



# BEYOND COMPLIANCE

SCAP for Intrusion and Vulnerability Analysis



# Extending OVAL and SCAP

- Expanding data collection capabilities
- Building a comprehensive awareness of asset state
- Leveraging SCAP standards and existing process



# Overview

- Why OVAL?
- Asking the right questions
- Saving detailed system information
- Leveraging new capabilities
- Looking ahead



## Why OVAL?

- 20 compatible products from 28 organizations
- Powerful compliance assessment capabilities
- Framework for sharing state information



# Asking The Right Questions

- How do you find out which patches are installed?
  - Enumerate through all possible patches
- Is it possible to identify which software is installed on an asset?
  - Ask the Operating System
- Which data can better be seen with an unbounded approach?
  - Anything with a non-trivial number of possible values

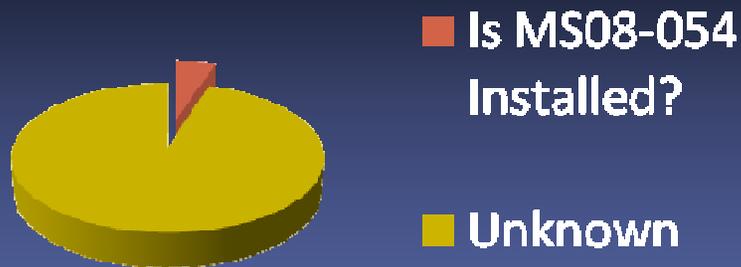


# Asking the right questions

## Bounded

- Very concise
- Only report the known

### Microsoft Patches



## Unbounded

- Large breadth
- Identify the unknown

### Microsoft Patches





# Asking the right questions

- Define a new “collector” type within OVAL
  - It’s a test without a target state

```
- <collectors>
- <service_collector id="oval:g2-inc.net:dc:1" version="1" comment="WindowsNT Service Collector">
  <object object_ref="oval:g2-inc.net:obj:1" />
</service_collector>
</collectors>
- <objects>
- <service_object id="obj:g2-inc.net:obj:1" version="1">
  <startup_type>system</startup_type>
</service_object>
</objects>
```



# Saving Detailed System Information

- How do you report this new data?
  - Use the System Characteristics Schema

```
- <system_data>
- <service_item id="1">
  <display_name>Application Experience</display_name>
  <service_name>AeLookupSvc</service_name>
  <current_state>SERVICE_ACTIVE</current_state>
</service_item>
- <service_item id="2">
  <display_name>Application Layer Gateway Service</display_name>
  <service_name>ALG</service_name>
  <current_state>SERVICE_INACTIVE</current_state>
</service_item>
- <service_item id="3">
  <display_name>Application Information</display_name>
  <service_name>Appinfo</service_name>
  <current_state>SERVICE_ACTIVE</current_state>
</service_item>
</system_data>
```



# Leveraging New Capabilities

- Example 1: System Detail
- Example 2: Simple Search
- Example 3: Complex Correlation



## Example 1: System Detail

- Question: Which services are running on Chris' development environment?

Host Name cfoosterdev.g2-inc.net  
Collection Timestamp 2008-09-15T16:58:06

id	service name	display name	state
1	AeLookupSvc	Application Experience	SERVICE_ACTIVE
2	ALG	Application Layer Gateway Service	SERVICE_INACTIVE
3	AppHostSvc	Application Host Helper Service	SERVICE_ACTIVE
4	Appinfo	Application Information	SERVICE_ACTIVE
5	AppMgmt	Application Management	SERVICE_INACTIVE
6	aspnet_state	ASP.NET State Service	SERVICE_INACTIVE
7	AudioEndpointBuilder	Windows Audio Endpoint Builder	SERVICE_ACTIVE
8	AudioSrv	Windows Audio	SERVICE_ACTIVE
9	BFE	Base Filtering Engine	SERVICE_ACTIVE
10	BITS	Background Intelligent Transfer Service	SERVICE_ACTIVE
11	Browser	Computer Browser	SERVICE_ACTIVE
12	BthFilterHelper	Bluetooth Feature Support	SERVICE_ACTIVE
13	BthServ	Bluetooth Support Service	SERVICE_ACTIVE
14	CertPropSvc	Certificate Propagation	SERVICE_ACTIVE
15	clr_optimization_v2.0.50727_32	Microsoft .NET Framework NGEN v2.0.50727_X86	SERVICE_INACTIVE
16	clr_optimization_v2.0.50727_64	Microsoft .NET Framework NGEN v2.0.50727_X64	SERVICE_INACTIVE
17	COMSysApp	COM+ System Application	SERVICE_INACTIVE
18	CryptSvc	Cryptographic Services	SERVICE_ACTIVE
19	CscService	Offline Files	SERVICE_ACTIVE



