Tanium Endpoint Detection and Response

(ISC)² East Bay Chapter Training Day
July 13, 2018

$> Whoaml

- **11 Years of Security Experience**
  - Multiple Verticals (Technology, Industrial, Healthcare, Biotech)
- **9 Years in Incident Response / Consulting**
  - Worked for 3 of the largest IR Consulting firms in the US
  - Personally responded to over 150 active incidents in over 10 countries
  - Several high profile / public data breach investigations
  - Primary expertise in Digital Forensics, APT mitigation, Threat Intelligence
- **Education:**
  - BS, University of Central Florida
- **Certifications:**
  - SANS: GCFA, GCIH, GREM
  - CISSP

The Old Way of Performing Incident Response

The Traditional Approach Doesn't Scale

- One of the security tools detects "something"
  - IDS signature, A/V hit, Threat Intelligence alert
- Reactive Approach
- Image the entire disk and/or dump memory
  - This takes a huge amount of time / Huge amount of data to analyze
    - 8-10 hours as most laptops are at least 500GB
    - Add another 12 hours for indexing with popular forensics tools
    - Very effective, but not scalable for large incidents

It’s Time to Re-think the Problem Statement

What Data is essential for Enterprise-scale incident response?

Matt Swann, https://github.com/swannman/ircapabilities

Logistics

- Lab environment URL
- Lab environment credentials
- Handouts
  - Slides
  - Lab supplements

Class outline

- Tanium Platform Overview
- Tanium Threat Response Workflow
- Hands on Labs

Tanium Platform Overview

Reviewing the basics

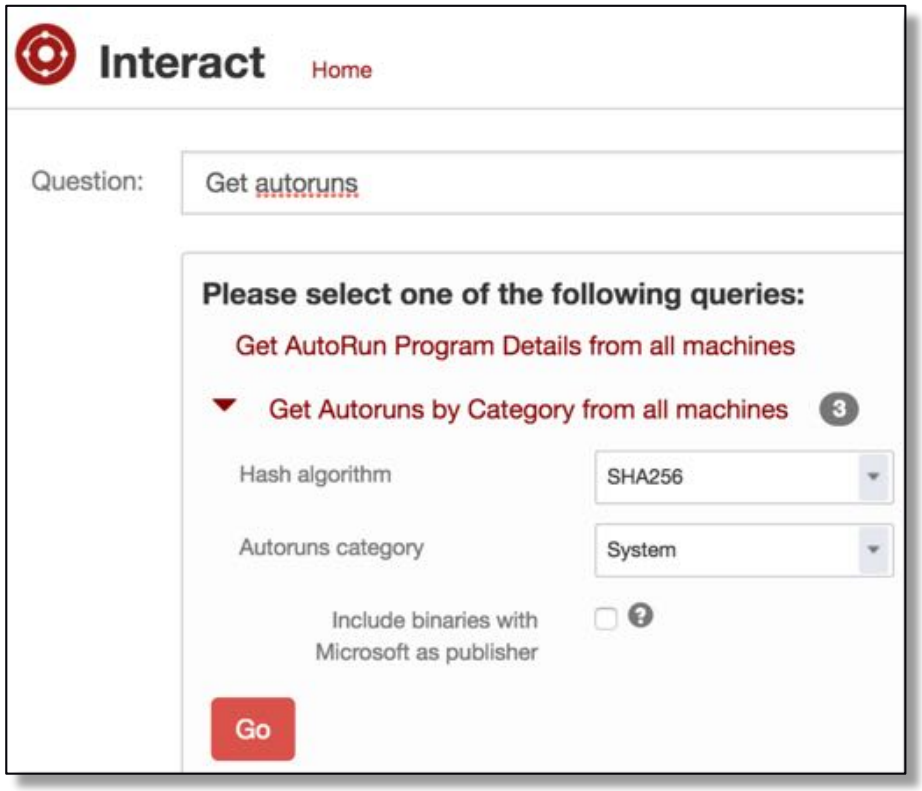
Tanium 101

Reviewing the basics

- Sensors
- Saved questions
- Actions

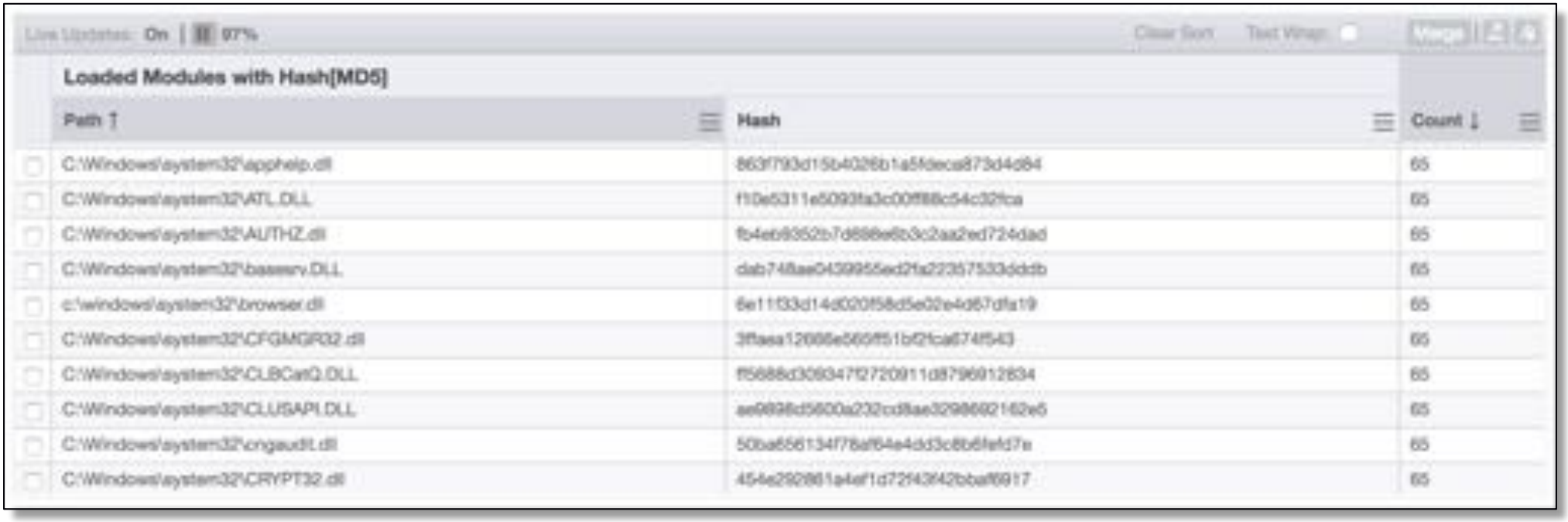
What's a sensor?

- "Ask a question" across all endpoints
- Search or collect data
  - "Live artifacts" native to the system
  - Evidence preserved by Tanium components (Index, Trace)
- Combine and "stack" common results for outlier analysis



Sensors can collect broad, unfiltered data…

List all loaded DLLs and their paths and hashes



Live Updates: On | 97% Clear Sort Text Wrap

Loaded Modules with Hash[MD5]

Path	Hash	Count
C:\Windows\system32\apphelp.dll	863f793d15b4026b1a5fdeca873d4d84	65
C:\Windows\system32\ATL.DLL	f10e5311e5093fa3c00ff88c54c32fca	65
C:\Windows\system32\AUTHZ.dll	fb4eb8352b7d886e6b3c2aa2ed724dad	65
C:\Windows\system32\baseisrv.DLL	dab748ae0439955ed2fa2235753dddb	65
c:\windows\system32\browser.dll	6e11f33d14d020f58d5e32e4d67dfa19	65
C:\Windows\system32\CFGMGR32.dll	3ffaaa12666e565ff51bf2fca874f543	65
C:\Windows\system32\CLBCatQ.DLL	ff5688d3080477f272091 1d8796912834	65
C:\Windows\system32\CLUSAPI.DLL	ae6896d5600a232cd8ae3298692162e6	65
C:\Windows\system32\cngaudit.dll	50ba656134f78af64e4dd3c8b6fefd7e	65
C:\Windows\system32\CRYPT32.dll	454e292861a4ef1d72143f42bbaf6917	65

