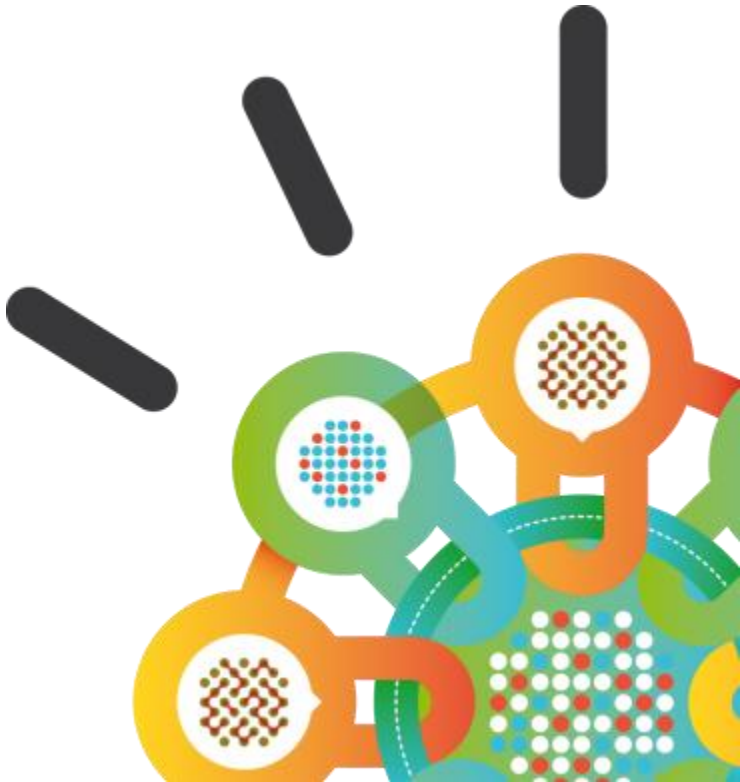
Comprehensive Cyber Intelligence

Chris Cardran
WW i2 Cyber Intelligence SME

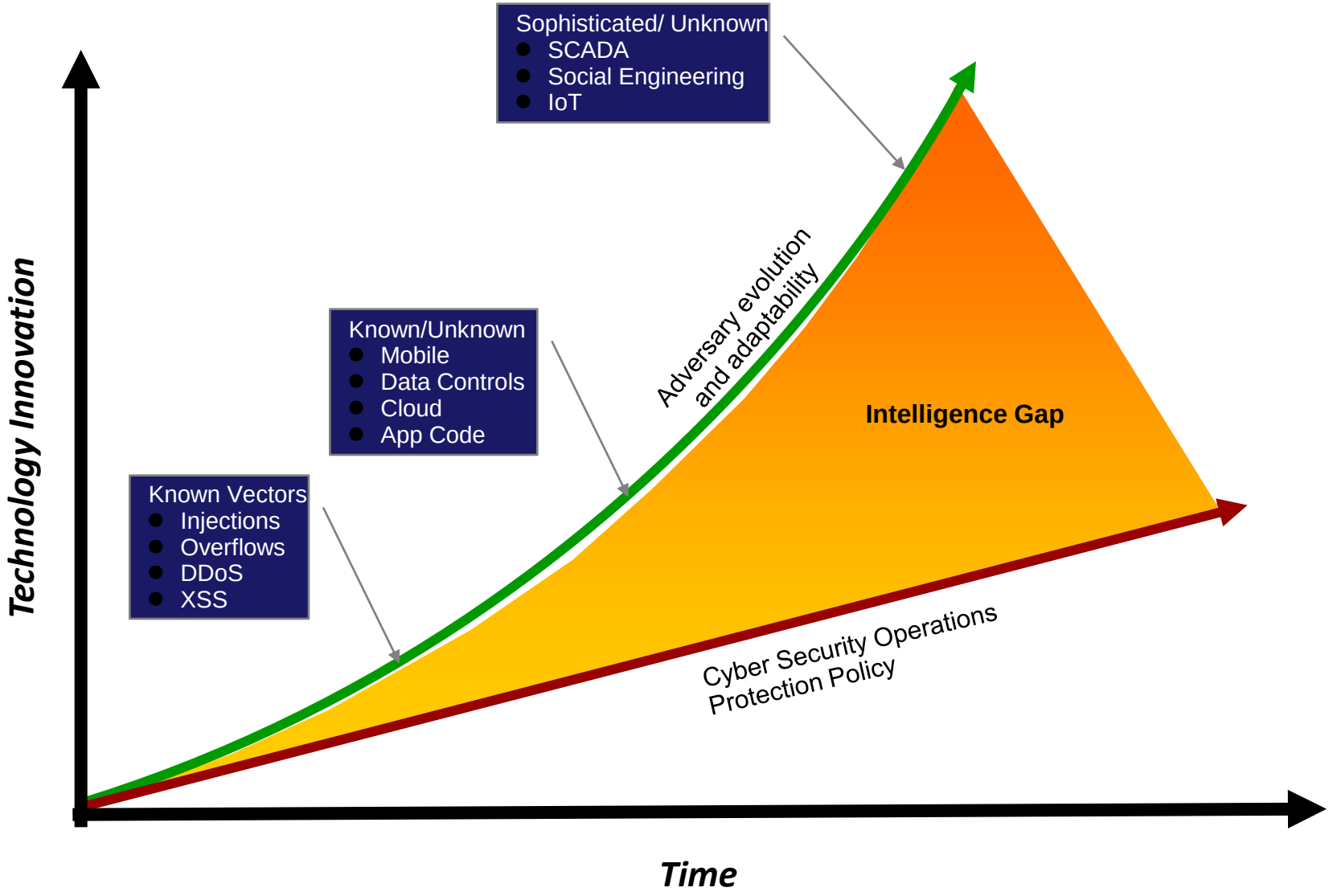


What is Cyber Intelligence?

