splunk> .conf2017

Bringing Sweetness to Sour Patch Tuesday

Pacific Northwest National Laboratory

Justin Brown & Arzu Gosney

September 27, 2017 | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf2017

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Arzu Gosney
Arzu.Gosney@pnnl.gov
@ArzuGosney

About Me

- IT Engineer
- Technical Lead
- Automation & Monitoring Team
- Joined PNNL in 2000

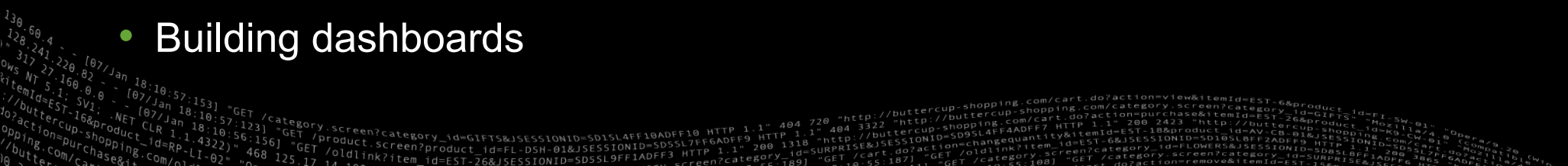
splunk> .conf2017

About PNNL

(Pacific Northwest National Laboratory)

Agenda

- Where We Were
  - Problem description
  - Goals
- Where We Are Now
  - Current process demonstration
  - Explaining Why
- How We Did It
  - Key Components
  - Writing queries
  - Building dashboards



splunk> .conf2017

Where We Were

The Problems with Patch Week

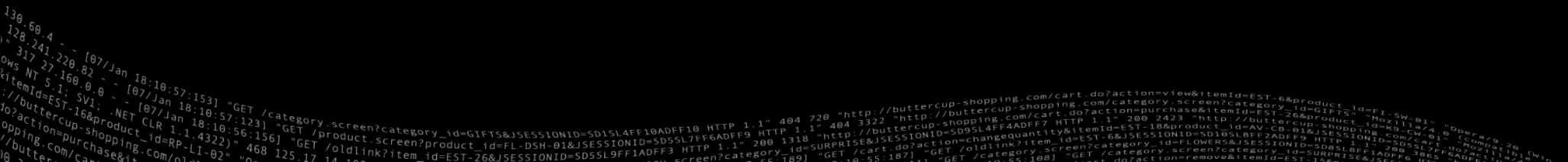
Goals for Improvement

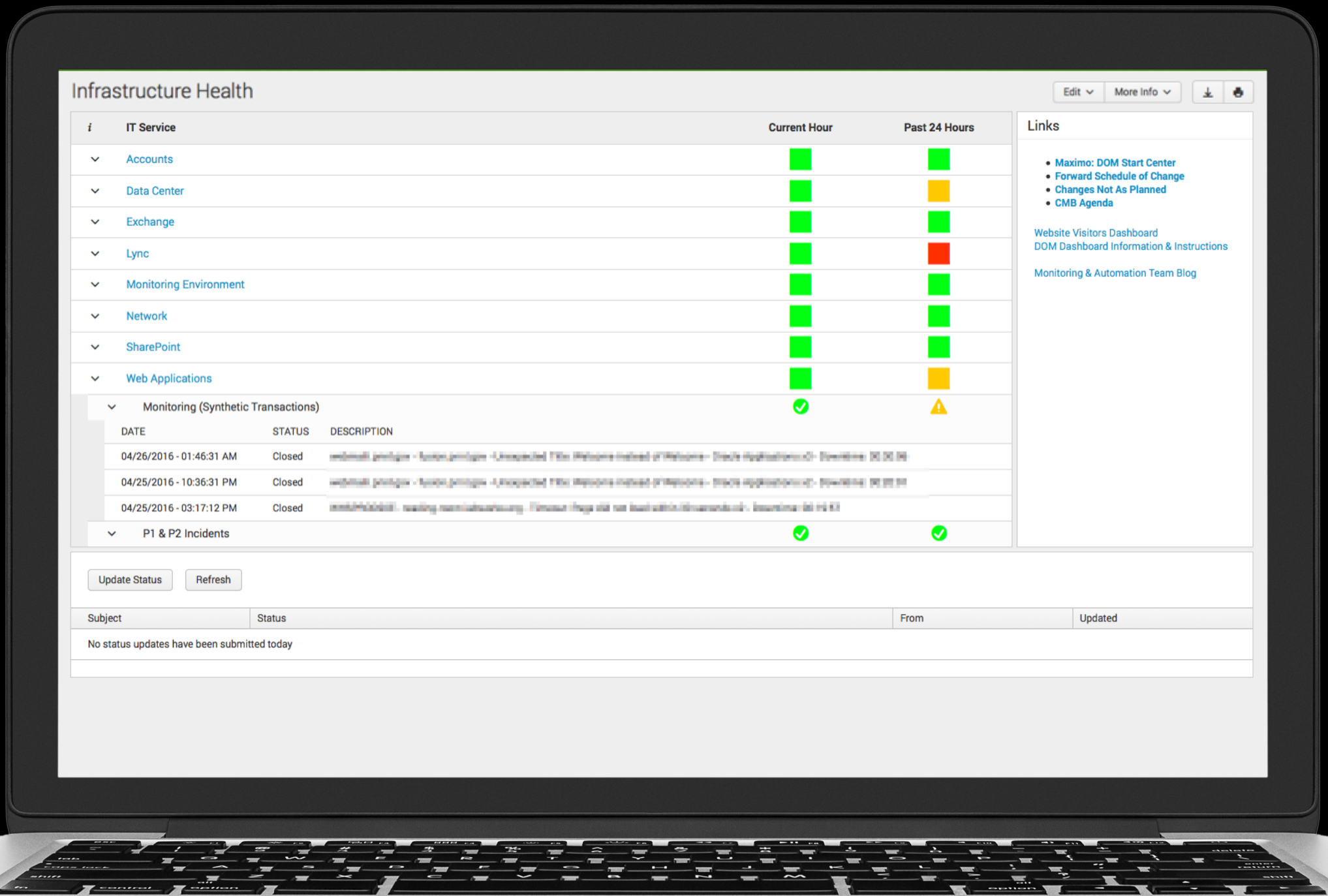
splunk> .conf2017

Where We Were

The Problems with Patch Week

- Slow problem discovery
  - Failed patches
  - Multiple reboots
  - False positives
- Manual Processes
  - Servers checked in SCOM, SCCM, Splunk, manually
  - Applications checked manually (SharePoint checklist)
  - Resource intensive





Monitoring - Web Applications

Edit | More Info

Last 4 hours

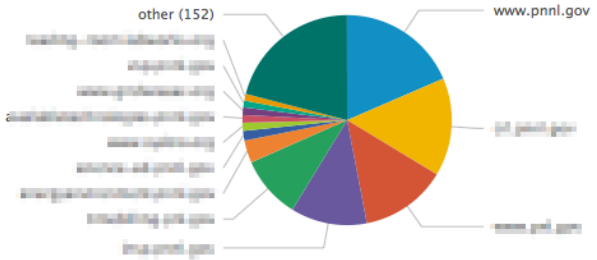
Monitoring Dashboard | Monitoring - Web Applications | Website Owner's Dashboard | Website Visitor's Dashboard

Website Traffic

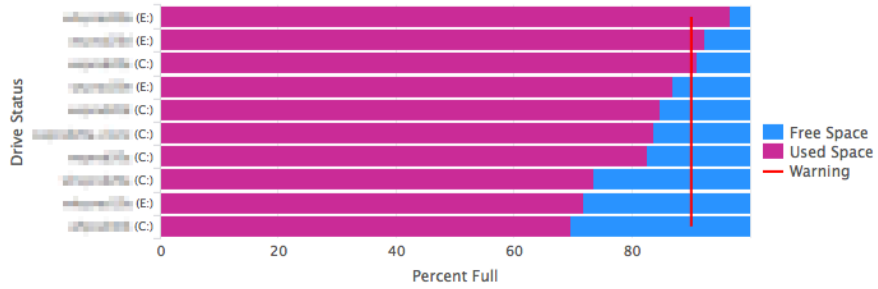
site	count	status
www.pnnl.gov	1167	
[redacted]	951	
[redacted]	840	
[redacted]	742	
[redacted]	610	
[redacted]	217	
[redacted]	94	
[redacted]	78	
[redacted]	75	
[redacted]	74	

« prev 1 2 3 4 5 6 7 8 9 10 next »

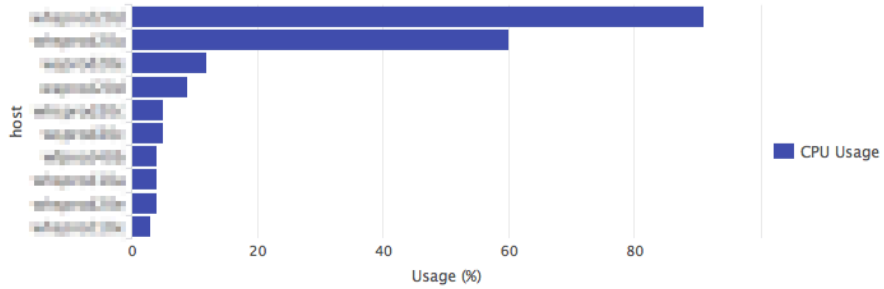
Top Sites Visited



Web Server Drive Status



Server CPU Usage



CPU Utilization Trend Per Server

Website Owner's Dashboard

captures site traffic by user

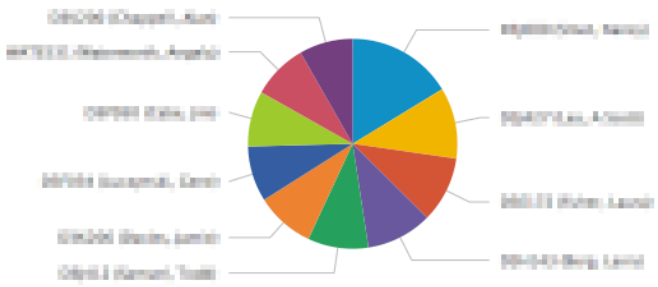
Edit | More Info

Site | User's Name | Network ID | Time Frame

Filter by user: | Filter by Network ID: | Last 24 hours | Submit

< Infrastructure Health | Monitoring - Web Applications | Website Owner's Dashboard | Website Visitor's Dashboard

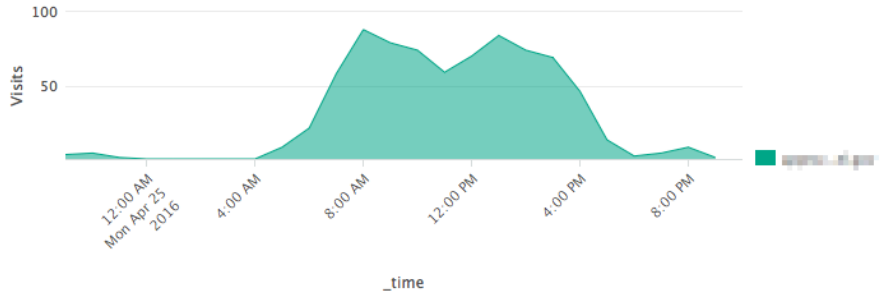
Site Visits - Top 10 Users



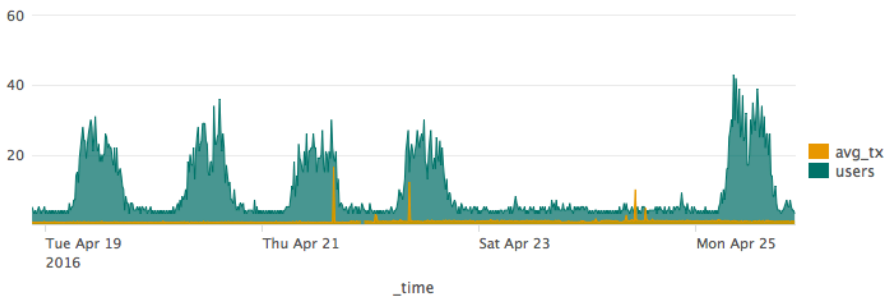
Average Site Visits Every Hour

SITE	Average
[redacted]	38

Website Traffic Trend

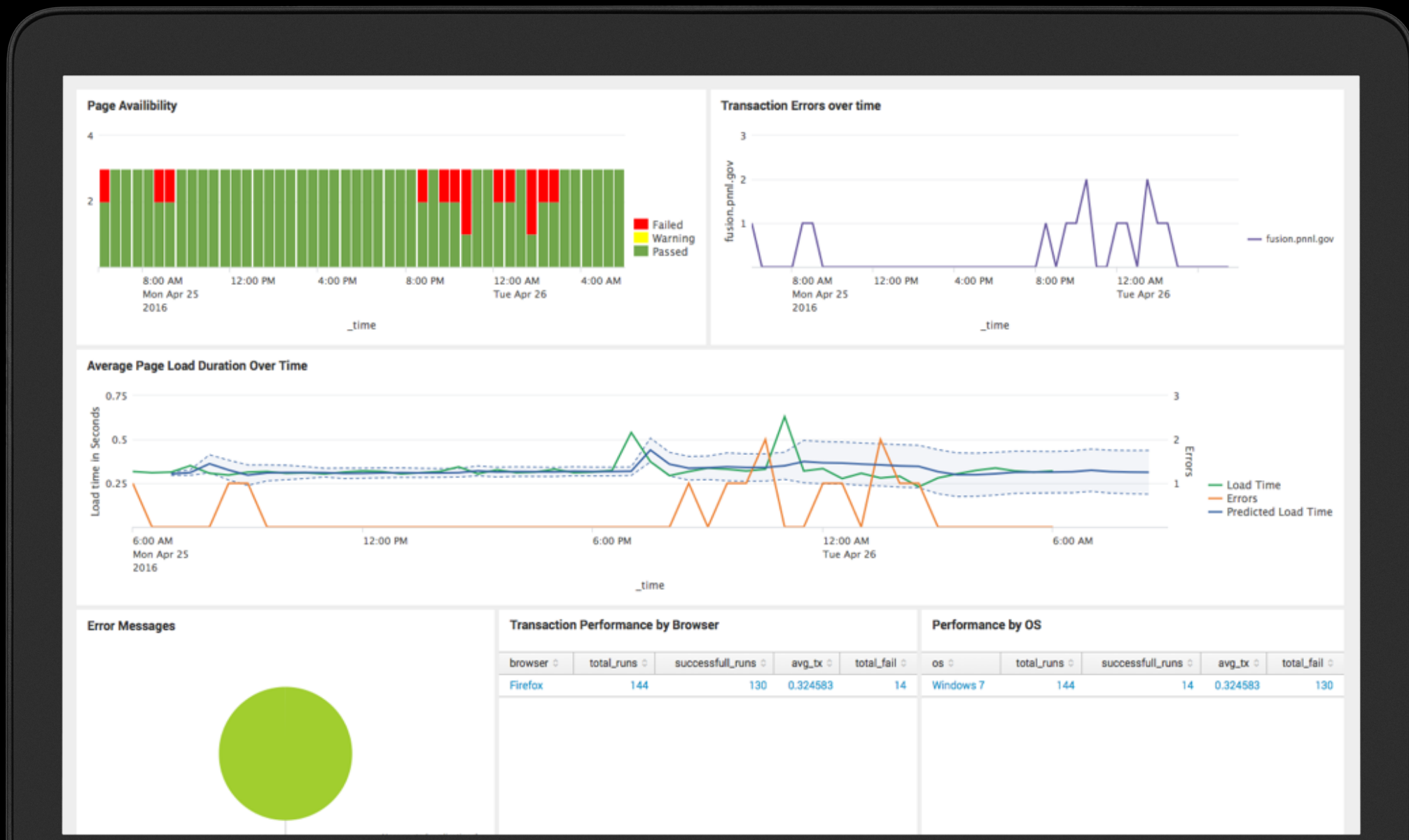


Site Responsiveness Based on Load (Last 7 Days)