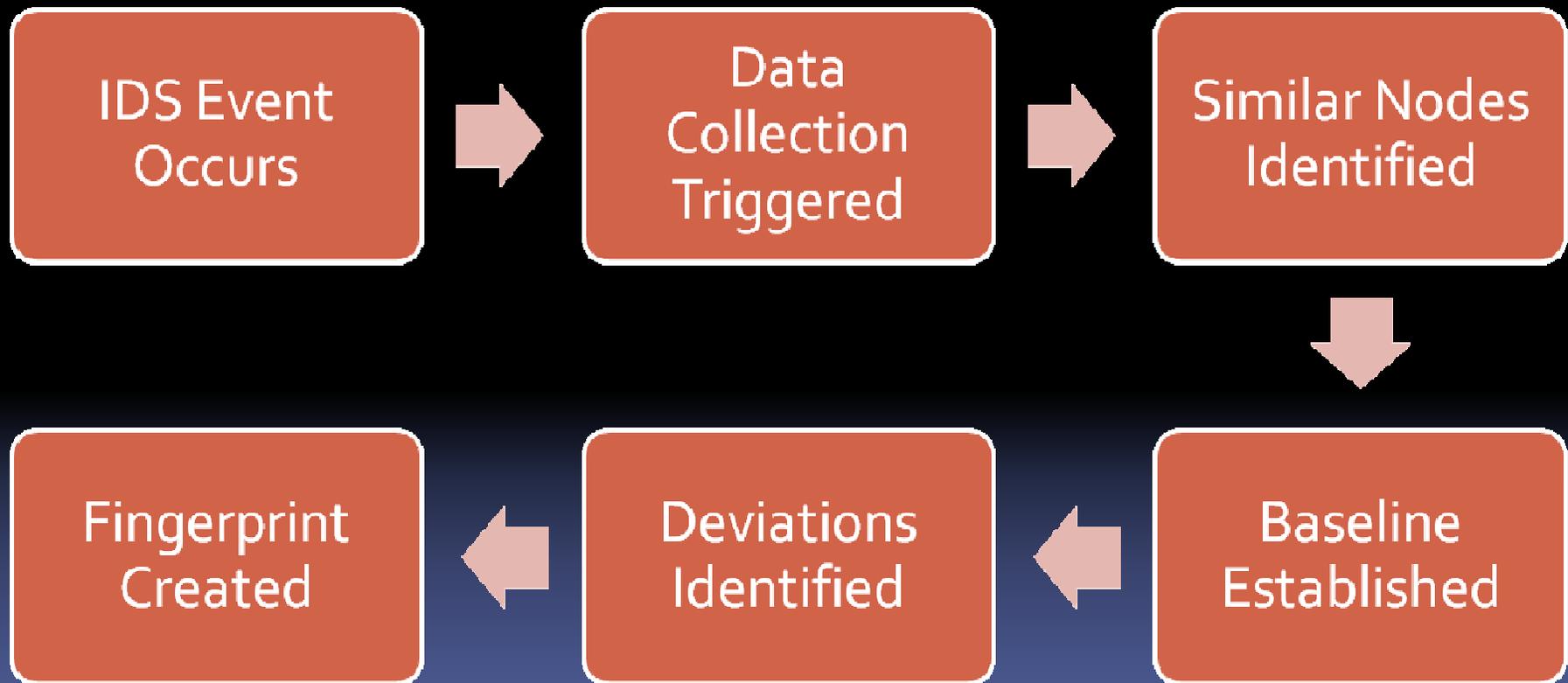
## Example 2: Simple Search

- Question: Which assets run SQL Express?

