Discovering Threats by Monitoring Behaviors on Endpoints

Michael Kemmerer

Cybersecurity Engineer, The MITRE Corporation

MITRE

Approved for Public Release; Distribution Unlimited. Case Number 14-2948

Introduction – Michael Kemmerer

- **Work**
  - Senior Cybersecurity Engineer at The MITRE Corporation
  - EIC - network and endpoint sensor integration and analytic platform development
- **Splunk**
  - Deployed 3 distributed Splunk instances
  - Developed numerous custom Splunk apps
  - Co-authored technical guidance on deploying Splunk for a US Government Agency
- **Education**
  - M.S. in Engineering Management, Cybersecurity focus from UMBC
  - B.S. in Electrical Engineering from Lehigh University.

MITRE

Adversaries on Endpoints

The Problem

MITRE

The Problem– Adversaries Blend In

Adversaries, post-exploit, can look very similar to normal users[1]

Commonly used tools often look for the exploit or compliance and aren't very effective at finding the operating adversary[2]

Adversaries hide or masquerade their tools to blend in to the operating environment

Advanced adversaries are on the network an average of 243 days before being detected[3]

Photo Credits to Habib M'henni

1 - Chan et al. Effect of Malicious Synchronization. National University of Singapore. http://www.comp.nus.edu.sg/~chanmc/papers/herd2.pdf

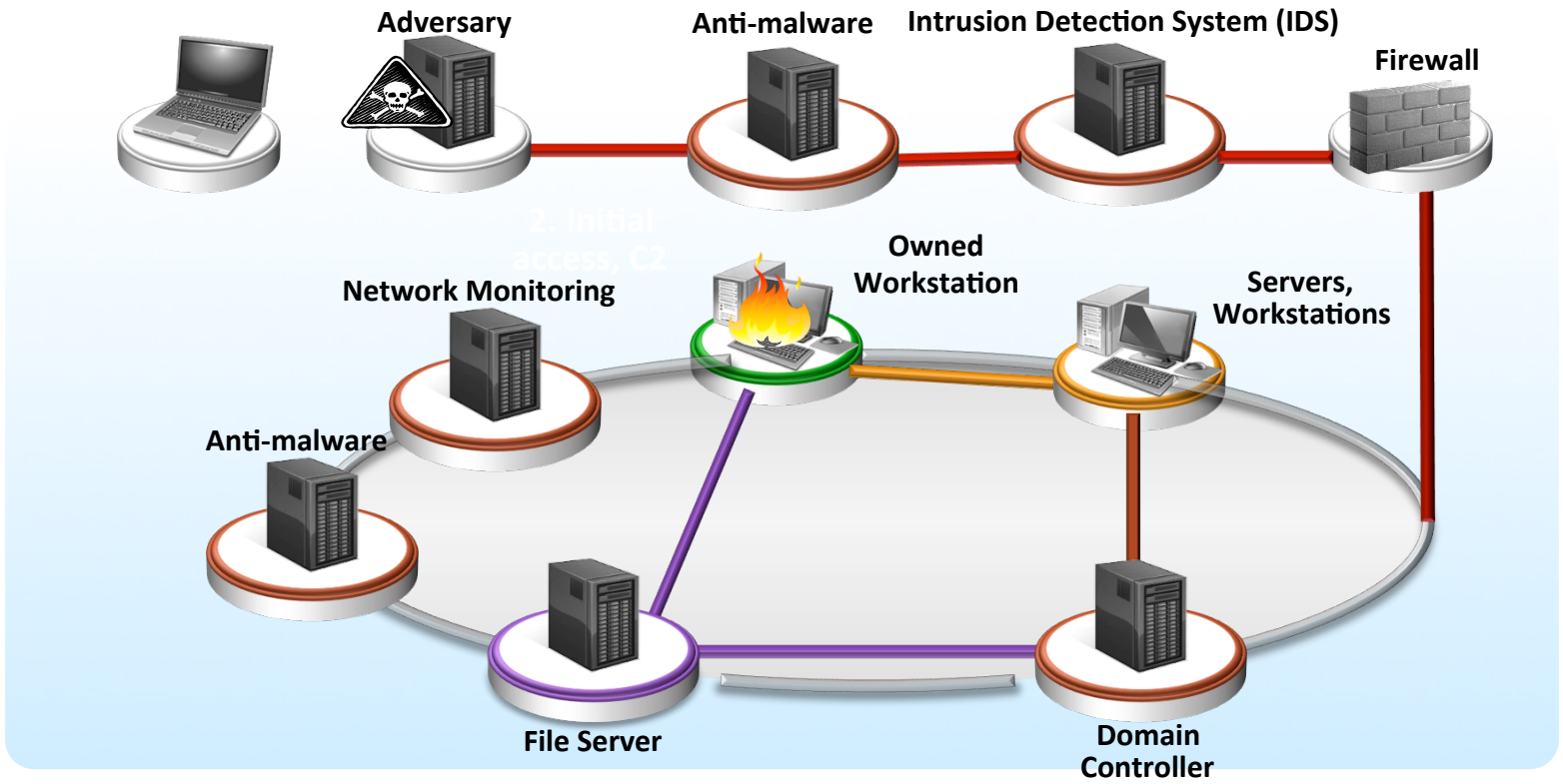
2 - Salem & Stolfo. Masquerade Attack Detection Using a Search-Behavior Modeling Approach. Columbia University. http://academiccommons.columbia.edu/download/fedora_content/download/ac:127675/CONTENT/cucs-027-09.pdf

