

OS Analysis with RegRipper



Shoaib Arshad

@shoaibDFIR



RegRipper

<http://github.com/keydet89>



RegRipper

<http://github.com/keydet89>

Creator: “Harlan Carvey”



RegRipper is an open-source application for extracting, correlating, and displaying **specific information from Windows Registry hive** files, by running specific plugins against Registry hive files.



RegRipper, written in Perl, is the fastest and easiest tool for **Windows Registry analysis** during forensics examinations.

It can be downloaded at <https://github.com/keydet89>.

RegRipper uses a **plugins based** modular approach that helps capture specific information from the Windows Registry.

RegRipper plugins eliminate the need to memorize registry keys and value paths.



RegRipper is not a Registry viewer



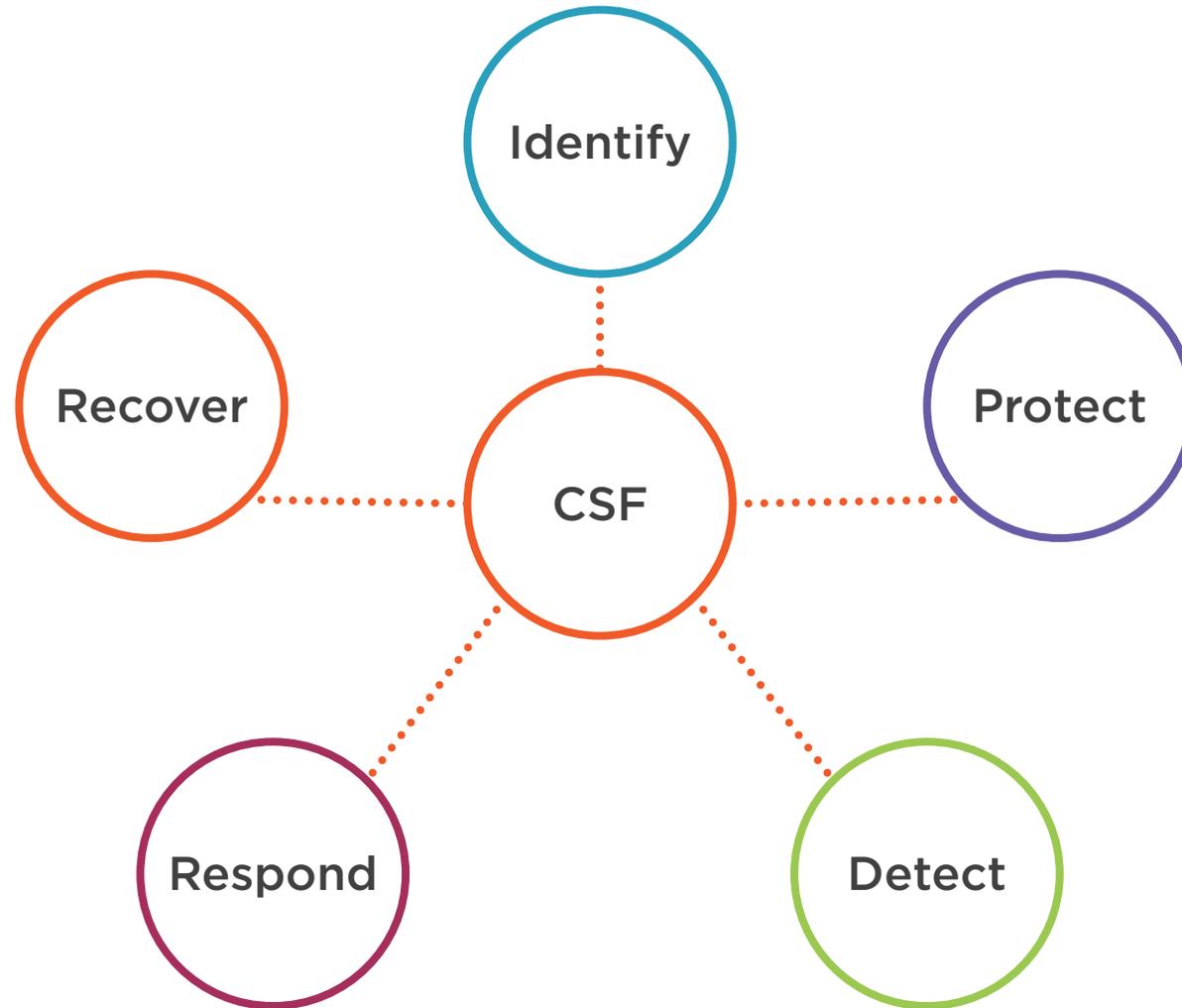


Improve detection and response

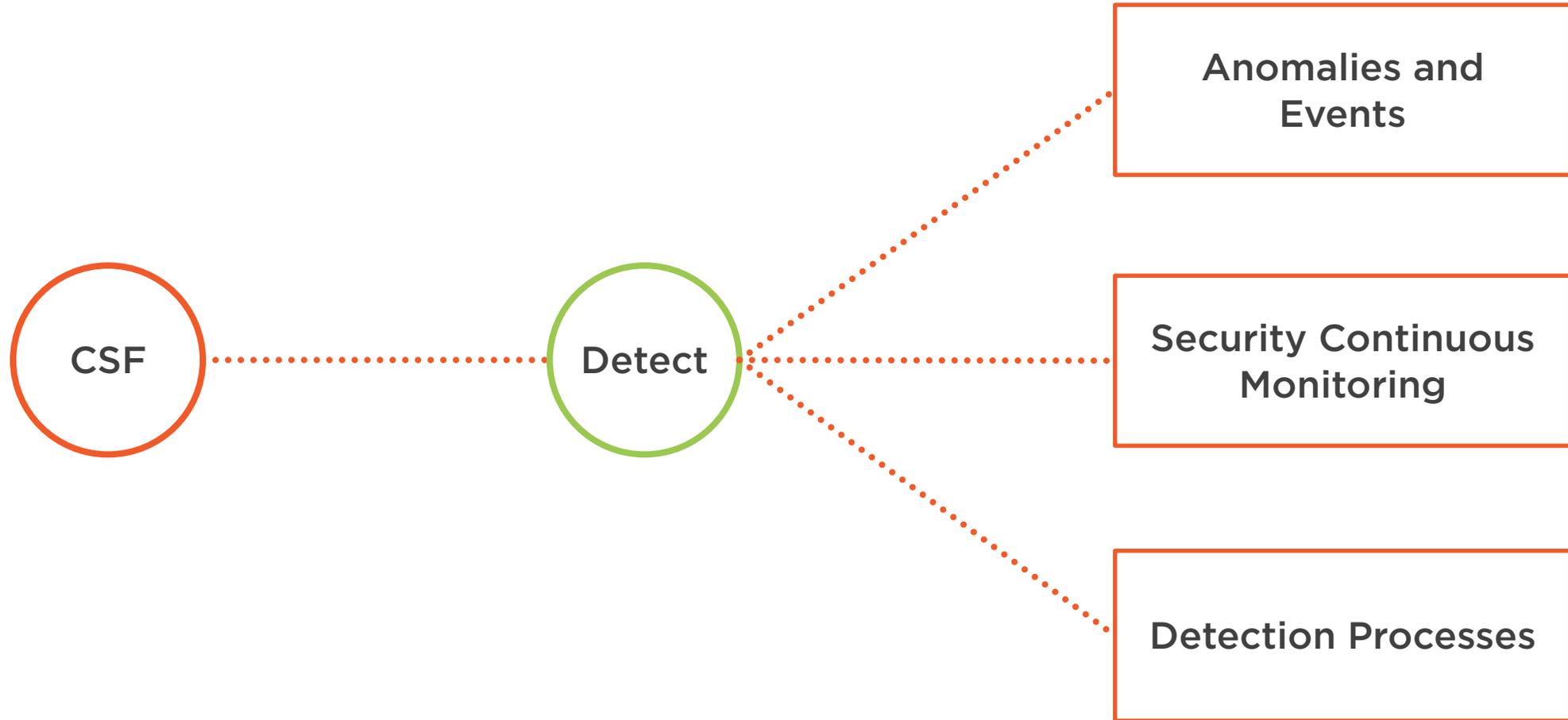