The screenshot shows a web browser window displaying search results for 'SQLEXPRESS' on a Google Search Appliance. The browser's address bar shows the URL: `http://172.16.1.210/search?q=SQLEXPRESS&btnG=G2+SCAP+Search&acc`. The search interface includes a search box with 'SQLEXPRESS' entered, a 'G2 SCAP Search' button, and radio buttons for 'public content' (selected) and 'public and secure content'. Below the search box, the results are displayed under the heading 'Search' with the text 'Results 1 - 2 of about 2 for SQLEXPRESS. Search took 0.02 seconds.' and a link to 'Sort by date / Sort by relevance'. The first result is titled 'CFosterDEV System Information' and contains the text: '... 59, msftesql\$SQLEXPRESS, SQL Server FullText Search (SQLEXPRESS), SERVICE\_ACTIVE. ... 63, MSSQL\$SQLEXPRESS, SQL Server (SQLEXPRESS), SERVICE\_ACTIVE. ... 172.16.1.101/cfosterdev.system.htm - 26k - 2008-09-22 - Cached'. The second result is titled 'KSittoDEV System Information' and contains the text: '... SERVICE\_INACTIVE, 48, msiserver, Windows Installer, SERVICE\_INACTIVE, 49, MSSQL\$SQLEXPRESS, SQL Server (SQLEXPRESS), SERVICE\_ACTIVE, 50, MSSQLServerADHelper, ... 172.16.1.101/ksittodev.system.htm - 22k - 2008-09-22 - Cached'. At the bottom of the search interface, there is a search box with 'SQLEXPRESS', a 'G2 SCAP Search' button, and radio buttons for 'public content' (selected) and 'public and secure content'. The footer of the page reads 'Powered by Google Search Appliance'.



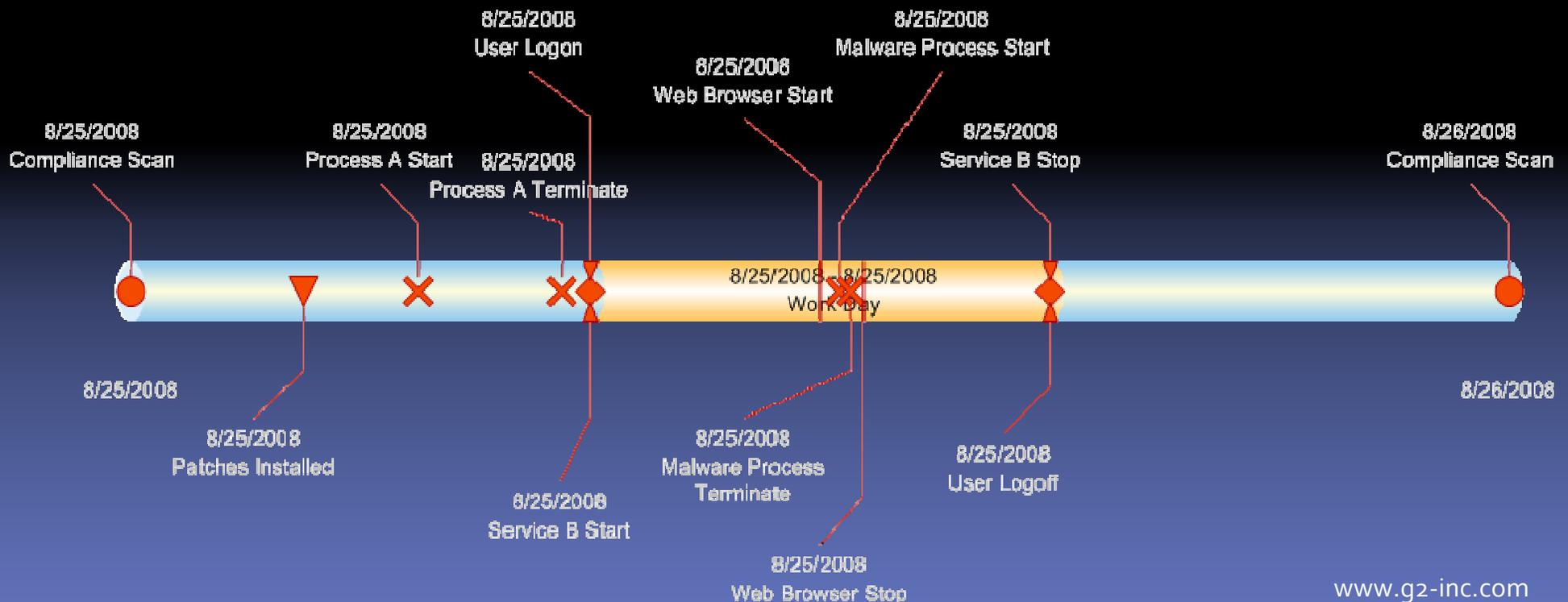
## Example 3: Complex Correlation





# Looking Ahead

- Continuous Monitoring
  - Detect Short-Lived Events
  - Immediate Notification





## Contacts

- Kevin Sitto – [kevin.sitto@g2-inc.com](mailto:kevin.sitto@g2-inc.com)
- Shane Shaffer – [shane.shaffer@g2-inc.com](mailto:shane.shaffer@g2-inc.com)
- Matt Kerr – [matt.kerr@g2-inc.com](mailto:matt.kerr@g2-inc.com)
  
- <http://www.G2-Inc.com>