8h ago

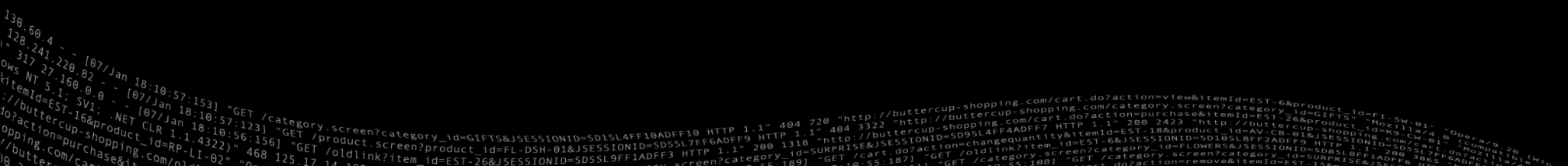
HTTP Errors



Where We Were

Goals for Improvement

- Patching status for all Windows servers
  - Drilldown for individual server details
  - Dashboard for patches by status
- Web Application health dashboard
  - Rollup of website and database monitoring
- Automated Reports & Alerts
  - Reports emailed to teams with status
  - Alerts sent to incident responders



Where We Are Now

Current Process Demonstration

Explaining Why

splunk> .conf2017

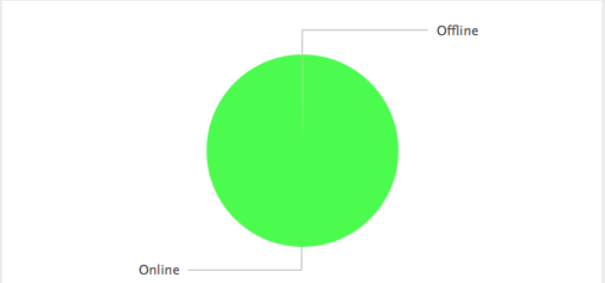
IT - Platform Services - Server Monitoring for Patch Weekend

Edit | More Info

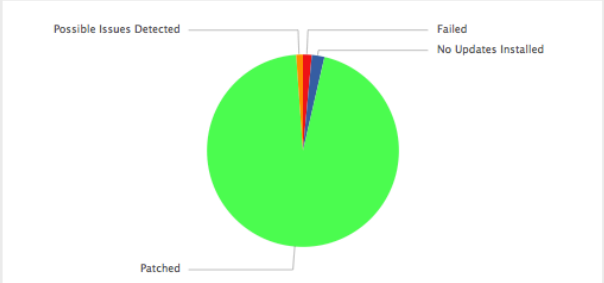
Need Help?

Show Icon Key

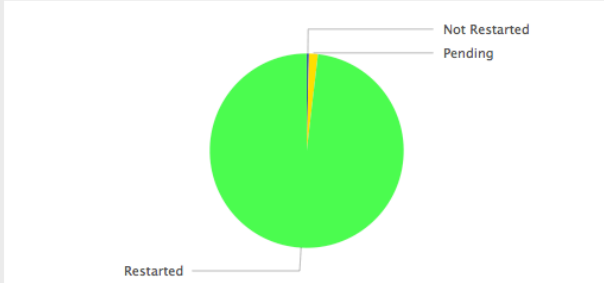
Servers Online



Servers Patched



Servers Restarted



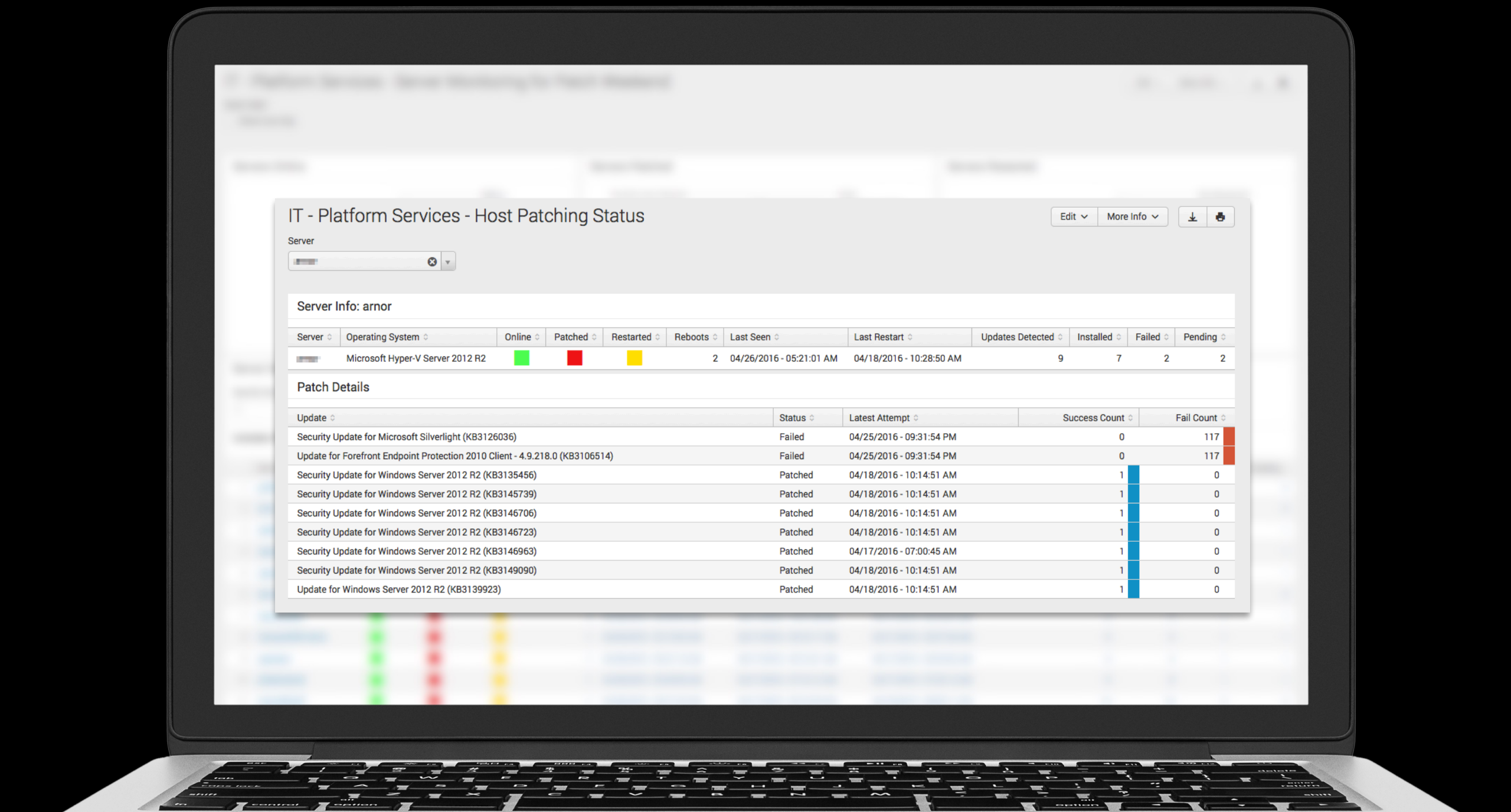
Server Details

Specify Server

*

Includes Windows 2008 & 2012 Servers

	Server	Online	Patched	Restarted	Reboots	Last Seen	Last Restart	Latest Install	Updates Attempted	Installed	Failed	Pending
1	[redacted]				1	04/25/2016 - 05:15:54 AM	04/17/2016 - 03:09:40 AM	-	0	0	0	0
2	[redacted]				2	04/26/2016 - 05:21:01 AM	04/18/2016 - 10:28:50 AM	04/18/2016 - 10:14:51 AM	9	7	2	2
3	[redacted]				3	04/26/2016 - 05:20:14 AM	04/14/2016 - 07:36:16 PM	04/14/2016 - 07:45:43 PM	18	17	1	1
4	[redacted]				3	04/26/2016 - 05:21:00 AM	04/17/2016 - 09:45:47 AM	04/17/2016 - 03:26:44 AM	5	4	1	1
5	[redacted]				3	04/26/2016 - 05:21:19 AM	04/17/2016 - 09:42:48 AM	04/17/2016 - 03:25:20 AM	5	4	1	1
6	[redacted]				6	04/26/2016 - 05:15:25 AM	04/21/2016 - 03:45:56 PM	04/21/2016 - 03:51:49 PM	23	21	2	2
7	[redacted]				3	04/26/2016 - 05:20:54 AM	04/17/2016 - 10:21:28 AM	04/17/2016 - 03:19:51 AM	6	5	1	1
8	[redacted]				1	04/26/2016 - 05:19:53 AM	04/17/2016 - 03:16:17 AM	04/17/2016 - 03:27:40 AM	6	5	1	1
9	[redacted]				1	04/26/2016 - 05:21:10 AM	04/17/2016 - 03:12:51 AM	04/17/2016 - 03:24:03 AM	5	4	1	1
10	[redacted]				1	04/26/2016 - 05:20:56 AM	04/17/2016 - 07:10:12 AM	04/17/2016 - 07:20:13 AM	9	8	1	1
11	[redacted]				1	04/26/2016 - 05:21:35 AM	04/17/2016 - 05:15:29 AM	04/18/2016 - 08:39:11 AM	12	10	2	2



