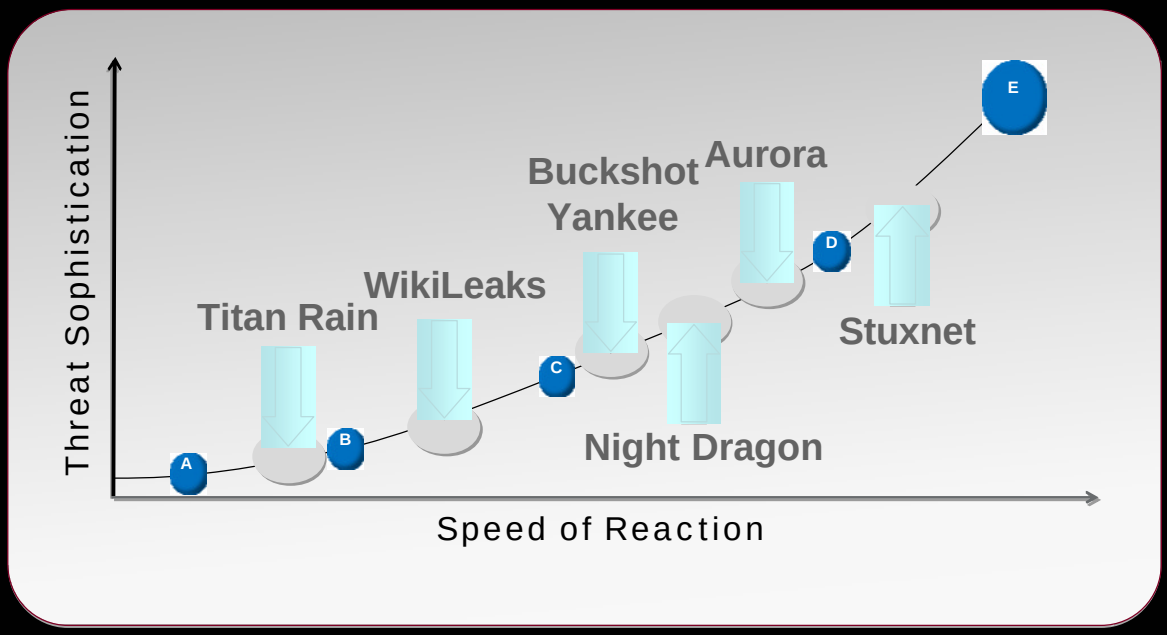
AFCEA TechNet Europe

Delivering Cyber Intelligence from the Cloud

May 2011

Mo Cashman
Director, Security Architecture
Global Defense and Central Governments
McAfee, Inc

Driving the Need for Speed

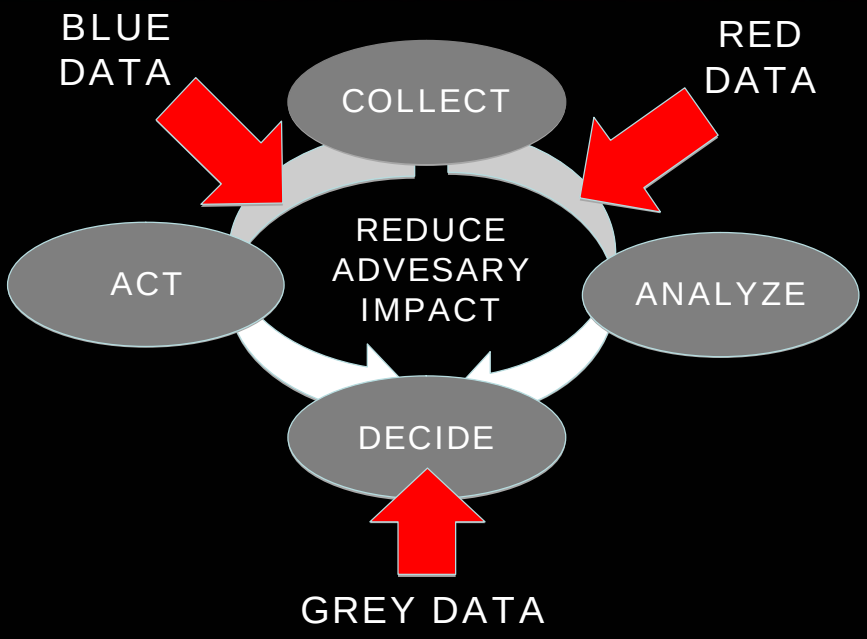


As threat sophistication rises, the need for real time delivery of cyber intelligence increases.