3 - Mandiant, Threat Landscape, https://www.mandiant.com/threat-landscape/

MITRE

The Problem– Perimeter-Centric Defenses

The adversary uses legitimate means of communication through the infrastructure for command and control



MITRE

Technique Matrix

Persistence	Privilege Escalation	Credential Access	Host Enumeration	Defense Evasion	Lateral Movement	Command and Control	Exfiltration
New service	Exploitation of vulnerability	Credential dumping	Process enumeration	Software packing	RDP	Common protocol, follows standard	Normal C&C channel
Modify existing service	Service file permissions weakness	User interaction	Service enumeration	Masquerading	Windows admin shares (C$, ADMIN$)	Common protocol, non-standard	Alternate data channel
DLL Proxying	Service registry permissions weakness	Network sniffing	Local network config	DLL Injection	Windows shared webroot	Commonly used protocol on non-standard port	Exfiltration over other network medium
Hypervisor Rookit	DLL path hijacking	Stored file	Local network connections	DLL loading	Remote vulnerability	Communications encrypted	Exfiltration over physical medium
Winlogon Helper DLL	Path interception		Window enumeration	Standard protocols	Logon scripts	Communications are obfuscated	Encrypted separately
Path Interception	Modification of shortcuts		Account enumeration	Obfuscated payload	Application deployment software	Distributed communications	Compressed separately
Registry run keys / Startup folder addition	Editing of default handlers		Group enumeration	Indicator removal	Taint shared content	Multiple protocols combined	Data staged
Modification of shortcuts	Scheduled task		Owner/user enumeration	Indicator blocking	Access to remote services with valid credentials		Automated or scripted data exfiltration
MBR / BIOS rootkit	Legitimate Credentials		Operating system enumeration		Pass the hash		Size limits
Editing of default handlers			Security software enumeration				Scheduled transfer
Scheduled task			File system enumeration				

Source: ATT&CK™ Technique Matrix: The MITRE Corporation.

MITRE

Detecting the Adversary

The Experiment

MITRE

Our Experiment @ MITRE

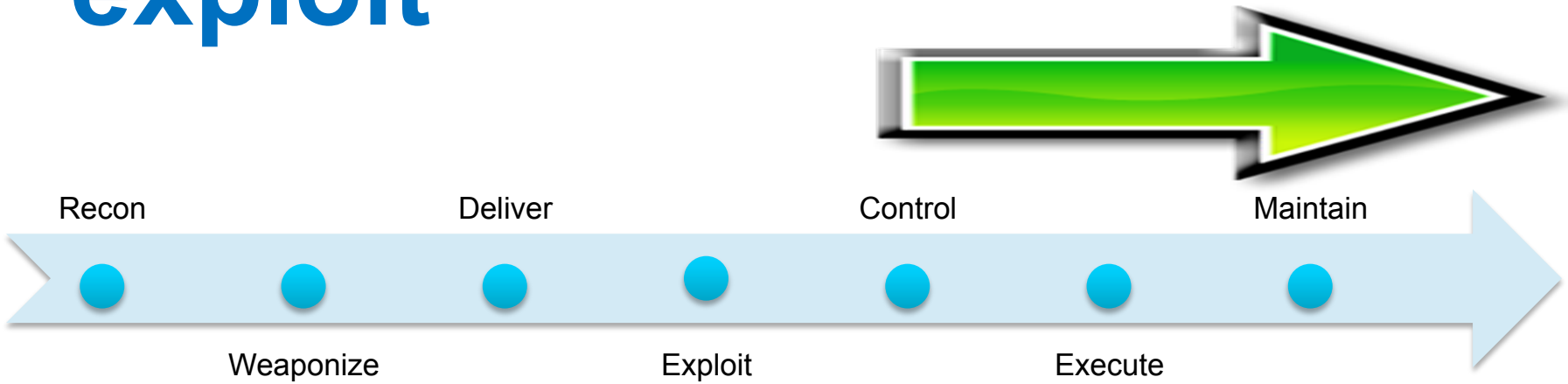
MITRE is exploring methods to detect the cyber-adversary operating within the enterprise network.
Our experiment demonstrates that novel end-point sensing can be used to detect the adversary operating on enterprise infrastructure.

Summary of the Experiment

- Develops sensors and analytics that can detect advanced cyber-adversaries that aren't detected by traditional tools
- Conducts Cyber-Games to test our results
- Is an experiment testing a sensing methodology that may lead to advances in cyber-incident detection

Our Objective

The experiment focuses on finding the adversary post exploit



Cyber Kill Chain: Intelligence-Driven Computer Network Defense by Eric Hutchins, Michael Cloppert and Dr. Rohan Amin - Lockheed Martin

MITRE

We Have a Living Lab

Our entire site participates

Corporate-owned computers

Environment of homogenous Windows desktops

Several users doing everything!

(email, writing documents, coding, web surfing, etc.)

MITRE

Endpoint Sensing

Awareness of Host Activity

MITRE

End-Point Awareness

Adversaries engage in similar behaviors as they execute their mission.