IT - Platform Services - Host Patching Status

Edit | More Info

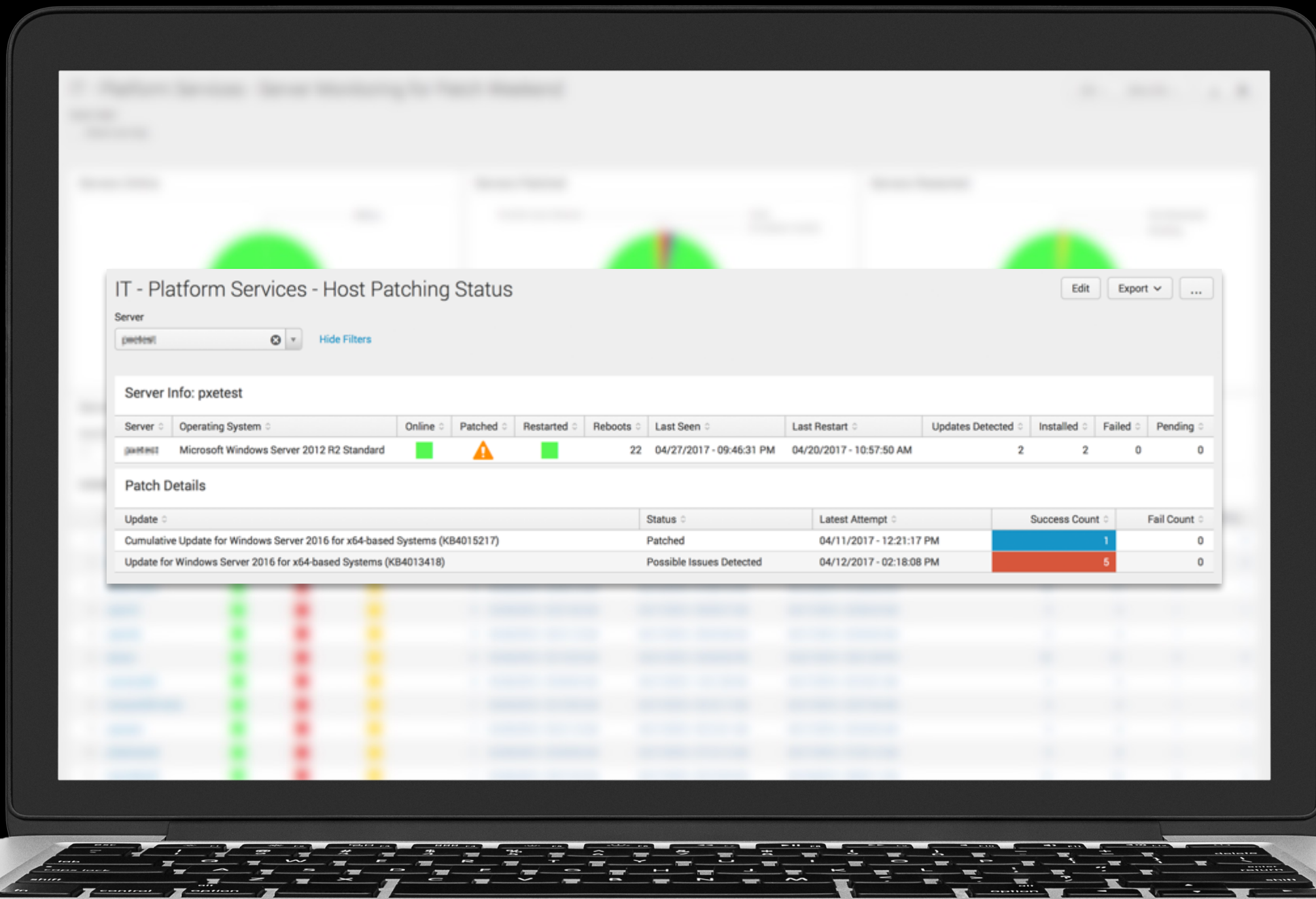
Server

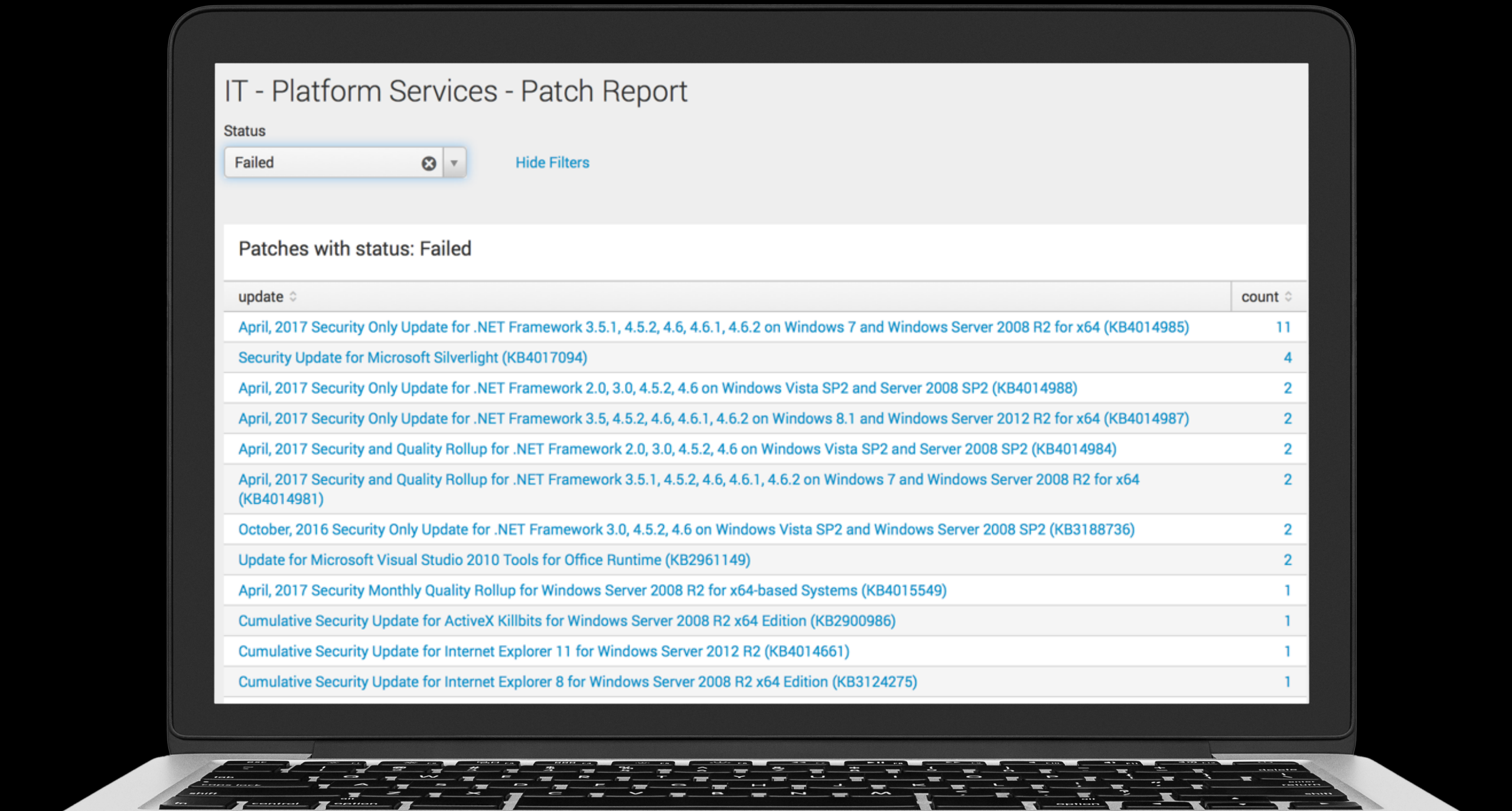
Server Info: arnor

Server	Operating System	Online	Patched	Restarted	Reboots	Last Seen	Last Restart	Updates Detected	Installed	Failed	Pending
[redacted]	Microsoft Hyper-V Server 2012 R2				2	04/26/2016 - 05:21:01 AM	04/18/2016 - 10:28:50 AM	9	7	2	2

Patch Details

Update	Status	Latest Attempt	Success Count	Fail Count
Security Update for Microsoft Silverlight (KB3126036)	Failed	04/25/2016 - 09:31:54 PM	0	117
Update for Forefront Endpoint Protection 2010 Client - 4.9.218.0 (KB3106514)	Failed	04/25/2016 - 09:31:54 PM	0	117
Security Update for Windows Server 2012 R2 (KB3135456)	Patched	04/18/2016 - 10:14:51 AM	1	0
Security Update for Windows Server 2012 R2 (KB3145739)	Patched	04/18/2016 - 10:14:51 AM	1	0
Security Update for Windows Server 2012 R2 (KB3146706)	Patched	04/18/2016 - 10:14:51 AM	1	0
Security Update for Windows Server 2012 R2 (KB3146723)	Patched	04/18/2016 - 10:14:51 AM	1	0
Security Update for Windows Server 2012 R2 (KB3146963)	Patched	04/17/2016 - 07:00:45 AM	1	0
Security Update for Windows Server 2012 R2 (KB3149090)	Patched	04/18/2016 - 10:14:51 AM	1	0
Update for Windows Server 2012 R2 (KB3139923)	Patched	04/18/2016 - 10:14:51 AM	1	0





IT - Platform Services - Patch Report

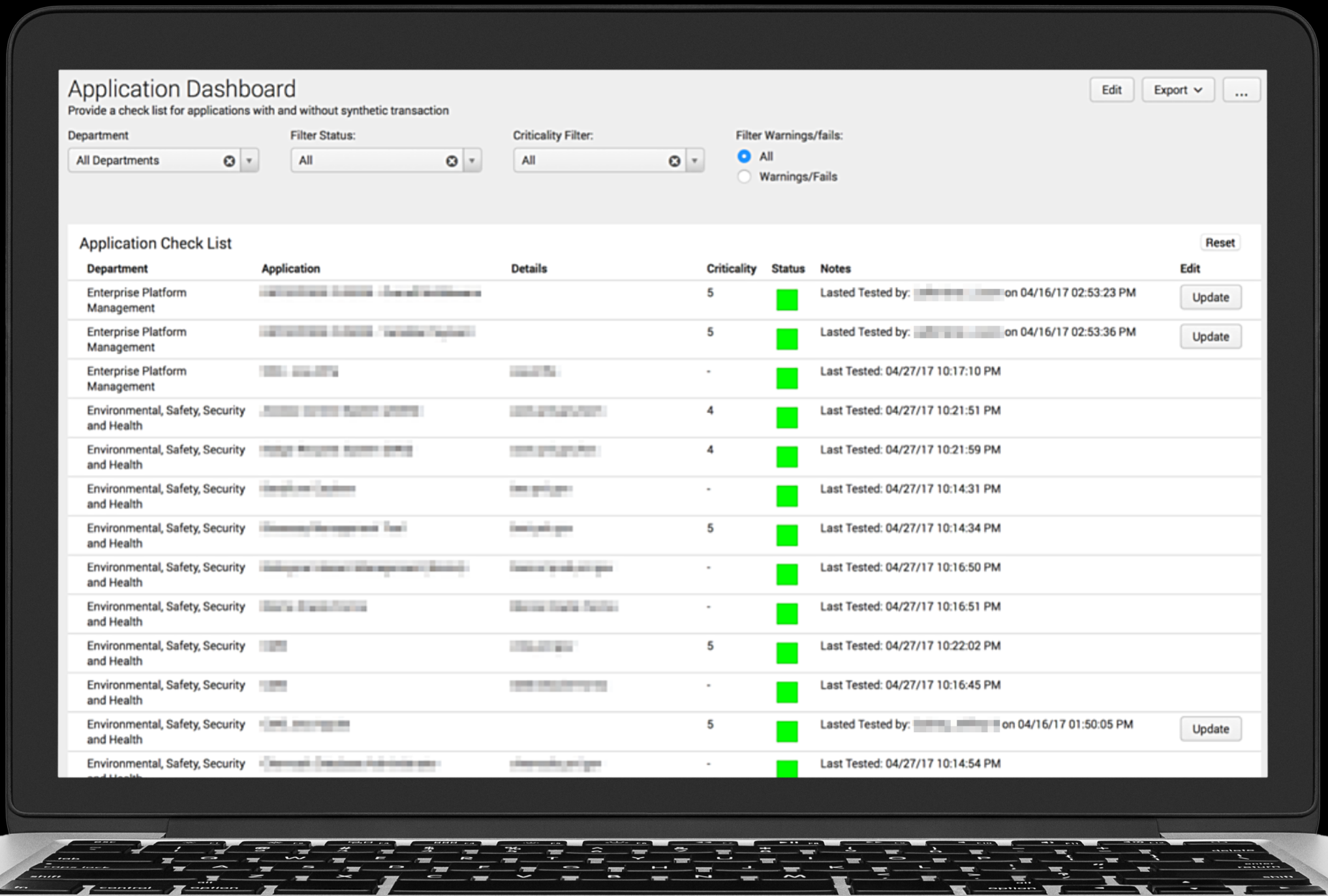
Status

Failed

Hide Filters

Patches with status: Failed

update	count
April, 2017 Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 7 and Windows Server 2008 R2 for x64 (KB4014985)	11
Security Update for Microsoft Silverlight (KB4017094)	4
April, 2017 Security Only Update for .NET Framework 2.0, 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Server 2008 SP2 (KB4014988)	2
April, 2017 Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB4014987)	2
April, 2017 Security and Quality Rollup for .NET Framework 2.0, 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Server 2008 SP2 (KB4014984)	2
April, 2017 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 7 and Windows Server 2008 R2 for x64 (KB4014981)	2
October, 2016 Security Only Update for .NET Framework 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 (KB3188736)	2
Update for Microsoft Visual Studio 2010 Tools for Office Runtime (KB2961149)	2
April, 2017 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4015549)	1
Cumulative Security Update for ActiveX Killbits for Windows Server 2008 R2 x64 Edition (KB2900986)	1
Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB4014661)	1
Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 Edition (KB3124275)	1



Application Dashboard

Provide a check list for applications with and without synthetic transaction

Edit | Export | ...

