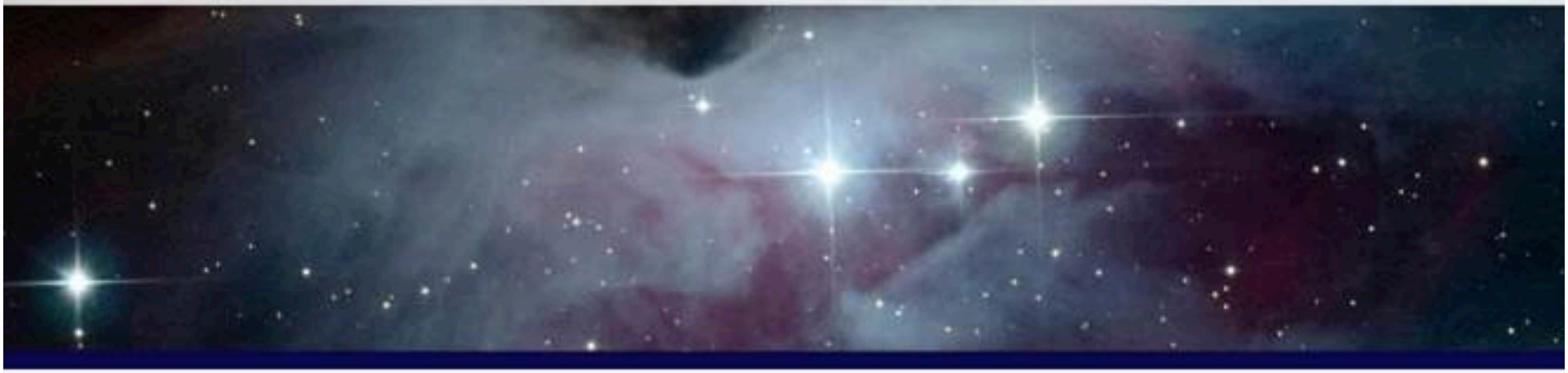


Proactive Defense with Automated First Responder (AFR)

Anuj Soni

Jason Losco

July 18, 2013

Booz | Allen | Hamilton

Combating increasingly sophisticated attackers requires a proactive cyber program incorporating diverse solution sets

How serious is the problem?

Is my sector/industry being targeted, and if so why and how?

How does my posture compare to that of my industry peers?

Are my existing detection and response capabilities sufficient?

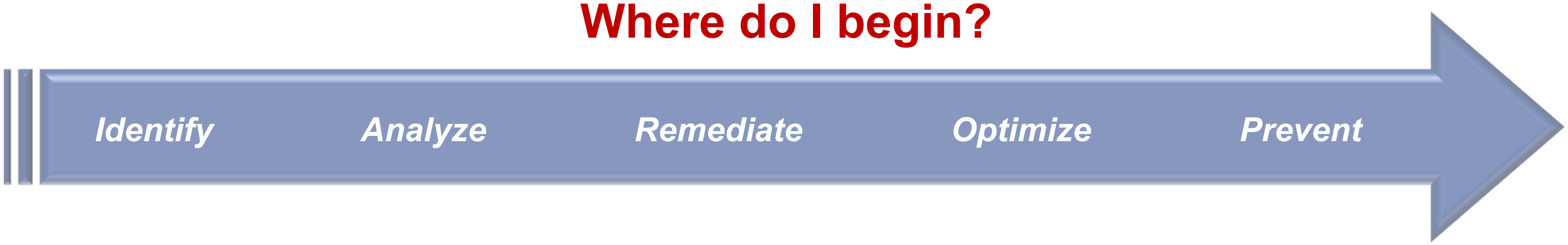
Are my networks and systems current compromised or under attack?

How can we optimize our existing people, processes, and technologies?

How do we attract, retain, and develop staff with the right skills?

What tactical and strategic responses can I implement?

Where do I begin?



