Site Reliability Engineering with Phantom

Tanuj Arcot, Victor Menezes, Tim Pacl
Dell Technologies
During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.
Tim Pacl

Splunk Architect | Dell Technologies
Victor Menezes

Splunk Admin  |  Dell Technologies
Agenda
SRE with Phantom

Phantom.
It’s not just for security anymore!

1) What is SRE?
   What is Site Reliability Engineering?

2) Why Phantom for SRE?
   What Phantom delivers for SRE

3) Walkthrough: Investigate
   Fraud Investigations, DB Investigations

4) Walkthrough: Remediate
   IIS Remediations, Forwarder Remediation

5) Walkthrough: Extending Phantom Playbooks
   Integrating with ServiceNow, Teams, Twilio, and more

6) Call to Action
   How can you get started
What Is SRE?

Site reliability engineering

A cross-functional team of IT professionals across the disciplines needed to ensure stability of the “site”.
What Is SRE?

Site reliability engineering

A cross-functional team of IT professionals across the disciplines needed to ensure stability of the “site”. Primary objectives are:

1. Improve Observability
What Is SRE?
Site reliability engineering

A cross-functional team of IT professionals across the disciplines needed to ensure stability of the “site”. Primary objectives are:

1. Improve Observability
2. Reduce MTTF
   - Mean Time to Find Issues
What Is SRE?

Site reliability engineering

A cross-functional team of IT professionals across the disciplines needed to ensure stability of the “site”. Primary objectives are:

1. Improve Observability
2. Reduce MTTF
   – Mean Time to Find Issues
3. Reduce MTTR
   – Mean Time to Resolve Issues
Why Phantom for SRE?

You Can Build on Your Splunk Expertise
Why Phantom for SRE?

You Can Build on Your Splunk Expertise

• Years of Experience with Splunk Enterprise and ITSI
Why Phantom for SRE?

You Can Build on Your Splunk Expertise

• Years of Experience with Splunk Enterprise and ITSI
• Thousands of Engaged Splunk Users
Why Phantom for SRE?

You Can Build on Your Splunk Expertise
• Years of Experience with Splunk Enterprise and ITSI
• Thousands of Engaged Users
• Splunk Certified Users to Architects
Why Phantom for SRE?

You Can Build on Your Splunk Expertise

- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Users
- Splunk Certified Users to Architects

Easy Integration with Splunk
Why Phantom for SRE?

You Can Build on Your Splunk Expertise
- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Users
- Splunk Certified Users to Architects

Easy Integration with Splunk
- Scheduled / Interval Pull of Splunk Data into Phantom
Why Phantom for SRE?

You Can Build on Your Splunk Expertise
- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Users
- Splunk Certified Users to Architects

Easy Integration with Splunk
- Scheduled / Interval Pull of Splunk Data into Phantom
- Interval Push Splunk Data into Phantom
Why Phantom for SRE?

You Can Build on Your Splunk Expertise

- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Users
- Splunk Certified Users to Architects

Easy Integration with Splunk

- Scheduled / Interval Pull of Splunk Data into Phantom
- Interval Push Splunk Data into Phantom
- Trigger Push of Splunk Data into Phantom with Splunk Alert
Why Phantom for SRE?

You Can Build on Your Splunk Expertise
- Years of Experience with Splunk Enterprise and ITSI
- Thousands of Engaged Users
- Splunk Certified Users to Architects

Easy Integration with Splunk
- Scheduled / Interval Pull of Splunk Data into Phantom
- Interval Push Splunk Data into Phantom
- Trigger Push of Splunk Data into Phantom with Splunk Alert
- Trigger Phantom Playbook Execution from Splunk Alert
Why Phantom for SRE?

Data-driven Orchestration
Why Phantom for SRE?

Data-driven Orchestration

• Key Differentiator Compared to other Orchestration Tools
Why Phantom for SRE?

Data-driven Orchestration

• Key Differentiator Compared to other Orchestration Tools
• Making Our Data Truly Actionable!
Why Phantom for SRE?

Data-driven Orchestration
• Key Differentiator Compared to other Orchestration Tools
• Making Our Data Truly Actionable!