RegRipper gives you an upper hand



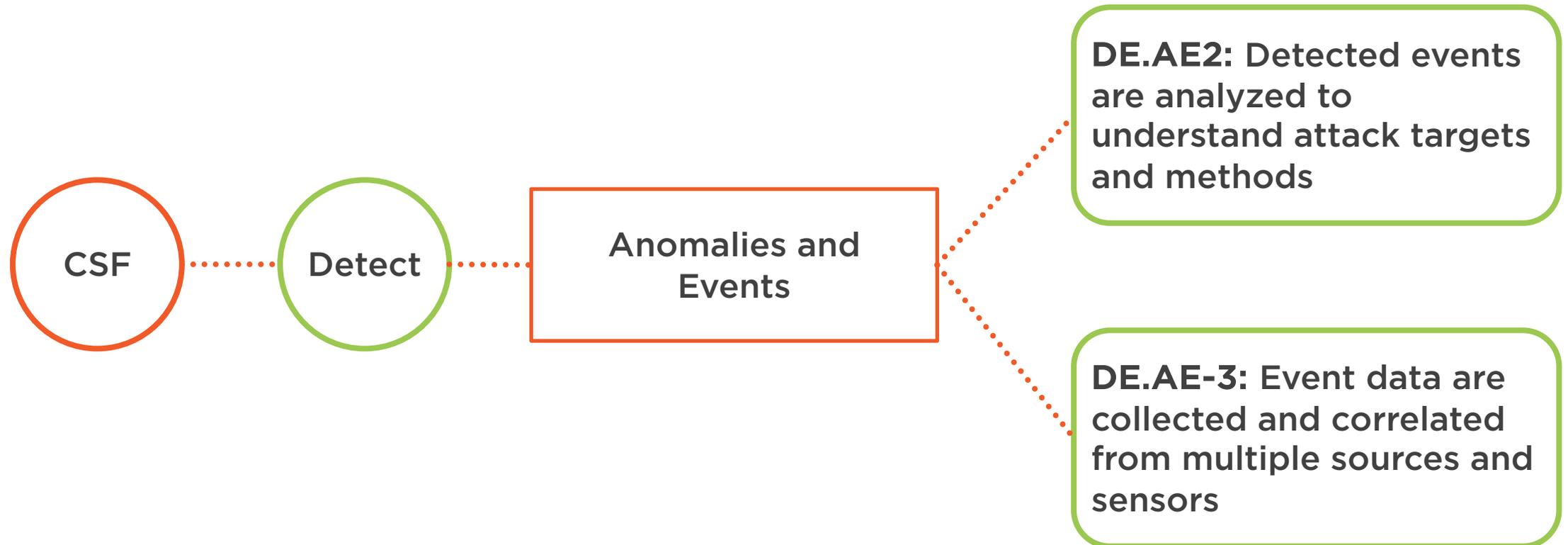
NIST Cybersecurity Framework



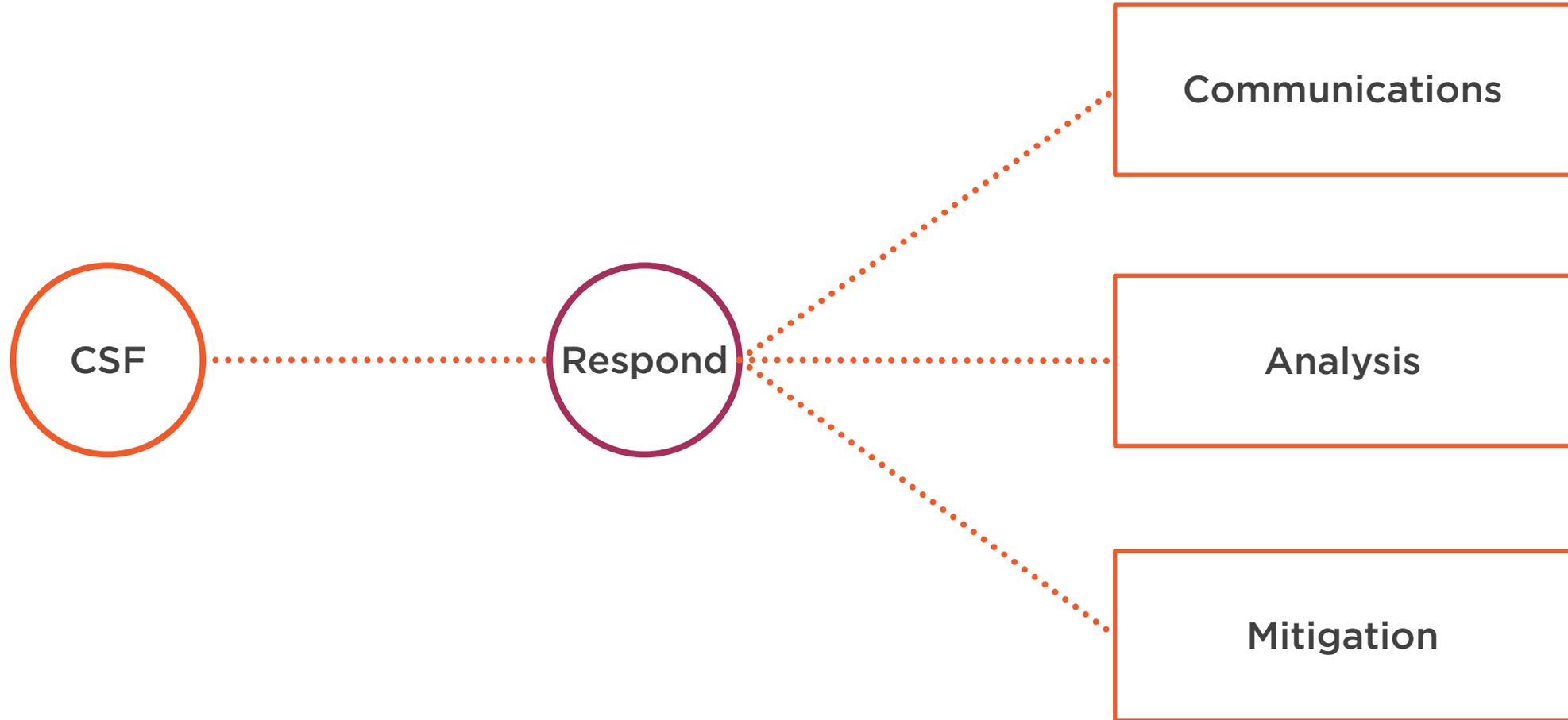
NIST Cybersecurity Framework



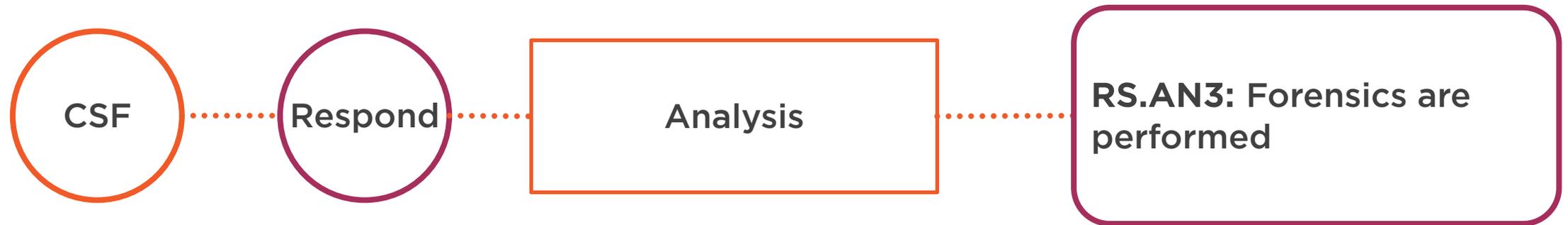
NIST Cybersecurity Framework



NIST Cybersecurity Framework



NIST Cybersecurity Framework



MITRE ATT&CK

Data Analysis Type

Network Analysis

OS Analysis

Application Analysis

Infrastructure Analysis

File Analysis

