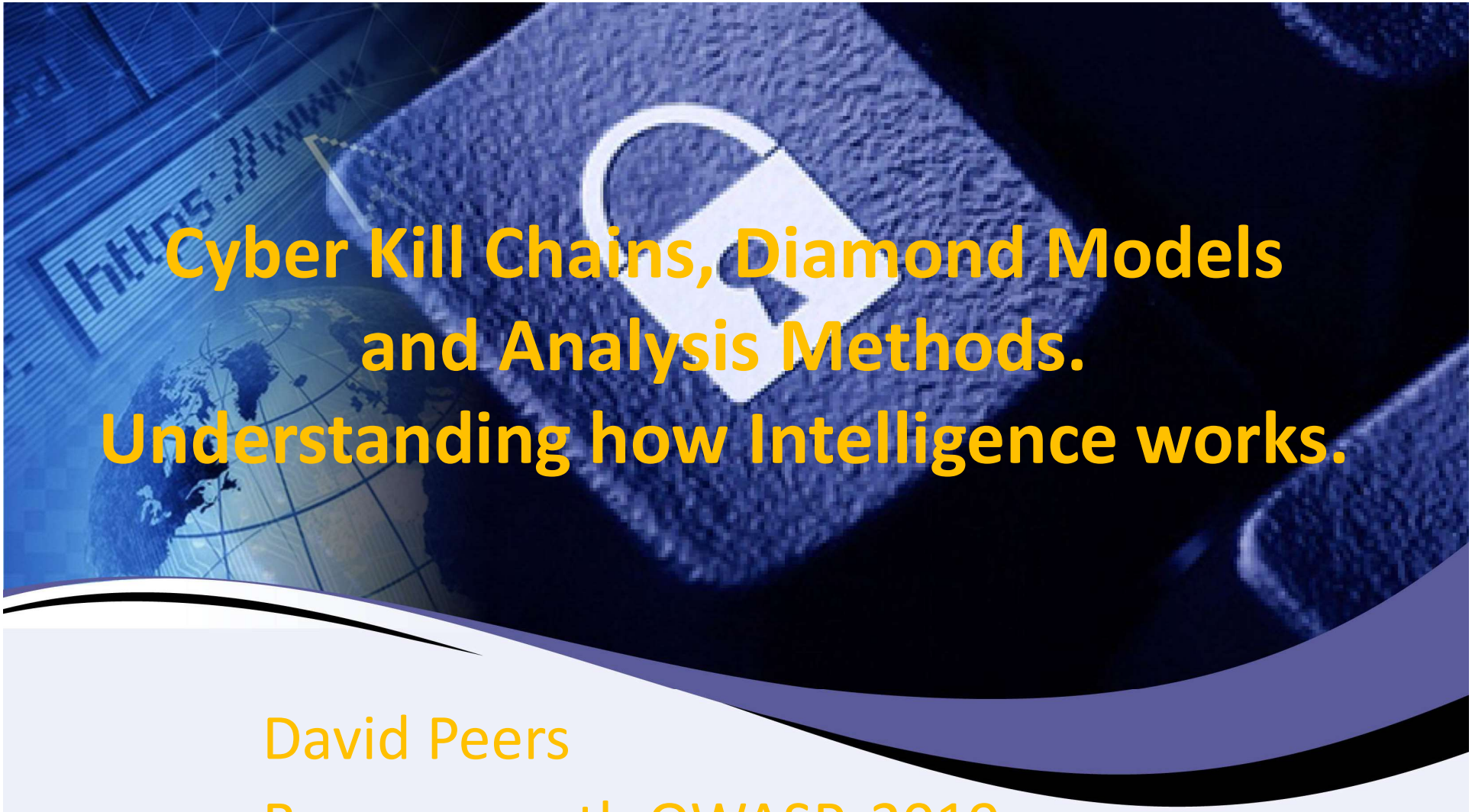


Cyber Kill Chains, Diamond Models and Analysis Methods. Understanding how Intelligence works.

David Peers

Bournemouth OWASP, 2019

OWASP

The Open Web Application Security Project

Introductions

OWASP
The Open Web Application Security Project

Who am I?