Scaling Our Organizations Through Automation
Why Phantom for SRE?

Data-driven Orchestration
• Key Differentiator Compared to other Orchestration Tools
• Making Our Data Truly Actionable!

Scaling Our Organizations Through Automation
• Doing More with What We Have
Why Phantom for SRE?

Data-driven Orchestration
• Key Differentiator Compared to other Orchestration Tools
• Making Our Data Truly Actionable!

Scaling Our Organizations Through Automation
• Doing More with What We Have
• Reacting Quicker to What is Happening
Why Phantom for SRE?

Data-driven Orchestration
• Key Differentiator Compared to other Orchestration Tools
• Making Our Data Truly Actionable!

Scaling Our Organizations Through Automation
• Doing More with What We Have
• Reacting Quicker to What is Happening
• Reducing the Cost of What We do
Why Phantom for SRE?

Keep the lights on for legacy platforms
Why Phantom for SRE?

Keep the lights on for legacy platforms

• Broad Compatibility with Both Container and Legacy Platforms
Why Phantom for SRE?

Keep the lights on for legacy platforms
  • Broad Compatibility with Both Container and Legacy Platforms

Agentless Action
Why Phantom for SRE?

Keep the lights on for legacy platforms
• Broad Compatibility with Both Container and Legacy Platforms

Agentless Action
• No Agent Software to Install 😊
Why Phantom for SRE?

Keep the lights on for legacy platforms
• Broad Compatibility with Both Container and Legacy Platforms

Agentless Action
• No Agent Software to Install 😊
• Using APIs and Existing Tools to Take Action
Why Phantom for SRE?

Keep the lights on for legacy platforms
• Broad Compatibility with Both Container and Legacy Platforms

Agentless Action
• No Agent Software to Install 😊
• Using APIs and Existing Tools to Take Action

Native Extensibility
Walkthrough: Fraud Use Case
Credit Card Fraud Investigations

Single IP using more than 10 creditcards within 30 mins

One Credit Card being accessed from more than 2 IPs
Credit Card Fraud Investigations

- Single IP using more than 10 creditcards within 30 mins
  - Lookup past 30 days Order history
    - Identify unique IPs used
    - Identify unique Visitor IDs used
    - Identify unique Shipping Address used
    - Identify unique email Address used
- One Credit Card being accessed from more than 2 IPs
Credit Card Fraud Investigations

- Single IP using more than 10 credit cards within 30 mins
  - Lookup past 30 days Order history
    - Identify unique Visitor IDs used
    - Identify unique Shipping Address used
    - Identify unique email Address used

- One Credit Card being accessed from more than 2 IPs
  - Identify unique IPs used

- Merge Lists
  - Rerun the Query with Broader dataset
    - Check for IP Reputation
      - Check 3D Secure Logs for responses
    - Check Payment Logs for authorization responses

- Build Email
  - Notify Fraud Team
### Results

#### Splunk Alert - Last 4 hours Activity

<table>
<thead>
<tr>
<th>IP Address</th>
<th>IP Country</th>
<th>Country</th>
<th>Earliest Time</th>
<th>Latest Time</th>
<th>Visitor IDs used</th>
<th>Cart IDs used</th>
<th>Credit Cards used</th>
<th>Avg time per IPAddress</th>
<th>Total Time Spent</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 5 14,13</td>
<td>5 14,13 18,137,14,146</td>
<td>South Korea, United States</td>
<td>United States</td>
<td>08/26/20 06:32:05</td>
<td>08/26/20 06:18:05</td>
<td>3</td>
<td>5</td>
<td>1</td>
<td>35 minutes</td>
</tr>
</tbody>
</table>

#### Credit Card Salted Hash

5E26B8A0A8F2CCF21F1E2A63CE30A8D7ACA2B06DF7CAAF3F3AAAP09C19852E686E7F35FP51DC85326E7F30F238E354005B6DA5812C785D7F8BED8FBE8E548188D