Hyper-sensing of the desktop provides visibility into user behaviors

We use a combination of COTS and custom sensors to monitor the desktop

Examples of Sensors

Host-based sensors

- Anti-Virus: McAfee, Symantec
- Process monitoring: Sysinternals Sysmon, whitelisting tools
- Network monitoring: tshark
- Multi-faceted: Event tracing for Windows, CarbonBlack, HIPS

Network sensors

- Signature-based: IDS/IPS
- Always-on: Netflows, PCAP

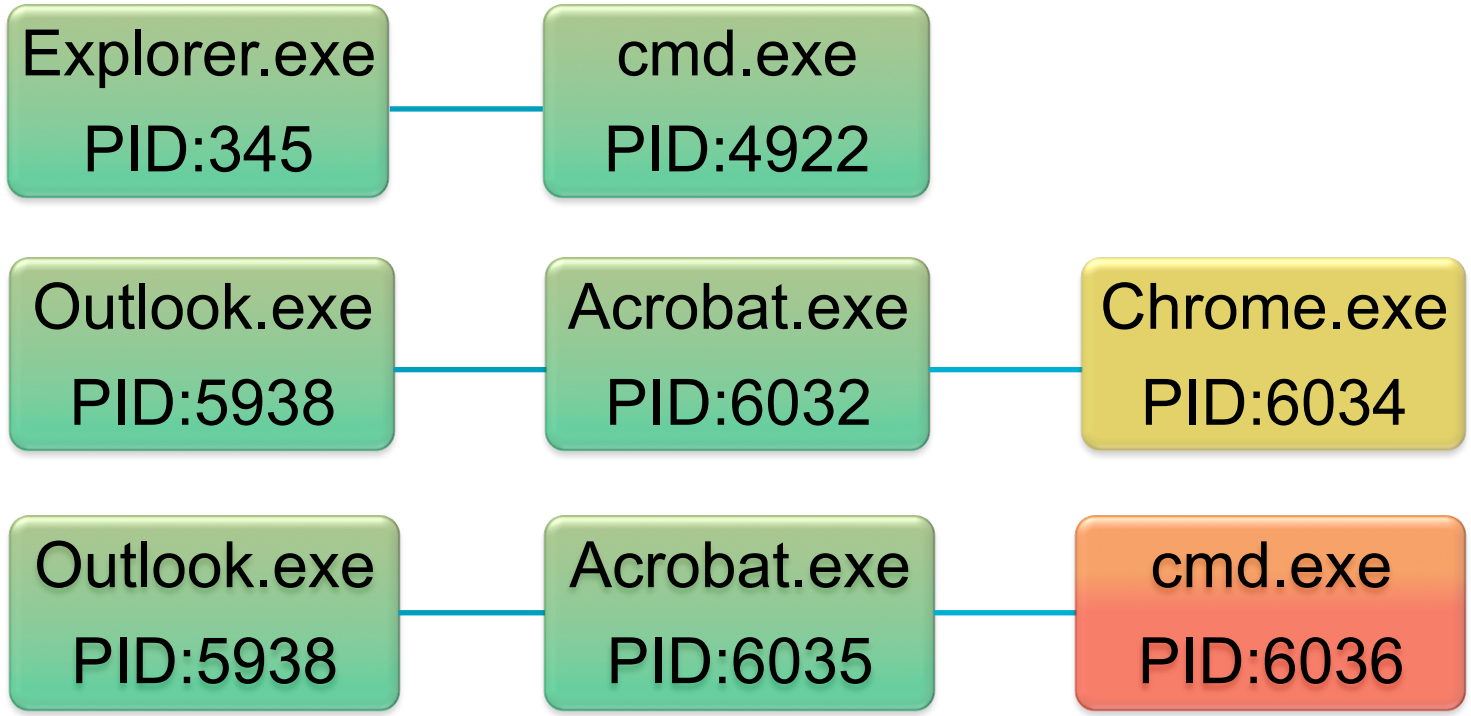
On-demand functions

- Powershell Scripts

Process Monitoring Tool

Provides details on processes

Process chains provide context around system activity.



MITRE

Host-Based Network Sensor

Metadata on Network Connections

- IP Addresses
- Ports
- Protocol information
- Message contents

Pivot Point Between Host and Network Data

- Process initiating connection
- PID, PPID

Profile process behavior
identify covert channels

MITRE

Analytics – Advancing the State of the Art

Analytics based on publicly available tools, techniques, and procedures (TTP)

MITRE

Analytics – Sharing Means Caring

Tested, shareable analytics that are effective at finding adversary behavior are the output of the project.

	Summary	Hypothesis
CAR-2013-01-001	Process Summary Index	A running process is defined by the events "PROCESS_STARTED" and "PROCESS_EXITED". An alternative definition for process execution, this will be a building block analytic that will allow an analyst to look at process execution times, process run duration, orphan processes and other characteristics that can be used in more sophisticated analytics.
CAR-2013-01-002	Autorun Differences	By monitoring changes to registry entries that are set to run automatically we hope to observe indicators of malicious behavior on hosts (primarily modifications to registry entries)
CAR-2013-01-003	SMB Events Monitoring	By Monitoring SMB events we hope to identify malicious activity occurring over the network, particularly remote access. Of particular interest are file events (file reads and writes) across the network. Identifying such traffic not only helps in identifying the potential scope of compromise.
CAR-2013-02-001	Programs accessing files of common types	Most common file types (.docx, .pptx, .pdf, .txt, etc.) are accessed by a small number of different programs. Identifying programs accessing such files that are not part of the "normal" list may be indicative of malicious behavior.
CAR-2013-02-002	User Controlled Processes that End Quickly (LT 10 sec)	Processes that are opened for user interaction (ex. Office programs) will typically be open long enough for user to see and possibly interact with the data.
CAR-2013-02-003	Processes Spawning cmd.exe	Certain parent-child relationships between processes are indicative of malice. One such example is cmd.exe spawning from adobe acrobat.
CAR-2013-02-004	Suspicious Program Run Locations	Files run from: %systemdrive%\RECYCLER, %systemdrive%\SystemVolumeInformation, %systemroot%\Tasks, %systemroot%\debug could be malicous