Threat Intelligence

Incident Management



MITRE ATT&CK

Data Type

Network Analysis

OS Analysis

Application Analysis

Infrastructure Analysis

File Analysis

Threat Intelligence

Incident Management

T1543:

Create or Modify System Process

T1543.003:

Windows Service

T1547:

Boot or Logon Autostart Execution

T1547.001:

Registry Run Keys

T1052:

Exfiltration Over Physical Medium

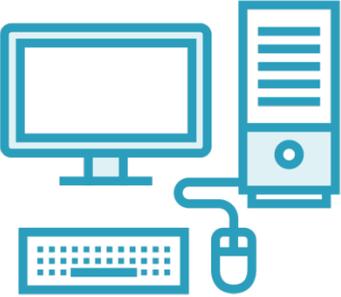
T1052.001:

Exfiltration over USB





FTK Imager

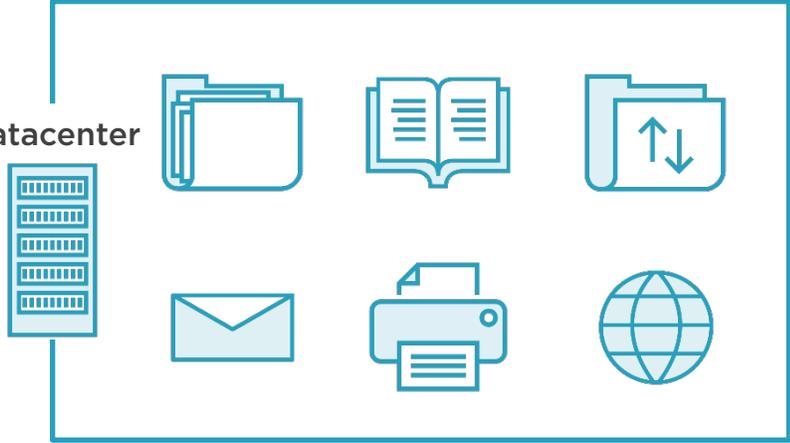


End-User

Acquisition

F-Response
Mount Image Pro

Datacenter



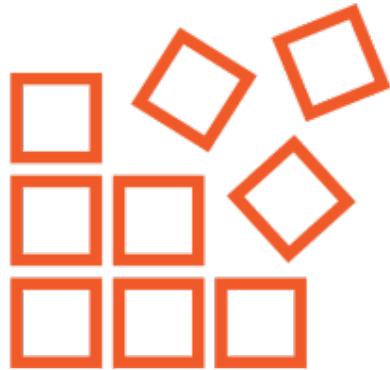
So, you're telling me...



Windows Registry is more than just configuration settings!



Windows Registry



Hierarchical database

OS configuration settings

Software programs

Hardware devices

User preferences

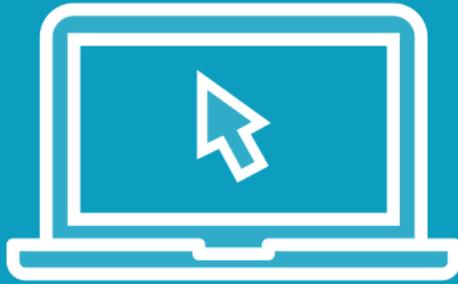
And more...

