Mastering The Art of Cyber Threat Intelligence
2500 years ago...
Sun Tzu
*544 B.C. – †496 B.C.

THE ART OF WAR

Sun Tzu
“If you know others and know yourself, you will not be beaten in a hundred battles.

If you do not know others but know yourself, you win one and lose one.

If you do not know others and do not know yourself, you will be beaten in every single battle.”

Sun Tzu

*544 b.c. – †496 b.c.
Know Your Enemy

• Who?
• Where?
• Size?
• Weapons?
• Motivation?
• Tactics and Techniques?
Know Yourself

- Assets?
- Priorities?
- Strengths?
- Vulnerabilities?
Filter and Correlate Information

• Threat?
• Relevance?
• Priority?
Share Information

- Right Information
- Right Place
- Right Time
What Turns Threat Data Into Intelligence?

- **Accurate:**
  - Is the information reliable and detailed?

- **Relevant:**
  - Does the information apply to you and your mission/business?

- **Timely:**
  - Did you receive the information with enough time to do something about it?
Know Your Enemy

Enemies and TTPs

Adversaries

Campaigns

Indicators
Know Yourself

Asset Database
SIEM
Sandbox
Vulnerability Assessment
Ticketing
Endpoint Protection
Log Repository

Me

Assets
Vulnerabilities
Alarms
Find Relevant Threats

Enemies and TTPs

- Adversaries
- Campaigns
- Indicators

Me

- Assets
- Vulnerabilities
- Alarms

Threat Library

Aggregate
Normalize
Correlate
Analyse and Enrich

SCORING

ACCURATE
RELEVANT
TIMELY
Share Threat Information
Content, Format, Frequency

Executives/Board of Directors
CISO

Security Status
Detailed Intel

Threat Library
Alarms
IoCs

Risk Management
Business Units
Investigations Team

Vulnerability Management
Patch Management
Security Infrastructure

Incident Response Team
Security Operations Center
Cyber Threat Intelligence Team

ACCURATE
RELEVANT
TIMELY
Conclusion

• It’s all about actionable threat data and sharing of information!
• Need to do your homework!
• Need to change and automate processes!
• Assess your current technology landscape!
• Start your CTI program now!
THANK YOU!