Department: All Departments

Filter Status: All

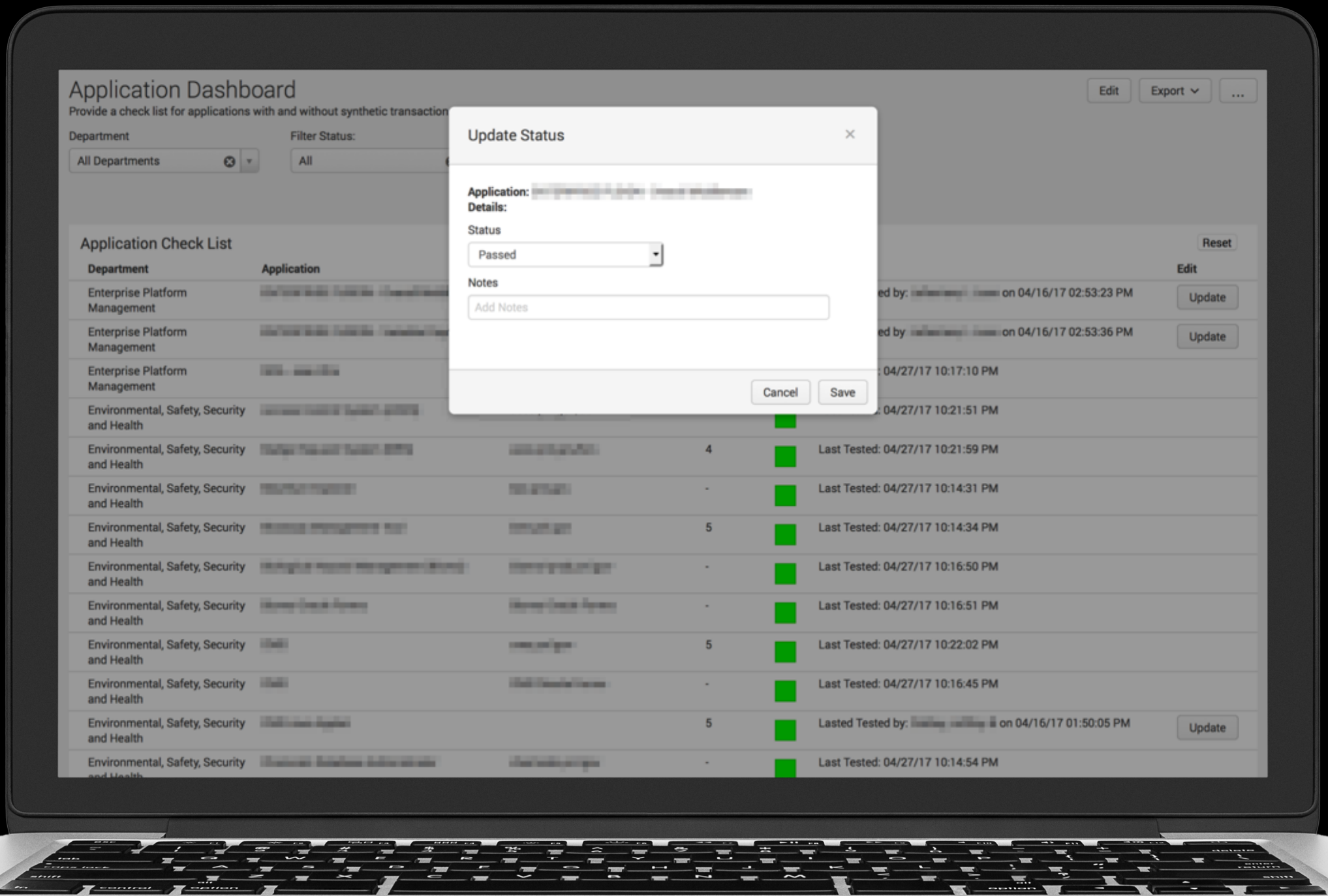
Criticality Filter: All

Filter Warnings/fails:
- (•) All
- ( ) Warnings/Fails

Application Check List

Reset

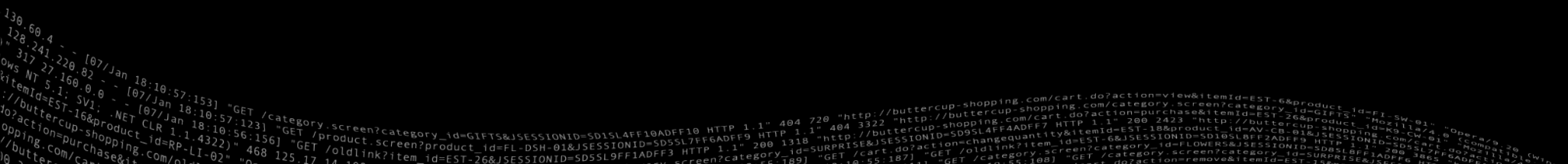
Department	Application	Details	Criticality	Status	Notes	Edit
Enterprise Platform Management			5		Lasted Tested by: on 04/16/17 02:53:23 PM	Update
Enterprise Platform Management			5		Lasted Tested by: on 04/16/17 02:53:36 PM	Update
Enterprise Platform Management			-		Last Tested: 04/27/17 10:17:10 PM	
Environmental, Safety, Security and Health			4		Last Tested: 04/27/17 10:21:51 PM	
Environmental, Safety, Security and Health			4		Last Tested: 04/27/17 10:21:59 PM	
Environmental, Safety, Security and Health			-		Last Tested: 04/27/17 10:14:31 PM	
Environmental, Safety, Security and Health			5		Last Tested: 04/27/17 10:14:34 PM	
Environmental, Safety, Security and Health			-		Last Tested: 04/27/17 10:16:50 PM	
Environmental, Safety, Security and Health			-		Last Tested: 04/27/17 10:16:51 PM	
Environmental, Safety, Security and Health			5		Last Tested: 04/27/17 10:22:02 PM	
Environmental, Safety, Security and Health			-		Last Tested: 04/27/17 10:16:45 PM	
Environmental, Safety, Security and Health			5		Lasted Tested by: on 04/16/17 01:50:05 PM	Update
Environmental, Safety, Security			-		Last Tested: 04/27/17 10:14:54 PM	



Where We Are Now

Explaining Why

- Centralized Reports
- Centralized Management Interfaces
- Centralized Alerts
- Time Savings



splunk> .conf2017

Where We Are Now

Time Savings

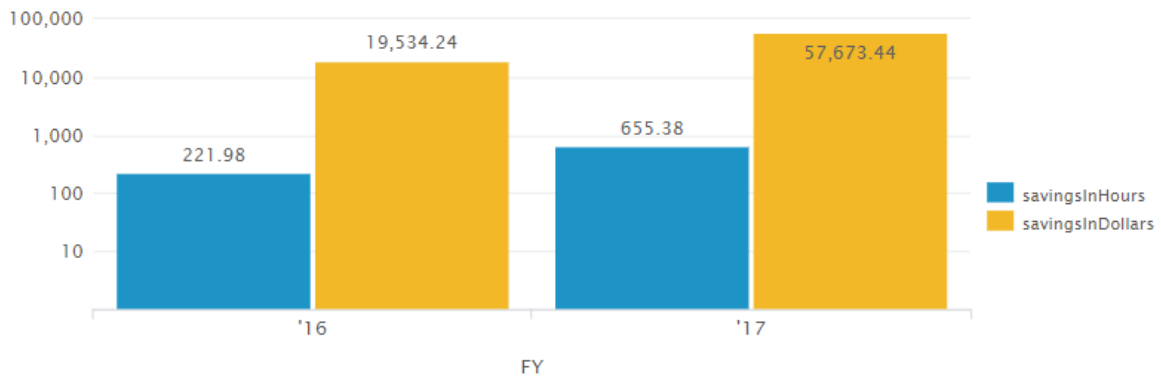
Time Savings on Patch Dashboard

Shows the ROI for the patch dashboard

Edit | Export | ...

Infrastructure Health | Monitoring | Reporting | Automation

Savings in Hours & Dollars by Fiscal Year



Savings in Hours & Dollars by Patch Dashboard

Dashboard	TotalRunCount	TotalHoursSaved	TotalDollarsSaved
application_dashboard	903	765.05	$67,324.40
it_platform_services_server_monitoring_for_patch_weekend	5923	98.72	$8,687.36
it_platform_services_host_patching_status	804	13.40	$1,179.20
it_platform_services_patch_report	12	0.20	$17.60

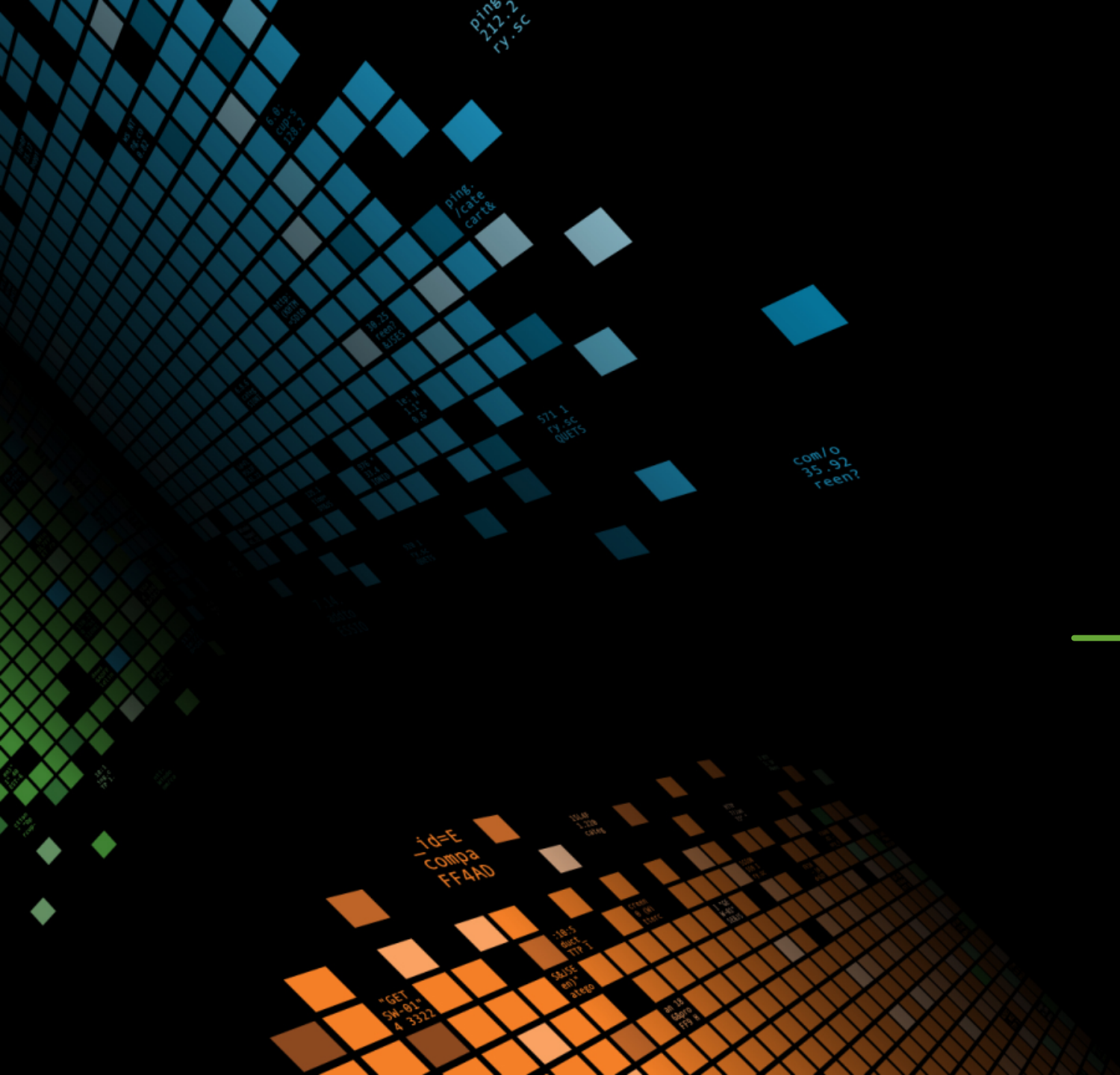
Total Raw Hours Saved Since FY15

877

Total Raw Hour Dollar Savings Since FY15

$77,207.68

splunk> .conf2017



How We Did It

Key Components

Writing Queries

Building Dashboards

splunk> .conf2017

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Justin Brown
justin@pnnl.gov
@theOtherJustinB

About Me

- IT Engineer
- Splunk Technical Lead
- Automation & Monitoring Team
- Joined PNNL in 2000

Key Components

Splunk

splunk>

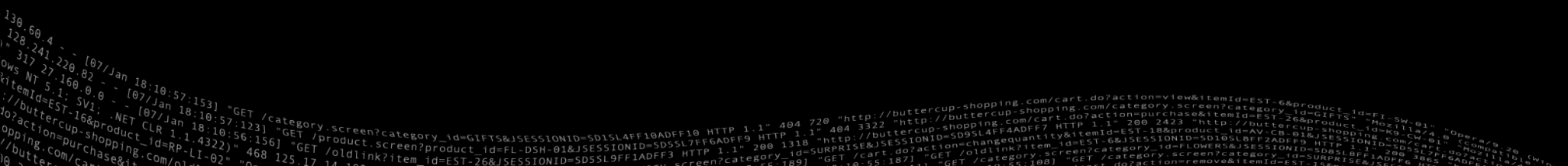
- All of our data in one place
- Reporting and visualization tools
- Monitoring and alerting capabilities
- Custom development features

Key Components

WLS (Windows Logging Service)

- Windows Logging Service (WLS)
  - Developed by Jason McCord at Kansas City National Security Campus
  - https://digirati82.com/wls-information

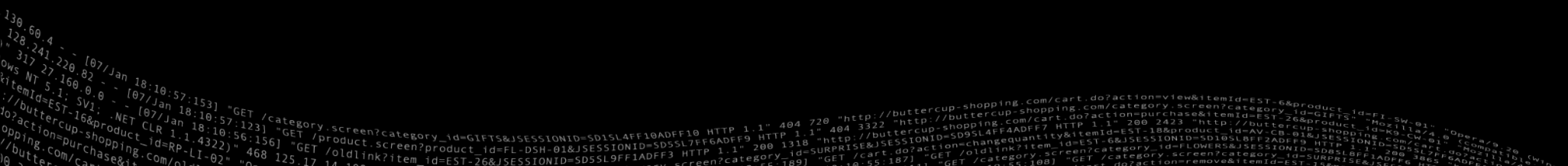
- Certificates
- Devices
- Drives
- File metadata
- File system changes
- Loaded Modules
- Named Pipes
- Performance Counters
- Port Monitoring
- Registry Changes
- Windows Objects
- WMI Queries



Key Components

Other Data Sources

- SCOM Alerts
- Universal Forwarder
  - IIS logs
- DBConnect
  - https://splunkbase.splunk.com/app/2686/
  - Database Connection testing

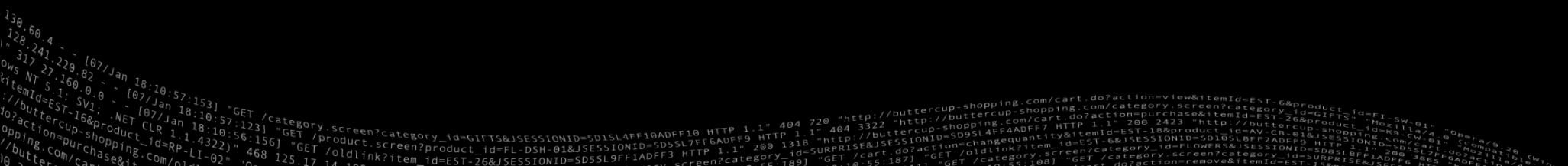


WARNING!

Writing the Queries

Things we need to know

- Is it patched?
  - False positives?
- Are there patches pending?
- Have patches failed?
- Has it rebooted?
  - Multiple times?
- Is it online?