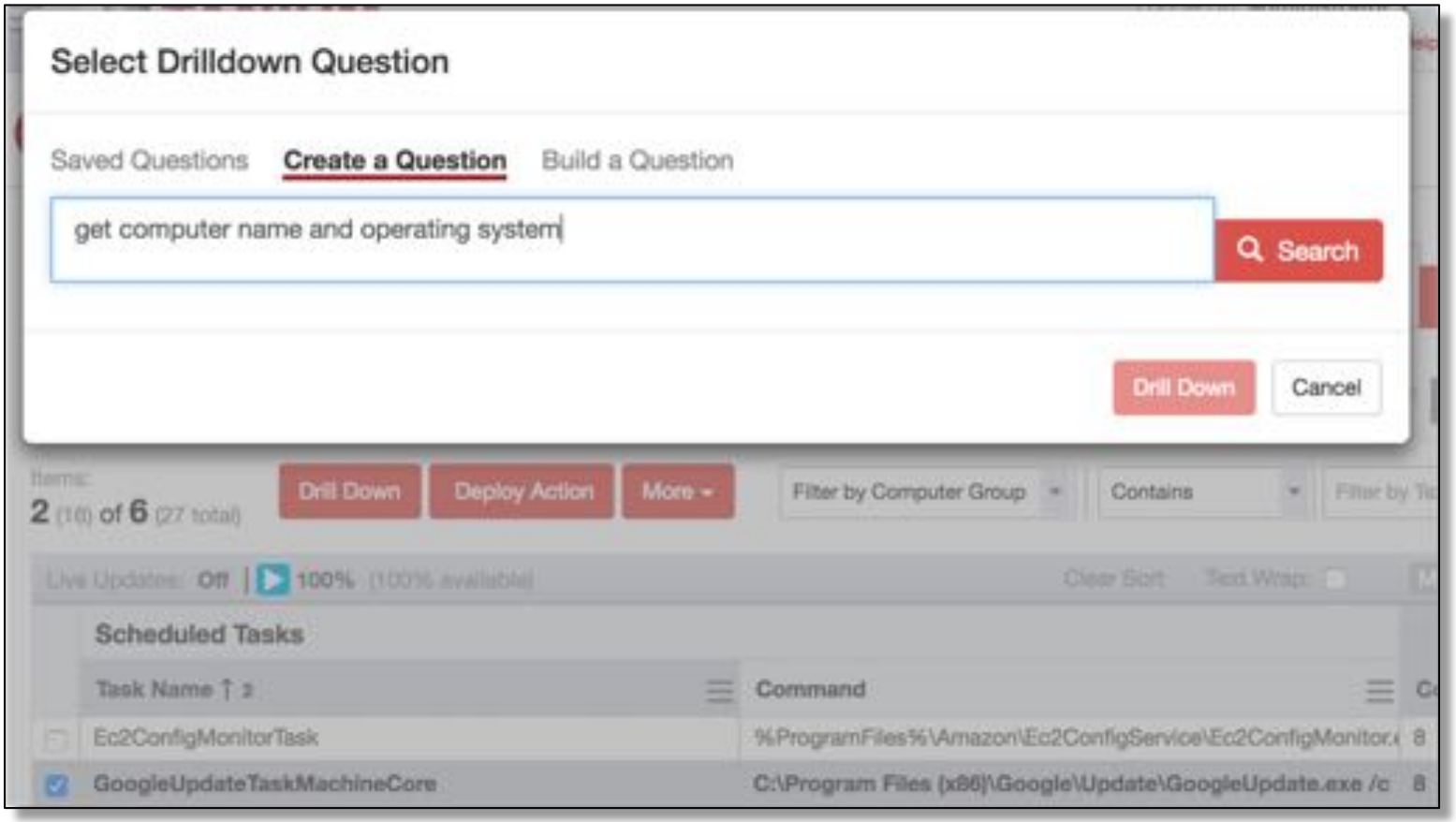
Or they can take parameters to find specific items…

Find any file on disk starting with the name “java”

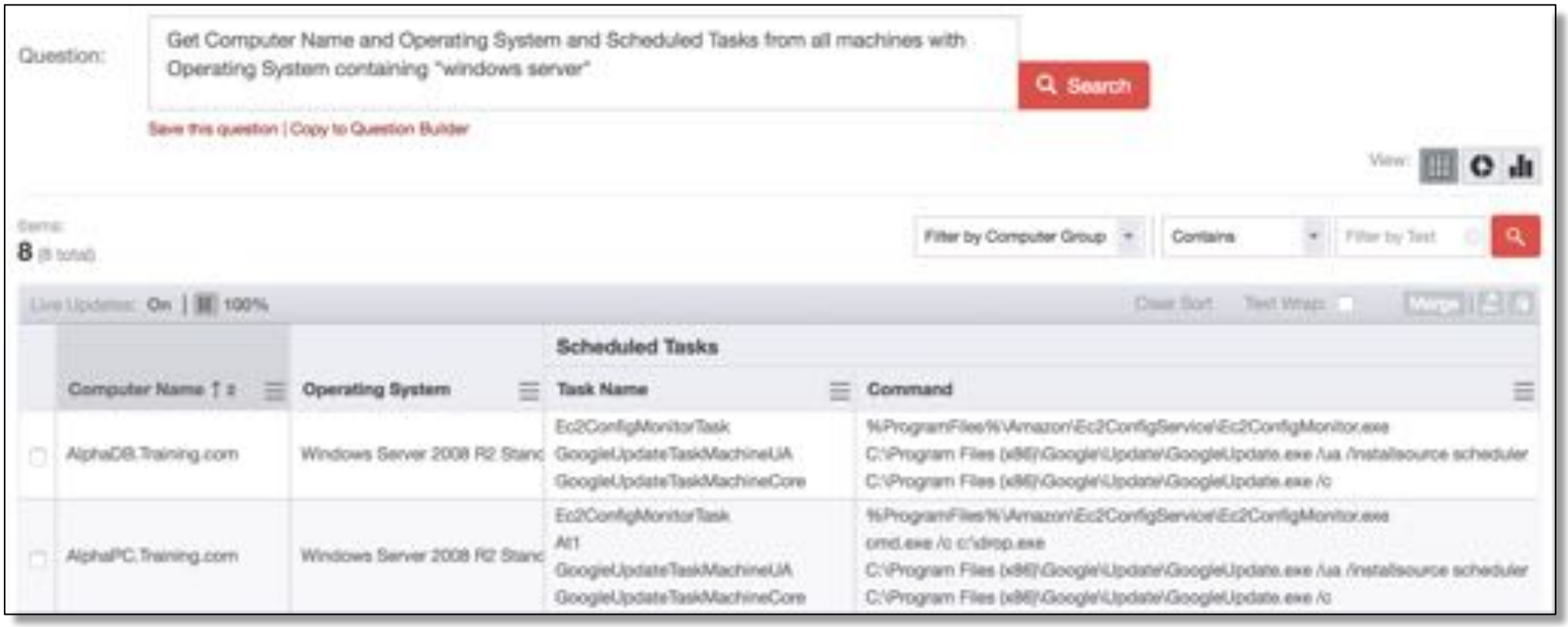
Index Query File Details Using Name[java*]

File Path	File Size (Bytes)	Creation Date	Last Modification	File MD5 Hash	File Magic
C:\Program Files (x86)\Java\jre7\bin\javaw.exe	175528	2015-09-29 19:04:22	2015-09-29 19:04:22	431b3f716a156dd628	4D5A9000
C:\Program Files (x86)\Java\jre7\bin\javaws.exe	272808	2015-09-29 19:04:22	2015-09-29 19:04:22	a1f71601e9578a7b49	4D5A9000
C:\Program Files (x86)\Java\jre7\bin\java_crw_demo.dll	23976	2015-09-29 19:04:22	2015-09-29 19:04:22	0ce8105fb7cf990667	4D5A9000
C:\Program Files (x86)\Java\jre7\lib\javafx.properties	29	2015-09-29 19:04:22	2015-09-29 19:04:22	670fd7ff0f62ac0239e	6A617661

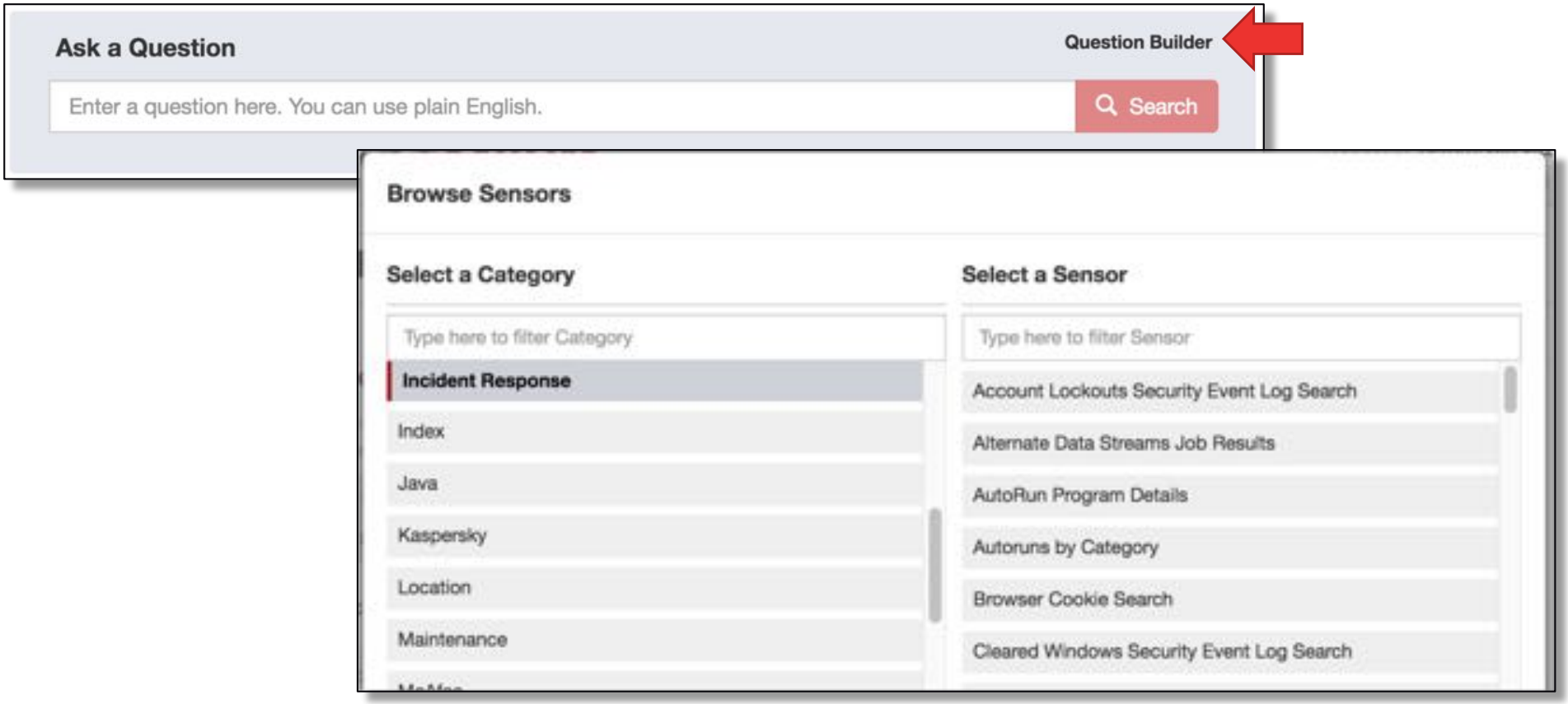
You can “drill down” on results to ask follow-up questions