Identify

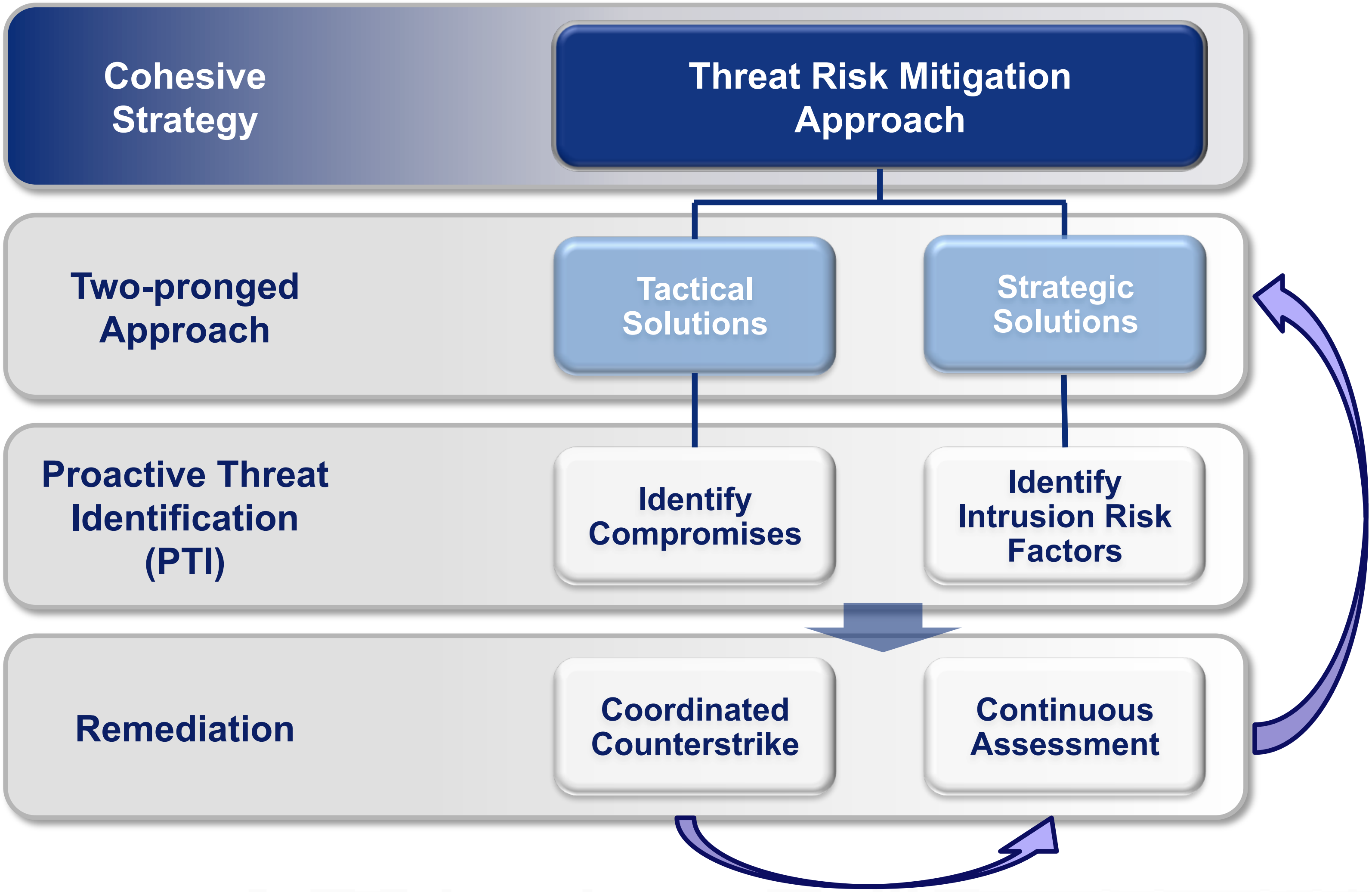
Analyze

Remediate

Optimize

Prevent

Comprehensive risk mitigation requires a cohesive strategy integrating both tactical and strategic solutions



Cohesive Strategy

Threat Risk Mitigation Approach

Two-pronged Approach

Tactical Solutions

Strategic Solutions

Proactive Threat Identification (PTI)

Identify Compromises

Identify Intrusion Risk Factors

Remediation

Coordinated Counterstrike

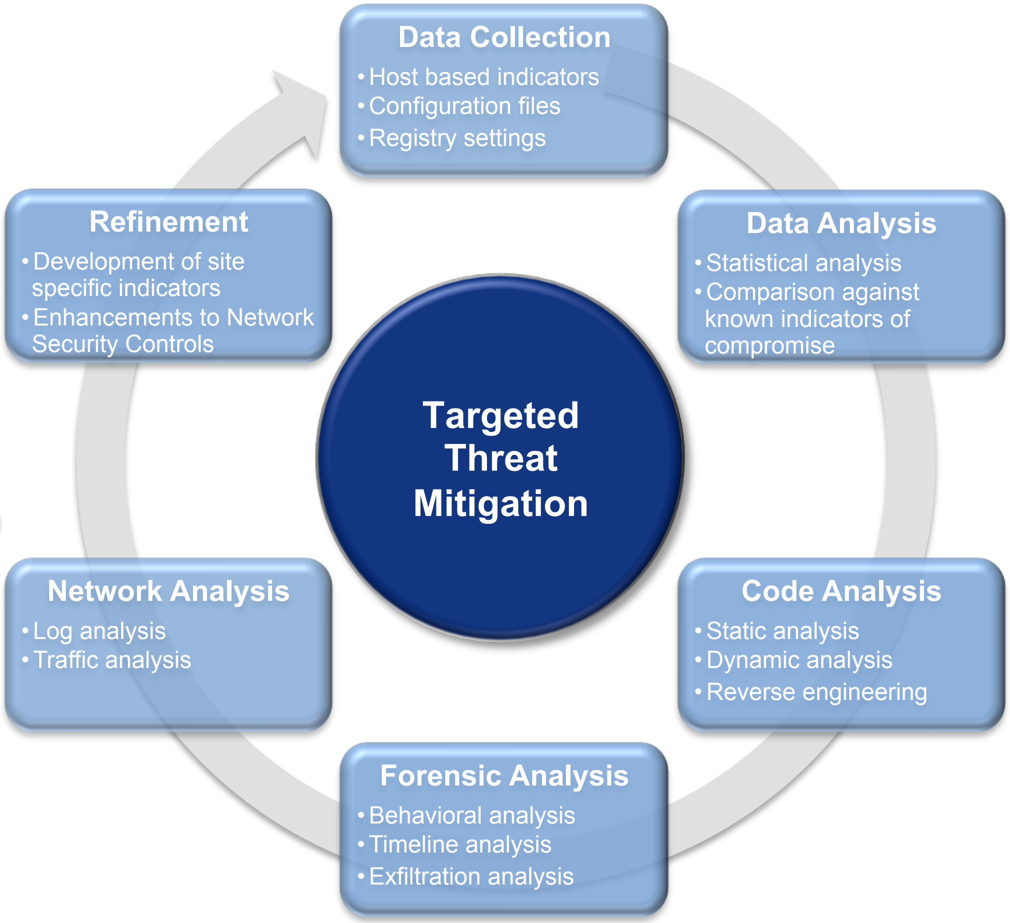
Continuous Assessment

Our Proactive Threat Identification offering is based on Hunt methodologies refined through analysis of data from millions of hosts

APT Discovery & Hunt

- **Iterative phases of analysis and refinement to pinpoint specific APT indicators and behaviors:**
  - Host based indicator analysis
  - Binary code analysis
  - Digital forensics analysis
  - Network analysis
- **Refinement enables the discovery of:**
  - Unauthorized system or network access
  - Malware on other systems on the network
  - Variants of the malware already discovered
  - Attack vectors

Results in Tactical and Strategic mitigation of targeted threats to the enterprise



Targeted Threat Mitigation

Data Collection
- Host based indicators
- Configuration files
- Registry settings