Royal Corps of Signals

Microsoft

CREST

GCHQ

What am I?

dpeers@protonmail.com

Covered tonight…

OWASP
The Open Web Application Security Project

- Jargon
- Intelligence Cycle
- Typical installation of malware
- Cyber Kill Chains
- Diamond Model
- Threat actor types
- 3 Scenarios

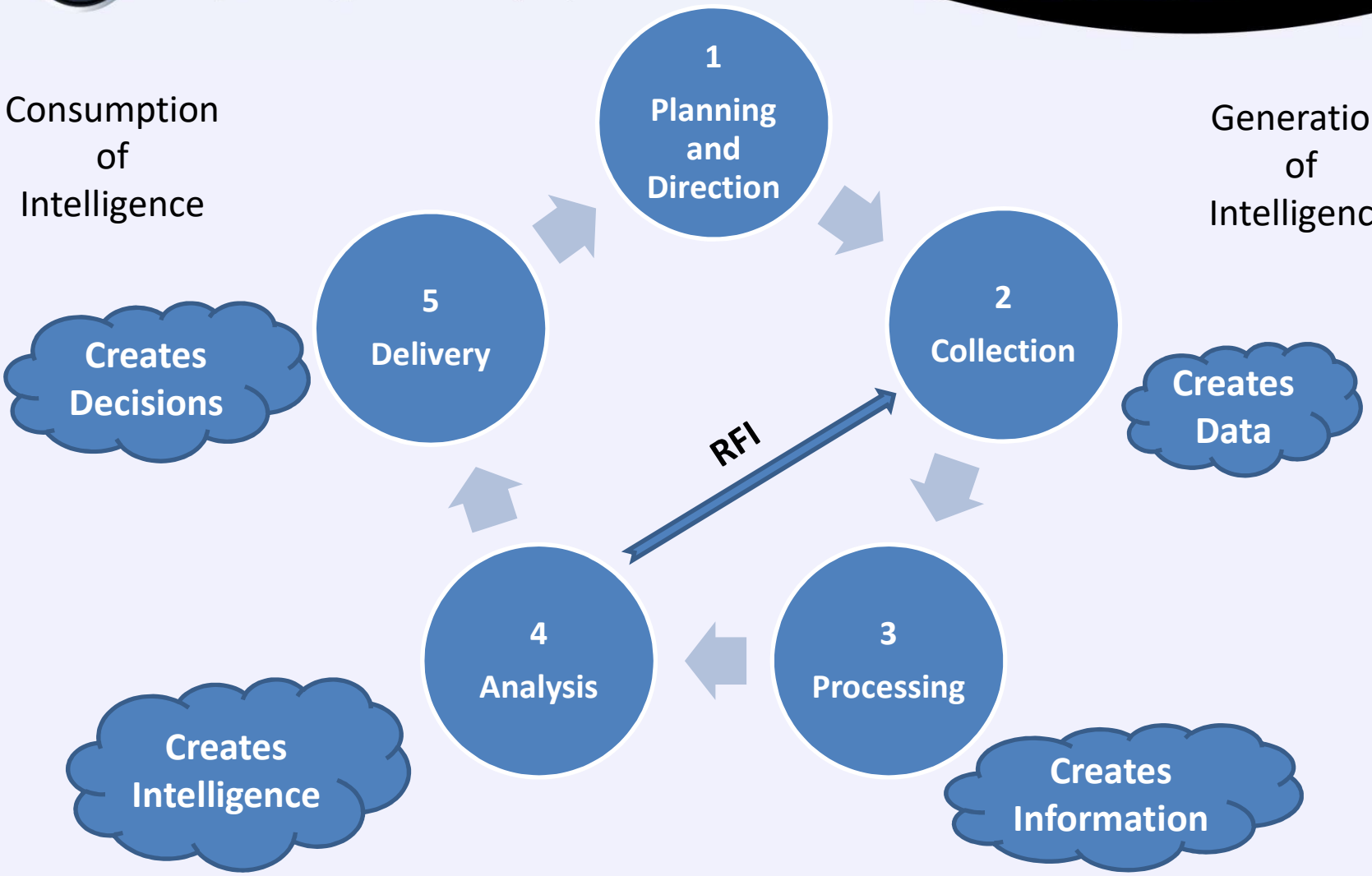
Jargon

OWASP
The Open Web Application Security Project

- Events and Incidents
- IoA
- IoC
- IoT
- TTP
- Bias
- Risk
- Black Swan
- Hypothesis
- APT
- Assets
- Asset
- Adversary
- Adversary Operator
- Adversary Customer
- Attack
- Campaign
- Cyber (enabled) crime