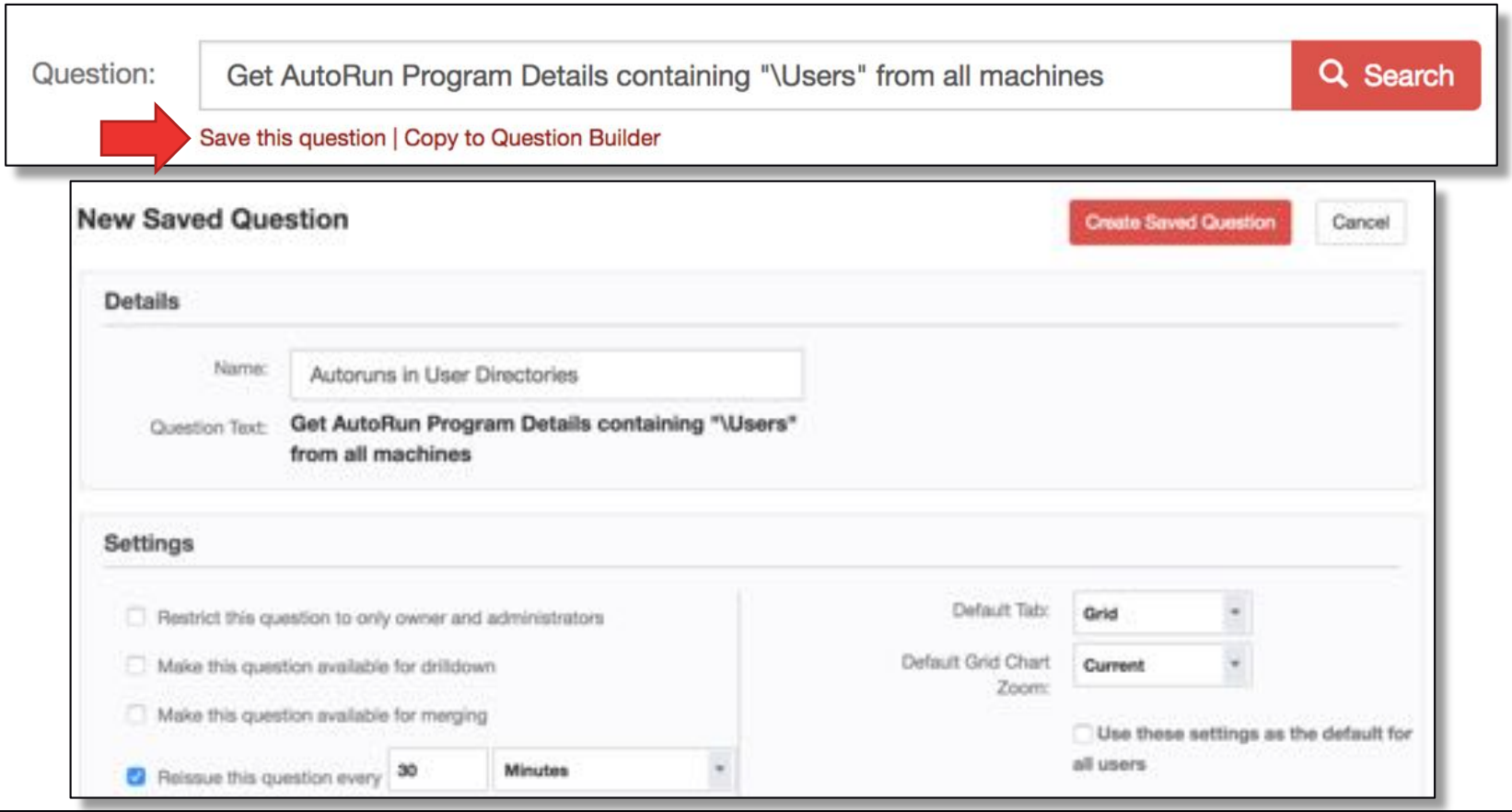
“Compound” questions combine output from multiple sensors



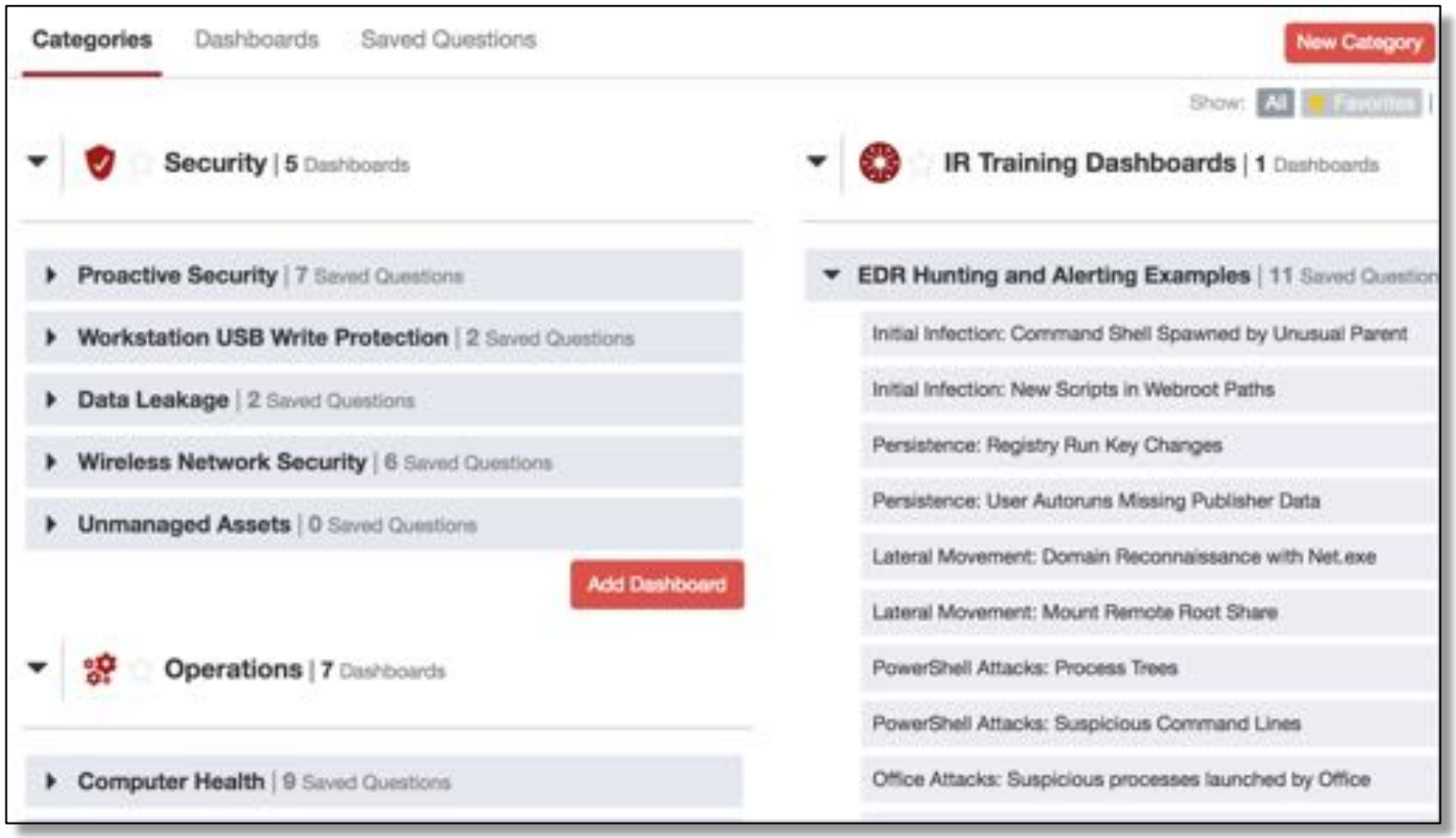
Tanium provides several tools to help you discover sensors