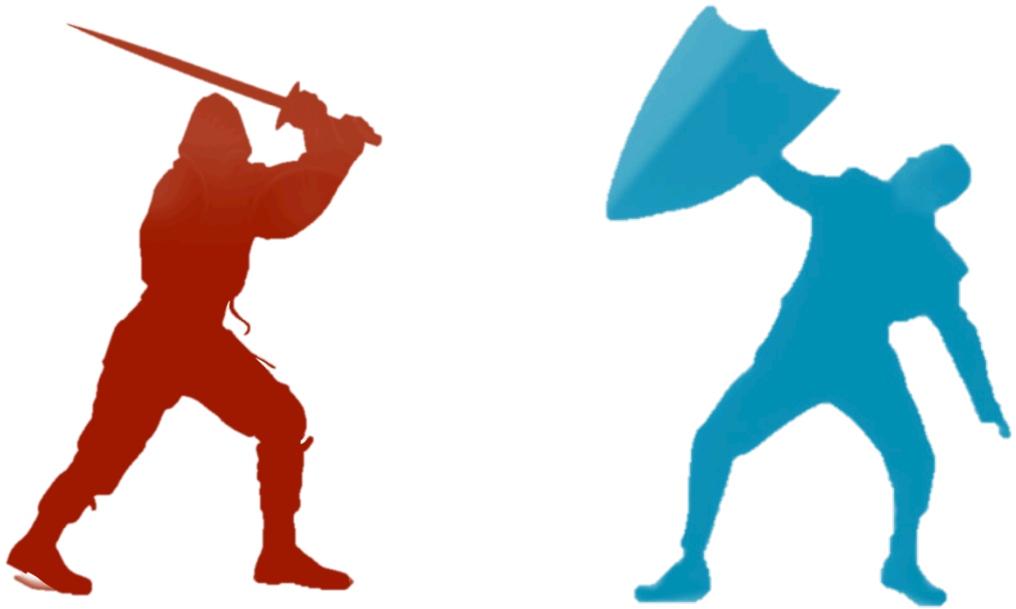
MITRE

Cyber Games – Testing the Capabilities

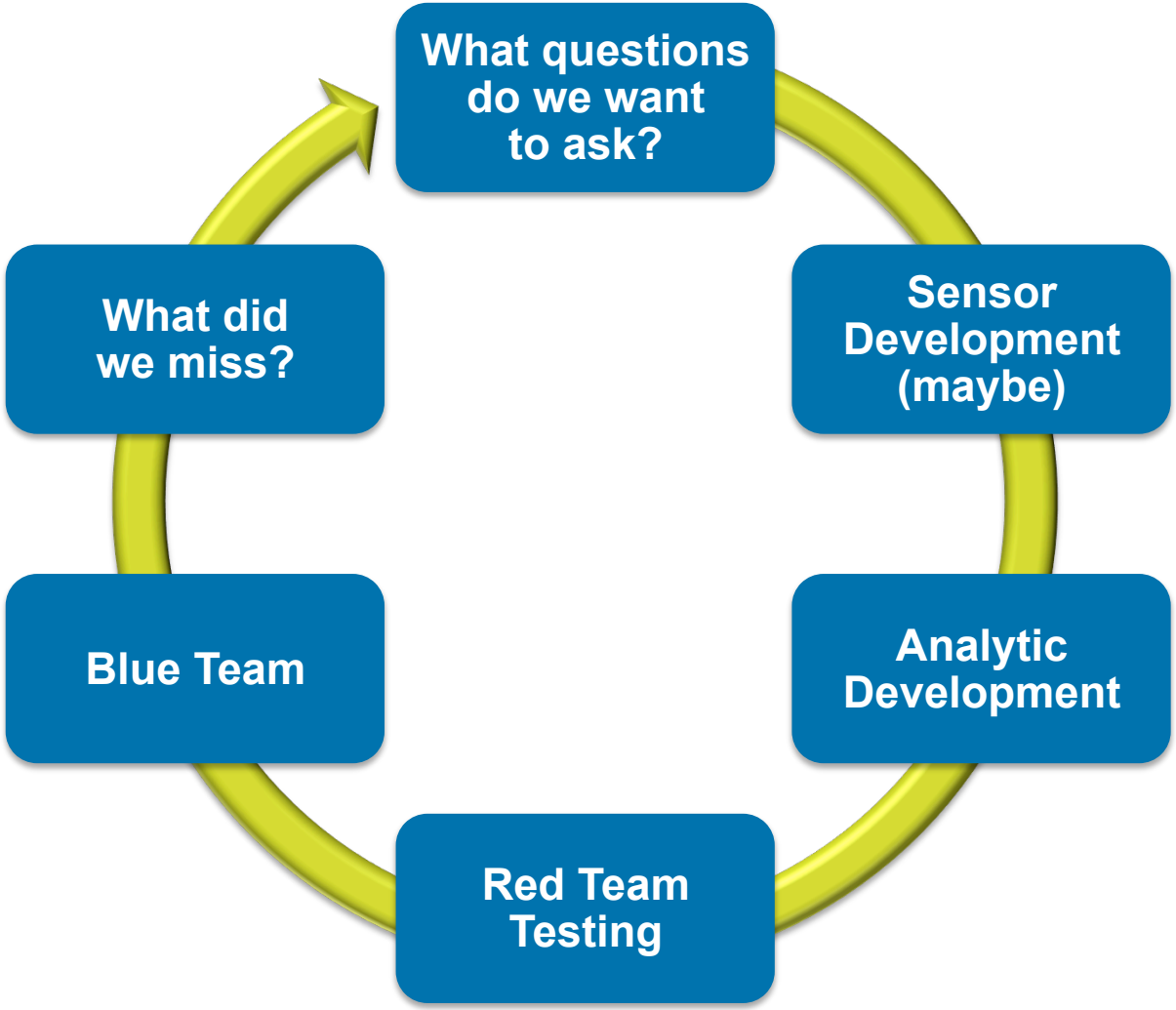
Testing our sensing capabilities and analytics using a collection of TTPs