### Activity Overview for the last 30 days

<table>
<thead>
<tr>
<th>Order Submissions</th>
<th>IP Address used</th>
<th>Email Addresses used</th>
<th>MCDMID used</th>
<th>Order Count</th>
<th>Revenue</th>
<th>Shipping Street Address used</th>
<th>Products purchased</th>
<th>Order Count</th>
<th>Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Orders 6</td>
<td>Order Count</td>
<td>Revenue</td>
<td>Order Count</td>
<td>Revenue</td>
<td></td>
<td></td>
<td></td>
<td>Order Count</td>
<td>Revenue</td>
</tr>
<tr>
<td>136</td>
<td>137</td>
<td>1</td>
<td>799.19</td>
<td>3</td>
<td>5,995.95</td>
<td></td>
<td></td>
<td>4</td>
<td>1,996.76</td>
</tr>
<tr>
<td>117</td>
<td>14</td>
<td>2</td>
<td>3,598.58</td>
<td>3</td>
<td>2,397.57</td>
<td></td>
<td></td>
<td>3</td>
<td>799.19</td>
</tr>
<tr>
<td>144</td>
<td>145</td>
<td>3</td>
<td>894.059.53</td>
<td>3</td>
<td>832.000.00</td>
<td></td>
<td></td>
<td>1</td>
<td>632.500.00</td>
</tr>
</tbody>
</table>

Product: Inspiron 15 5000

Product: Dell 27 Gaming Monitor - S2721DGF

Product: L515 NE 148TH AVE STE 302

Product: 228 703
## Results

### ThreeDSecure Overview for the last 30 days

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Total Hits</th>
<th>Authentication Successful (Y)</th>
<th>Authentication Attempted (A)</th>
<th>Authentication Failed (N)</th>
<th>Authentication Unavailable (U)</th>
<th>Empty</th>
</tr>
</thead>
<tbody>
<tr>
<td>117.110.14</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>118.6.137</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24.4.145</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Transactions for the last 30 days

<table>
<thead>
<tr>
<th>Time</th>
<th>Dp_id</th>
<th>MIDID</th>
<th>IP Address</th>
<th>Email</th>
<th>Payment Type</th>
<th>Shipping Address</th>
<th>Product ID</th>
<th>Product Name</th>
<th>Gross Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/25/2020, 08:19</td>
<td>200</td>
<td>200012</td>
<td>827502030046033818895533596053562709939</td>
<td><a href="mailto:vxd782@nevery.com">vxd782@nevery.com</a></td>
<td>CreditCardMasterCard</td>
<td>5512.146</td>
<td></td>
<td>3500.14</td>
<td>500.00</td>
</tr>
<tr>
<td>08/26/2020, 07:50</td>
<td>200</td>
<td>200003</td>
<td>82125245004633381889553356036562709939</td>
<td><a href="mailto:vxd782@nevery.com">vxd782@nevery.com</a></td>
<td>CreditCardMasterCard</td>
<td>3512.146</td>
<td></td>
<td>3500.14</td>
<td>500.00</td>
</tr>
<tr>
<td>08/26/2020, 07:16</td>
<td>200</td>
<td>200003</td>
<td>82125245004633381889553356036562709939</td>
<td><a href="mailto:vxd782@nevery.com">vxd782@nevery.com</a></td>
<td>CreditCardMasterCard</td>
<td>3512.146</td>
<td></td>
<td>3500.14</td>
<td>500.00</td>
</tr>
</tbody>
</table>
Walkthrough: DB Investigation
Database Investigations

- High CPU
- Blocking/Locking
- High Response Times
- Network Glitches and Availability Group Listener(ACL) timeouts
Database Investigations

- High CPU
- Blocking/Locking
- High Response Times
- Network Glitches and Availability Group Listener(AGL) timeouts
  - Connect to the Database
  - Run Query to Capture Live Sessions
    - Check for Head blockers
    - Check for VMotion
      - Check for I/O Latency
Database Investigations

- High CPU
- Blocking/Locking
- High Response Times
- Network Glitches and Availability Group Listener(AGL) timeouts