Data Analysis
- Statistical analysis
- Comparison against known indicators of compromise

Code Analysis
- Static analysis
- Dynamic analysis
- Reverse engineering

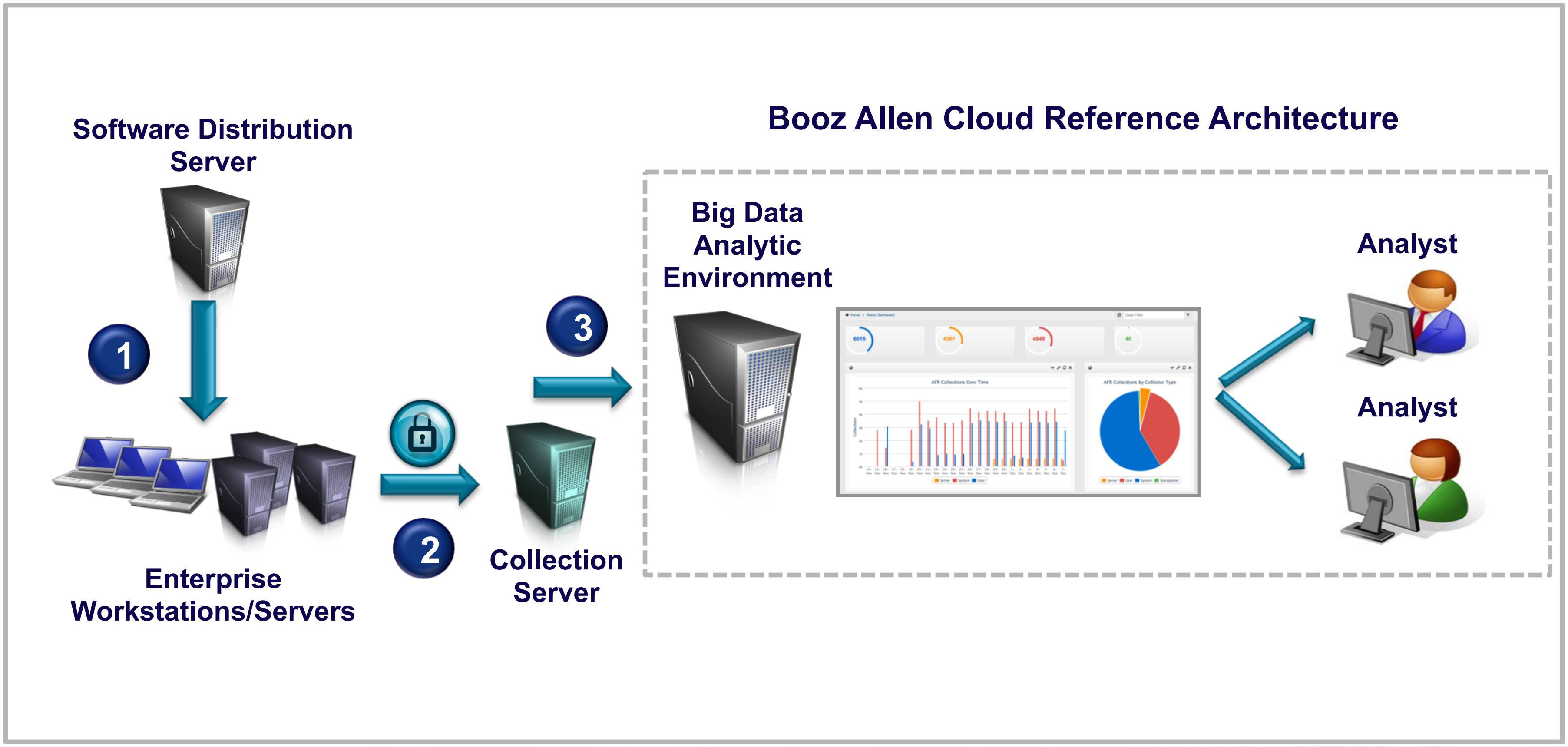
Forensic Analysis
- Behavioral analysis
- Timeline analysis
- Exfiltration analysis

Network Analysis
- Log analysis
- Traffic analysis

Refinement
- Development of site specific indicators
- Enhancements to Network Security Controls

Automated First Responder (AFR) helps us rapidly detect malware and triage hosts

- Utilizes statistical analysis to identify malware
- Focused on detecting ***anomalies*** rather than signatures