How fast do I need that Intelligence?

THREAT ATTRIBUTE	THEN	NOW
Vector	Services Email	Applications Users Web /Email USB Services File Content Network
Attack Surface	PC OS	Applications OS Virtual RTOS Mobile Embedded Users
Time to Exploit	@ 26 Days	Less than 0
Reconnaissance	Almost None	0 – 2 Years
Speed of Delivery	HUMAN SPEED	NETWORK SPEED

Cyber Intelligence Process



Cyber Intelligence increases the Speed of Reaction and Decision

Intelligence System Attributes

COLLECTION	Sensor Grids = Everything IP
STORAGE & AGGREGATION	Billions of Queries, Multiple Years of data
ANALYSIS	Reputation, Over-the-Horizon Correlation
DISTRIBUTION & ACTION	Real Time and Relevant

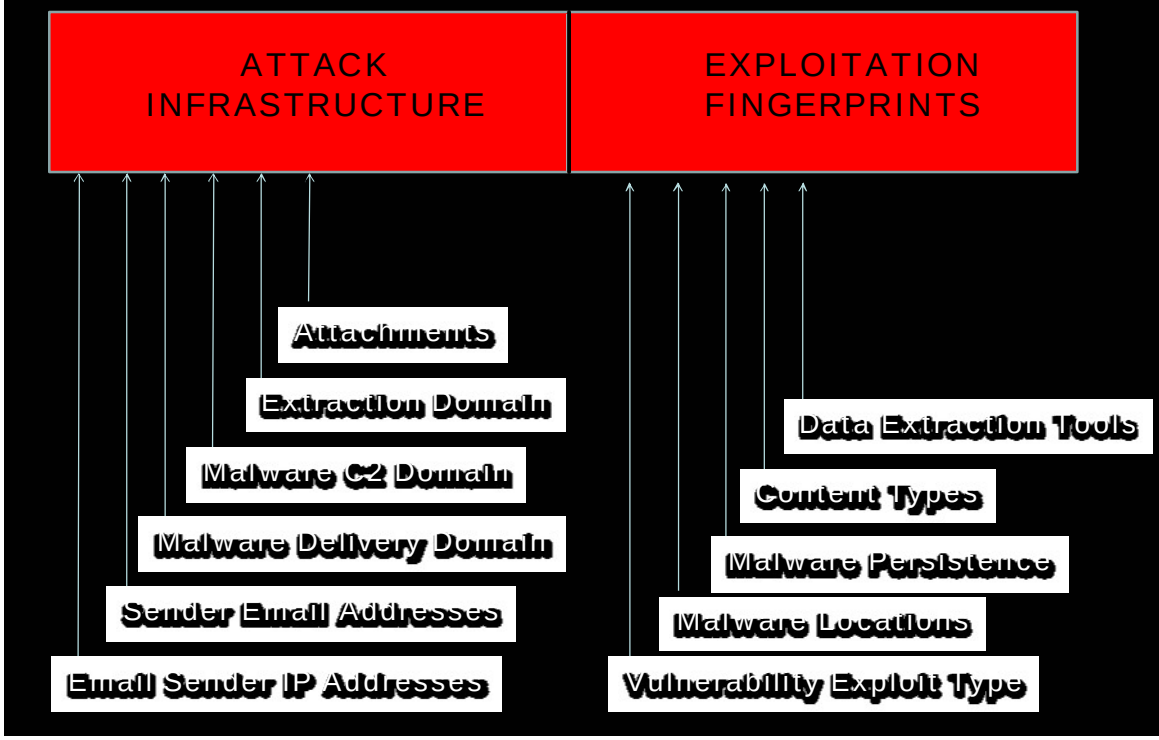
Data Definitions

BLUE DATA	Your own network data; *known good attributes*
RED DATA	*Threat information*, commercial or classified; known bad attributes
GREY DATA	Maybe good or Maybe bad; changing attribute *reputation*