1. Connect to the Database
2. Run Query to Capture Live Sessions
3. Check for VMotion
4. Check for AGL Health
5. Check for File share Witness and Quorum
6. Merge Results and Process HTML
7. Send Email to DBAs
8. Stop
### AG Quorum Details

<table>
<thead>
<tr>
<th>Member_Name</th>
<th>Member_Score_Desc</th>
<th>Member_Type_Desc</th>
<th>Number_of_Quorum_Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUSPWB28B0D1</td>
<td>DOWN</td>
<td>CLUSTER_NODE</td>
<td>1</td>
</tr>
<tr>
<td>AUSPWB28B0D2</td>
<td>UP</td>
<td>CLUSTER_NODE</td>
<td>1</td>
</tr>
<tr>
<td>File Share Witness</td>
<td>UP</td>
<td>FILE_SHARE_WITNESS</td>
<td>1</td>
</tr>
</tbody>
</table>

#### AG Health Status

| AG Name       | AG Format Name | AG Enabled | AG Name Timezone | AG Status | AG Status Time | AG Status Time Zone  | AG Status Time Zone Zone  | AG Status Time Zone Zone Zone  | AG Status Time Zone Zone Zone Zone  | AG Status Time Zone Zone Zone Zone Zone  |
|---------------|----------------|------------|------------------|-----------|----------------|----------------------|-----------------------------|---------------------------------|---------------------------------------------|

The availability group `GLOBAL-BAGG01` is not healthy. Current primary: `AUSPWB28B0D2`
## Results

### DB Current Processes

<table>
<thead>
<tr>
<th>Host Name</th>
<th>DB Name</th>
<th>Login Name</th>
<th>SessionID</th>
<th>BlockingID</th>
<th>Status</th>
<th>Command</th>
<th>Open Traces</th>
<th>Wait Resource</th>
<th>Request Start Time</th>
<th>Running Time</th>
<th>Statement and SQL Handle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host: DellRCM IP: 10.166.15.128</td>
<td>DELLRCM</td>
<td>asplLogin</td>
<td>52</td>
<td>79</td>
<td>suspended</td>
<td>UPDATE 2</td>
<td></td>
<td></td>
<td>2020-08-25 20:00:21:757000</td>
<td>0 hours, 0 min, 0 sec</td>
<td>UPDATE (DELETE), also ASPIrateTempSessions SET Expires = DATEADD(D, @now), LockDate = CASE LockDate WHEN 0 THEN @now ELSE LockDate END, LockDateLocal = CASE LockDate WHEN 0 THEN @nowLocal ELSE LockDateLocal END, @lockedge = CASE LockDate WHEN 0 THEN 0 ELSE DATEDIFF</td>
</tr>
<tr>
<td>Host: DellRCM IP: 10.166.15.128</td>
<td>DELLRCM</td>
<td>asplLogin</td>
<td>59</td>
<td>52</td>
<td>suspended</td>
<td>UPDATE 2</td>
<td></td>
<td></td>
<td>2020-08-25 20:00:21:760000</td>
<td>0 hours, 0 min, 0 sec</td>
<td>UPDATE (DELETE), also ASPIrateTempSessions SET Expires = DATEADD(D, @now), LockDate = CASE LockDate WHEN 0 THEN @now ELSE LockDate END, LockDateLocal = CASE LockDate WHEN 0 THEN @nowLocal ELSE LockDateLocal END, @lockedge = CASE LockDate WHEN 0 THEN 0 ELSE DATEDIFF</td>
</tr>
<tr>
<td>Host: DellRCM IP: 10.166.15.128</td>
<td>DELLRCM</td>
<td>asplLogin</td>
<td>75</td>
<td>52</td>
<td>suspended</td>
<td>UPDATE 2</td>
<td></td>
<td></td>
<td>2020-08-25 20:00:21:777000</td>
<td>0 hours, 0 min, 0 sec</td>
<td>UPDATE (DELETE), also ASPIrateTempSessions SET Expires = DATEADD(D, @now), LockDate = CASE LockDate WHEN 0 THEN @now ELSE LockDate END, LockDateLocal = CASE LockDate WHEN 0 THEN @nowLocal ELSE LockDateLocal END, @lockedge = CASE LockDate WHEN 0 THEN 0 ELSE DATEDIFF</td>
</tr>
<tr>
<td>Host: DellRCM IP: 10.166.15.128</td>
<td>DELLRCM</td>
<td>asplLogin</td>
<td>79</td>
<td>0</td>
<td>suspended</td>
<td>UPDATE 1</td>
<td></td>
<td></td>
<td>2020-08-25 20:00:21:775000</td>
<td>0 hours, 0 min, 0 sec</td>
<td>UPDATE (DELETE), also ASPIrateTempSessions SET Expires = DATEADD(D, @now), LockDate = CASE LockDate WHEN 0 THEN @now ELSE LockDate END, LockDateLocal = CASE LockDate WHEN 0 THEN @nowLocal ELSE LockDateLocal END, @lockedge = CASE LockDate WHEN 0 THEN 0 ELSE DATEDIFF</td>
</tr>
</tbody>
</table>
Walkthrough: Windows Webserver Auto Remediation
Windows Webserver Auto Remediation