“Saved Questions” collect data over time

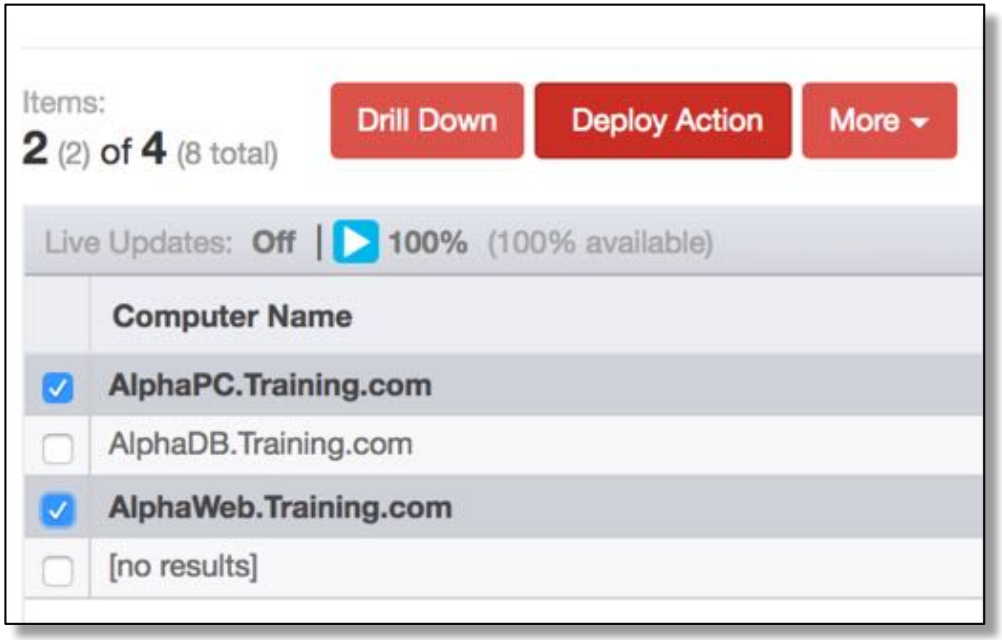


Dashboards group together saved questions



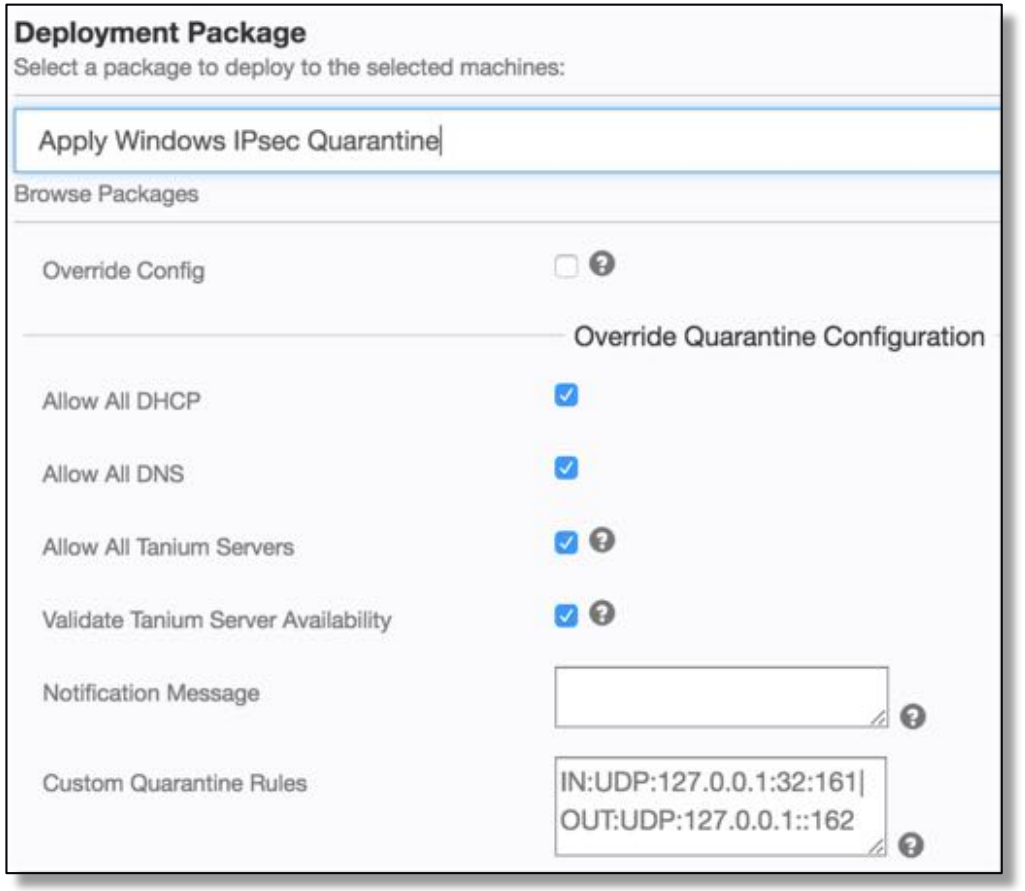
What's an action?

- Change the state of a system
- Distribute a package of files and run a command
- Can target system(s) from any set of question results
- Can run once, or recur over time



Common actions for Threat Response workflows

- Quarantine host (isolate on the network)
- Launch IR Gatherer
- Kill process
- Edit registry
- Edit hosts file
- Patch system



Training Lab: Practicing Basic Questions

Use "Ask a Question" in Interact to discover sensors and complete this lab

Practicing basic sensor questions

1. What operating systems are present in the demo environment?
2. What is the IP address of hostname "AlphaPC"?
3. Do any systems have Google Chrome as an installed application? What version?
4. Who is the last logged in user on client-1?
5. How many systems are listening for connections on port 3389? What are their hostnames?