Multiple games run throughout the year

Cyber Games documents include analytic successes and failures for internal review

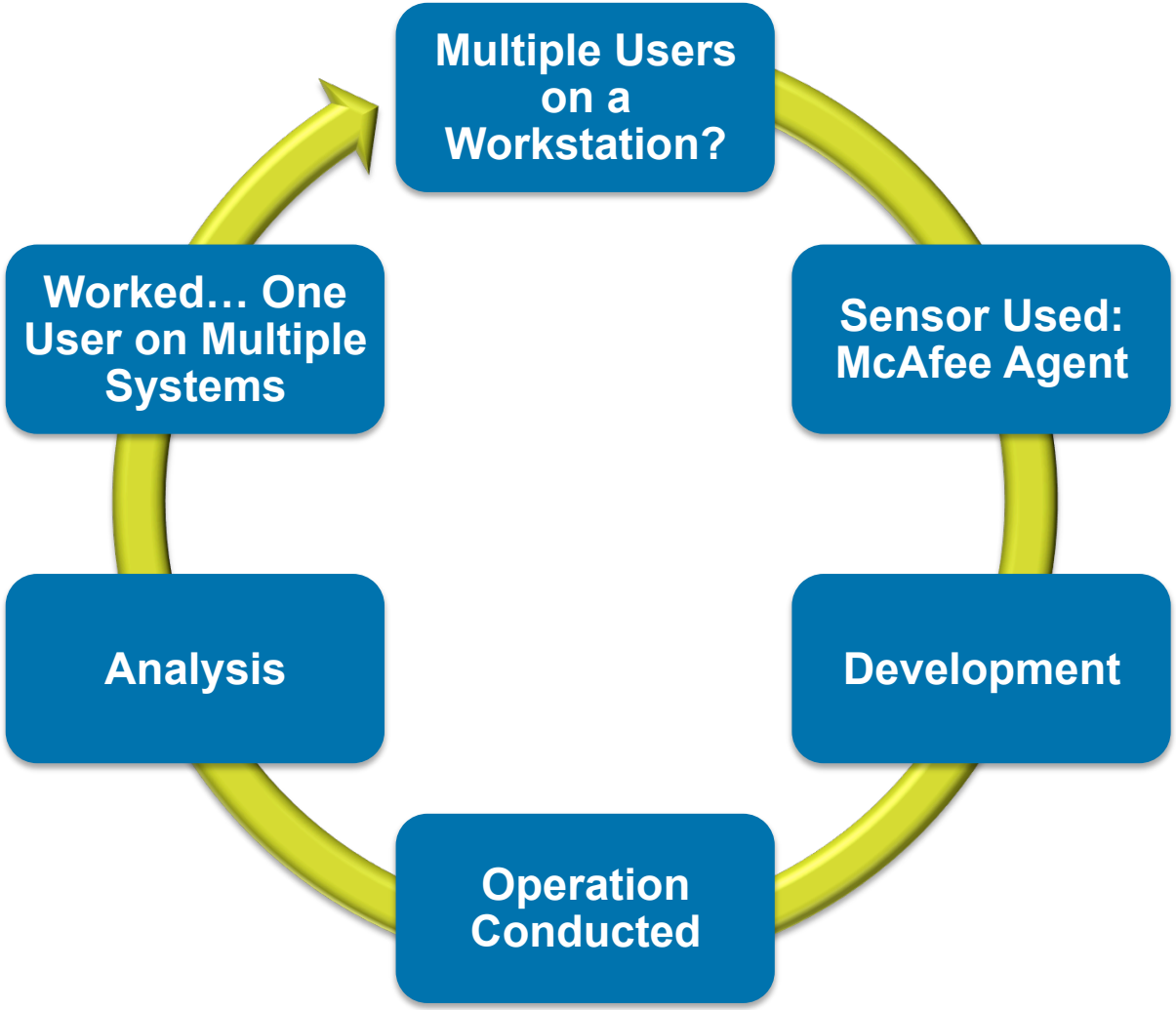


Analytic Development Cycle



MITRE

Cyber Games Drive the Cycle and Analytic Improvement



MITRE

What Can I Do Right Now?