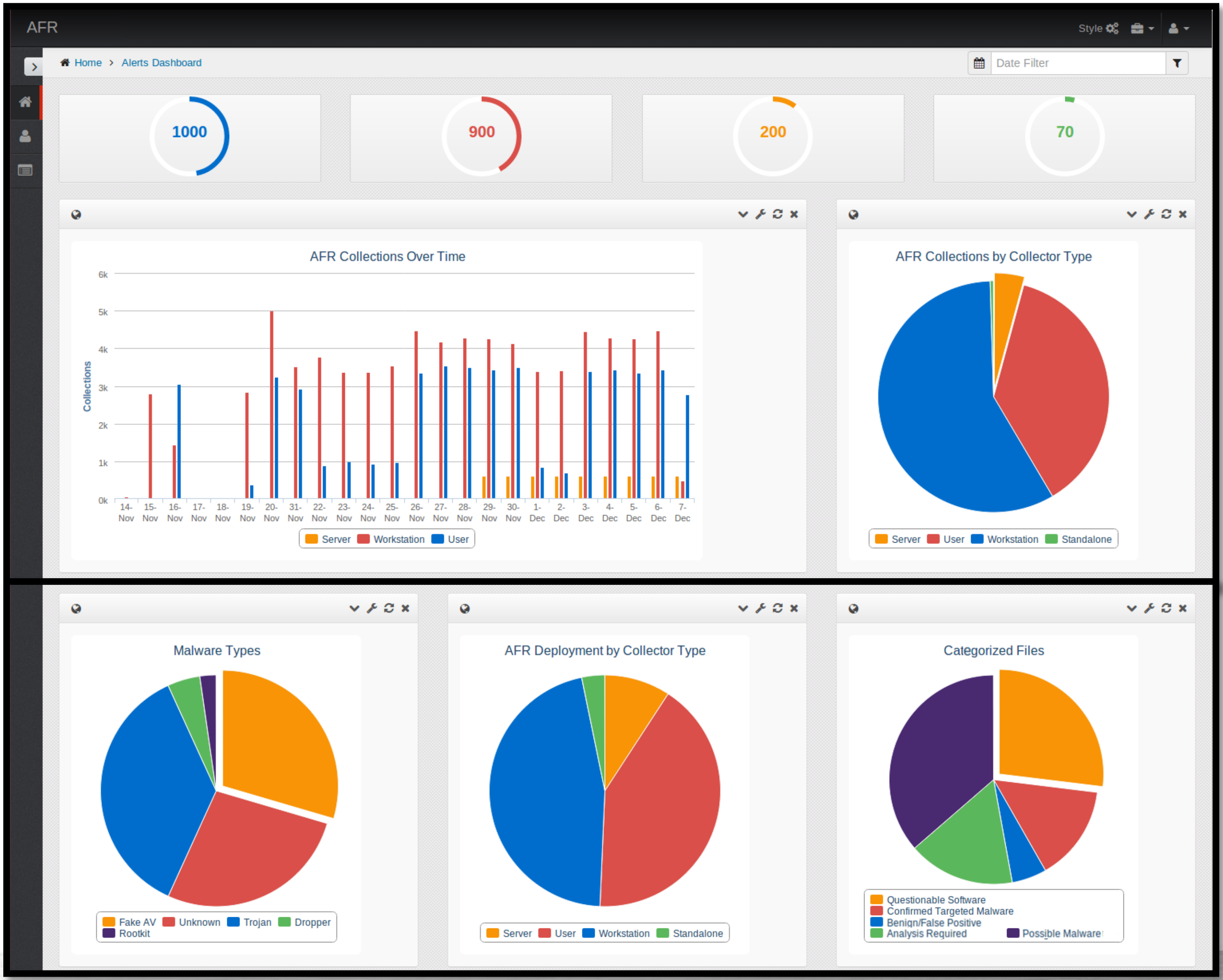

Software Distribution Server
1
Enterprise Workstations/Servers
2
Collection Server
3
Booz Allen Cloud Reference Architecture
Big Data Analytic Environment
Home > Alerts Dashboard
Date Filter
6015
4361
4848
40
AFR Collections Over Time
Collections
6k
5k
4k
3k
2k
1k
0k
Server
System
User
AFR Collections by Collector Type
Server
User
System
Standalone
Analyst
Analyst

AFR is a flexible, scalable, lightweight toolset

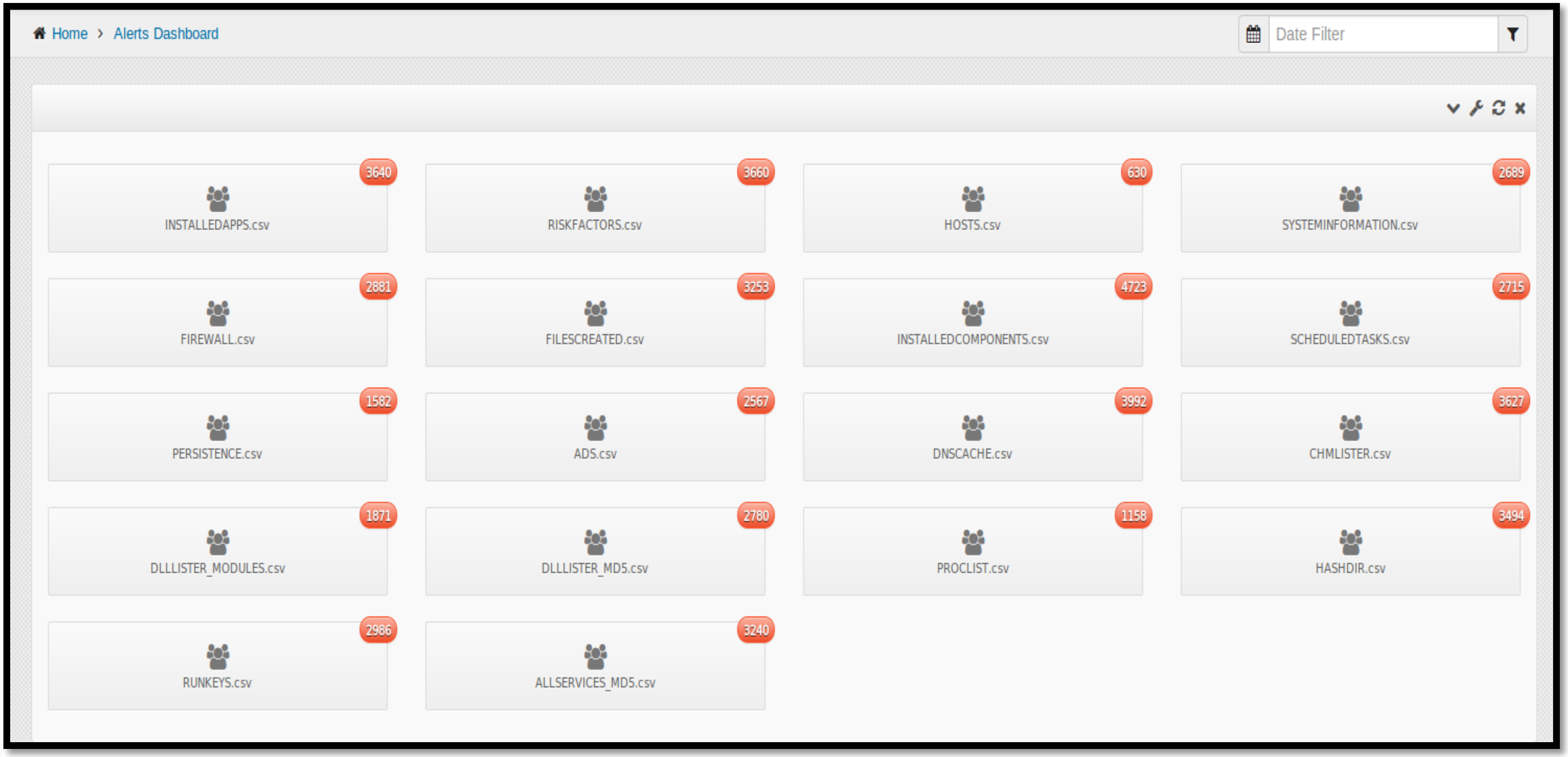
- Collects data including activity, persistence, investigative info and risk factors
- Non-persistent agent, no installation required
- Scalable – deployed to networks with >400k hosts
- Combines benefits of automated analysis and human intelligence
- Easily modifiable as attacker tactics change
- Execution occurs in background with no impact to user experience
- Lightweight