IBM i2 for Cyber Intelligence helps organizations understand who their adversaries are, the construct of their criminal network, their strategies, motivations, and locations by layering large, disparate quantities of Cyber and real-world data into a fused comprehensive Intelligence picture; in order to better secure themselves from, and investigate on-going cyber attacks.

Intelligence is a force multiplier for Smarter Security

The Cyber Intelligence Concept



Cyber Intelligence "sweet spots"

Cyber Intelligence (Proactive)

Impact Analysis
Analyze attack surface and the negative effects of a vulnerability or threat on an organization.

Actor/Team Analysis
Analyze actors and groups over time to ascertain capabilities and common threat vector utilized.

Attack Tree Development
Analyze attack scenarios against current controls. Develop accurate decisions for policy and response.

Traditional Security Operations

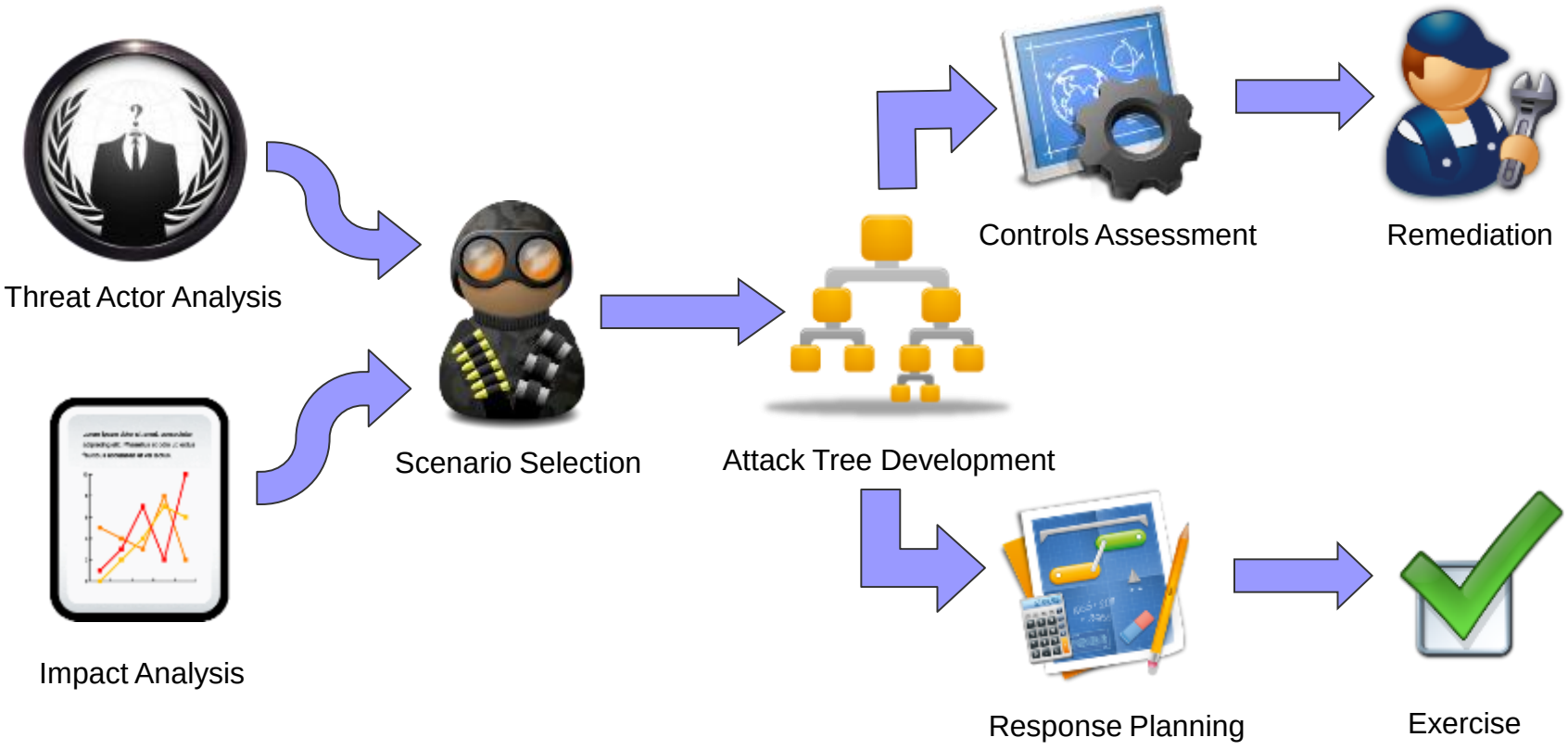
Detection
Development of policy and rules
Development of response procedures
Detect in real time if an exploit
Vulnerability scanning

Prevention
Policy and rules implementation
Adversary disruption
Patch remediation

Security Investigation
Internal IT investigation
Remediation procedures
Reporting

Cyber Intelligence (Investigation)

Investigation
Traditional Security Investigation is limited to IT related information an metrics and augmented by threat feeds, such as reputation lists. Cyber Intelligence investigations allow the security data to be combined with other internal data, such as Human Resources records and Open Source Intelligence. Additionally, discoveries can be used to update security operations controls.

Improved Threat Planning

i2 Investigations aid Cyber Scenario Planning and Attack Tree Analysis