By making small changes to your configuration, you can begin seeing more details

MITRE

Monitoring for Credential Theft

Credential dumping

- Monitor c:\windows\system32\lsass.exe on 1 or 2 endpoints
- Don’t block. Just see what programs are “touching” it
- Observe over time
- Begin to whitelist known programs (best if done by hash and/or signature information)
- Continue to add programs to the whitelist or filter in Splunk

MITRE

Monitoring for Credential Theft – Continued

Offline techniques

- Monitor reading of the following registry locations:
  - hklm\sam
  - hklm\security
  - hklm\system
- Saving of these locations can allow for offline retrieval of cached credentials (via secretsdump)

Reference: https://securusglobal.com/community/2013/12/20/dumping-windows-credentials/

Monitoring for Persistence

Files and Directories

- **fschange (deprecated)**
  - Tasks
  - Start menu startup directory
  - .ini files

Registry

- **HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms**
- **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup**
- **Dozens more…**

Other Techniques

- **Registry shell spawning**
- **Extension hiding**
- **Active-X components**

Reference: http://bytes.com/topic/windows/insights/860759-windows-autorun-faqs-list-autostart-locations

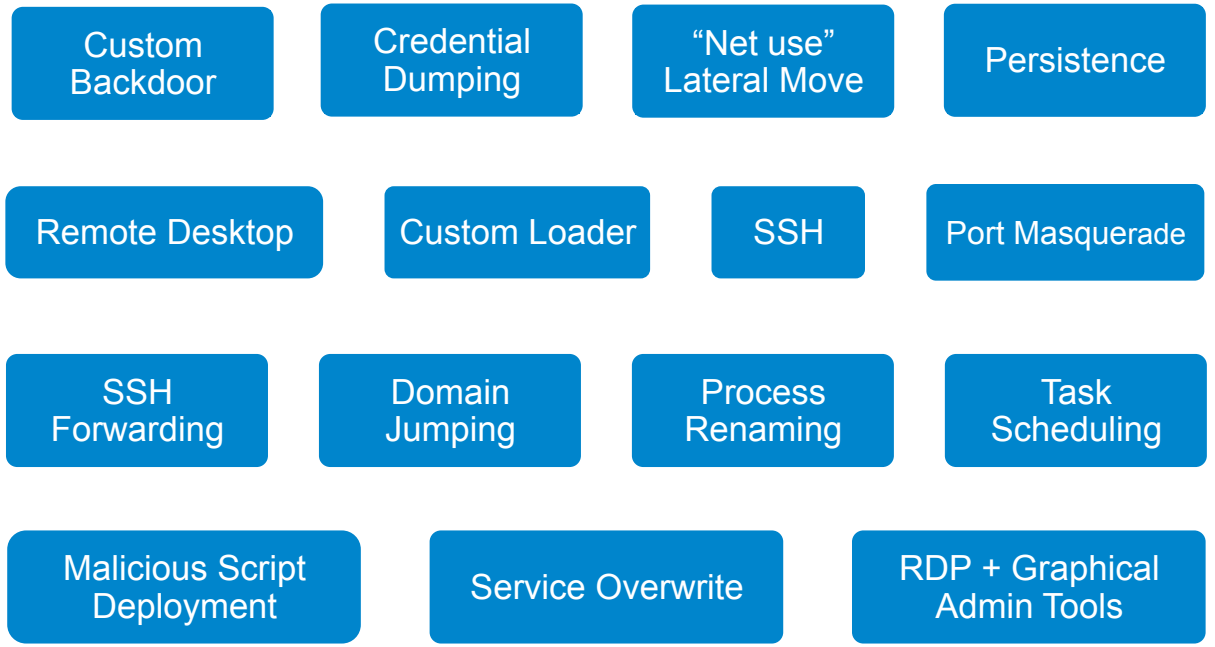
MITRE

Monitoring for Persistence – Continued

Periodic and scripted scans

- **Sysinternals' autorunsc.exe**
  - Run periodically and search for changes using Splunk
- **McAfee Asset Baseline Monitor (ABM)**
  - Monitor registry locations noted previously

Key TTPs To Be Aware Of



MITRE

Lessons Learned

Our experiments validate that end-point sensing can be used to detect the cyber adversary

Some information types are starting to emerge as highly valuable

We continue to develop both analytics and new sensing abilities to better detect adversary behavior

Questions & Answers

Michael Kemmerer
mkemmerer@mitre.org

MITRE

Learn, share and hack

Security office hours: 11:00 AM – 2:00 PM @Room 103
Everyday

Red Team / Blue Team - Challenge your skills and learn new tricks
Mon-Wed: 3:00 PM – 6:00 PM @Splunk Community Lounge
Thurs: 11:00 AM – 2:00 PM

Birds of a feather- Collaborate and brainstorm with security ninjas
Thurs: 12:00 PM – 1:00 PM @Meal Room