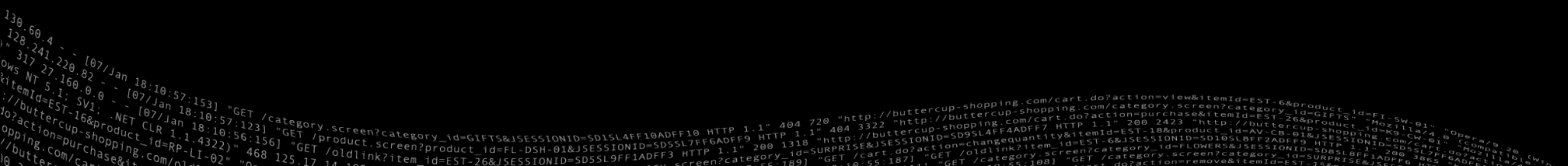


splunk> .conf2017

Writing the Queries

Getting Patch Status from Windows Events

- Updates Downloaded or Pending
  - EventID 18
  - EventID 41 or 44 (Windows Server 2016)
- Update Installation Events
  - EventID 19 – Success
  - EventID 20 – Failed
- Install Complete – Reboot Pending
  - EventID 21 or 22
- Event Collection Note
  - If you are using WLS, turn on the Backfill option



splunk> .conf2017

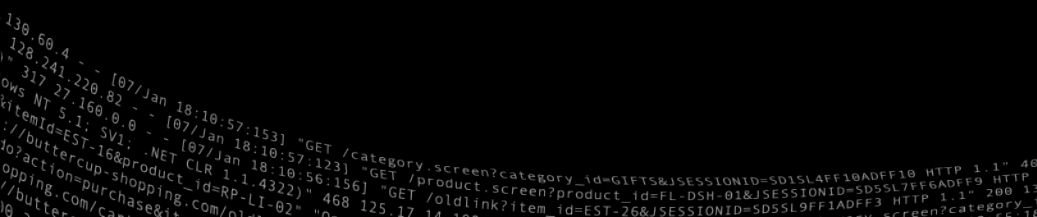
Writing the Queries

Detecting Reboots

- Using Windows Event Logs
  - Event ID 6005 indicates start up
- Using WMI queries in WLS
  - Collected every hour or on reboot
  - Includes last boot up time

```
source=wls:wmi OperatingSystem
```

host ^	os	Version	LastBootUpTime
[redacted]	Microsoft Windows Server 2012 R2 Standard	6.3.9600	20170416062613.379030-420



Writing the Queries

Narrowing results to just servers

- Servers seen online in the last 30 days

```
source=wls:wmi OperatingSystem ProductType>1
| dedup host | table host, Caption | rename Caption as os
| outputlookup windows_servers_discovered
```

- Servers online recently
  - Splunk keeps track of which systems are sending data
  - WLS sends updates at least every five minutes

```
| inputlookup windows_servers_discovered
| join host [| metadata type=hosts index=os
| where lastTime > relative_time(now(), "-2h") | fields host]
| outputlookup windows_servers_online
```

Writing the Queries

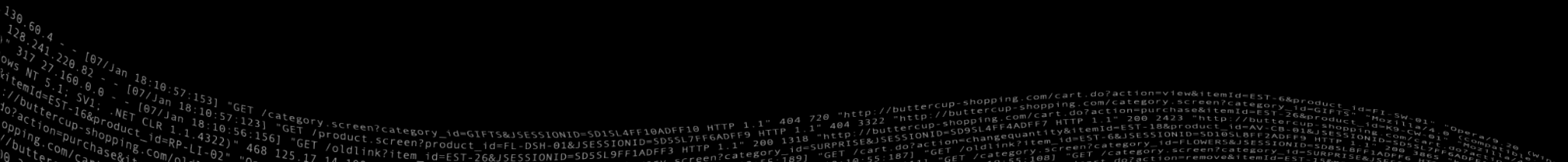
Putting it all together

```
index=os Microsoft-Windows-WindowsUpdateClient updatelist OR updateTitle NOT "EventID=\"17\"" NOT "EventID=\"43\"" NOT "Definition Update"
    [| inputlookup windows_servers_online | fields host]
| appendpipe
    [| search updatelist=* | stats latest(updatelist) as updatelist, latest(_time) as _time by host, EventID
    | makemv delim=";" updatelist
    | eval updateTitle = ltrim(updatelist,"- ")]
| rex field=updateTitle "^(?<update>[^\(]+\(KB\d+\))"
| append [| inputlookup windows_servers_online.csv | fields host | eval update="No Updates Found"]
| stats count(eval(EventID=19)) as install_primary,
    count(eval(EventID=21 OR EventID=22)) as install_backup,
    max(eval(if(EventID=19 OR EventID=21 OR EventID=22,_time,NULL))) as latest_install,
    count(eval(EventID=20)) as fail_count,
    max(eval(if(EventID=20,_time,NULL))) as latest_fail,
    max(eval(if((EventID==21 OR EventID==22),_time,NULL))) as latest_reboot_pending by host, update
| join type=left host
    [ search index=os source=wls:wmi OperatingSystem [| inputlookup windows_servers_online.csv | fields host]
    | addinfo
    | eval last_restart = strptime(LastBootUpTime,"%Y%m%d%H%M%S.%f")
    | stats latest(Caption) as os,
        max(last_restart) as last_restart,
        dc(eval(if(last_restart > info_min_time,last_restart,NULL))) as restart_count by host]
| eval pending_reboot = if(latest_reboot_pending > last_restart, 1, 0)
| eval install_count = if(install_primary==0,install_backup,install_primary)
| join type=left host
    [| metadata type=hosts index=os | fields host, lastTime]
| eval online=if(lastTime > relative_time(now(),"-60m"),1,0)
| eventstats count(eval(update!="No Updates Found")) as real_updates by host
| search real_updates=0 OR update!="No Updates Found"
| eval patch_status = case(real_updates==0, 1, install_count > 2, 3, install_count > 0,0, fail_count == 0, 2, fail_count > 0, 4)
```

Writing the Queries

Breaking it down

```
index=os Microsoft-Windows-WindowsUpdateClient updatelist OR updateTitle NOT
"EventID=\"17\"" NOT "EventID=\"43\"" NOT "Definition Update"
    [| inputlookup windows_servers_online | fields host]
| appendpipe
    [| search updatelist=*
    | stats latest(updatelist) as updatelist, latest(_time) as _time by host, EventID
    | makemv delim=";" updatelist
    | eval updateTitle = ltrim(updatelist,"- ")]
| rex field=updateTitle "^(?<update>[^\(]+\(KB\d+\))"
| append
    [| inputlookup windows_servers_online.csv
    | fields host
    | eval update="No Updates Found"]
```



splunk> .conf2017

Writing the Queries

Breaking it down

_time	host	EventID	updatelist	updateTitle	update
9/14/17 12:42	sample	18	- Microsoft Visual Studio 2010 Service Pack 1 - 2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)	Microsoft Visual Studio 2010 Service Pack 1 2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)	2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)
9/14/17 13:39	sample	19		2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)	2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)
9/14/17 13:19	sample	20		Microsoft Visual Studio 2010 Service Pack 1	
9/14/17 9:15	sample	20		2017-09 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4038777)	2017-09 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4038777)
9/14/17 13:35	sample	21	- 2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)	2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)	2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)
9/13/17 13:09	sample	41		Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - September 2017 (KB890830)	Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - September 2017 (KB890830)
9/13/17 13:09	sample	44		Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - September 2017 (KB890830)	Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - September 2017 (KB890830)

Search Tip

Searching raw text is faster than non-indexed fields

splunk> App: Search & Reporting | Brown, Justin | Messages | Settings | Activity | Help | Find

Search | Datasets | Reports | Alerts | Dashboards | Search & Reporting

New Search

Save As | Close

```
1  index=os ProviderName="Microsoft-Windows-WindowsUpdateClient" updatelist=* OR updateTitle=* NOT EventID=17 NOT EventID=43
2      [| inputlookup windows_servers_online.csv | fields host]
3  | fields _time, host, EventID, updatelist, updateTitle
4  | appendpipe
5      [| stats latest(updatelist) as updatelist, latest(_time) as _time by host, EventID
6      | makemv delim=";" updatelist
7      | eval updateTitle = ltrim(updatelist,"- ") ]
8  | rex field=updateTitle "^(?<update>[^\(]+\(KB\d+\))"
9  | inputlookup windows_servers_online.csv append=t
10 | fillnull value="No Updates Found" update
```

from Jul 11 through ...

✓ 48,120 events (7/11/17 12:00:00.000 AM to 7/25/17 12:00:00.000 AM) No Event Sampling | Job | Smart Mode

Search job inspector

This search has completed and has returned **50,497** results by scanning **5,801,048** events in **554.121** seconds

(SID: 1502232189.1705199) search.log

Search Tip

Searching raw text is faster than non-indexed fields

i	Time	Event
>	8/9/17 8:03:41.000 AM	Aug 9 08:03:41 [redacted] System: LogType="WLS",Channel="System", Computer="[redacted]", EventID="18", EventRecordID="386914", ExecutionProcessID="904", ExecutionThreadID="5028", Keywords="0x8000000000000014", Level="4", Opcode="12", ProviderGuid="{945A8954-C147-4ACD-923F-40C45405A658}", ProviderName="Microsoft-Windows-WindowsUpdateClient", schedinstalldate="Sunday, August 13, 2017", schedinstalltime="10:00 AM", SecurityUserID="S-1-5-18", SecurityUserName="NT AUTHORITY\SYSTEM", Task="2", updatelist="- 2017-07 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4025341);- Cumulative Security Update for Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems (KB4034733);- 2017-08 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB4034679)", Version="0" index = os ¦ source = wls:system ¦ sourcetype = syslog

i	Time	Event
>	8/9/17 1:33:45.000 AM	Aug 9 01:33:45 [redacted] System: LogType="WLS", Channel="System", Computer="[redacted]", EventID="19", EventRecordID="432430", ExecutionProcessID="472", ExecutionThreadID="2100", Keywords="0x8000000000000018", Level="4", Opcode="13", ProviderGuid="{945a8954-c147-4acd-923f-40c45405a658}", ProviderName="Microsoft-Windows-WindowsUpdateClient", SecurityUserID="S-1-5-18", SecurityUserName="NT AUTHORITY\SYSTEM", Task="1", updateGuid="{1BC66974-0122-4176-B17D-D1B99BF8EA0B}", updateRevisionNumber="200", updateTitle="Security Update for Windows Server 2008 for x64-based Systems (KB4022750)", Version="0" index = os ¦ source = wls:system ¦ sourcetype = syslog

```
index=os ProviderName="Microsoft-Windows-WindowsUpdateClient" updatelist=* OR updateTitle=* NOT EventID=17 NOT EventID=43
```

```
index=os Microsoft-Windows-WindowsUpdateClient updatelist OR updateTitle NOT "EventID=\"17\"" NOT "EventID=\"43\""
```

Search Tip

Searching raw text is faster than non-indexed fields

- Before

Search job inspector

This search has completed and has returned **50,497** results by scanning **5,801,048** events in **554.121** seconds

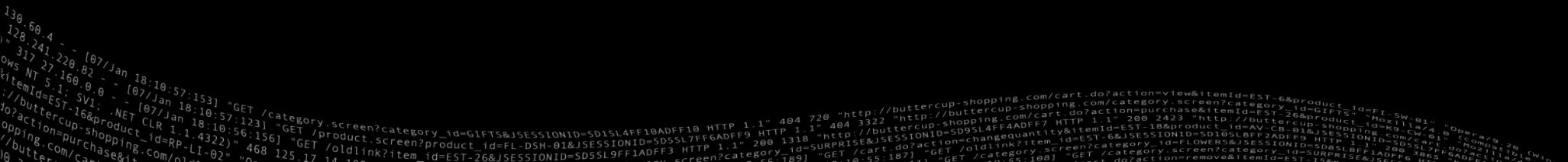
(SID: 1502232189.1705199) search.log

- After

Search job inspector

This search has completed and has returned **50,497** results by scanning **77,544** events in **85.945** seconds

(SID: 1502233019.1705940) search.log

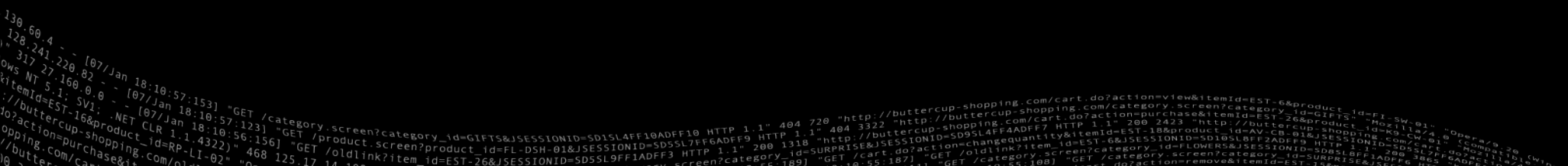


splunk> .conf2017

Writing the Queries

Breaking it down

```
| stats count(eval(EventID=19)) as install_primary,
    count(eval(EventID=21 OR EventID=22)) as install_backup,
    max(eval(if(EventID=19 OR EventID=21 OR EventID=22,_time,NULL))) as latest_install,
    count(eval(EventID=20)) as fail_count,
    max(eval(if(EventID=20,_time,NULL))) as latest_fail,
    max(eval(if((EventID==21 OR EventID==22),_time,NULL))) as latest_reboot_pending by host, update
```



splunk> .conf2017

Writing the Queries

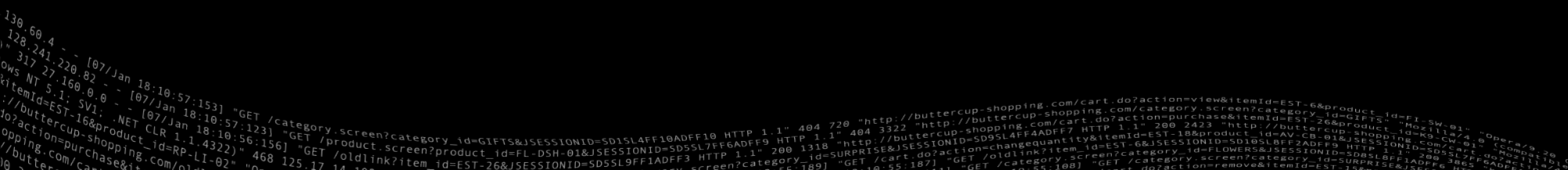
Breaking it down

host	update	install_primary	install_backup	latest_install	fail_count	latest_fail	latest_reboot_pending
sample1	No Updates Found	0	0		0		
sample2	2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)	3	1	1505325478	0		1505317194
sample2	2017-09 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4038793)	1	1	1505324961	0		1505317194
sample2	2017-09 Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7 on Windows 8.1 and Server 2012 R2 for x64 (KB4041092)	1	1	1505324961	0		1505317194
sample2	Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB4036586)	1	1	1505324962	0		1505317194
sample2	Update for Windows Server 2012 R2 (KB4033428)	1	1	1505324961	0		1505317194
sample2	No Updates Found	0	0		0		
sample3	2017-08 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4034664)	1	1	1505400183	0		1505399639
sample3	2017-09 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB4038779)	0	0		1	1505399639	
sample3	2017-09 Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7 on Windows 7 and Server 2008 R2 for x64 (KB4041090)	1	1	1505400183	0		1505399639
sample3	2017-09 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7 on Windows 7 and Server 2008 R2 for x64 (KB4041083)	1	1	1505400183	0		1505399639
sample3	Cumulative Security Update for Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems (KB4036586)	1	1	1505400183	0		1505399639
sample3	No Updates Found	0	0		0		

Writing the Queries

Breaking it down

```
| join type=left host
    [ search index=os source=wls:wmi OperatingSystem [| inputlookup
windows_servers_online.csv | fields host]
    | addinfo
    | eval last_restart = strptime(LastBootUpTime,"%Y%m%d%H%M%S.%f")
    | stats latest(Caption) as os,
        max(last_restart) as last_restart,
        dc(eval(if(last_restart > info_min_time,last_restart,NULL))) as restart_count
        by host]
```