Intelligence Cycle

OWASP
The Open Web Application Security Project



Typical Installation of Malware

OWASP
The Open Web Application Security Project

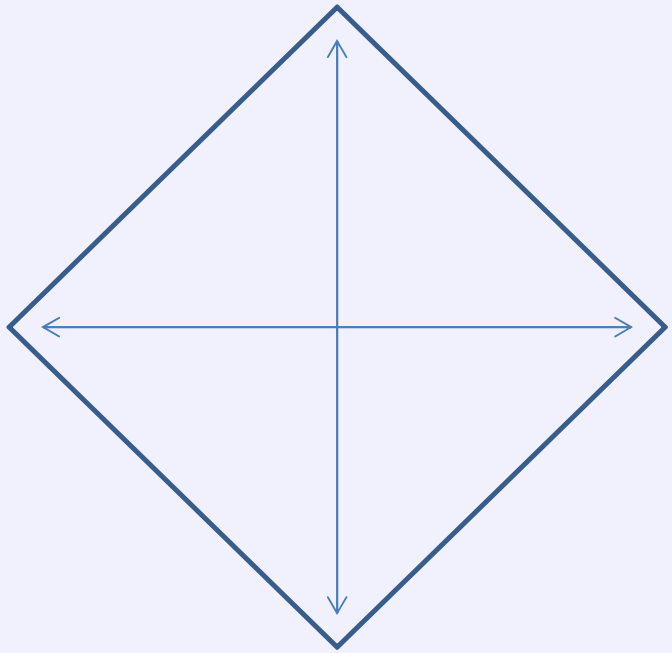
Cyber Kill Chain

OWASP
The Open Web Application Security Project

7 step process, developed by Lockheed Martin, to breakdown the process of intrusion and compromise.