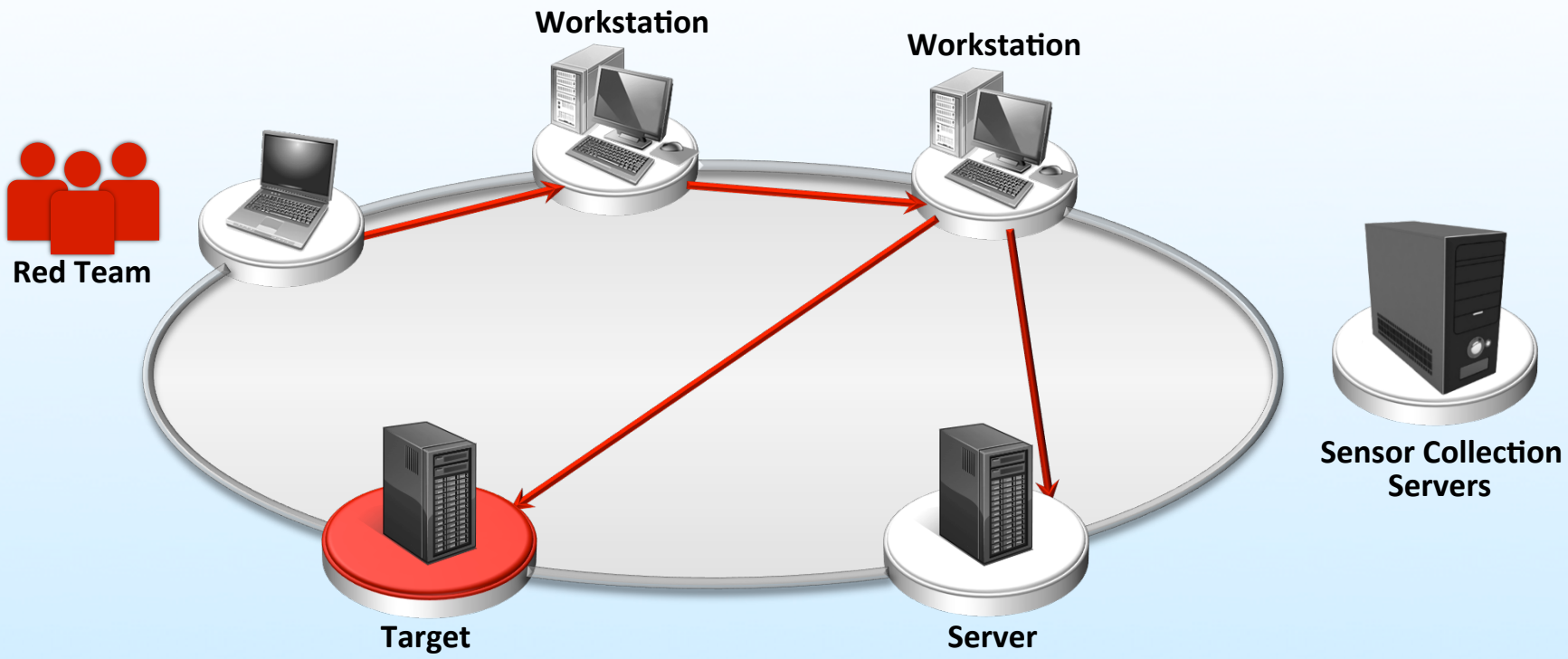
Backup Slides

MITRE

Cyber Games – Red Team

TTP Emulation

Analytic Outcome Focused

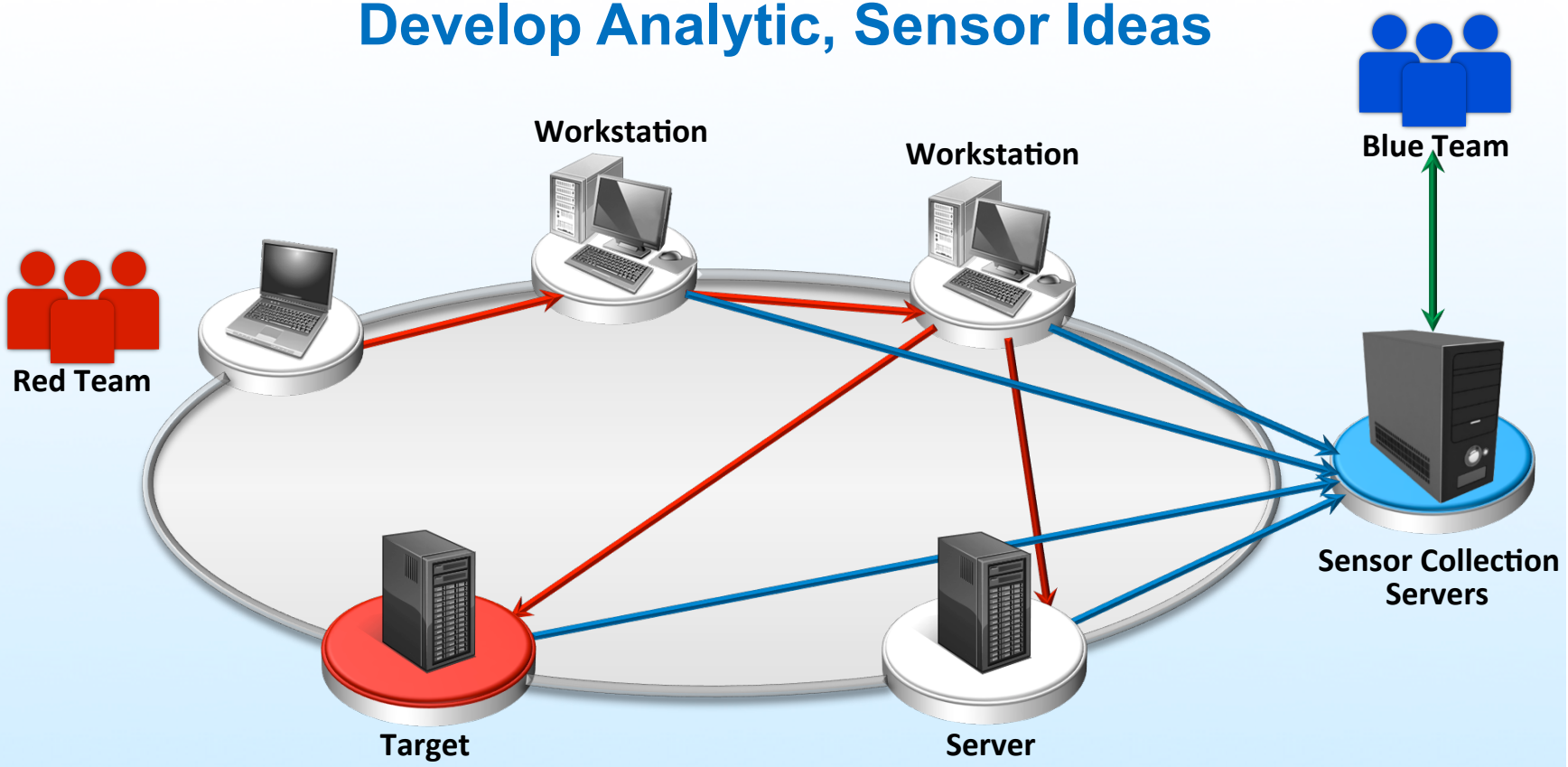