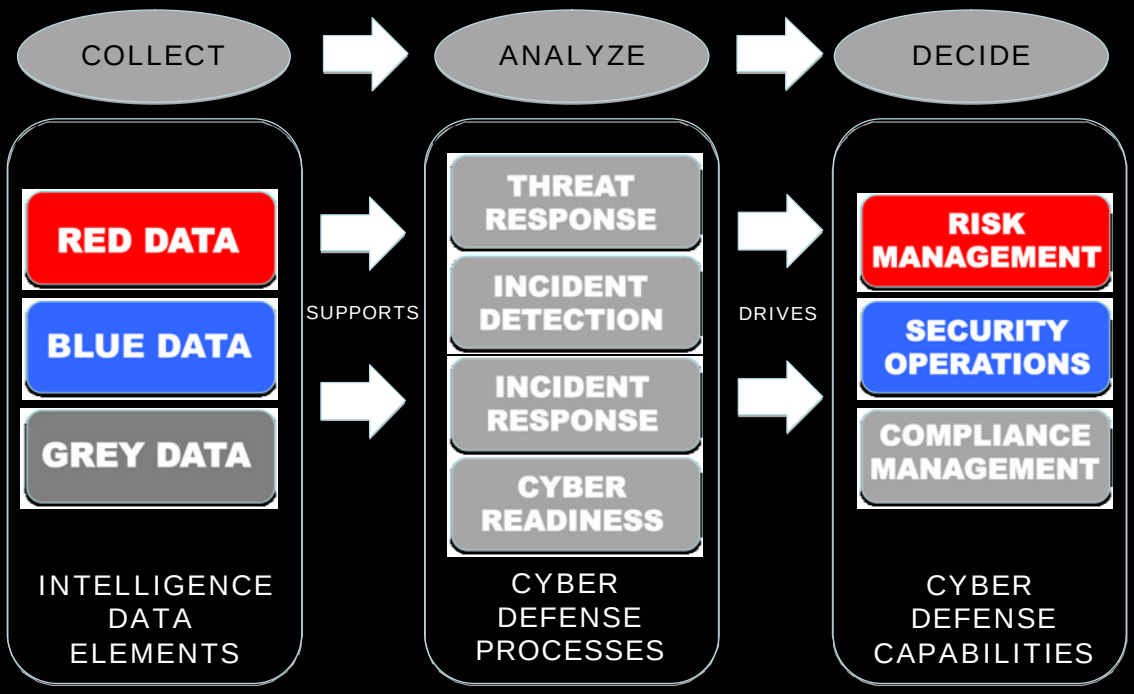
Blue Data Elements

ASSETS	Data, Machines, Users
EXPOSURES	Vulnerabilities, Threats
STATUS	Configurations, Patches
EVENTS	Incidents, Infections, Loss

