RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: SPO2-T06B

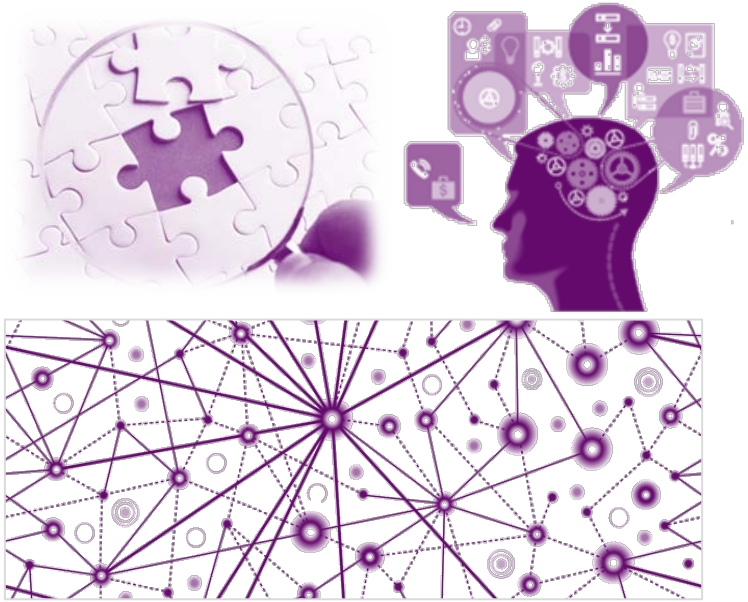
[Proactive Security]
Building a Threat Hunting Program