Threat Response Workflow

Tanium Threat Response overview

Monitor and Alert

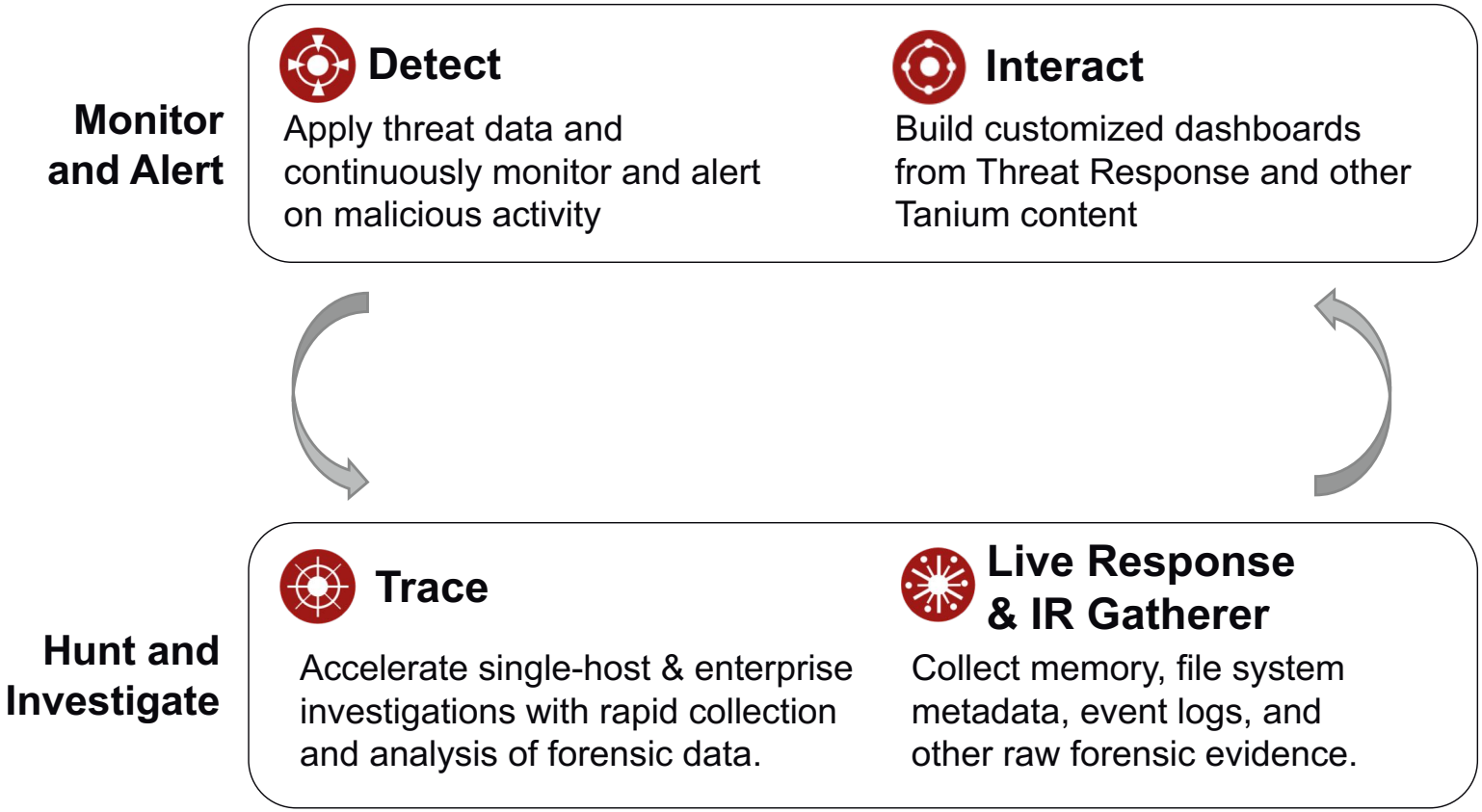
Detect

Apply threat data and continuously monitor and alert on malicious activity

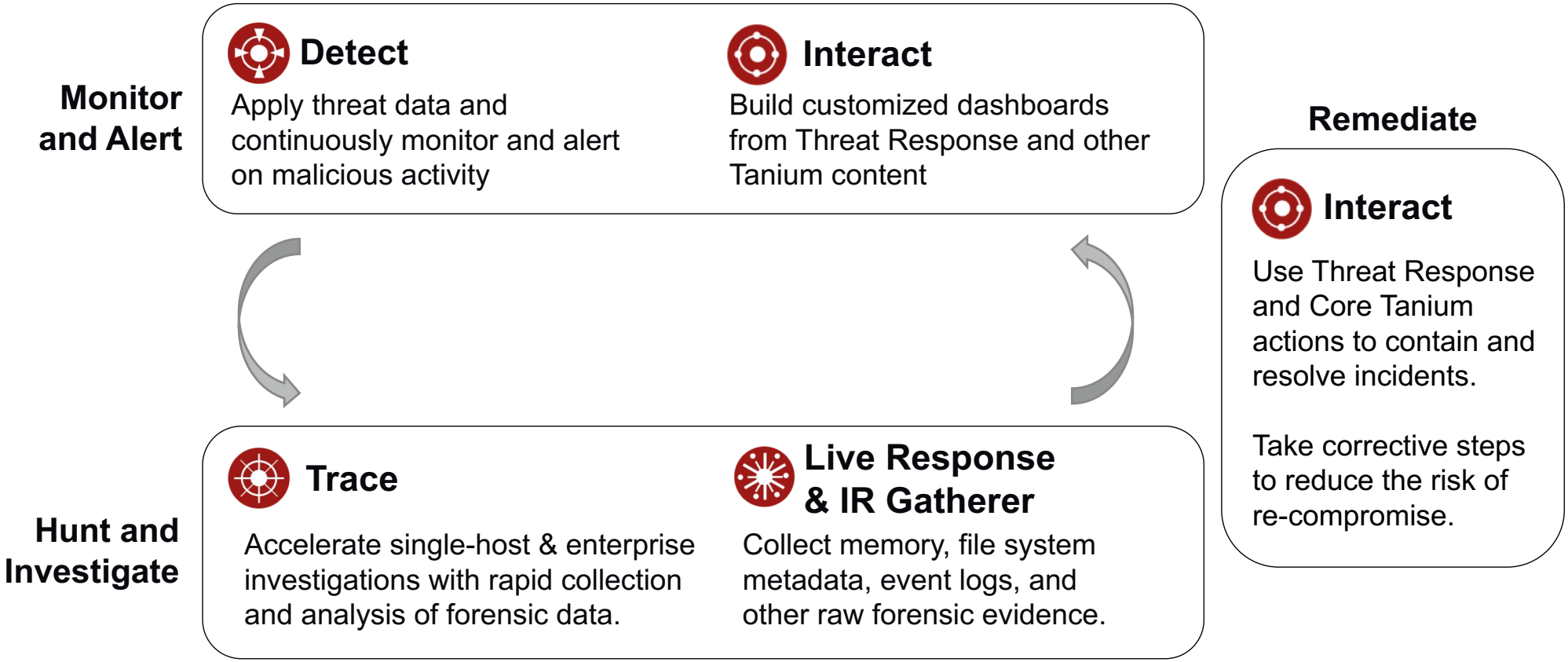
Interact

Build customized dashboards from Threat Response and other Tanium content

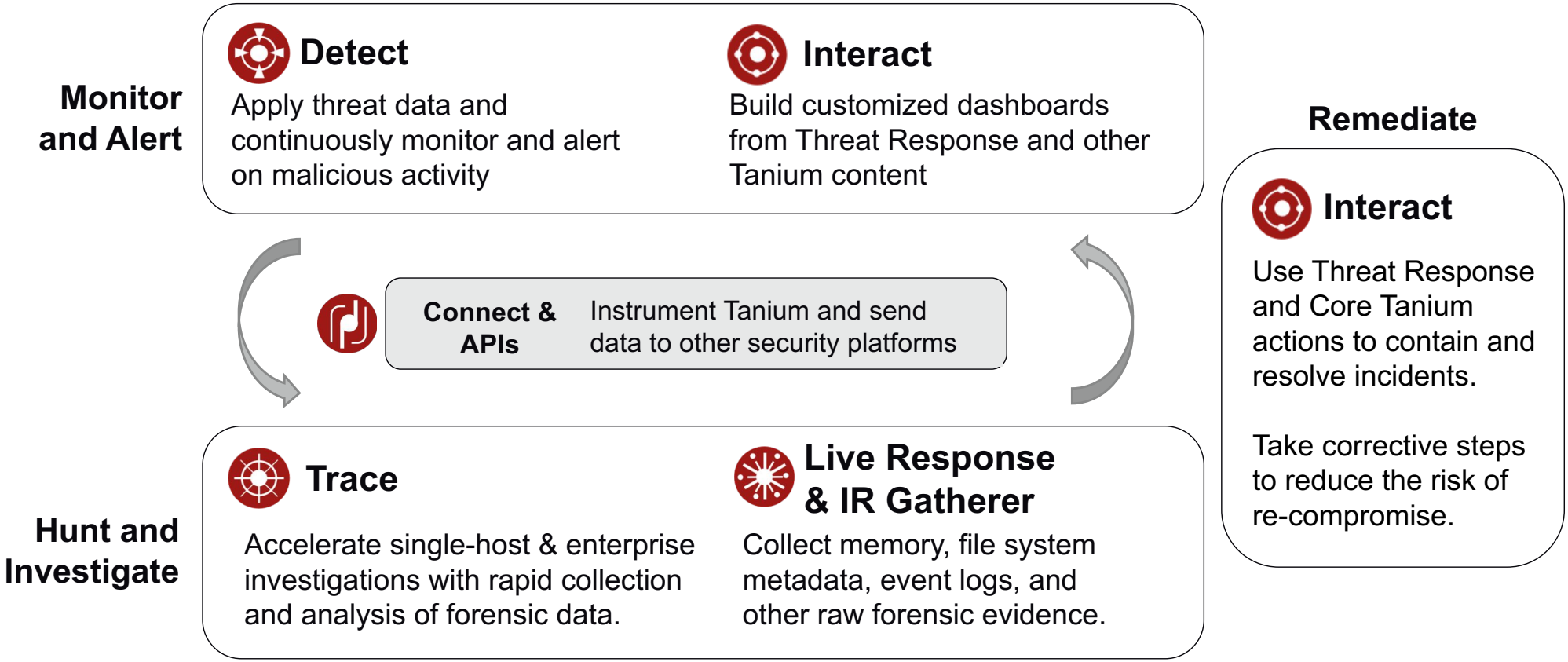
Tanium Threat Response overview



Tanium Threat Response overview



Tanium Threat Response overview



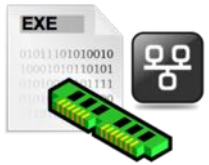
Tanium Threat Response

Sources of evidence

Incident Response

Index

Trace Recorder

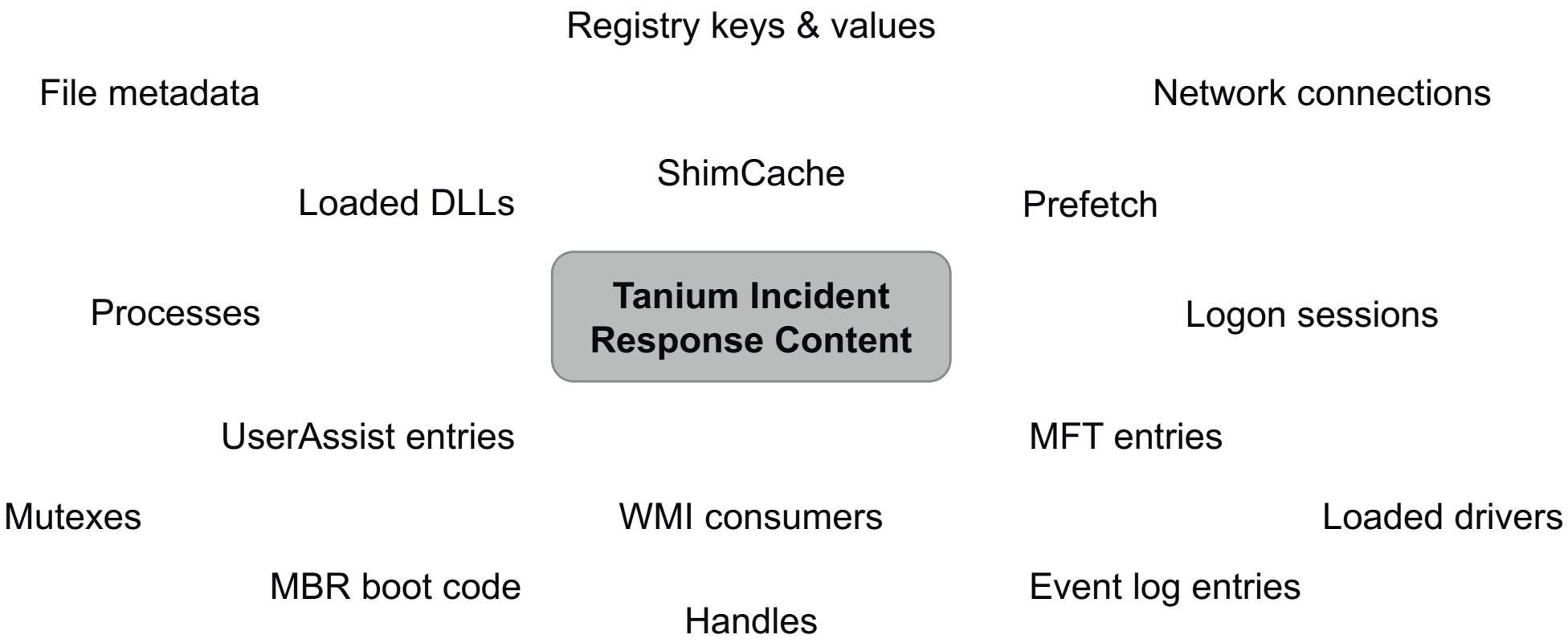


Current State
Active processes, network connections, loaded files, in-memory artifacts