Writing the Queries

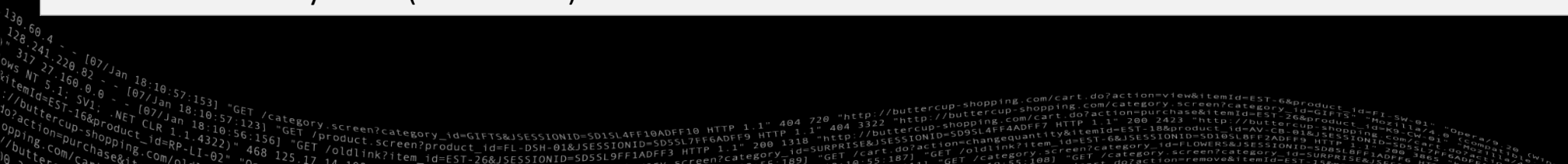
Breaking it down

```
| eval pending_reboot = if(latest_reboot_pending > last_restart, 1, 0)
| eval install_count = if(install_primary==0,install_backup,install_primary)
| join type=left host
    [| metadata type=hosts index=os | fields host, lastTime]
| eval online=if(lastTime > relative_time(now(),"-60m"),1,0)
| eventstats count(eval(update!="No Updates Found")) as real_updates by host
| search real_updates=0 OR update!="No Updates Found"
| eval patch_status = case(
    real_updates == 0, 1,
    install_count > 2, 3,
    install_count > 0, 0,
    fail_count   == 0, 2,
    fail_count    > 0, 4)
```

Writing the Queries

Breaking it down

host	update	install_primary	install_backup	install_count
sample1	No Updates Found	0	0	0
sample2	2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)	1	1	1
sample2	2017-09 Security Update for Adobe Flash Player for Windows Server 2012 R2 for x64-based Systems (KB4038806)	1	1	1
sample2	2017-09 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7 on Windows 8.1 and Server 2012 R2 for x64 (KB4041085)	1	1	1
sample2	Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB4036586)	1	1	1
sample2	Update for Windows Server 2012 R2 (KB4033428)	1	1	1
sample3	2017-08 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4034664)	1	1	1
sample3	2017-09 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB4038779)	0	0	0



splunk> .conf2017

Search Tip

Using the LOADJOB command

splunk> App: Search & Reporting | Brown, Justin | Messages | Settings | Activity | Help | Find

Search | Datasets | Reports | Alerts | Dashboards | Search & Reporting

New Search

Save As | Close

```
1  index=os Microsoft-Windows-WindowsUpdateClient updatelist OR updateTitle NOT "EventID=\"17\"" NOT "EventID=\"43\""
2      [| inputlookup windows_servers_online.csv | fields host]
3  | fields _time, host, EventID, updatelist, updateTitle
4  | appendpipe
5      [| stats latest(updatelist) as updatelist, latest(_time) as _time by host, EventID
6      | makemv delim=";" updatelist
7      | eval updateTitle = ltrim(updatelist,"- ") ]
8  | rex field=updateTitle "^(?<update>[^\(]+\(KB\d+\))"
9  | inputlookup windows_servers_online.csv append=t
10 | fillnull value="No Updates Found" update
```

from Jul 11 through ...

✓ 48,120 events (7/11/17 12

Smart Mode

Search job inspector

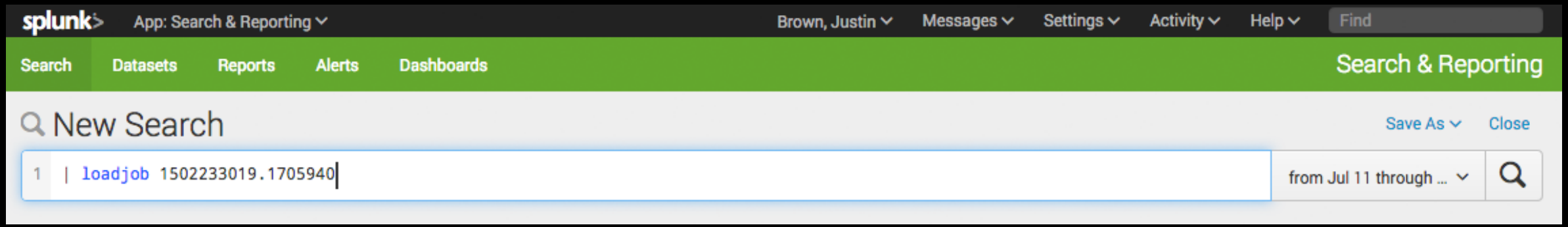
This search has completed and has returned **50,497** results by scanning **77,544** events in **85.945** seconds

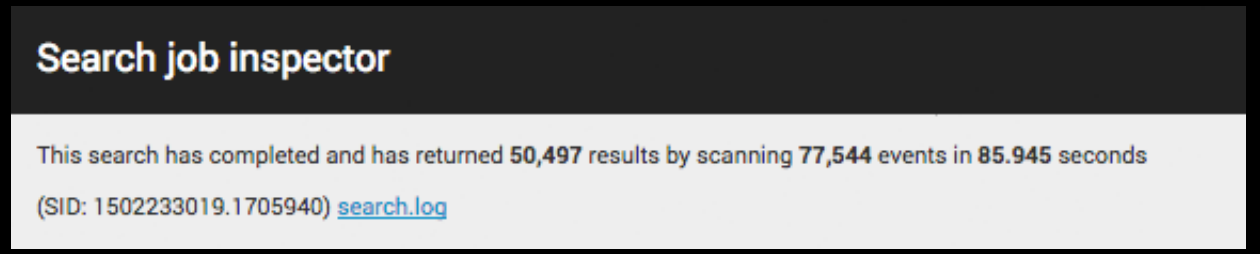
(SID: 1502233019.1705940) search.log

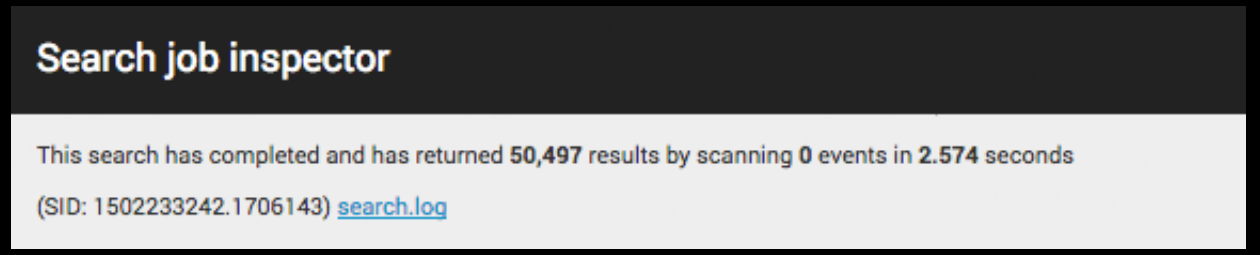
splunk> .conf2017

Search Tip

Using the LOADJOB command







splunk> .conf2017

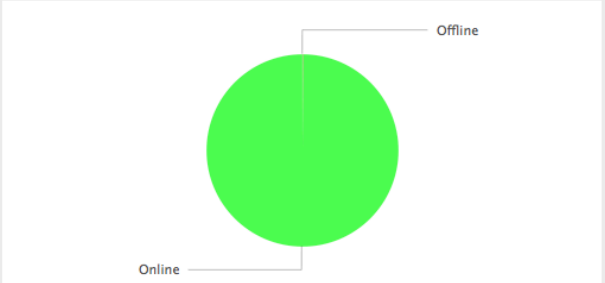
IT - Platform Services - Server Monitoring for Patch Weekend

Edit | More Info

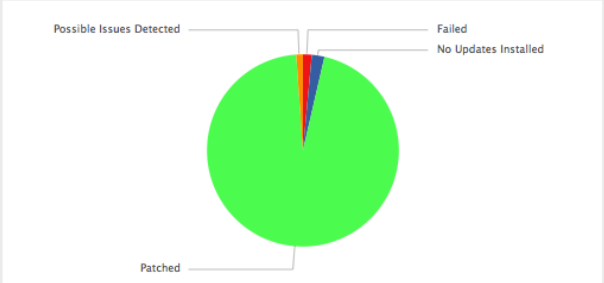
Need Help?

