and craft of doing work with tools
- **Technologist**, a person who enhances the quality, efficiency, or capability of work through tools.
- **Intelligence** is a form of **technology** and technology is inherently multi-disciplinary because EVERYBODY uses tools. Kind of what makes us human.
- Threat intelligence is an assessment of the tactics, techniques, tools, and procedures that impact the information enterprise.
- And, I have a bachelors and masters degree in computer science

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

Structuring analysis towards actionable intelligence products

$$Risk = \frac{Threat * Vulnerability}{Countermeasures - OpportunityCost} * Impact$$

Based on the work of Dr. Dan Ryan and Dr. Julie Ryan

Enterprise know thyself

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

CERIAS

Slides located at http://selil.com

Incident Response

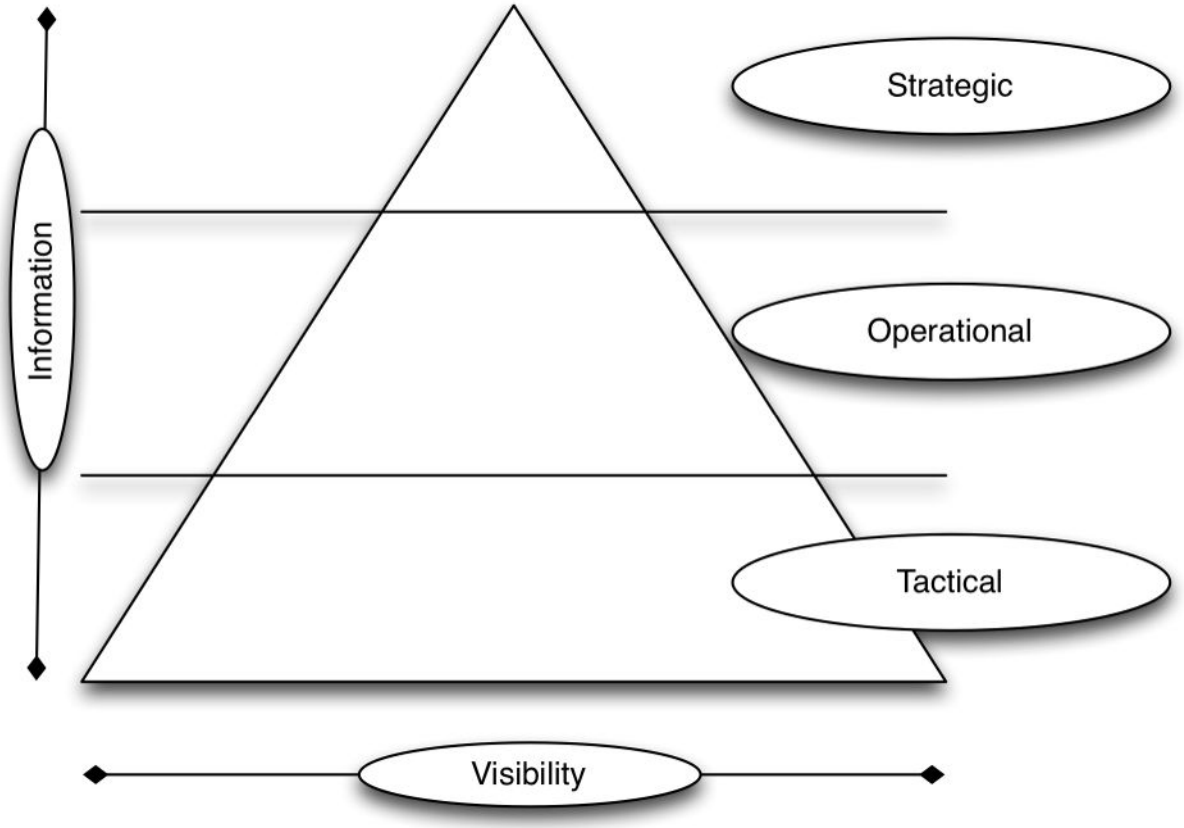
- The **sanity sensor** in the enterprise
- The point where when everything fails the answers **can be** found
- The point everybody is going to be **looking** at when everything hits the fan
- The “c” in protect, detect, correct
- Take a bow you are awesome now back to reality