Data at Rest
Files on disk, registry entries, logs, caches and other OS artifacts

Historical Data
Telemetry of process, network, file, registry, security, and driver events

Incident Response content searches **native sources of evidence**



Index provides **full-disk** search for file metadata

File hashes

```
MD5: fc5e038d38a57032085441e7fe7010b0
SHA1: 6adfb183a4a2c94a2f92dab5ade762a47889a5a1
SHA256: 936a185caaa266bb9cbe981e9e05cb78cd732b0b3...
```

File name and path

```
C:\temp\salary.xlsx
```

Tanium Index

File magic number

```
4D 5A 00 02
```

File timestamps

```
Created: 2015-05-09 10:09:43
Modified: 2015-05-09 10:20:01
```

Trace continuously records **historical data**

Filesystem events
- User & process context
- Type of event (Create, Delete, Rename, Write)

Process execution
- User context
- Command line & parent
- Hash
- Time created & terminated

Driver loads
- User & process context
- Path
- Hash
- Digital signature

Registry events
- User & process context
- Type of event (key created, key deleted, value set, value deleted)

Tanium Trace Recorder

Network connections
- Type of connection
- Remote & local port and IP
- DNS query and response
- User & process context

Security events
- Based on OS audit policy
- Logon / logoff, policy change, account and group changes, etc.

Detection and alerting

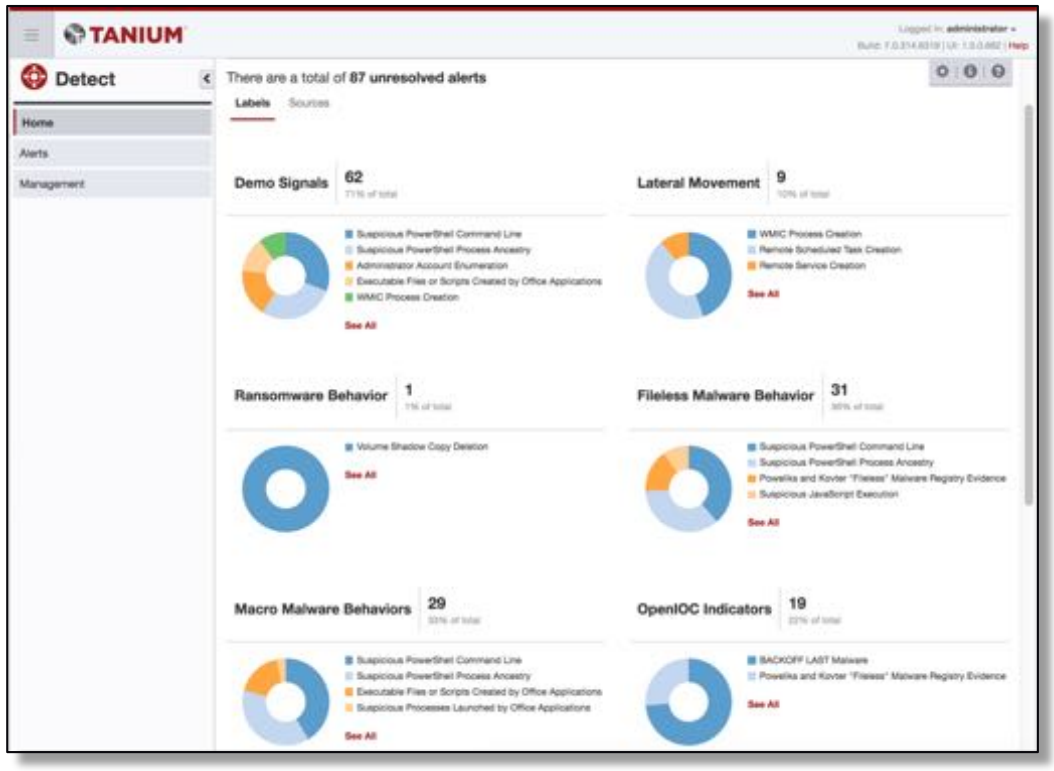
Introducing Tanium Detect 3.0

Detection methods

Signals

Indicators and Rules

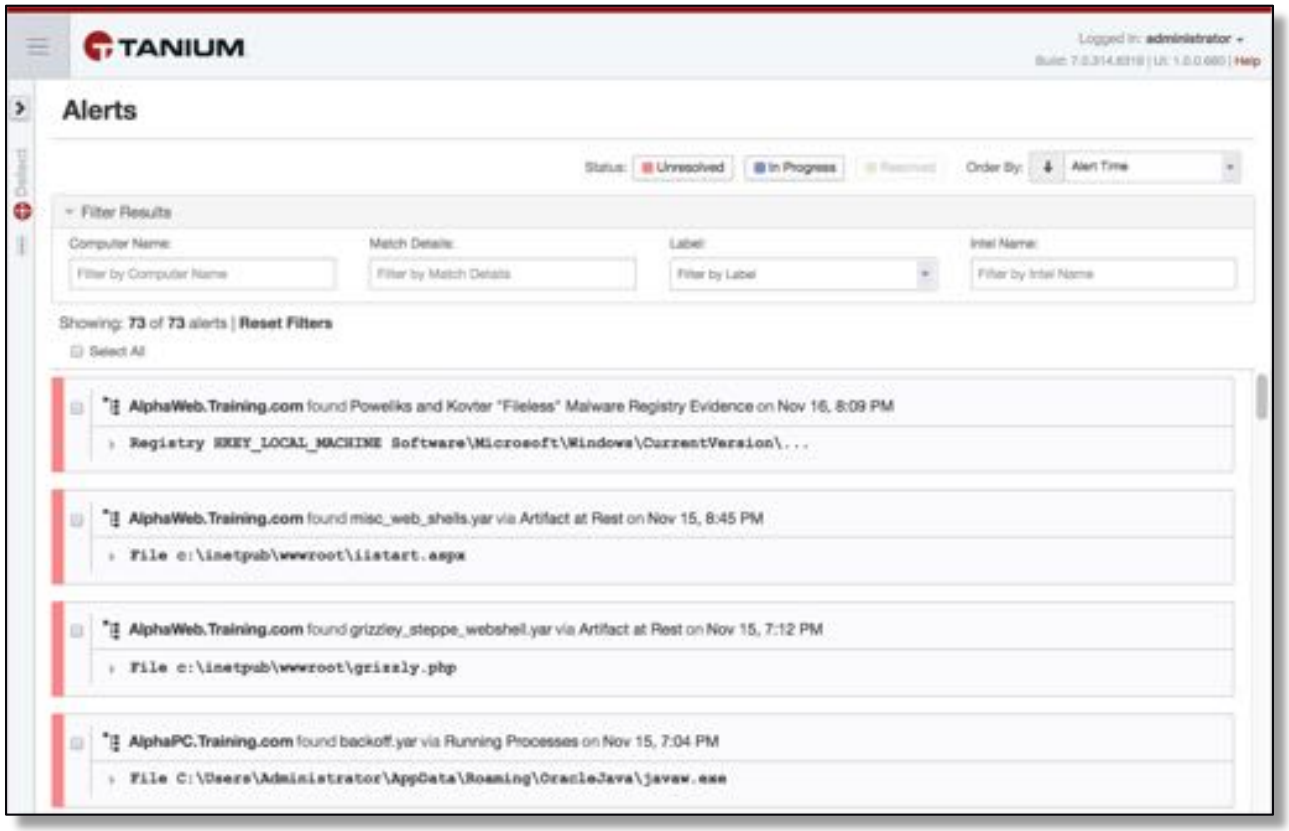
Reputation



Basic navigation

Detect homepage and alerts

- **Filter by**
  - Computer Name
  - Match Details (artifact in an alert)
  - Label
  - Intel Name
- **Status**
  - Unresolved
  - In Progress
  - Resolved



Signals

Signals

- Continuously monitor endpoint activity using Trace
- Detect any combination of **file**, **process**, **network**, or **registry** events
- Issue alerts to the Tanium console within seconds of a signal “match”

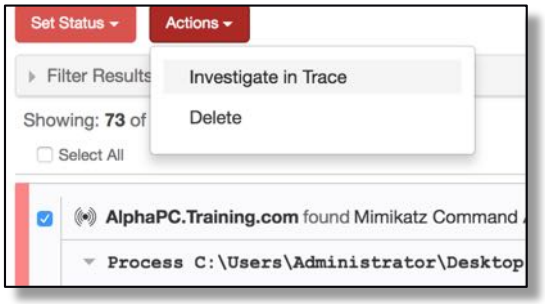
```
process.path ends with 'certutil.exe'
AND (process.command_line contains '-
decode' OR process.command_line
contains '-urlcache')
```

```
file.operation is create AND
(file.path ends with '.vbs' OR
file.path ends with '.ps1') and
process.path contains 'winword.exe'
```

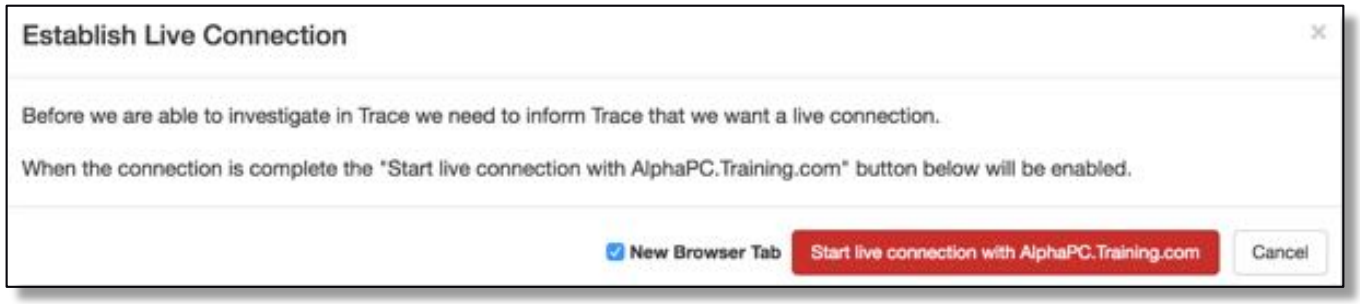
What's in a signal alert?