Show Icon Key

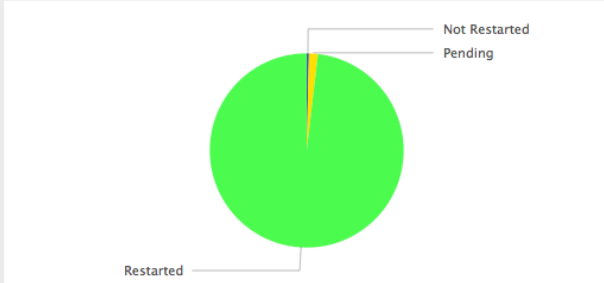
Servers Online



Servers Patched



Servers Restarted



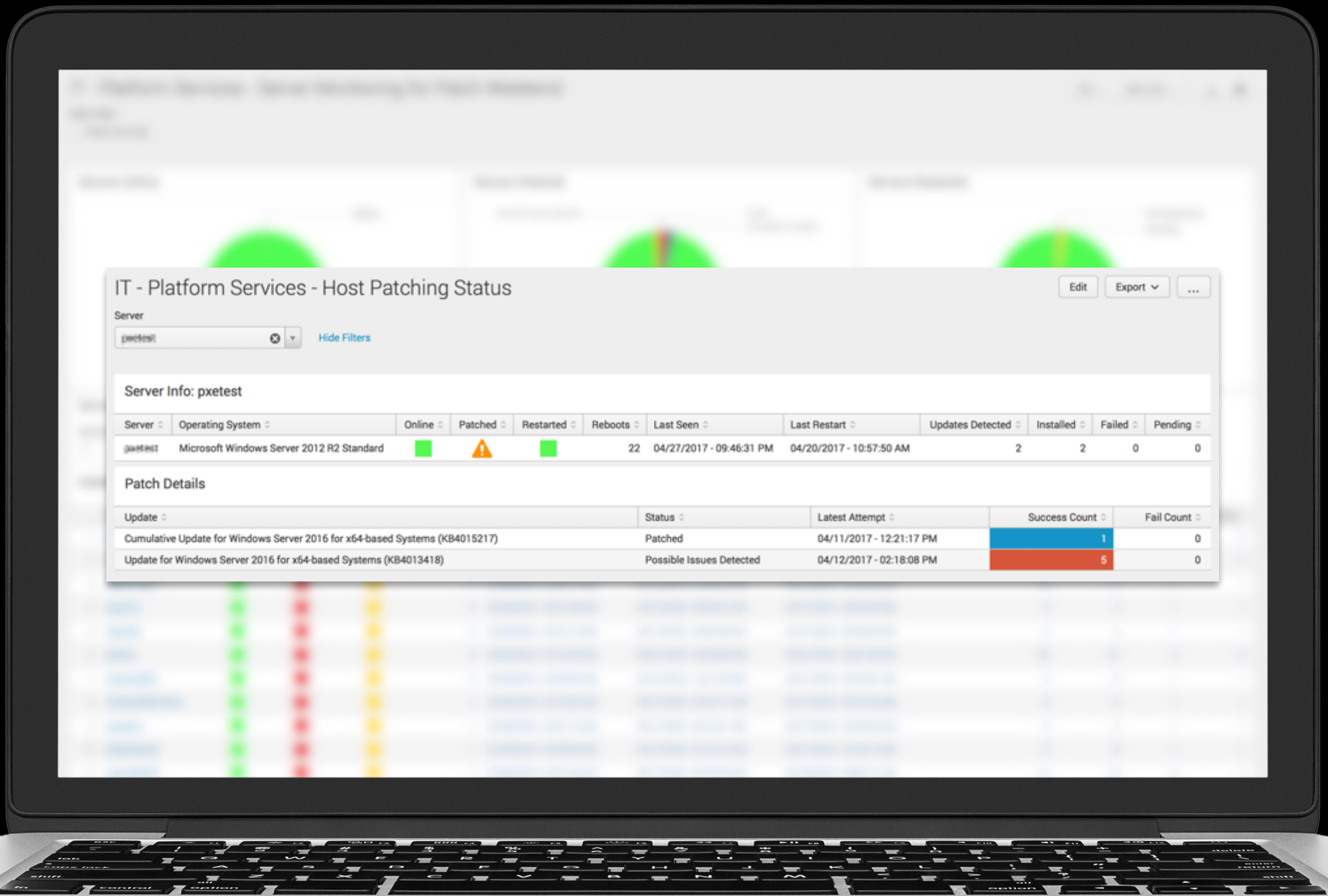
Server Details

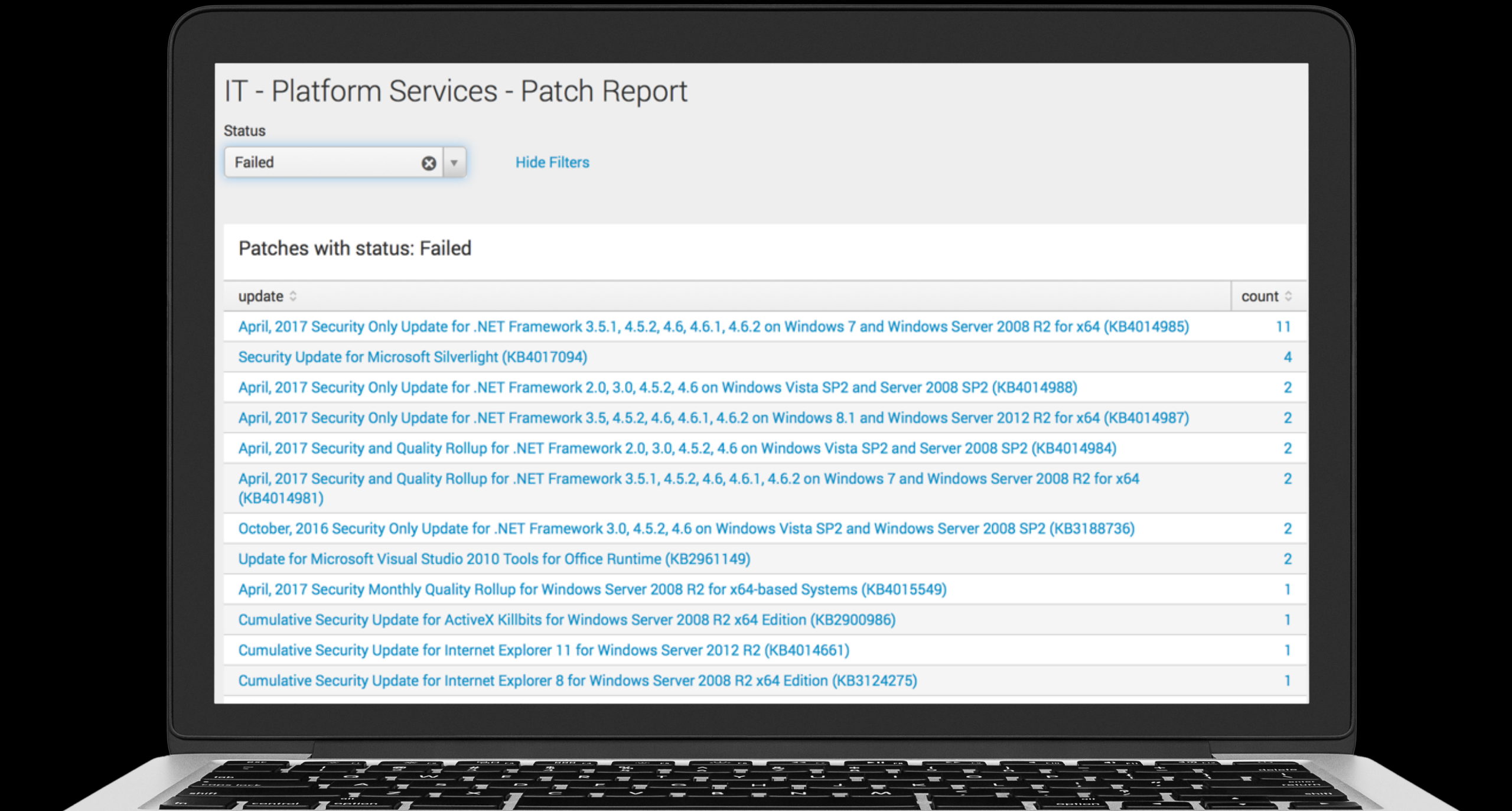
Specify Server

*

Includes Windows 2008 & 2012 Servers

	Server	Online	Patched	Restarted	Reboots	Last Seen	Last Restart	Latest Install	Updates Attempted	Installed	Failed	Pending
1					1	04/25/2016 - 05:15:54 AM	04/17/2016 - 03:09:40 AM	-	0	0	0	0
2					2	04/26/2016 - 05:21:01 AM	04/18/2016 - 10:28:50 AM	04/18/2016 - 10:14:51 AM	9	7	2	2
3					3	04/26/2016 - 05:20:14 AM	04/14/2016 - 07:36:16 PM	04/14/2016 - 07:45:43 PM	18	17	1	1
4					3	04/26/2016 - 05:21:00 AM	04/17/2016 - 09:45:47 AM	04/17/2016 - 03:26:44 AM	5	4	1	1
5					3	04/26/2016 - 05:21:19 AM	04/17/2016 - 09:42:48 AM	04/17/2016 - 03:25:20 AM	5	4	1	1
6					6	04/26/2016 - 05:15:25 AM	04/21/2016 - 03:45:56 PM	04/21/2016 - 03:51:49 PM	23	21	2	2
7					3	04/26/2016 - 05:20:54 AM	04/17/2016 - 10:21:28 AM	04/17/2016 - 03:19:51 AM	6	5	1	1
8					1	04/26/2016 - 05:19:53 AM	04/17/2016 - 03:16:17 AM	04/17/2016 - 03:27:40 AM	6	5	1	1
9					1	04/26/2016 - 05:21:10 AM	04/17/2016 - 03:12:51 AM	04/17/2016 - 03:24:03 AM	5	4	1	1
10					1	04/26/2016 - 05:20:56 AM	04/17/2016 - 07:10:12 AM	04/17/2016 - 07:20:13 AM	9	8	1	1
11					1	04/26/2016 - 05:21:35 AM	04/17/2016 - 05:15:29 AM	04/18/2016 - 08:39:11 AM	12	10	2	2





IT - Platform Services - Patch Report

Status

Failed

Hide Filters

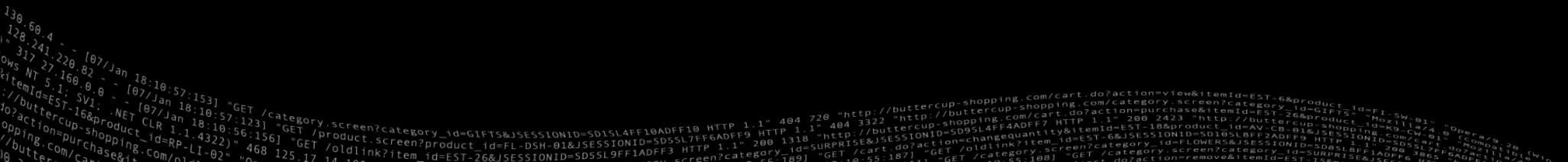
Patches with status: Failed

update	count
April, 2017 Security Only Update for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 7 and Windows Server 2008 R2 for x64 (KB4014985)	11
Security Update for Microsoft Silverlight (KB4017094)	4
April, 2017 Security Only Update for .NET Framework 2.0, 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Server 2008 SP2 (KB4014988)	2
April, 2017 Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 8.1 and Windows Server 2012 R2 for x64 (KB4014987)	2
April, 2017 Security and Quality Rollup for .NET Framework 2.0, 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Server 2008 SP2 (KB4014984)	2
April, 2017 Security and Quality Rollup for .NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 7 and Windows Server 2008 R2 for x64 (KB4014981)	2
October, 2016 Security Only Update for .NET Framework 3.0, 4.5.2, 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 (KB3188736)	2
Update for Microsoft Visual Studio 2010 Tools for Office Runtime (KB2961149)	2
April, 2017 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB4015549)	1
Cumulative Security Update for ActiveX Killbits for Windows Server 2008 R2 x64 Edition (KB2900986)	1
Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB4014661)	1
Cumulative Security Update for Internet Explorer 8 for Windows Server 2008 R2 x64 Edition (KB3124275)	1

Building the Dashboards

Use Base Searches

```
<form script="server_status.js" stylesheet="server_status.css" refresh="600">
<label>IT - Platform Services - Server Monitoring for Patch Weekend</label>
<search id="monitoring” ref="patch_monitoring_report"></search>
```



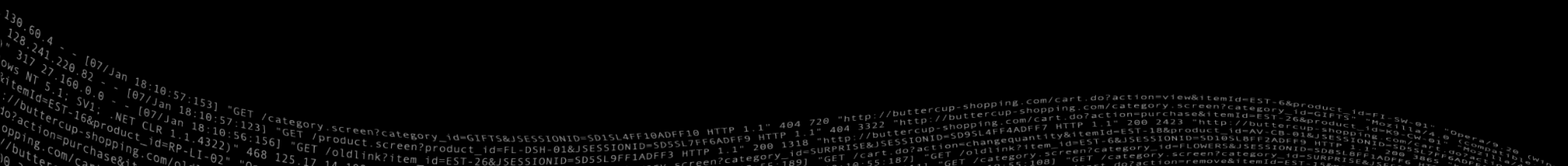
splunk> .conf2017

Building the Dashboards

Custom Icons

```
<form script="server_status.js" stylesheet="server_status.css" refresh="600">
<label>IT - Platform Services - Server Monitoring for Patch Weekend</label>
<search id="monitoring” ref="patch_monitoring_report"></search>
```

- File location:
  - $SPLUNK_HOME$/etc/apps/<your app name>/appserver/static



splunk> .conf2017

Building the Dashboards

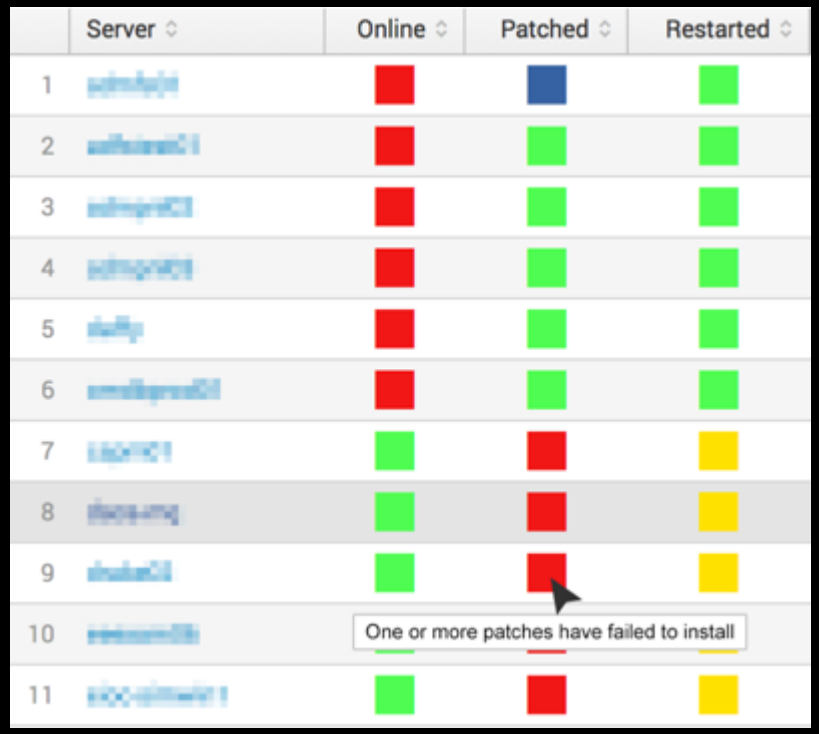
Custom Icons

- server_status.js

```
require([
» 'underscore',
» 'jquery',
» 'splunkjs/mvc',
» 'splunkjs/mvc/tableview',
» 'splunkjs/mvc/simplexml/ready!'
], function(_, $, mvc, TableView) {

» var ICONS = {
» » 0: 'box-filled',
» » 1: 'box-filled',
» » 2: 'box-filled',
» » 3: 'alert',
» » 4: 'box-filled'
» };

» var TITLES = {
» » 'Patched': {
» » » 0: 'All Patches Installed!',
» » » 1: 'No patches detected',
» » » 2: 'Patches detected and pending install',
» » » 3: 'An individual patch has "successfully" installed multiple times',
» » » 4: 'One or more patches have failed to install'
» » },
```



splunk> .conf2017

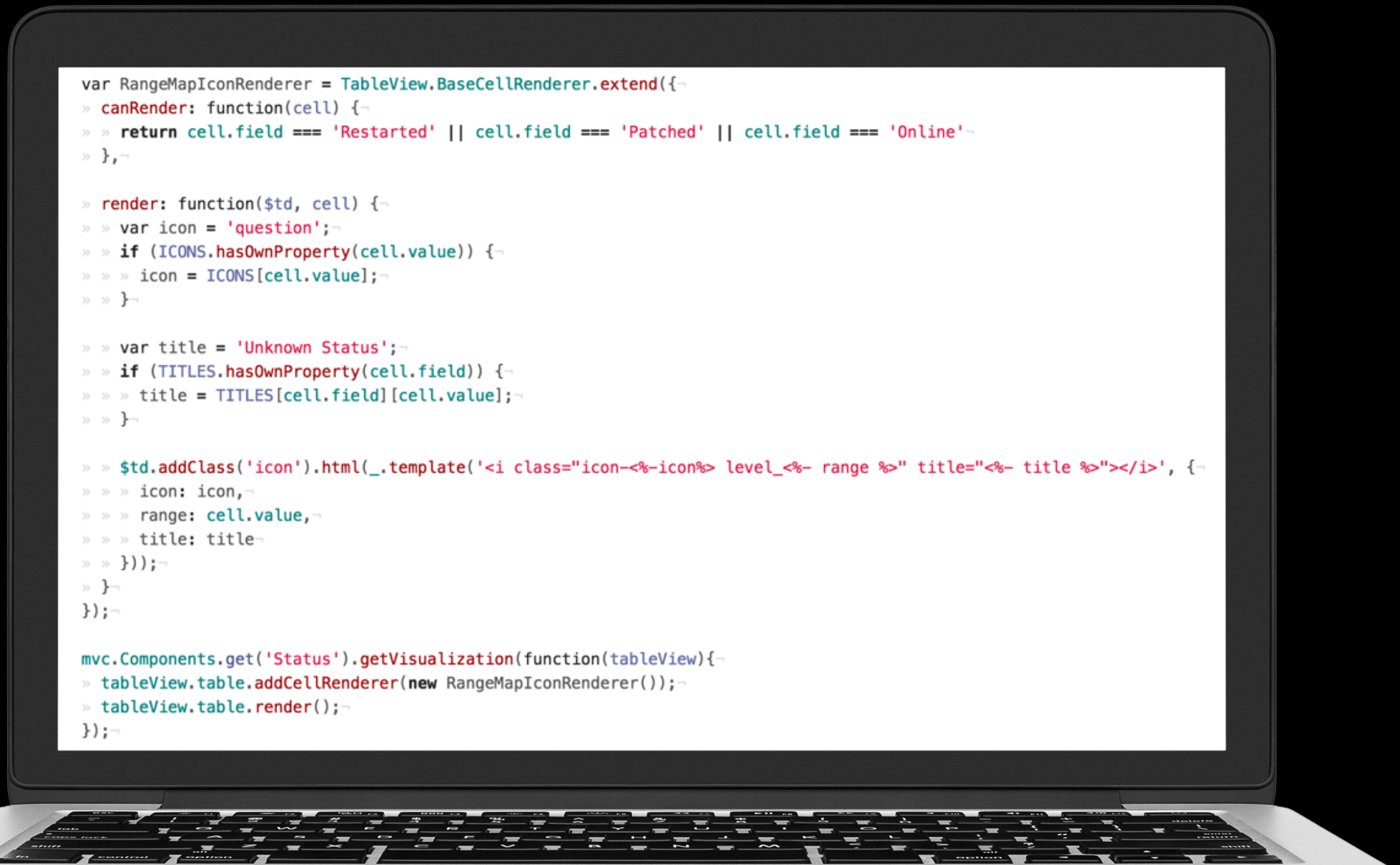
```
require([
» 'underscore',
» 'jquery',
» 'splunkjs/mvc',
» 'splunkjs/mvc/tableview',
» 'splunkjs/mvc/simplexml/ready!'
], function(_, $, mvc, TableView) {

» var ICONS = {
» » 0: 'box-filled',
» » 1: 'box-filled',
» » 2: 'box-filled',
» » 3: 'alert',
» » 4: 'box-filled'
» };

» var TITLES = {
» » 'Patched': {
» » » 0: 'All Patches Installed!',
» » » 1: 'No patches detected',
» » » 2: 'Patches detected and pending install',
» » » 3: 'An individual patch has "successfully" installed multiple times',
» » » 4: 'One or more patches have failed to install'
» » },
» » 'Online': {
» » » 0: 'Server is regularly checking in',
```