Hive files

Regedit.exe



Demo



Download RegRipper

RegRipper plugins

Plugin profiles



Case Study



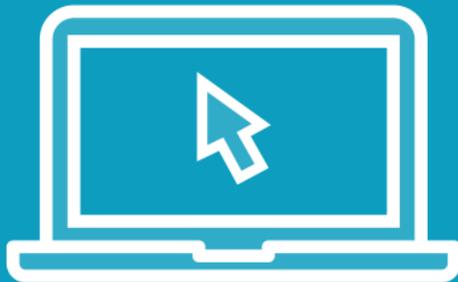
My system is behaving strangely!



Demo Place Holder



Demo

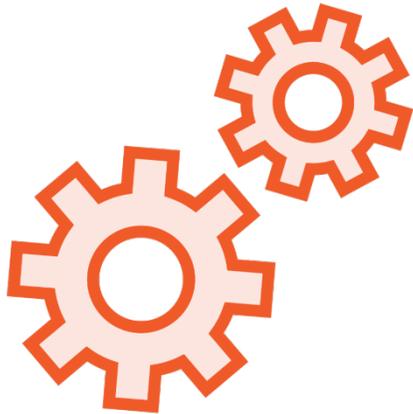


Windows Services

Create or modify Windows Services



Windows Services



Run automatically during boot

No user interaction

Used extensively by malware authors

Maintain persistence

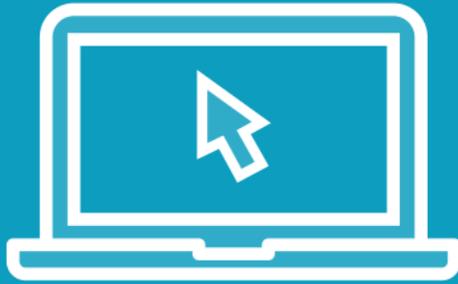
HKLM\SYSTEM\CurrentControlSet\Services



Demo Place Holder



Demo

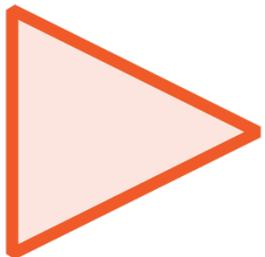


Registry Run Keys

Cause programs to run each time a user logs on



Registry Run Keys



Autostart execution

Program referenced in the “run keys” will be executed when a user logs in

Abuse of system features

Detect changes to “run keys” by any suspicious programs

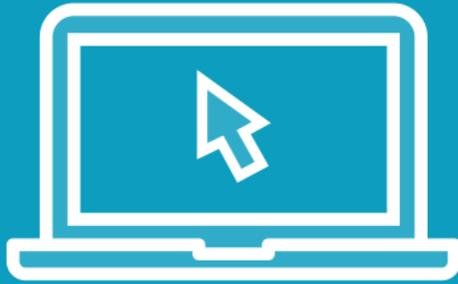
Run plugin from RegRipper



Demo Place Holder



Demo



Exfiltration over physical medium

Analyzing USB devices information



Exfiltration over USB

System Hive

USBSTOR key

System\ControlSet001\Enum\USBSTOR

MountedDevices key

System\MountedDevices

NTUSER.DAT Hive

MS Office RecentDocs key

NTUSER.DAT\Software\Microsoft\Office\\
<program>\FileMRU



Demo Place Holder



More Information

Capabilities

Plugin categories can be created!

Some plugins are mapped to
MITRE ATT&CK

Related Information

Windows Registry is a significant
forensic resource

Tools for Windows Registry forensics

- Registry Explorer
- RegistryChangesView
- YARU

