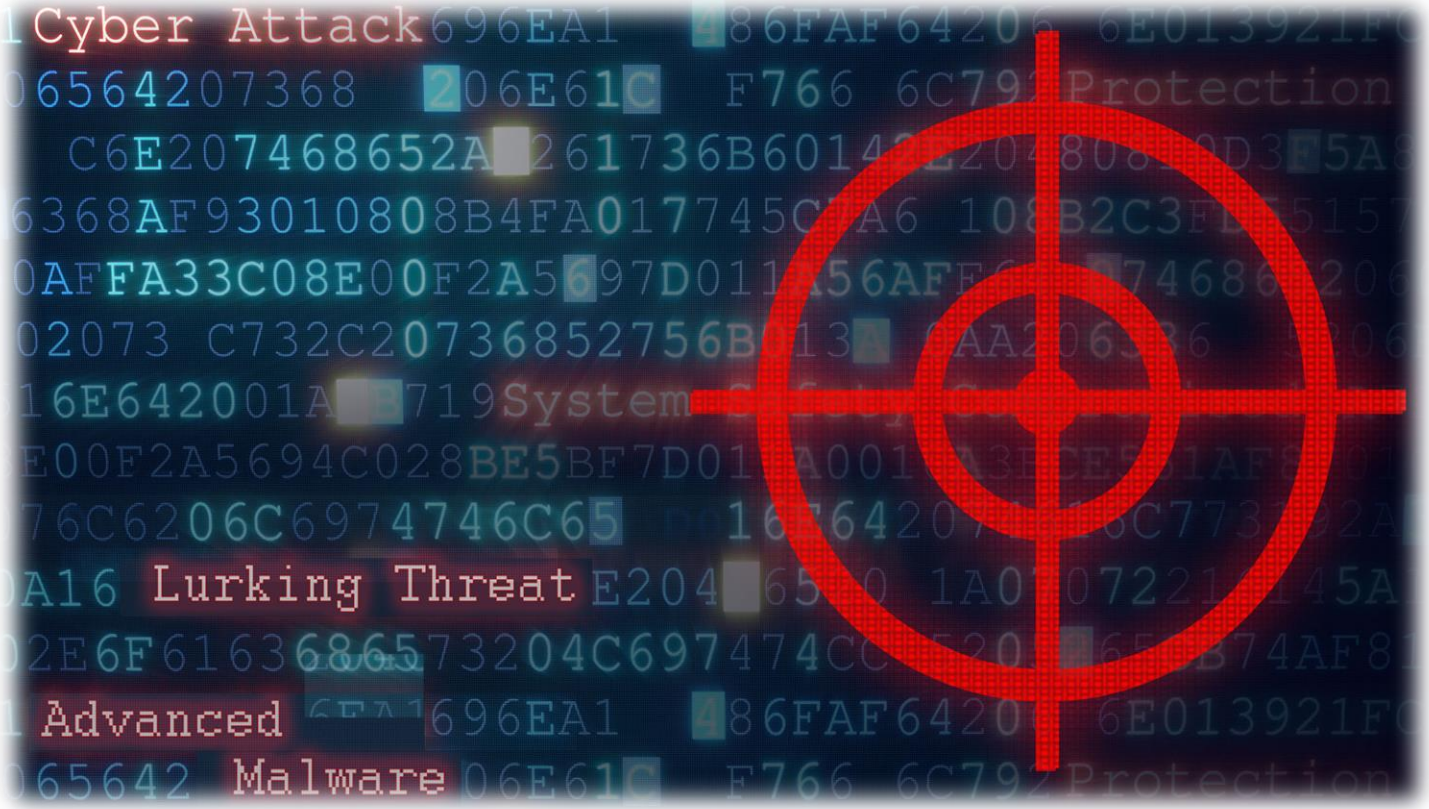
Raytheon
Foreground Security



[Proactive Security]
Building a Threat Hunting Program

Presented by:

