Play Like a Kid, Protect Like a Champion: A Reservist Model

Sept 30, 2019
On a flight from Atlanta to San Jose...
In Search of Greatness
PASSION
PASSION

SELF-AWARENESS
PASSION

PLAY

SELF-AWARENESS
What is play?
What is play?

Play is fun
What is play?

Play is fun

Play is voluntary
What is play?

Play is fun

Play is voluntary

Play can be structured or unstructured
Introduce unstructured play to implicitly train our teammates, increase visibility, and close security gaps.
Chris Cochran

Threat Intelligence Lead @ Netflix

Purple Team Facilitator

Builder of Programs
Making Play Integral
If I had a dollar...

- “The talent pool is too small.”
- “We don’t have the time or resources for training.”
- “We are too busy triaging alerts to execute hunting, red teaming, or intelligence missions.”
Our threat landscape...

...is ever-changing.
...is increasing with intensity.
...must be watched and turned into intelligence.
Practice and play in the development of German top-level professional football players.

https://www.scott.af.mil/News/Features/Display/Article/1813677/soccer-promotes-healthy-living-for-us-defenders/
Playing for Performance
Playing for Performance
How do we incorporate play in a way that makes sense for the enterprise?
Making an Impact
What does any of this have to do with threat intelligence?
The Intelligence EASY Button
The Intelligence EASY Button
The Intelligence EASY Button
The Intelligence EASY Button

Elicit Requirements
Assess Collection Plan
Strive for Impact
Yield to Feedback
Making the Best of What You Have
Strive for Impact

Intelligence
Feeds relevant TTPs to the red team for emulation and to the blue team for context.

Red Team
Emulates attacks and attempts to circumvent prevention and detection measures.

Continuous Improvement

Blue Team
Looks for evil where we do not have conventional mitigations, closes gaps, and aspires to automate hunts (Detection).
Doing more with less today…

- Reservist model
Doing more with less today...

- Reservist model
- 3 current teams
Doing more with less today…

- Reservist model
- 3 current teams
- Senior/ Junior Model
Challenges...

● Managing Time
Challenges...

- Managing Time
- Scalable inclusion
Challenges...

- Managing Time
- Scalable inclusion
- Continuity
Wins...

- Immediate Findings/ Value
Wins...

- Immediate Findings/ Value
- Growth Zone for Response
Wins...

- Immediate Findings/ Value
- Growth Zone for Response
- Fun
What’s next for the Netflix Purple Team?

- Convey the value to leadership
- Sync operations with our new risk program
- Bring on a purple team operator for continuity
What can you do today?
Vision and Wisdom
VS.
Speed and Strength
Thank You.