- High CPU
- High Memory
- Resource Exhaustion
- Too Many 5XX and Other Errors
Windows Webserver Auto Remediation

- High CPU
- High Memory
- Resource Exhaustion
- Too Many 5XX and Other Errors

Mark Down Server

Verify BigIP load balancing

Yes

Good to autoheal

No

Terminator
Windows Webserver Auto Remediation

- **High CPU**
- **High Memory**
- **Resource Exhaustion**
- **Too Many 5XX and Other Errors**

1. **Mark Down Server** → Wait 5 mins → **Perform IIS RESET**
   - Wait 5 mins
   - **Recovered?**
     - Yes → **Server Marked Up** → Stop
     - No → **Create Service Now Ticket for Server Team** → Stop

- **Splunk** → **ServiceNow** → **F5 BigIP/ Powershell**
## Results

<table>
<thead>
<tr>
<th>Splunk Alert</th>
<th>Script Results</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>P60</td>
<td>Mark Down</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Status</td>
</tr>
<tr>
<td>No Data</td>
<td>Success</td>
</tr>
<tr>
<td><strong>Load Balanced?</strong></td>
<td>Message</td>
</tr>
<tr>
<td>Yes</td>
<td>Mark Down performed successfully!</td>
</tr>
<tr>
<td><strong>Troux ID</strong></td>
<td>Pool Name</td>
</tr>
<tr>
<td>1000236</td>
<td>/Common/giopenbasket-svc-p60</td>
</tr>
<tr>
<td><strong>Application Name</strong></td>
<td>Controller IP</td>
</tr>
<tr>
<td>DCQO GII Quote Gateway</td>
<td>10.177.12.4</td>
</tr>
<tr>
<td><strong>Segment</strong></td>
<td>Mark Down</td>
</tr>
<tr>
<td>PED</td>
<td>Success</td>
</tr>
<tr>
<td><strong>Symptom/Issue</strong></td>
<td>Mark Down</td>
</tr>
<tr>
<td>Resource Exhaustion</td>
<td>Success</td>
</tr>
</tbody>
</table>

Mark Down Success

Mark Down performed successfully!

Mark Down performed successfully!

Mark Down performed successfully!

Mark Down performed successfully!

Mark Down performed successfully!

Mark Down performed successfully!

IIS RESET Success

IIS Reset Completed Successfully

Mark Up Success

Mark Up performed successfully!

Mark Up performed successfully!

Mark Up performed successfully!

Mark Up performed successfully!

Mark Up performed successfully!