Carl Manion

Managing Principal

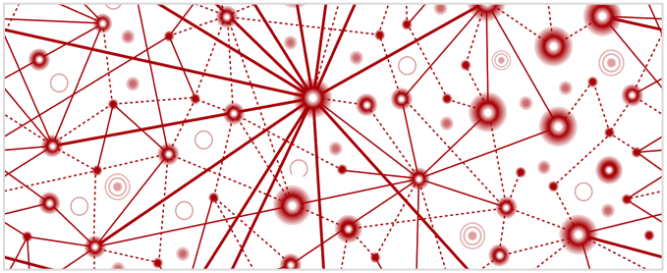
Adopt a Threat Hunting Mindset

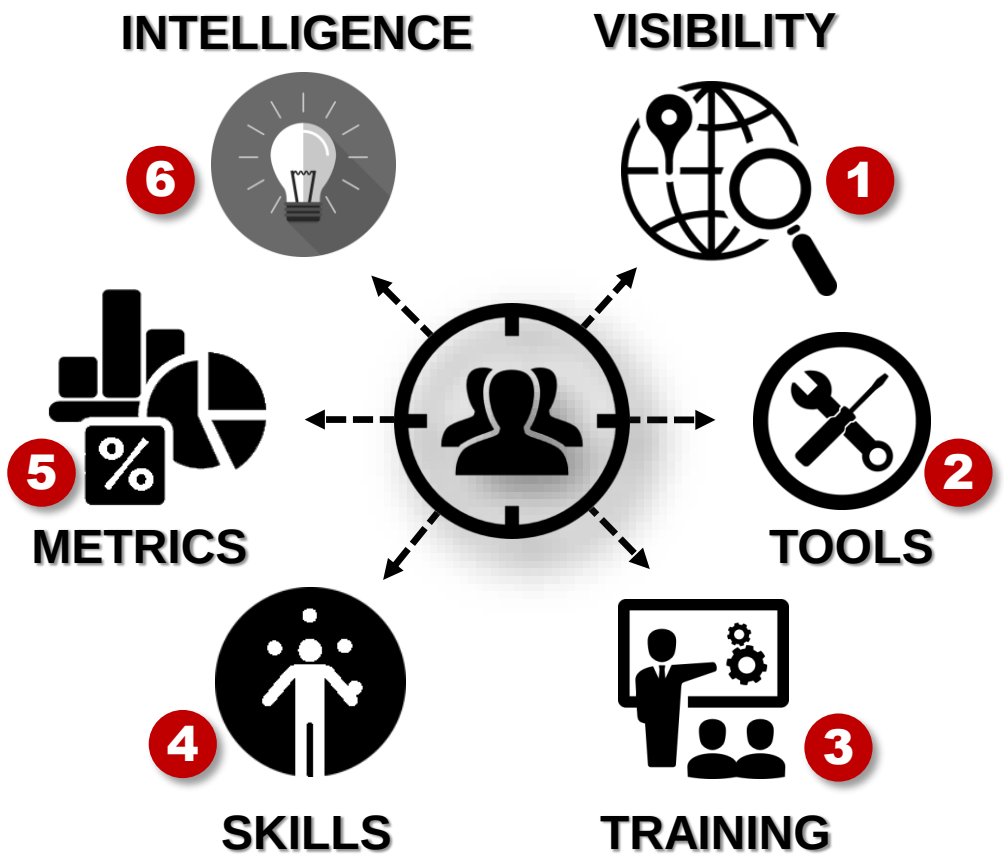
Raytheon
Foreground Security

Monitoring & Responding to Alerts

VS

Proactively Searching for threats, vulnerabilities and exploits



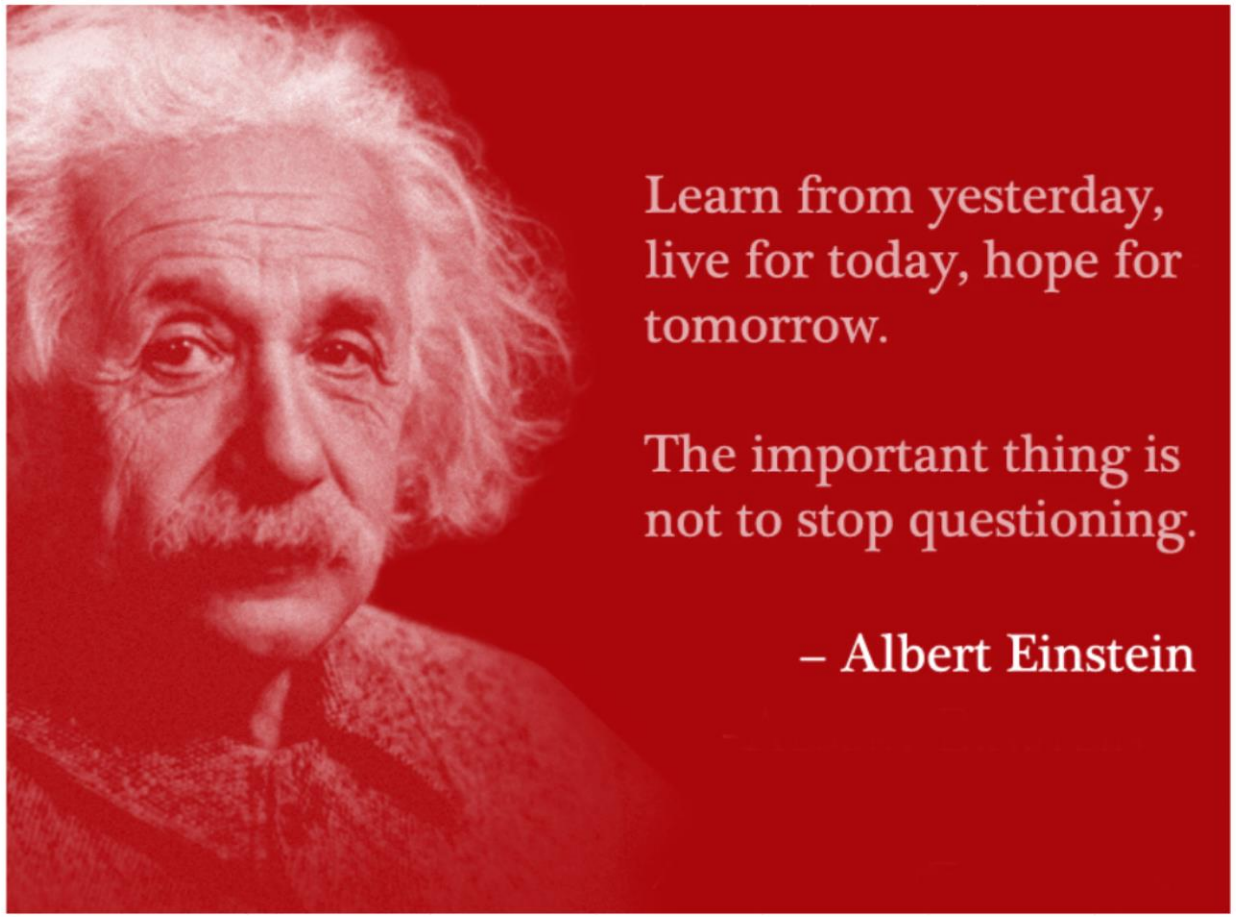


1) Hunting starts with **Visibility.**
2) Tools and Automation improve efficiency.
3) Use both formal and informal training.
4) Requires skilled, experienced analysts, engineers, and incident responders.
5) Track and measure hunting activities.
6) Intelligence is more than a buzzword.

1) Make threat hunting part of your overall security strategy – Integrate threat hunting into existing workflows.
2) Begin with a question, theory, or metric and work toward answering that question through research and proactive hunting.
3) Invest in threat hunting tools.
   - *Use tools and automation to minimize repeatable tasks.*
   - *Look for innovative, efficient ways to analyze data faster to identify patterns.*
   - *Leverage intelligence and machine learning to help prioritize hunting activities.*
4) Set ground rules regarding roles and responsibilities.
5) Continuous learning; Revisit investigations and hunting techniques!
6) Establish a repeatable and consistent process (use a cyclical/closed loop approach).
7) Maximize data collection, but be mindful of the quality of data you collect (use a combination of logs, network and host/endpoint data).
8) Build repeatable process workflows and queries back into your tools, through custom content, as you learn.
9) Seek to reduce mean-time-to-detection and response; find intrusions and compromises more quickly, and earlier in the cyber attack chain.
10) Understand that threat hunting is not a single task. Develop your capabilities progressively.

1) Too much reliance on “hunting tools” or any singular data type:
   - ✓*Logs lie*
   - ✓*Endpoint security tools miss things*
   - ✓*Vendors* can’t fully automate hunting
2) Alert-centric workflows
3) Open loop processes
4) Bias and fatigue (mix it up to keep the work interesting)
5) Failure to keep up with latest news / intelligence


Q&A


Learn from yesterday, live for today, hope for tomorrow.
The important thing is not to stop questioning.
– Albert Einstein