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

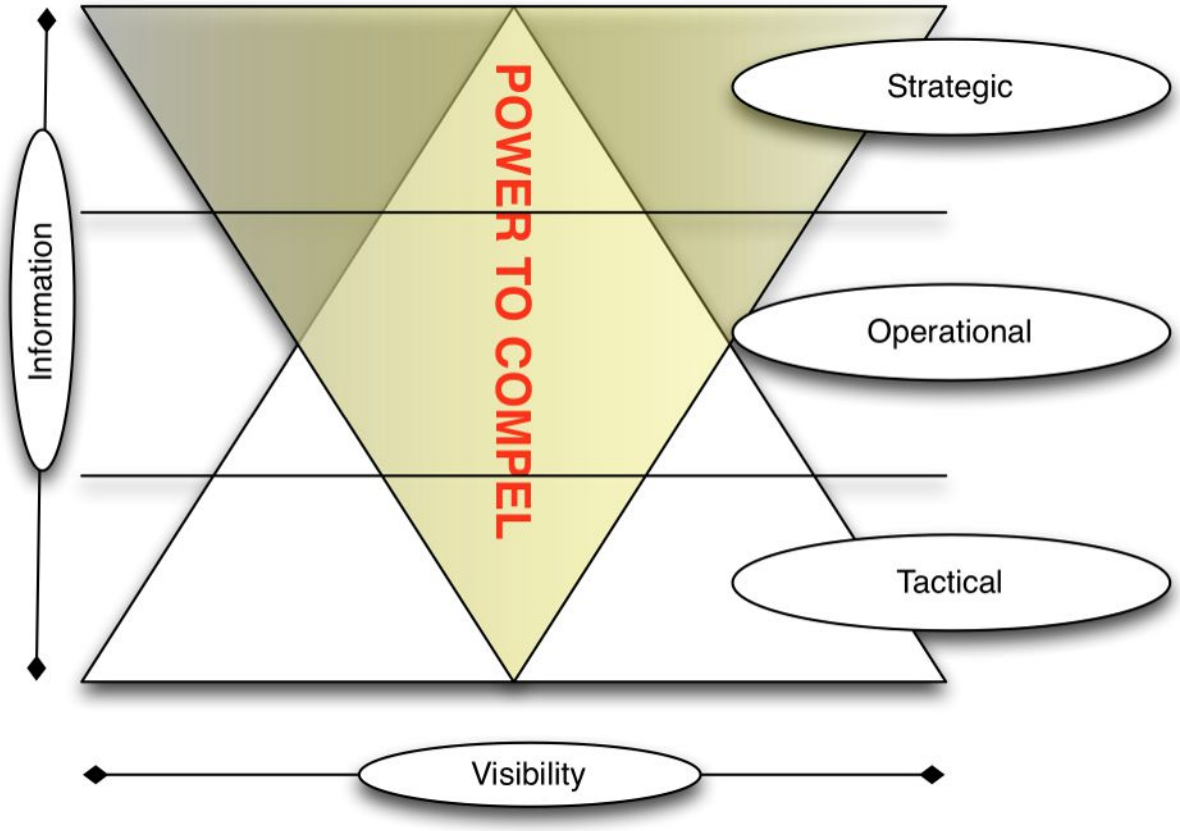


PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

CERIAS

Slides located at http://selil.com



PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

CERIAS

Slides located at http://selil.com

Hey kid can I sell you a threat feed?

- Indicators of compromise
  - IP's
  - URL's
  - Geo-location data
  - Hashes
  - IDS/IPS rules
  - Email heuristics
- OpenIOC, CybOX, IODEF
- In general pretty useless unless you know one thing

PURDUE UNIVERSITY
CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

Who do you serve and who do you trust?

- How do you know something is a threat?
- Technical intelligence is not forensic nor is attribution
- Do you know you have a vulnerability in your network that the threat can operate against?
  - Of course you have all the time in the world to add rules to boxes all day long…
- If you don't know your vulnerability posture you don't know what is a threat
  - Management will usually say it is all a threat but won't resource based on that assessment
- How do you to determine your attack surface?