Mark Up performed successfully!
Walkthrough: Forwarder Remediation
Walkthrough
Splunk forwarder remediation – is pinging
Walkthrough
Splunk forwarder remediation – is pinging

Manipulate filesystem files
Walkthrough
Splunk forwarder remediation – is pinging

Manipulate filesystem files
Call API endpoints

Get last 100 splunkd log rows and raise an incident with this log on the description
Walkthrough
Splunk forwarder remediation – is pinging

Manipulate filesystem files
Call API endpoints
Keeps the forwarders up-to-date
Walkthrough
Splunk forwarder remediation – is pinging

Manipulate filesystem files

Call API endpoints

Keeps the forwarders up-to-date

Trigger an incident with enriched data
Walkthrough
Splunk forwarder remediation – not pinging
Walkthrough
Splunk forwarder remediation – not pinging

Investigate reasons of unavailability
Walkthrough
Splunk forwarder remediation – not pinging

Investigate reasons of unavailability

Report server down to the responsible team
Walkthrough

Splunk forwarder remediation – full diagram
Walkthrough: Extending Phantom Playbooks
Integrations

Phantom integrations - overview

Over 200 built-in apps (and more xxx available in phantom portal)
Integrations
Phantom integrations - overview

Over 200 built-in apps (and more xxx available in phantom portal)

Install/update apps via UI
Integrations

Phantom integrations - overview

Over 200 built-in apps (and more xxx available in phantom portal)

Install/update apps via UI

Create your own apps via UI
Integrations
Phantom integrations - overview

Over 200 built-in apps (and more xxx available in phantom portal)

Install/update apps via UI

Create your own apps via UI

Configure multiple assets per app
## Walkthrough

**Phantom integrations - teams**

### HTTP post

![HTTP post screenshot]

**Description**
This App facilitates making HTTP requests as actions.

**ASSET CONFIGURATION**

<table>
<thead>
<tr>
<th>Asset (22)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ms teams - dce ire</td>
</tr>
</tbody>
</table>

**Asset Info**
- **Base URL for making queries (e.g. https://myenvision):**
  - https://outlook.office.com

**User credentials**
- **Phantom Auth token (for use with Phantom servers):**
  - 

- **Username (for HTTP basic auth):**
  - Optional
- **Password (for HTTP basic auth):**
  - Optional

**Advanced**

**Base URL endpoint for test connectivity (e.g. /same/specific/endpoint):**

- TEST CONNECTIVITY
Walkthrough
Phantom integrations - teams

HTTP post
Walkthrough
Phantom integrations - teams

Fully customized message card
Walkthrough
Phantom integrations – Twilio & Slack
Walkthrough

Phantom integrations – Twilio & Slack

Configure an asset
Walkthrough

Phantom integrations – Twilio & Slack

Configure an asset

Test connectivity
Walkthrough
Phantom integrations – Twilio & Slack

Configure an asset

Test connectivity

Add the action call in the playbook
Walkthrough
Phantom integrations – Twilio & Slack

Configure an asset

Test connectivity

Add the action call in the playbook
Walkthrough

Phantom integrations – Twilio & Slack

Configure an asset

Test connectivity

Add the action call in the playbook

Twilio configuration follows the same standard
Walkthrough

Phantom integrations – Twilio & Slack

Twilio

The [Dell.com](https://www.dell.com) ACC dashboard is alerting. Cart Services[96], Delivery Promise[1534], PCF Configurator[261], Responsive Cart[570], Server-Network[321].

ARR is alerting with more than 5174 5XX errors. Top offenders are External Website[5174] and datacenter stats are PC1[2751], S3B[2423].

Slack

Aug 22nd

The [Dell.com](https://www.dell.com) ACC dashboard is alerting. Server-Network[21]. [https://tinyurl.com/](https://tinyurl.com/) (edited)
## Walkthrough

### Phantom integrations - ServiceNow

**ServiceNow**

Publisher: Splunk
App version: 1.2.59
Python version: 2.7
Product vendor: ServiceNow
Documentation

**Description**

This app integrates with ServiceNow to perform investigative and generic actions.