AFR Type	Average File Size	Storage per 20,000 units
Workstation	160 KB	~ 3GB
Server	134 KB	~ 2.5 GB
User	43 KB	~ 1GB

Executive Dashboard

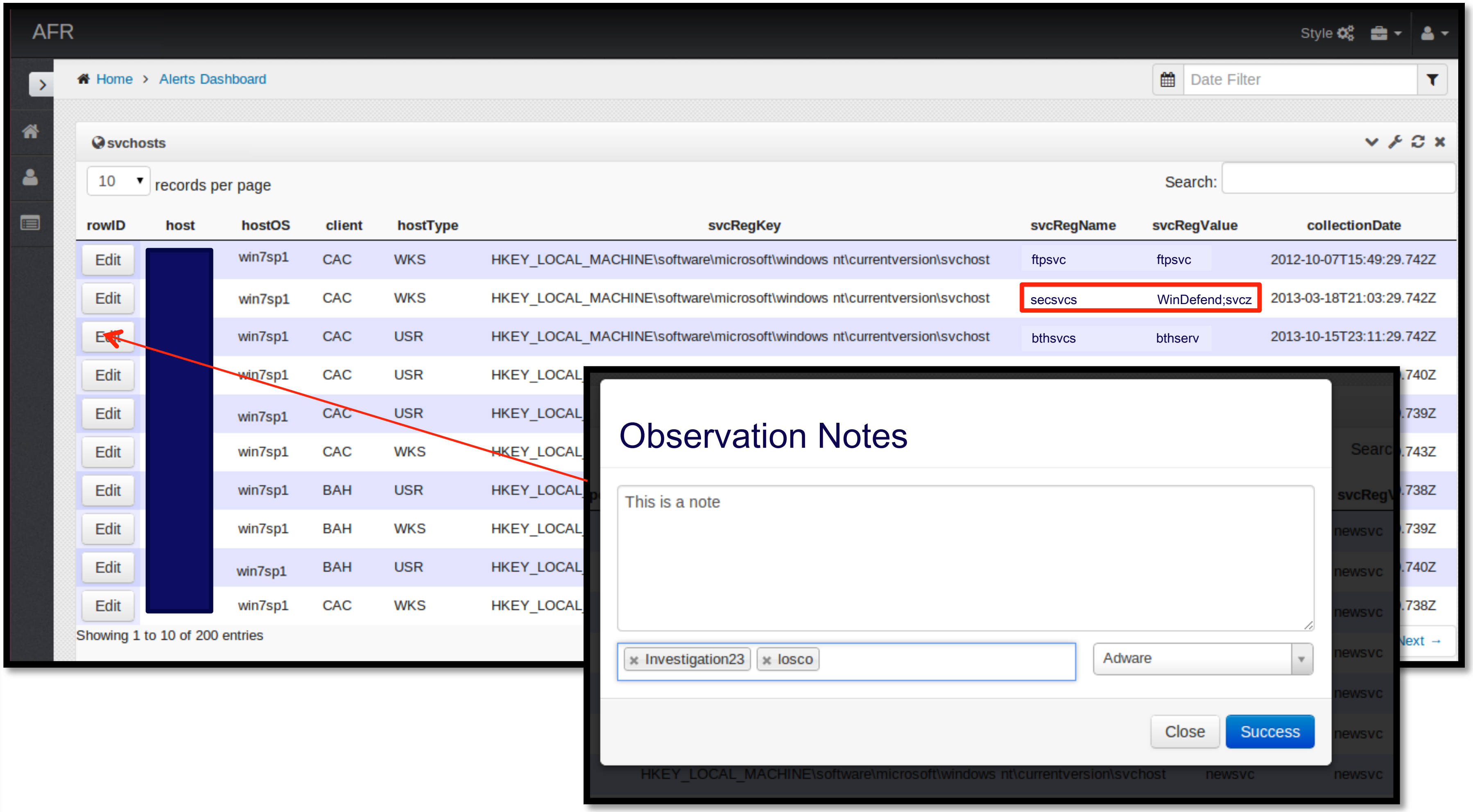


Alerts Dashboard



INSTALLEDAPPS.csv	3640
RISKFACTORS.csv	3660
HOSTS.csv	630
SYSTEMINFORMATION.csv	2689
FIREWALL.csv	2881
FILESCREATED.csv	3253
INSTALLEDCOMPONENTS.csv	4723
SCHEDULEDTASKS.csv	2715
PERSISTENCE.csv	1582
ADS.csv	2567
DNSCACHE.csv	3992
CHMLISTER.csv	3627
DLLLISTER_MODULES.csv	1871
DLLLISTER_MD5.csv	2780
PROCLIST.csv	1158
HASHDIR.csv	3494
RUNKEYS.csv	2986
ALLSERVICES_MD5.csv	3240