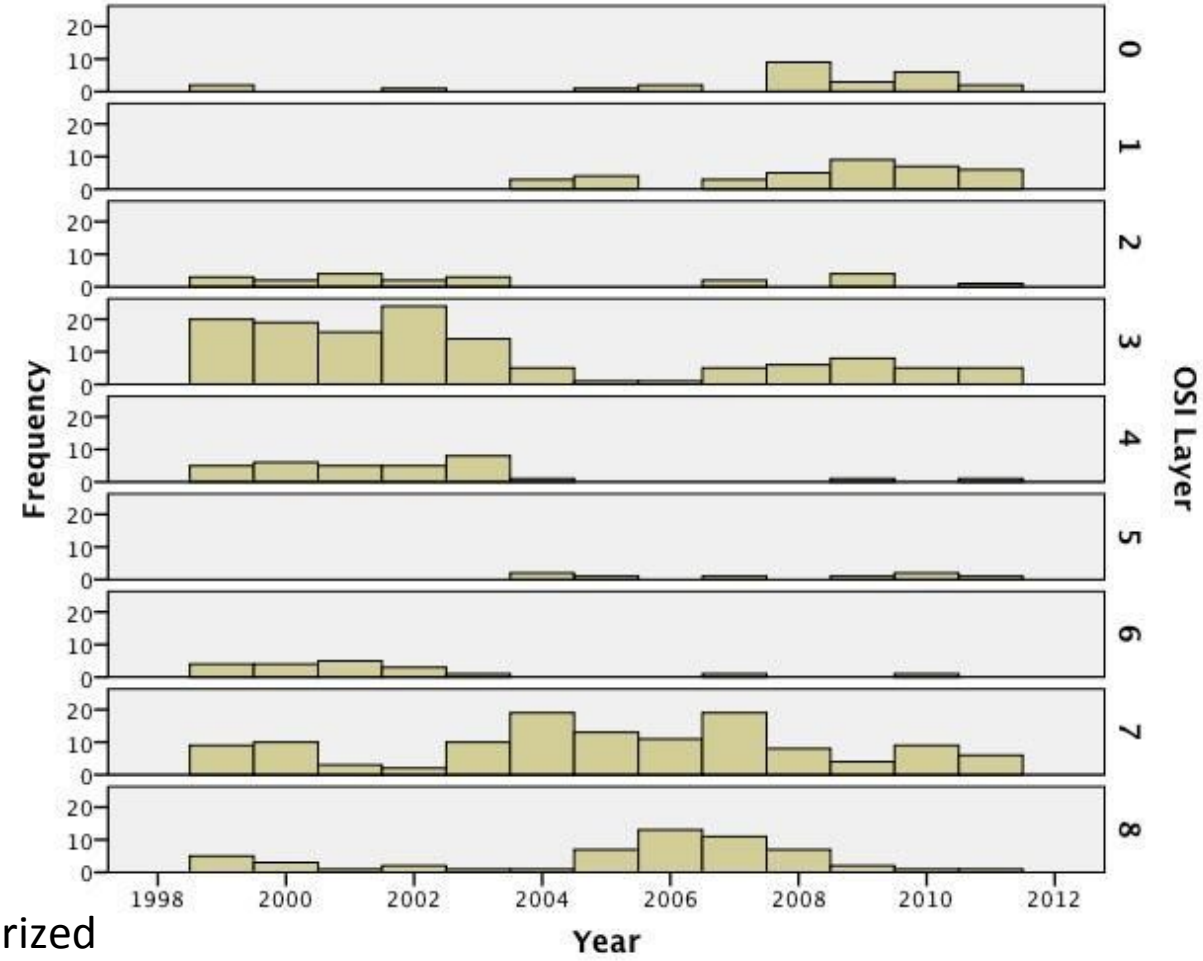
PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

Reporting data



Incidents categorized

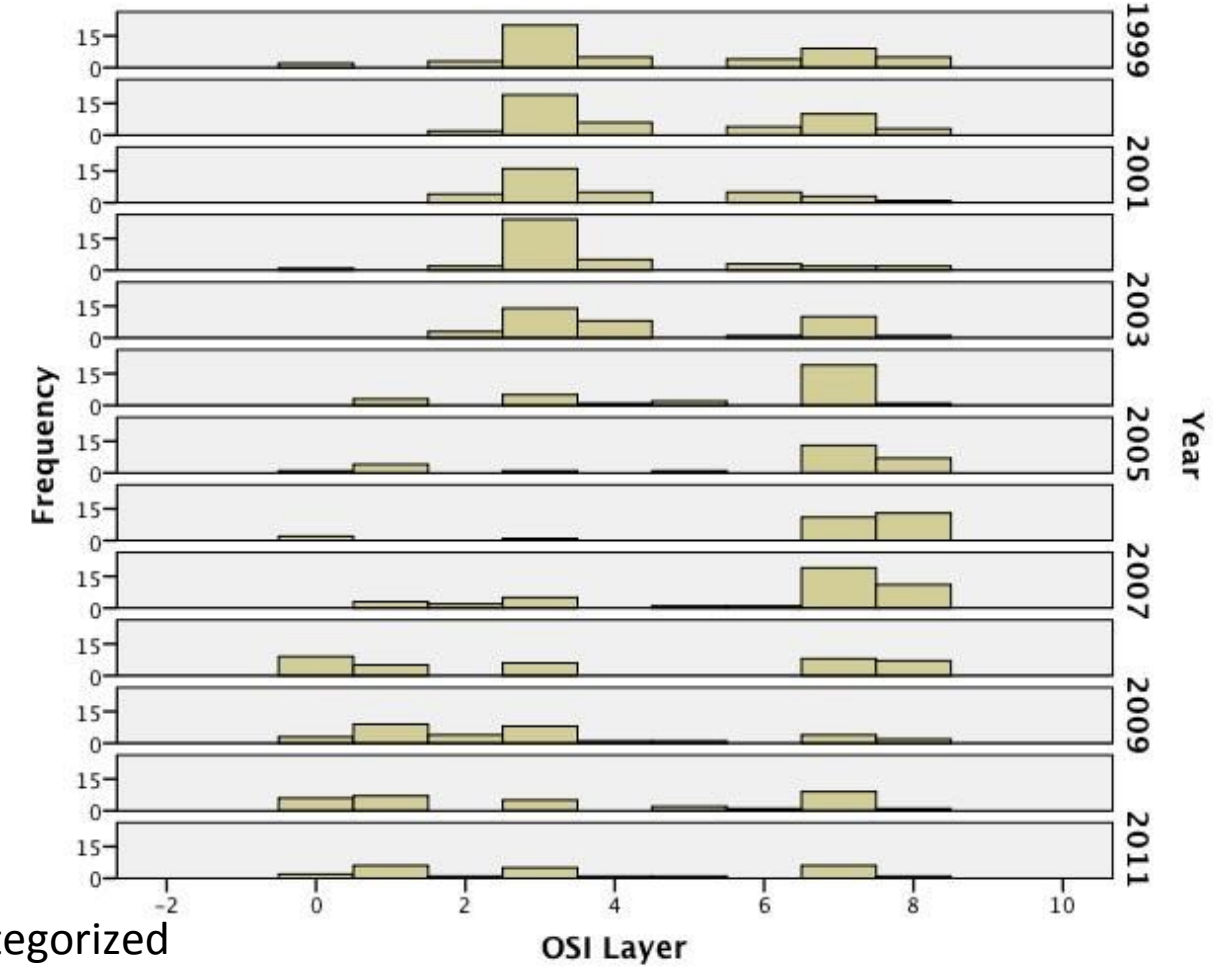
PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