Joshua Douglas
Chief Strategy Officer
Raytheon Foreground Security

#RSAC

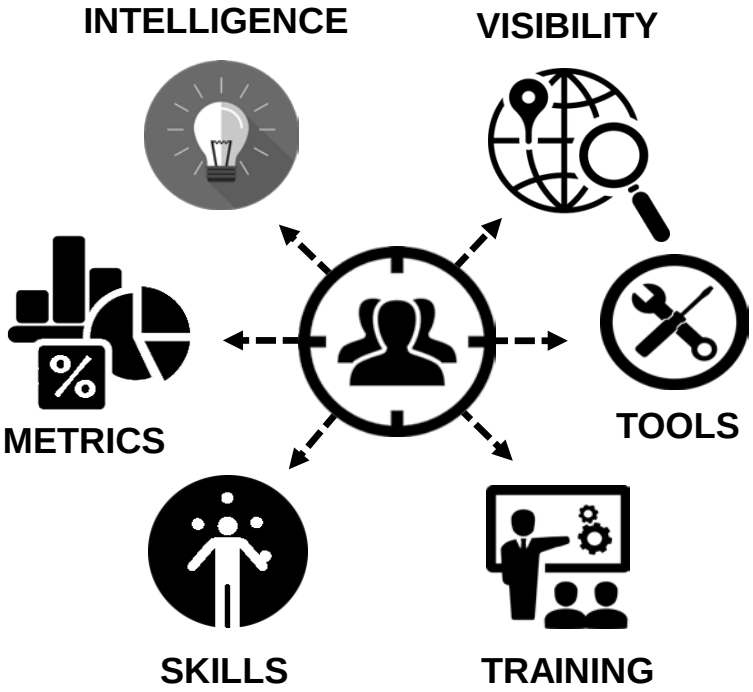
Adopting a Hunting Mindset

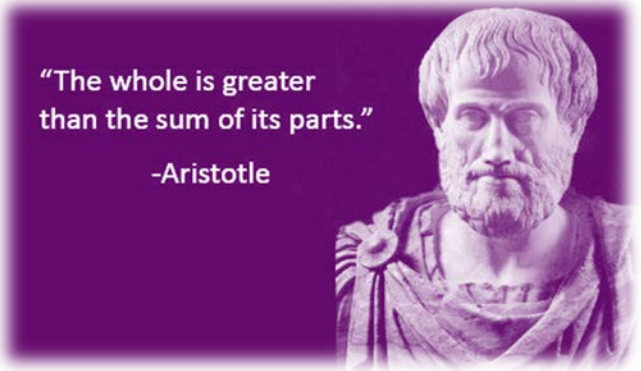
Monitoring & Responding to Alerts



Proactive Threat Hunting

THREAT HUNTING PROGRAM | **Key Focus Areas**





THREAT HUNTING PROGRAM | **Best Practices**

1) Make threat hunting part of your overall security strategy.
2) Integrate threat hunting into existing workflows.
3) Invest in threat hunting tools.
4) Use tools and automation to minimize repeatable tasks.
5) Look for innovative, efficient ways to analyze data faster to identify patterns.
6) Set ground rules regarding roles and responsibilities.
7) Establish a repeatable and consistent process.
8) Maximize data collection, but be mindful of the quality of data you collect.
9) Leverage intelligence and machine learning to help prioritize hunting activities.
10) Understand that threat hunting is not a single task but rather a progressive development of capabilities.

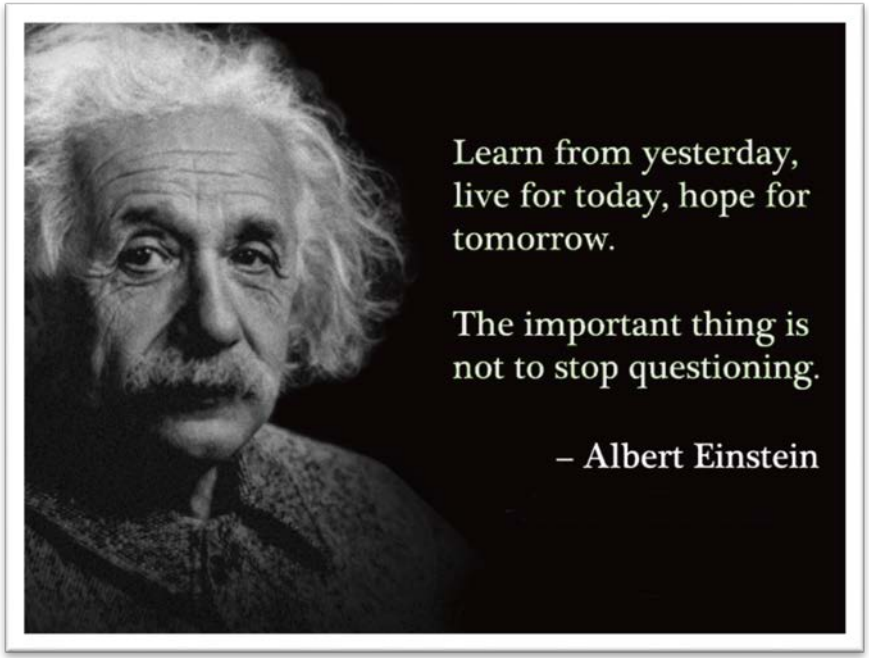
THREAT HUNTING PROGRAM | **Risks & Challenges**

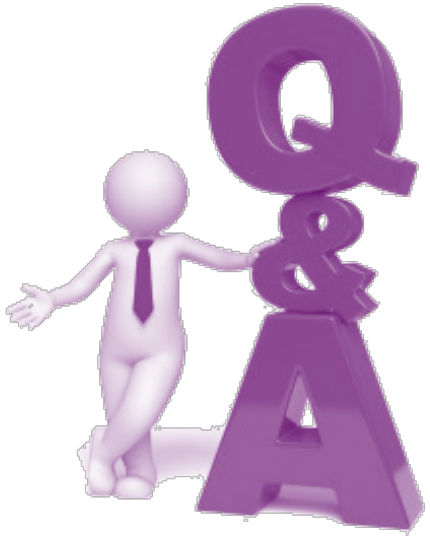
1) Too much reliance on “hunting tools” or any single data type:
   - *Logs can lie*
   - *Endpoint security tools miss things*
   - *Vendors can’t fully automate hunting*
2) Alert-centric workflows
3) Open loop processes
4) Bias and fatigue (mix it up to keep the work interesting)
5) Failure to keep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

THREAT HUNTING PROGRAM | Summary

COMPREHENSIVE APPROACH:

- Network, host, and log data (As much as you can get)
- **Begin with a question, theory, or metric**
- Be repeatable
- Seek to reduce mean-time-to-detection and response;
- **Train . Change it up. Train some more. Repeat.**


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


Q&A