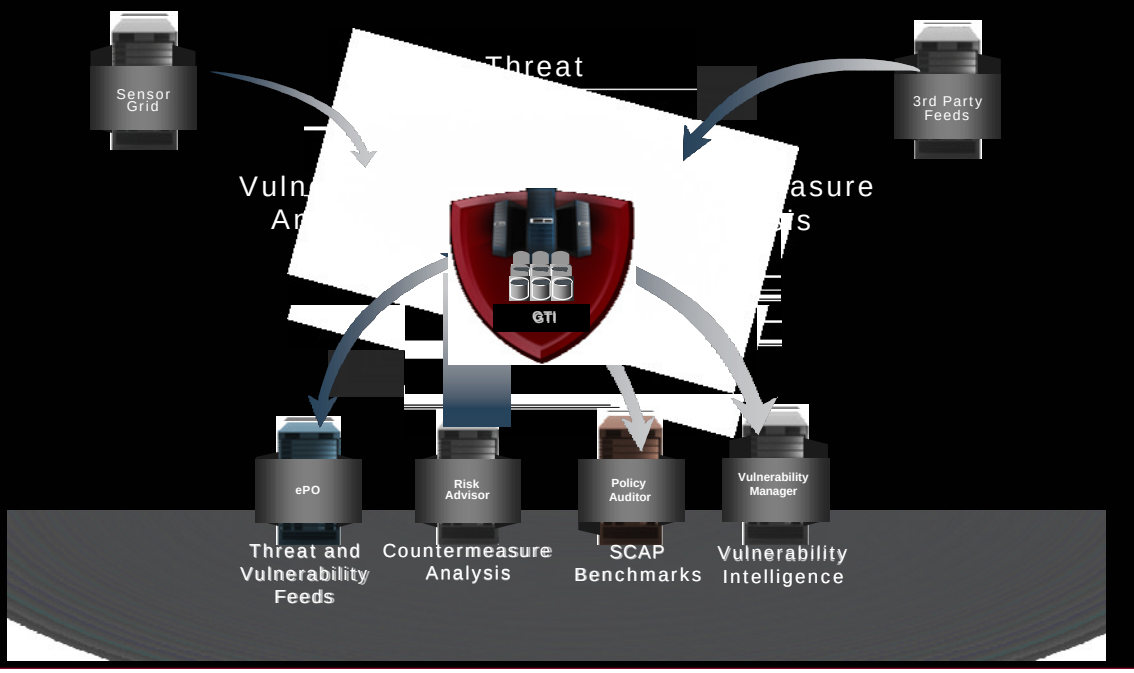
Red Data Examples



Intelligence Supports Process and Capability

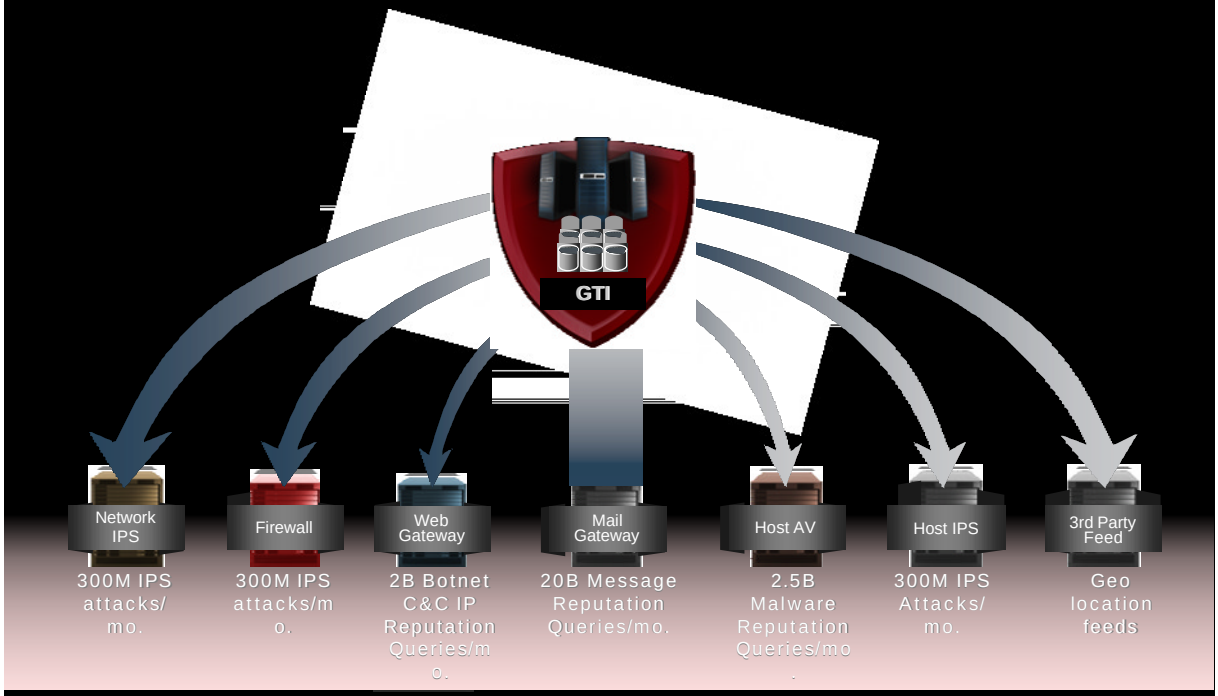


McAfee Distributes Relevant Cyber Intelligence



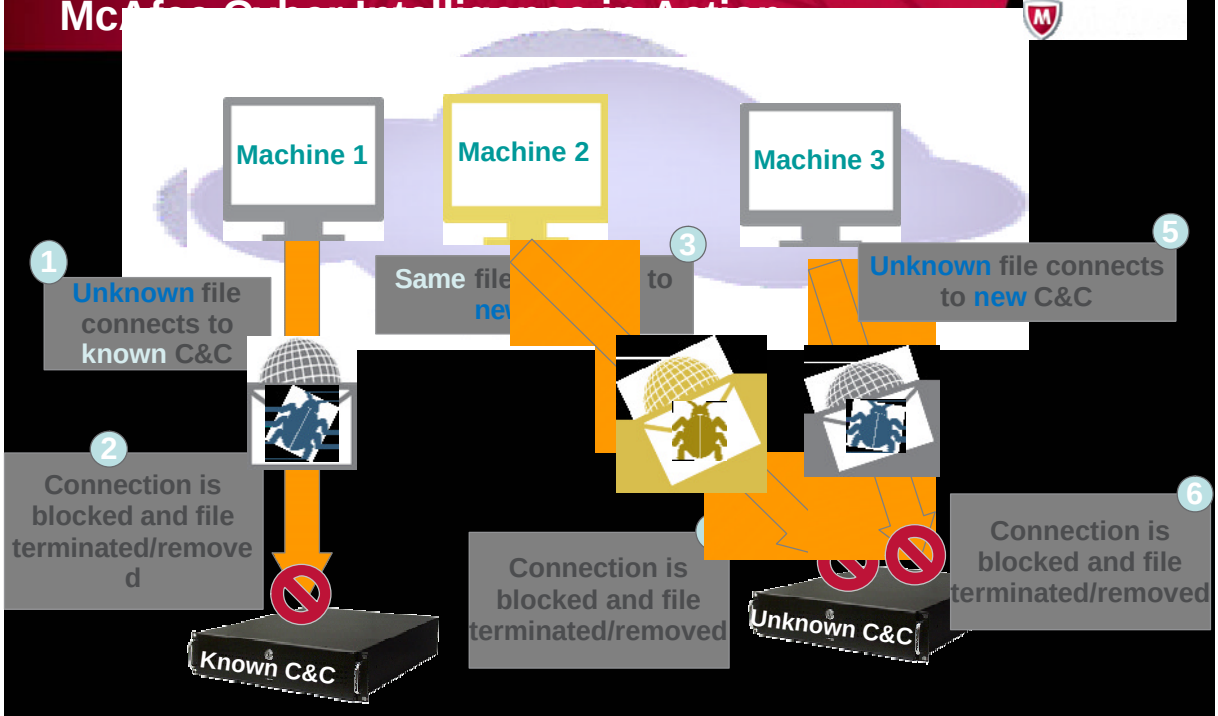
Actionable Red Data delivered direct to the Enterprise

McAfee Distributes Real-Time Cyber Intelligence



Grey Data that provides Real Time Protection

McAfee Cyber Intelligence in Action

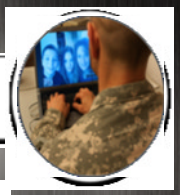


File and Network Connection Reputations correlated in real-time

McAfee Cyber Intelligence in Action

GTI delivers Grey Data direct to product for real time protection

ePO collects Blue Data for event analysis



GTI delivers Red Data for actionable risk assessments

McAfee Cloud-Based Cyber Intelligence architecture enables
Speed of Reaction and Decision