MITRE

Cyber Games – Blue Team

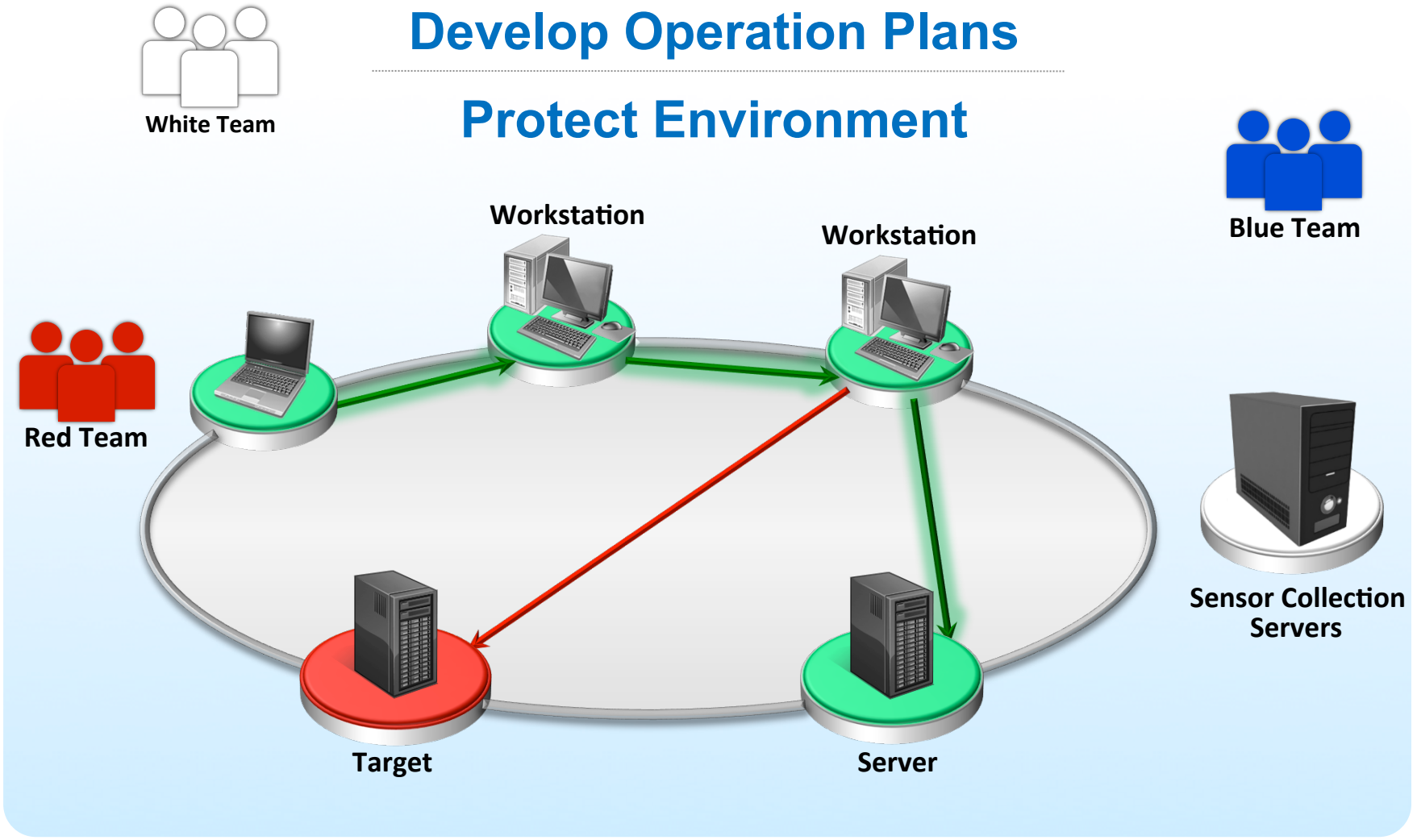
Verify Detection

Develop Analytic, Sensor Ideas



MITRE

Cyber Games – White Team



MITRE