Investigating a signal alert in Trace

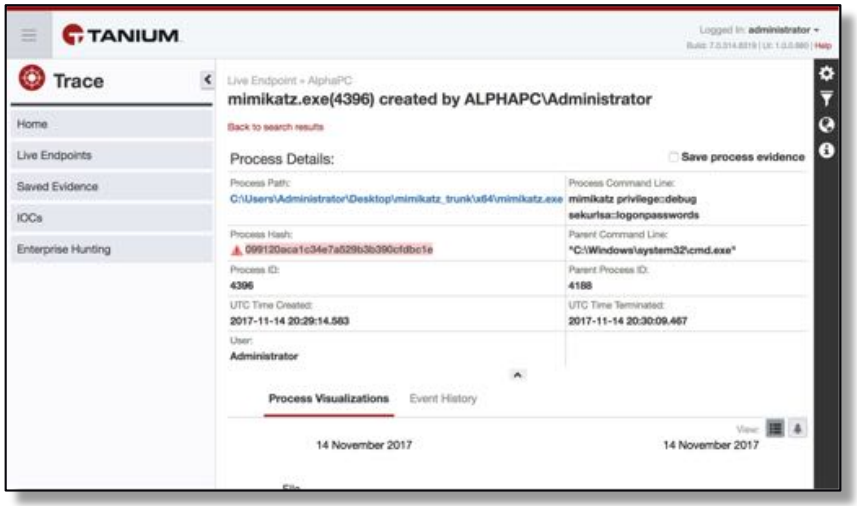
1



2



3



Signal alerts are linked to the corresponding process instance in Trace, allowing you to easily pivot into the complete forensic history around an event.

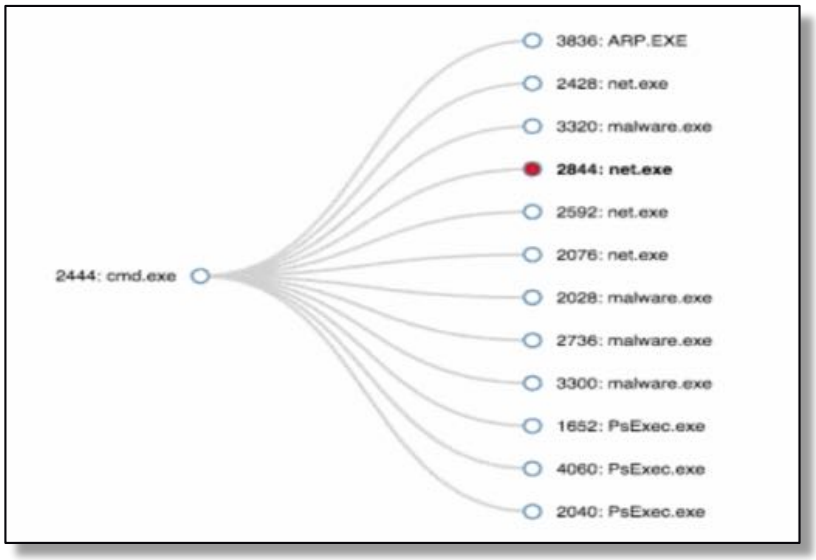
Investigating with Trace

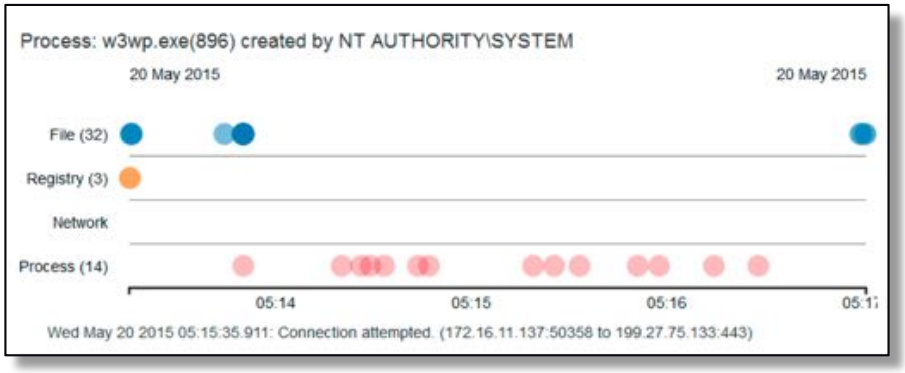
Overview

Tanium Trace

Key Components

- **Recorder**: Continuously preserve endpoint activity via kernel-level monitoring
- **Sensors**: Search Trace data across all systems via “Ask a question”
- **Workbench**: Web UI for investigation tasks (single-host and enterprise)





What does Trace record?

Windows and Linux

- **Process execution**
  - User context
  - Command line
  - Parent command line
  - Hash
  - Time created & terminated
- **File system**
  - User & process context
  - Type of event (Create, Delete, Rename, Write)
- **Registry (Windows-only)**
  - User & process context
  - Type of event (key created, key deleted, value set, value deleted)
- **Network Connection**
  - Type of connection event
  - Remote & local port and IP
  - User & process context
- **DNS (Server 2012R2 / Win8.1 & later)**
  - Queried domain
  - Response IP
  - Initiating process
- **Security**
  - Based on current audit policy
  - Can include: logon, logoff, lockout, auth. policy change, account and group changes
- **Driver load**
  - User & process context
  - Path
  - Hash
  - Digital signature

Single-host analysis workflow

- Live system
- Saved snapshot

- Automatic drill-down from Detect
- Browse timeline
- Filter by time & date
- Filter by event data

- Use timeline & tree visualizations
- Transfer files
- Save evidence

- Search the enterprise
- Generate IOCs for Detect
- Generate policies for Protect

Lab: Investigating an Office Macro Attack

Open the Trace snapshot for **client-1**:
Trace → Saved Evidence → Snapshots

Do not use a live connection for this lab.

Search for process **Z4U8K1S8.EXE** – drill down and pivot from there to answer the following questions

1. What processes did EXCEL.EXE launch (aside from **Z4U8K1S8.EXE)**?

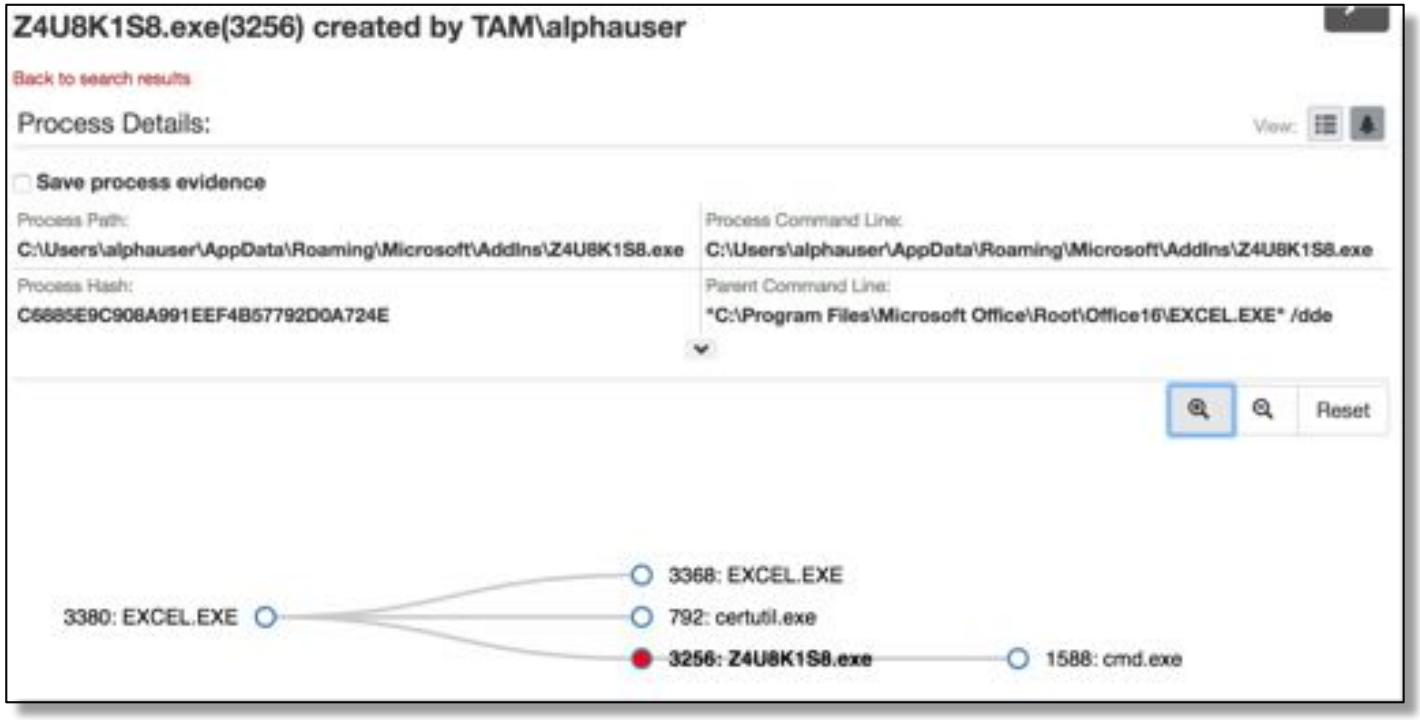
2. What was the purpose of the “certutil.exe” command? What did it do?