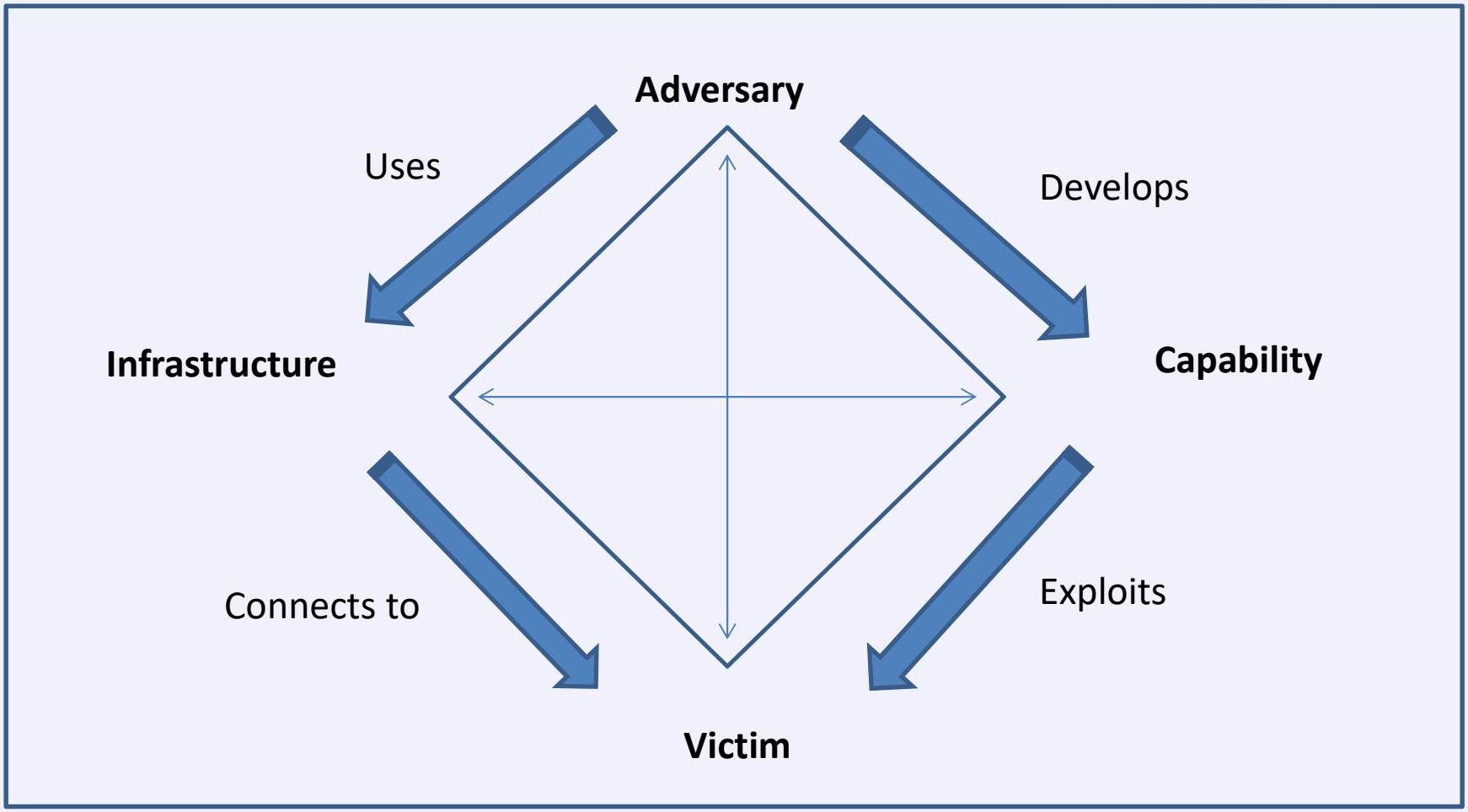
Diamond Model #1

OWASP
The Open Web Application Security Project



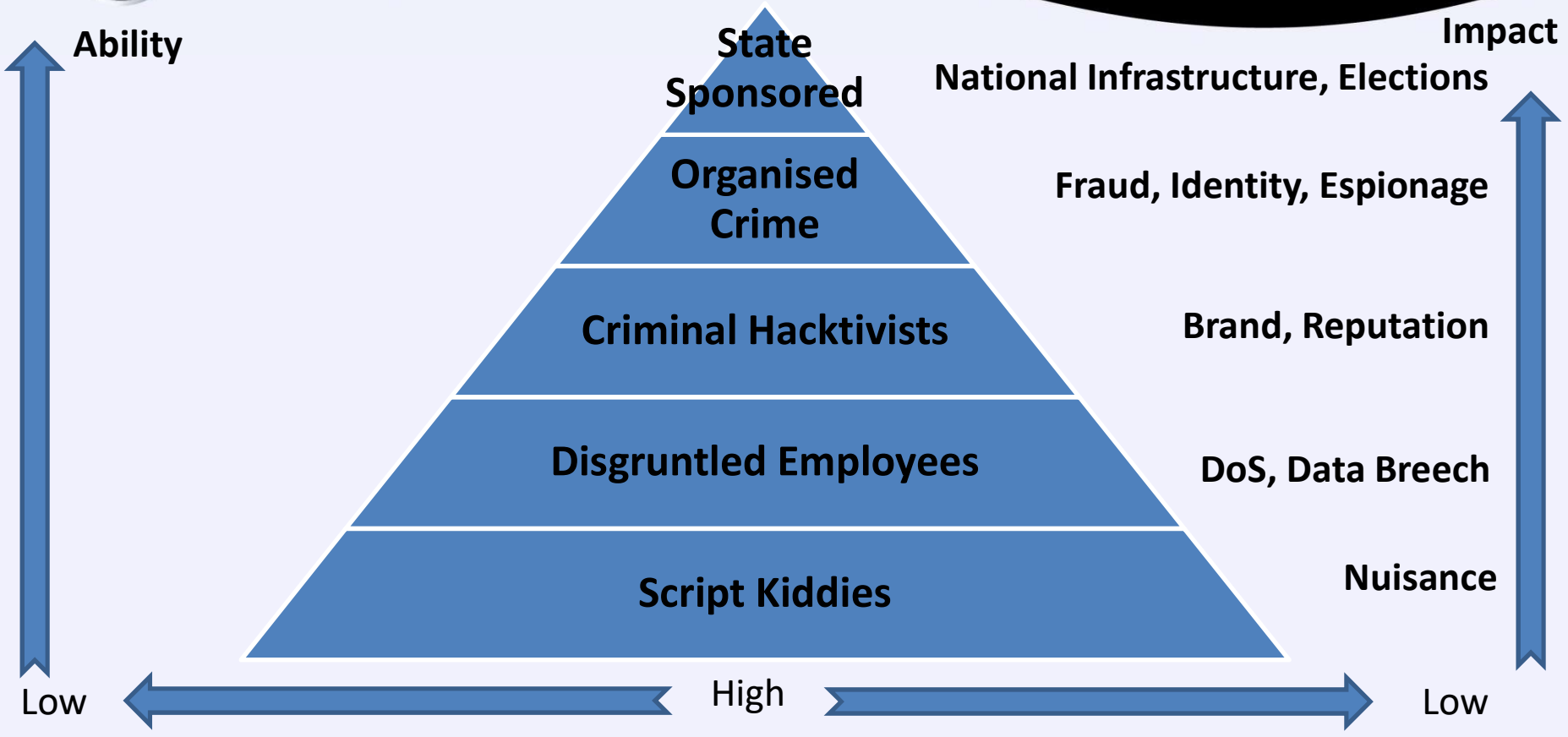
Diamond Model #2

OWASP
The Open Web Application Security Project



Threat Actor Types

OWASP
The Open Web Application Security Project



Population, Commitment, Time
Stealth, Knowledge, Funding

Scenarios 1, 2 & 3

OWASP
The Open Web Application Security Project

Let’s have some fun!

Questions?