CERIAS

Slides located at http://selil.com

Reporting meaningful data



Incidents categorized

PURDUE UNIVERSITY
CYBERFORENSICS LABORATORY

CERIAS

Slides located at http://selil.com

Diversity of views needed

- Technical savvy analysts who focus on the weeds and derive mitigation assessments
  - Read the logs, create the rules, report the issues, check the netflow repository, run the honeypot
- Strategic analysts who focus on the impact factor and focus resource assessments
  - Nature of the threats, history of the actors, what is the weather today, focus on the analytics and draw the big picture

PURDUE UNIVERSITY
CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

Know the customer

- Who is the customer?
  - Management?
  - Security team?
  - The analyst next employer?
- Negotiate a hold harmless from management up front. Blame slows things down and doesn't change the end result.
- What about the adversary?

PURDUE UNIVERSITY
CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

When the adversary is a breathing human being

- Knowledge
- Skills
- **Abilities**
- Morals
- Politics
- **Motives**
- Biases

PURDUE UNIVERSITY
CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

Indicators of compromise

- Starting point
- Adaptive adversary will nullify use of IOC
- Threat feeds tell you history not future
- Intelligence analysis gives strategic level warning (get in front of the attack)
- IOC and threat feeds are more information not necessarily better information
- Know your environment and tailor solutions to that environment

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS

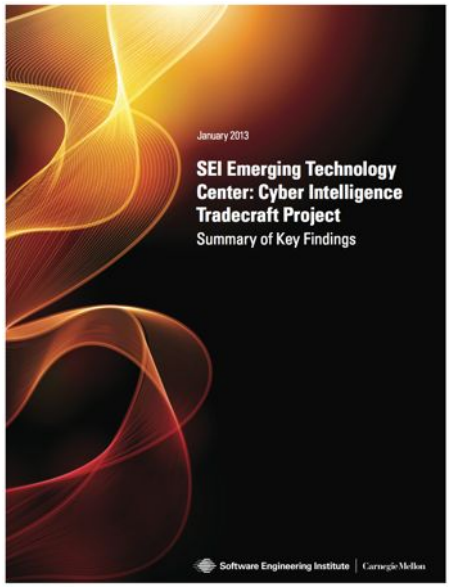
Questions, thoughts, concerns?

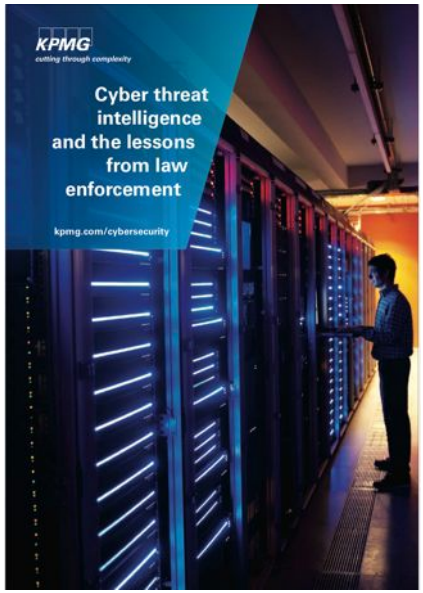
PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

Slides located at http://selil.com

CERIAS





PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

CERIAS®

Slides located at http://selil.com