Alerts – Svchost Drill Down



rowID	host	hostOS	client	hostType	svcRegKey	svcRegName	svcRegValue	collectionDate
Edit	[redacted]	win7sp1	CAC	WKS	HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\svchost	ftpsvc	ftpsvc	2012-10-07T15:49:29.742Z
Edit	[redacted]	win7sp1	CAC	WKS	HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\svchost	secsvcs	WinDefend;svcz	2013-03-18T21:03:29.742Z
Edit	[redacted]	win7sp1	CAC	USR	HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\svchost	bthsvcs	bthserv	2013-10-15T23:11:29.742Z
Edit	[redacted]	win7sp1	CAC	USR	HKEY_LOCAL_			.740Z
Edit	[redacted]	win7sp1	CAC	USR	HKEY_LOCAL_			.739Z
Edit	[redacted]	win7sp1	CAC	WKS	HKEY_LOCAL_			.743Z
Edit	[redacted]	win7sp1	BAH	USR	HKEY_LOCAL_			.738Z
Edit	[redacted]	win7sp1	BAH	WKS	HKEY_LOCAL_			.739Z
Edit	[redacted]	win7sp1	BAH	USR	HKEY_LOCAL_			.740Z
Edit	[redacted]	win7sp1	CAC	WKS	HKEY_LOCAL_			.738Z