	Server	Online	Patched	Restarted
1	[redacted]			
2	[redacted]			
3	[redacted]			
4	[redacted]			
5	[redacted]			
6	[redacted]			
7	[redacted]			
8	[redacted]			
9	[redacted]			
10	[redacted]			
11	[redacted]			

One or more patches have failed to install



```
var RangeMapIconRenderer = TableView.BaseCellRenderer.extend({
    canRender: function(cell) {
        return cell.field === 'Restarted' || cell.field === 'Patched' || cell.field === 'Online'
    },

    render: function($td, cell) {
        var icon = 'question';
        if (ICONS.hasOwnProperty(cell.value)) {
            icon = ICONS[cell.value];
        }

        var title = 'Unknown Status';
        if (TITLES.hasOwnProperty(cell.field)) {
            title = TITLES[cell.field][cell.value];
        }

        $td.addClass('icon').html(_.template('<i class="icon-<%-icon%> level_<%- range %>" title="<%- title %>"></i>', {
            icon: icon,
            range: cell.value,
            title: title
        }));
    }
});

mvc.Components.get('Status').getVisualization(function(tableView){
    tableView.table.addCellRenderer(new RangeMapIconRenderer());
    tableView.table.render();
});
```

Building the Dashboards

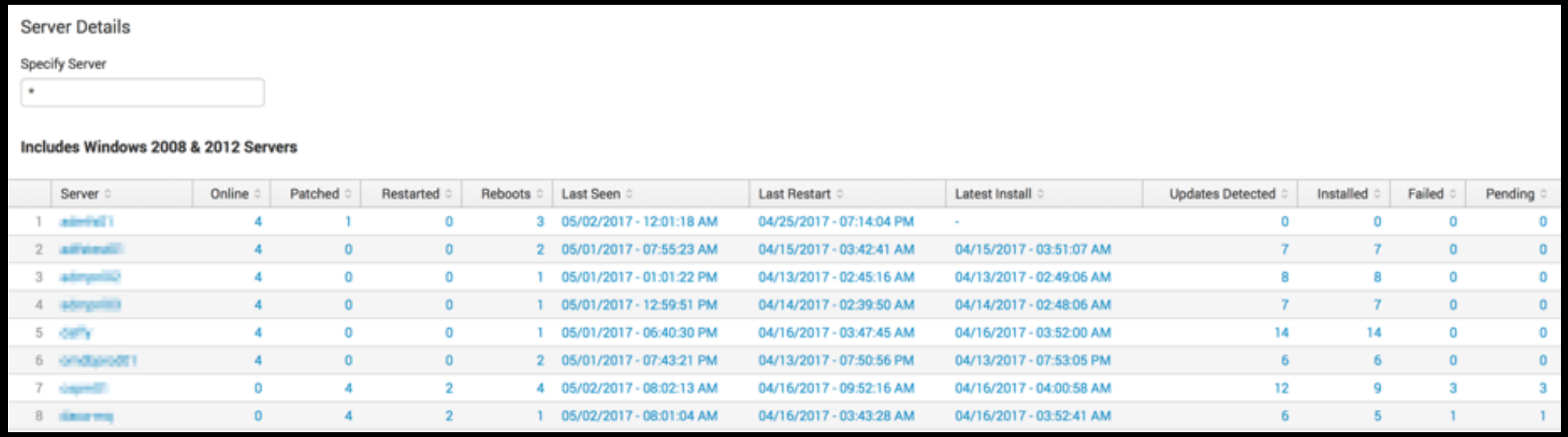
Set the ID of the table

```
<row>
  <panel>
    <title>Server Details</title>
    <table id="Status">
      <title>Includes Windows 2008 &amp;amp; 2012 Servers</title>
      <search base="monitoring">
      ....
```

Building the Dashboards

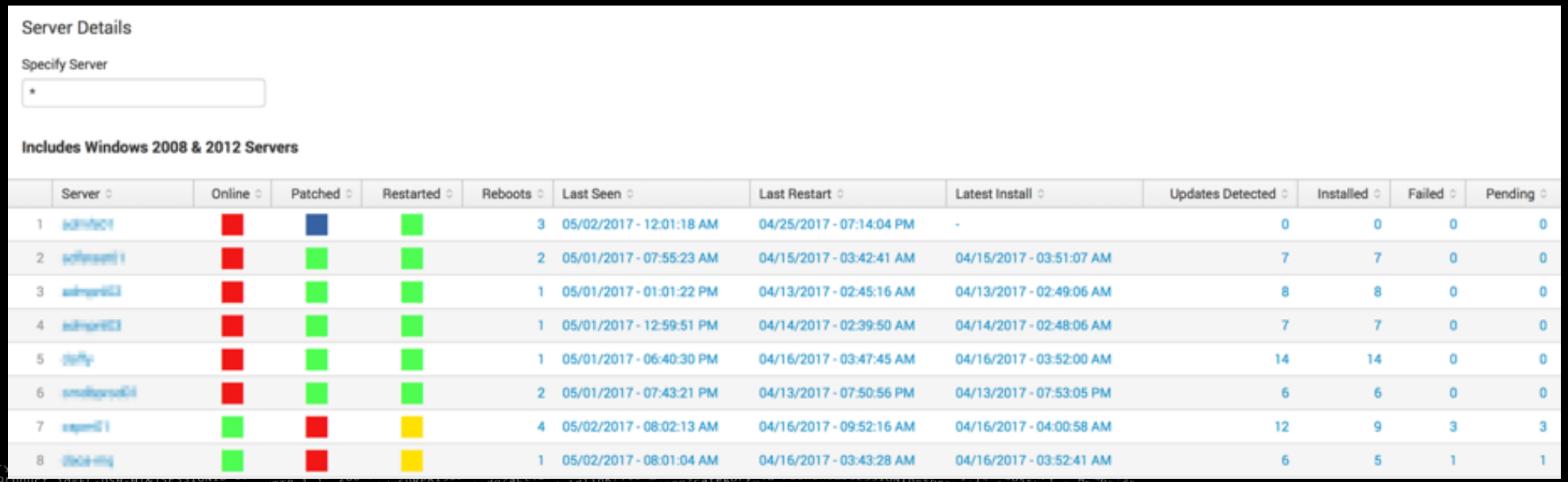
Custom Icons

Before



	Server	Online	Patched	Restarted	Reboots	Last Seen	Last Restart	Latest Install	Updates Detected	Installed	Failed	Pending
1	[redacted]	4	1	0	3	05/02/2017 - 12:01:18 AM	04/25/2017 - 07:14:04 PM	-	0	0	0	0
2	[redacted]	4	0	0	2	05/01/2017 - 07:55:23 AM	04/15/2017 - 03:42:41 AM	04/15/2017 - 03:51:07 AM	7	7	0	0
3	[redacted]	4	0	0	1	05/01/2017 - 01:01:22 PM	04/13/2017 - 02:45:16 AM	04/13/2017 - 02:49:06 AM	8	8	0	0
4	[redacted]	4	0	0	1	05/01/2017 - 12:59:51 PM	04/14/2017 - 02:39:50 AM	04/14/2017 - 02:48:06 AM	7	7	0	0
5	[redacted]	4	0	0	1	05/01/2017 - 06:40:30 PM	04/16/2017 - 03:47:45 AM	04/16/2017 - 03:52:00 AM	14	14	0	0
6	[redacted]	4	0	0	2	05/01/2017 - 07:43:21 PM	04/13/2017 - 07:50:56 PM	04/13/2017 - 07:53:05 PM	6	6	0	0
7	[redacted]	0	4	2	4	05/02/2017 - 08:02:13 AM	04/16/2017 - 09:52:16 AM	04/16/2017 - 04:00:58 AM	12	9	3	3
8	[redacted]	0	4	2	1	05/02/2017 - 08:01:04 AM	04/16/2017 - 03:43:28 AM	04/16/2017 - 03:52:41 AM	6	5	1	1

After

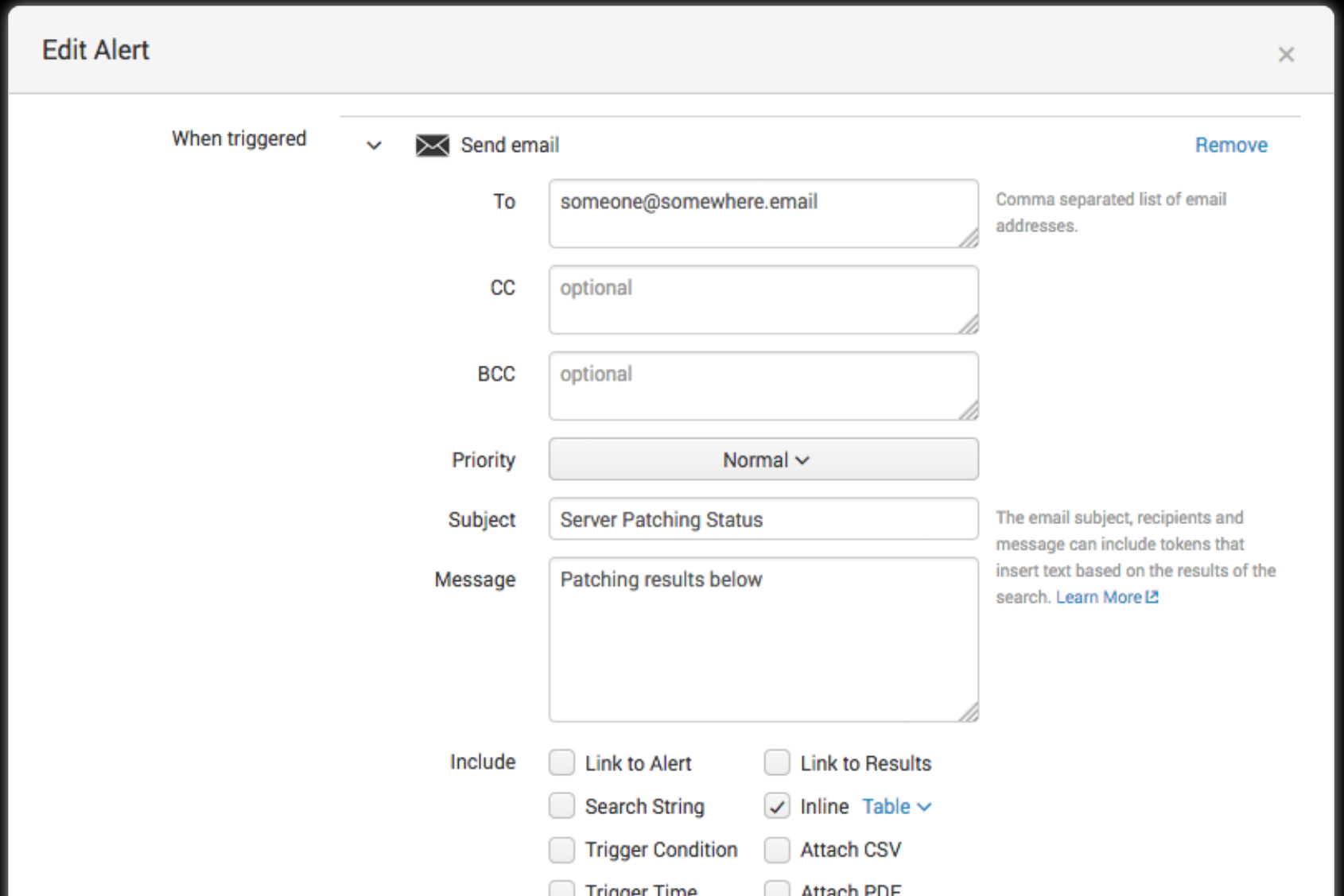


	Server	Online	Patched	Restarted	Reboots	Last Seen	Last Restart	Latest Install	Updates Detected	Installed	Failed	Pending
1	[redacted]				3	05/02/2017 - 12:01:18 AM	04/25/2017 - 07:14:04 PM	-	0	0	0	0
2	[redacted]				2	05/01/2017 - 07:55:23 AM	04/15/2017 - 03:42:41 AM	04/15/2017 - 03:51:07 AM	7	7	0	0
3	[redacted]				1	05/01/2017 - 01:01:22 PM	04/13/2017 - 02:45:16 AM	04/13/2017 - 02:49:06 AM	8	8	0	0
4	[redacted]				1	05/01/2017 - 12:59:51 PM	04/14/2017 - 02:39:50 AM	04/14/2017 - 02:48:06 AM	7	7	0	0
5	[redacted]				1	05/01/2017 - 06:40:30 PM	04/16/2017 - 03:47:45 AM	04/16/2017 - 03:52:00 AM	14	14	0	0
6	[redacted]				2	05/01/2017 - 07:43:21 PM	04/13/2017 - 07:50:56 PM	04/13/2017 - 07:53:05 PM	6	6	0	0
7	[redacted]				4	05/02/2017 - 08:02:13 AM	04/16/2017 - 09:52:16 AM	04/16/2017 - 04:00:58 AM	12	9	3	3
8	[redacted]				1	05/02/2017 - 08:01:04 AM	04/16/2017 - 03:43:28 AM	04/16/2017 - 03:52:41 AM	6	5	1	1

Alert Tip

Send multiple emails to different recipients using lookups

host	contact
sample1	admin1@sample.email
sample2	admin2@sample.email
sample3	admin3@sample.email
sample4	admin4@sample.email
sample5	admin5@sample.email
sample6	admin6@sample.email
sample7	admin7@sample.email



Summary

Everything from a single report

- Dashboards
  - Patching Progress Status
  - Server details
  - Patch details
- Reports
  - Schedule reports for specific groups of servers
  - Full status report
- Alerts
  - Notify specific teams if servers aren't patched

Thank You

Don't forget to rate this session in the .conf2017 mobile app