3. After initiating a command shell, what commands did the attacker execute?

4. What was the file name of the original malicious Excel document that led to the infection?

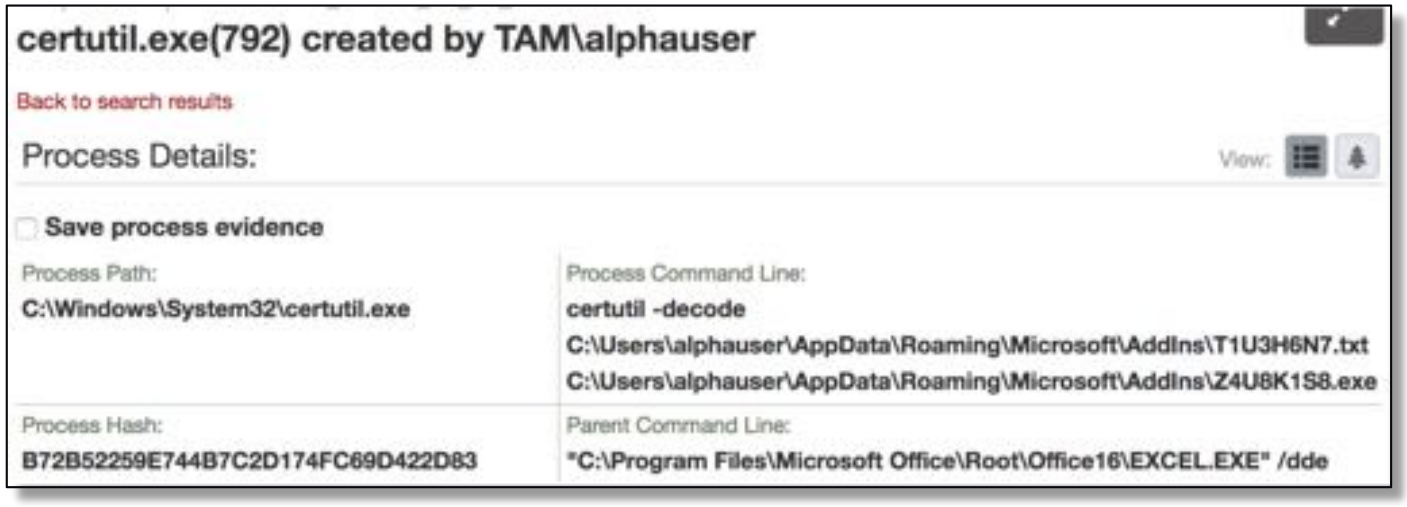
Answers

What processes did EXCEL.EXE launch (aside from Z4U8K1S8.EXE)?



Answers

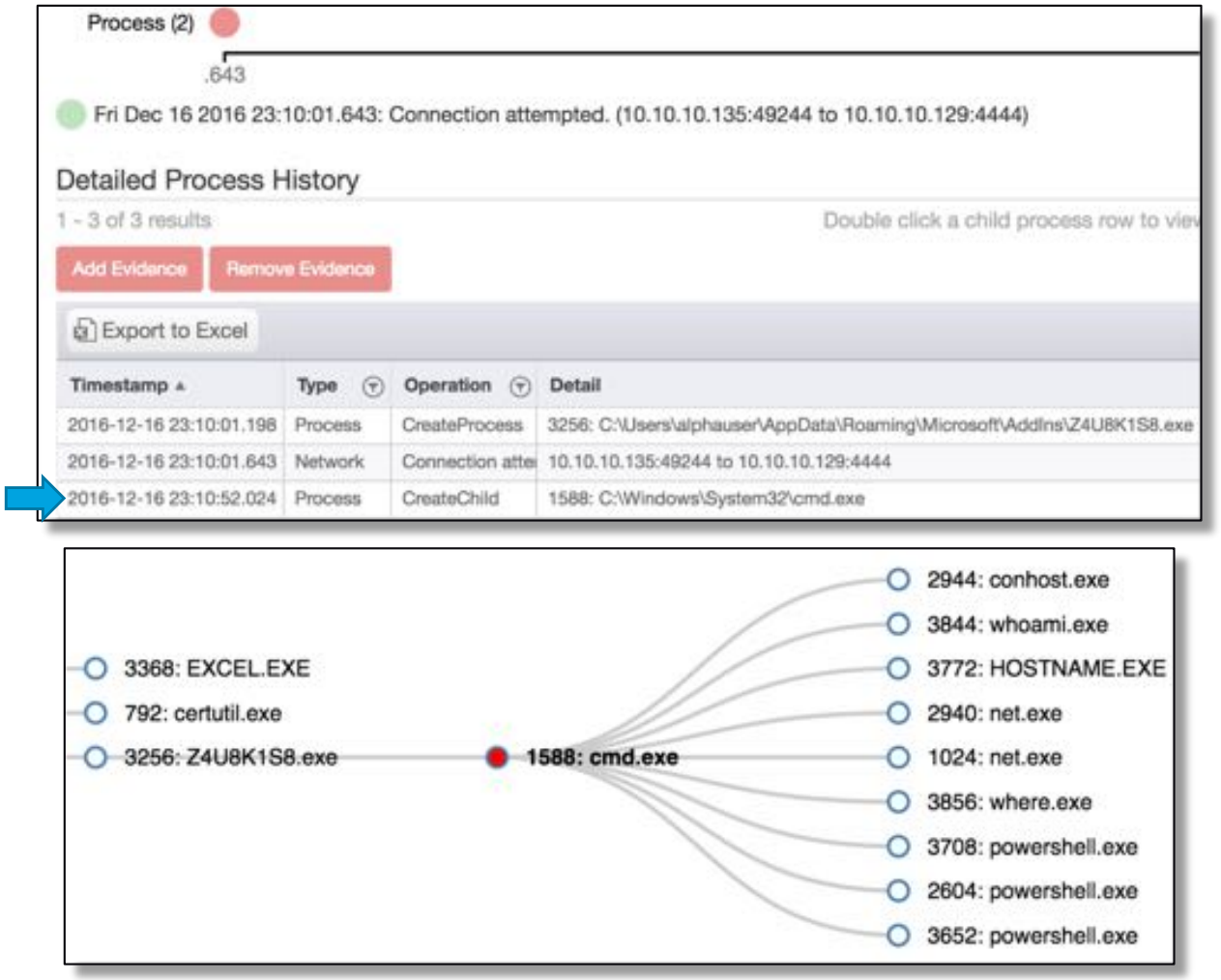
What was the purpose of the “certutil.exe” command? What did it do?



The macro launched "certutil.exe" to extract the malware payload, "Z4U8K1S8.EXE", from temporary file "T1U3H6N7.TXT"

Answers

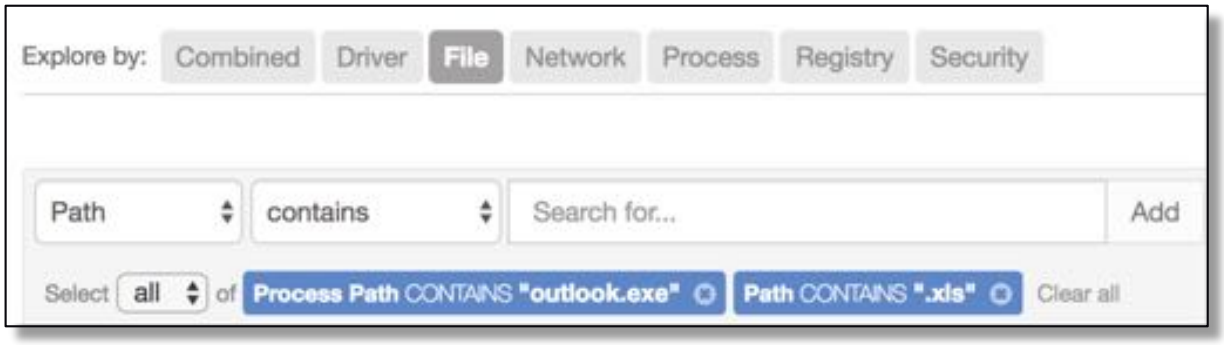
After Z4U8K1S8.EXE initiated a command shell, what commands did the attacker execute?



Answers

What was the file name of the original malicious Excel document that led to the infection?

Search File events for ".xls" files created by “outlook.exe” (in Excel ancestry)



Process Path	Operation	User	Path
C:\Program Files\Microsoft Office\	Write	alphauser	C:\Users\alphauser\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup (002).xls:Zone.Identifier
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup (002).xls:Zone.Identifier
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup (002).xls
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup (002).xls
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup.xls:Zone.Identifier
C:\Program Files\Microsoft Office\	Write	alphauser	C:\Users\alphauser\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup.xls
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup.xls
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup.xls

Next steps…

What didn’t we cover today?