Showing 1 to 10 of 200 entries

Observation Notes

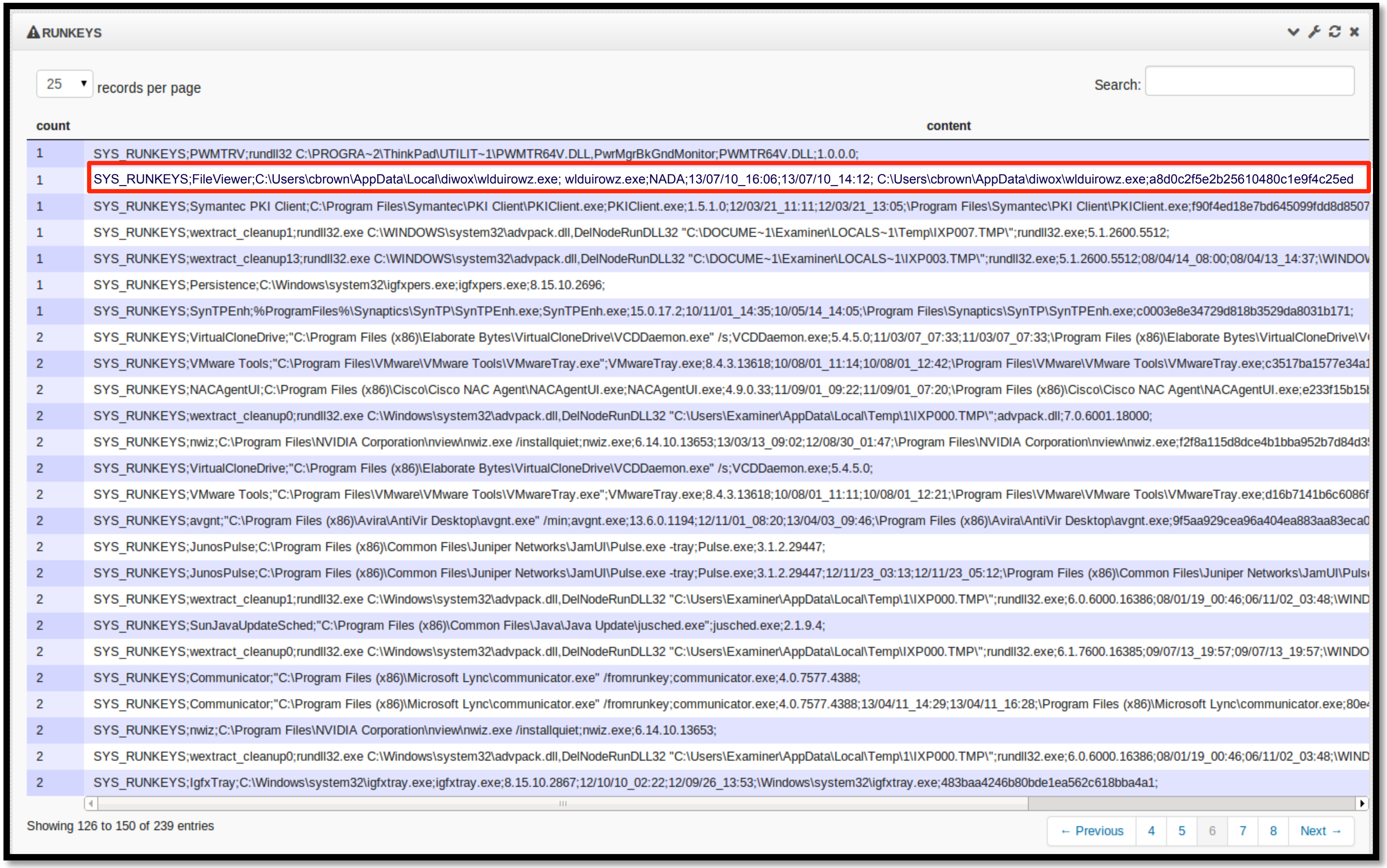
This is a note

Investigation23 × losco ×

Adware

HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\svchost newsvc newsvc

Indicators – Run Keys Drill Down



RUNKEYS

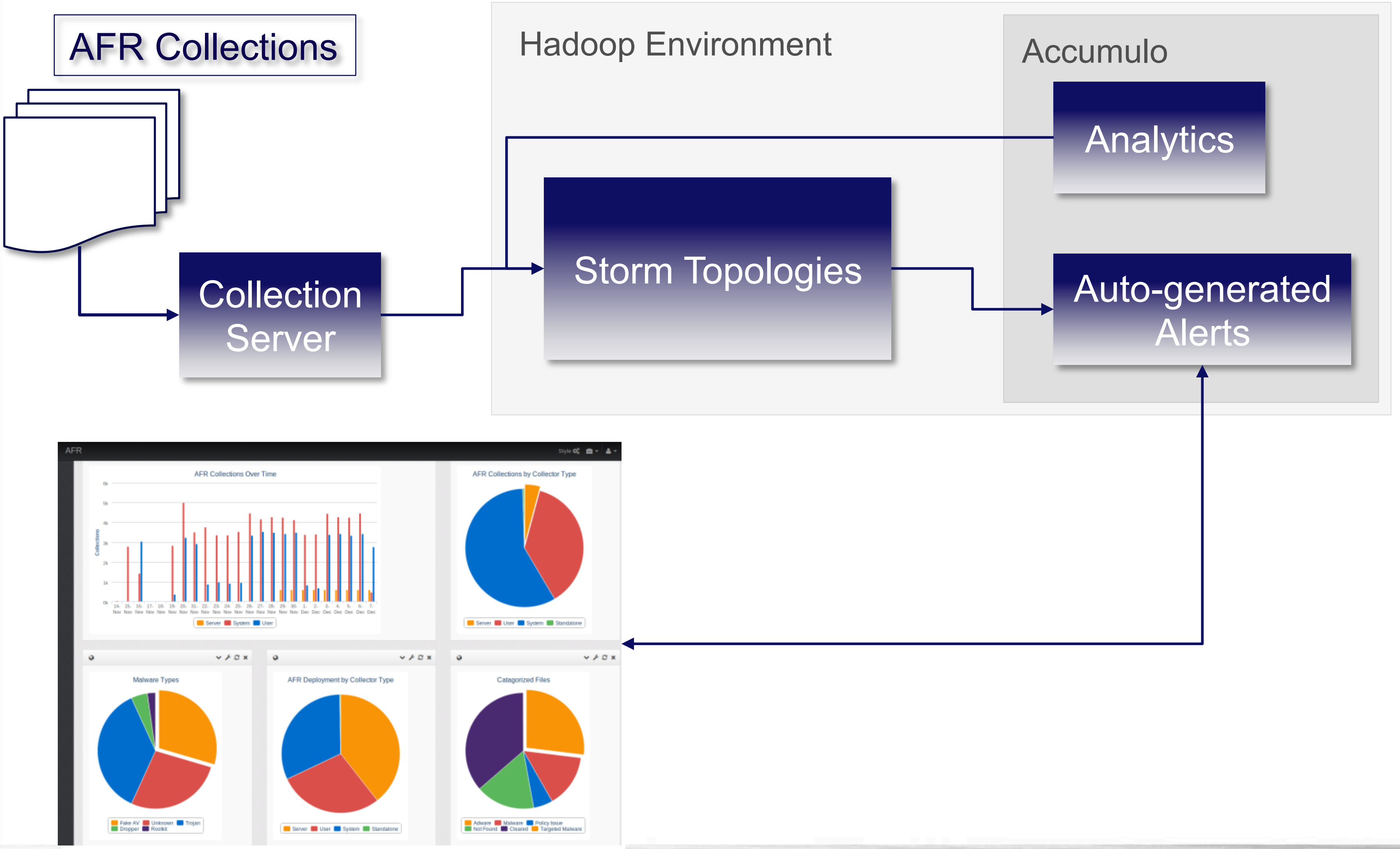
25 records per page

Search:

count	content
1	SYS_RUNKEYS;PWMTRV;rundll32 C:\PROGRA~2\ThinkPad\UTILIT~1\PWMTR64V.DLL,PwrMgrBkGndMonitor;PWMTR64V.DLL;1.0.0.0;
1	SYS_RUNKEYS;FileViewer;C:\Users\cbrown\AppData\Local\diwox\wlduirowz.exe; wlduirowz.exe;NADA;13/07/10_16:06;13/07/10_14:12; C:\Users\cbrown\AppData\diwox\wlduirowz.exe;a8d0c2f5e2b25610480c1e9f4c25ed
1	SYS_RUNKEYS;Symantec PKI Client;C:\Program Files\Symantec\PKI Client\PKIClient.exe;PKIClient.exe;1.5.1.0;12/03/21_11:11;12/03/21_13:05;\Program Files\Symantec\PKI Client\PKIClient.exe;f90f4ed18e7bd645099fdd8d8507
1	SYS_RUNKEYS;wextract_cleanup1;rundll32.exe C:\WINDOWS\system32\advpack.dll,DelNodeRunDLL32 "C:\DOCUME~1\Examiner\LOCALS~1\Temp\IXP007.TMP\";rundll32.exe;5.1.2600.5512;
1	SYS_RUNKEYS;wextract_cleanup13;rundll32.exe C:\WINDOWS\system32\advpack.dll,DelNodeRunDLL32 "C:\DOCUME~1\Examiner\LOCALS~1\IXP003.TMP\";rundll32.exe;5.1.2600.5512;08/04/14_08:00;08/04/13_14:37;\WINDOW
1	SYS_RUNKEYS;Persistence;C:\Windows\system32\igfxpers.exe;igfxpers.exe;8.15.10.2696;
1	SYS_RUNKEYS;SynTPEnh;%ProgramFiles%\Synaptics\SynTP\SynTPEnh.exe;SynTPEnh.exe;15.0.17.2;10/11/01_14:35;10/05/14_14:05;\Program Files\Synaptics\SynTP\SynTPEnh.exe;c0003e8e34729d818b3529da8031b171;
2	SYS_RUNKEYS;VirtualCloneDrive;"C:\Program Files (x86)\Elaborate Bytes\VirtualCloneDrive\VCDDaemon.exe" /s;VCDDaemon.exe;5.4.5.0;11/03/07_07:33;11/03/07_07:33;\Program Files (x86)\Elaborate Bytes\VirtualCloneDrive\V
2	SYS_RUNKEYS;VMware Tools;"C:\Program Files\VMware\VMware Tools\VMwareTray.exe";VMwareTray.exe;8.4.3.13618;10/08/01_11:14;10/08/01_12:42;\Program Files\VMware\VMware Tools\VMwareTray.exe;c3517ba1577e34a1
2	SYS_RUNKEYS;NACAgentUI;C:\Program Files (x86)\Cisco\Cisco NAC Agent\NACAgentUI.exe;NACAgentUI.exe;4.9.0.33;11/09/01_09:22;11/09/01_07:20;\Program Files (x86)\Cisco\Cisco NAC Agent\NACAgentUI.exe;e233f15b15
2	SYS_RUNKEYS;wextract_cleanup0;rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\Examiner\AppData\Local\Temp\1\IXP000.TMP\";advpack.dll;7.0.6001.18000;
2	SYS_RUNKEYS;nwiz;C:\Program Files\NVIDIA Corporation\nview\nwiz.exe /installquiet;nwiz.exe;6.14.10.13653;13/03/13_09:02;12/08/30_01:47;\Program Files\NVIDIA Corporation\nview\nwiz.exe;f2f8a115d8dce4b1bba952b7d84d3
2	SYS_RUNKEYS;VirtualCloneDrive;"C:\Program Files (x86)\Elaborate Bytes\VirtualCloneDrive\VCDDaemon.exe" /s;VCDDaemon.exe;5.4.5.0;
2	SYS_RUNKEYS;VMware Tools;"C:\Program Files\VMware\VMware Tools\VMwareTray.exe";VMwareTray.exe;8.4.3.13618;10/08/01_11:11;10/08/01_12:21;\Program Files\VMware\VMware Tools\VMwareTray.exe;d16b7141b6c6086f
2	SYS_RUNKEYS;avgnt;"C:\Program Files (x86)\Avira\AntiVir Desktop\avgnt.exe" /min;avgnt.exe;13.6.0.1194;12/11/01_08:20;13/04/03_09:46;\Program Files (x86)\Avira\AntiVir Desktop\avgnt.exe;9f5aa929cea96a404ea883aa83eca0
2	SYS_RUNKEYS;JunosPulse;C:\Program Files (x86)\Common Files\Juniper Networks\JamUI\Pulse.exe -tray;Pulse.exe;3.1.2.29447;
2	SYS_RUNKEYS;JunosPulse;C:\Program Files (x86)\Common Files\Juniper Networks\JamUI\Pulse.exe -tray;Pulse.exe;3.1.2.29447;12/11/23_03:13;12/11/23_05:12;\Program Files (x86)\Common Files\Juniper Networks\JamUI\Puls
2	SYS_RUNKEYS;wextract_cleanup1;rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\Examiner\AppData\Local\Temp\1\IXP000.TMP\";rundll32.exe;6.0.6000.16386;08/01/19_00:46;06/11/02_03:48;\WIND
2	SYS_RUNKEYS;SunJavaUpdateSched;"C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe";jusched.exe;2.1.9.4;
2	SYS_RUNKEYS;wextract_cleanup0;rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\Examiner\AppData\Local\Temp\IXP000.TMP\";rundll32.exe;6.1.7600.16385;09/07/13_19:57;09/07/13_19:57;\WINDO
2	SYS_RUNKEYS;Communicator;"C:\Program Files (x86)\Microsoft Lync\communicator.exe" /fromrunkey;communicator.exe;4.0.7577.4388;
2	SYS_RUNKEYS;Communicator;"C:\Program Files (x86)\Microsoft Lync\communicator.exe" /fromrunkey;communicator.exe;4.0.7577.4388;13/04/11_14:29;13/04/11_16:28;\Program Files (x86)\Microsoft Lync\communicator.exe;80e
2	SYS_RUNKEYS;nwiz;C:\Program Files\NVIDIA Corporation\nview\nwiz.exe /installquiet;nwiz.exe;6.14.10.13653;
2	SYS_RUNKEYS;wextract_cleanup0;rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\Examiner\AppData\Local\Temp\1\IXP000.TMP\";rundll32.exe;6.0.6000.16386;08/01/19_00:46;06/11/02_03:48;\WIND
2	SYS_RUNKEYS;IgfxTray;C:\Windows\system32\igfxtray.exe;igfxtray.exe;8.15.10.2867;12/10/10_02:22;12/09/26_13:53;\Windows\system32\igfxtray.exe;483baa4246b80bde1ea562c618bba4a1;

Showing 126 to 150 of 239 entries

AFR Automated Ingest and Analytics Pipeline



AFR Collections

Collection Server

Hadoop Environment

Storm Topologies

Accumulo

Analytics

Auto-generated Alerts

AFR
AFR Collections Over Time
Collections
Server System User
AFR Collections by Collector Type
Server User System Standalone
Malware Types
Fake AV Unknown Trojan Dropper Rootkit
AFR Deployment by Collector Type
Server User System Standalone
Catagorized Files
Adware Malware Policy Issue Not Found Cleared Targeted Malware

Kaizen:
CTF event hosted by Booz Allen Hamilton

Wednesday, July 31, 2013 – 2:15pm-6:00pm
Milano Ballroom III, Caesars Palace

Booz | Allen | Hamilton

Kaizen: CTF event hosted by Booz Allen Hamilton

Wednesday, July 31, 2013

2:15pm-6:00pm

Milano Ballroom III, Caesars Palace

Contact Information

Anuj Soni
Lead Associate

Booz | Allen | Hamilton

Booz Allen Hamilton, Inc.
soni_anuj@bah.com

Jason Losco
Associate

Booz | Allen | Hamilton

Booz Allen Hamilton, Inc.
losco_jason@bah.com

Questions & Answers

black hat
BRIEFINGS & TRAINING

- To join the Black Hat mailing list, email BH LIST to: feedback@blackhat.com
- To join our LinkedIn Group:
- http://www.linkedin.com/groups?gid=37658&trk=hb_side_g
- To follow Black Hat on Twitter:
- https://twitter.com/Blackhatevents
- Black Hat's Facebook Fan Page:
- http://www.facebook.com/blackhat
- Find out more at www.blackhat.com
- Next Webcast: August 15: Black Hat USA Highlights
- For more information, visit www.boozallen.com

Sponsored by

Booz | Allen | Hamilton
strategy and technology consultants