### Asset Configuration

#### Asset (1)

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device URL</td>
<td><a href="https://myservicenow.enterprise.com:8080">https://myservicenow.enterprise.com:8080</a></td>
</tr>
<tr>
<td></td>
<td><a href="https://delltechchat.service-now.com">https://delltechchat.service-now.com</a></td>
</tr>
<tr>
<td>Username</td>
<td>Optional</td>
</tr>
<tr>
<td>Client ID</td>
<td>Optional</td>
</tr>
<tr>
<td>Table to ingest issues from</td>
<td>Optional</td>
</tr>
<tr>
<td>Max container (For first run of schedule polling)</td>
<td>10000</td>
</tr>
</tbody>
</table>

**Advanced**

**Configure New Asset**

**Asset Settings**

- **Device URL**: Include the port, e.g., https://myservicenow.enterprise.com:8080
- **Username**: Optional
- **Client ID**: OAuth will be preferred if provided
- **Table to ingest issues from**: Optional
- **Max container (For first run of schedule polling)**: 10000
Walkthrough
Phantom integrations - ServiceNow

Manage incidents
Walkthrough

Phantom integrations - ServiceNow

Manage incidents

Run queries over API
Walkthrough
Phantom integrations - ServiceNow

Manage incidents
Run queries over API
List tickets
Walkthrough

Phantom integrations - ServiceNow

Manage incidents

Run queries over API

List tickets

Simple as adding a new action to your playbook
Walkthrough

Phantom integrations - ServiceNow
Walkthrough
Phantom integrations - ServiceNow
Add attachments
Walkthrough
Phantom integrations - ServiceNow

Add attachments
Update assignment
Walkthrough

Phantom integrations - ServiceNow

Add attachments
Update assignment
Change priority
Walkthrough

Phantom integrations - ServiceNow

Add attachments
Update assignment
Change priority
Manage Incident state
Walkthrough
Phantom integrations - Others

Ticketing

- servicenow
- bmc Remedyforce
- salesforce
- ATLASSIAN
- zendesk
Walkthrough

Phantom integrations - Others

Ticketing

Information

- servicenow
- slack
- Salesforce
- BMC Remedyforce
- Atlassian
- Zendesk
Walkthrough
Phantom integrations - Others

Ticketing
Information
Virtualization
Walkthrough

Phantom integrations - Others

Ticketing

Information

Virtualization

Database
Walkthrough
Phantom integrations - Others

Ticketing
Information
Virtualization
Database
Devops
More…
Summary
Putting it all together

Phantom Can Investigate, Remediate, and Inform
Summary
Putting it all together

Phantom Can Investigate, Remediate, and Inform
• Investigate – Query other sources, OS Scripting, etc. (SQL DB)
Summary
Putting it all together

Phantom Can Investigate, Remediate, and Inform

• Investigate – Query other sources, OS Scripting, etc. (SQL DB)
• Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
Summary
Putting it all together

Phantom Can Investigate, Remediate, and Inform
• Investigate – Query other sources, OS Scripting, etc. (SQL DB)
• Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
• Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)
Summary
Putting it all together

Phantom Can Investigate, Remediate, and Inform
• Investigate – Query other sources, OS Scripting, etc. (SQL DB)
• Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
• Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible
Summary
Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)
- Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
- Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible

- 200 Apps in Phantom
Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)
- Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
- Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible

- 200 Apps in Phantom
- 300 + Apps at my.phantom.us
Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

• Investigate – Query other sources, OS Scripting, etc. (SQL DB)
• Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
• Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible

• 200 Apps in Phantom
• 300 + Apps at my.phantom.us
• Custom Functions
Summary

Putting it all together

Phantom Can Investigate, Remediate, and Inform

- Investigate – Query other sources, OS Scripting, etc. (SQL DB)
- Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
- Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible

- 200 Apps in Phantom
- 300 + Apps at my.phantom.us
- Custom Functions
- Build Your Own Apps
Summary
Putting it all together

Phantom Can Investigate, Remediate, and Inform
• Investigate – Query other sources, OS Scripting, etc. (SQL DB)
• Remediate – OS Scripting, REST API, WMI, SSH, etc. (IIS, Splunk Forwarder)
• Inform – Email, ServiceNow, Slack, Teams, SMS, etc. (All)

Phantom is Highly Extensible
• 200 Apps in Phantom
• 300 + Apps at my.phantom.us
• Custom Functions
• Build Your Own Apps
• Only Limited by Your Imagination
Call to Action
How you can get started with Phantom

Get an Account on my.phantom.us
• Account is free
• Access to documentation, product downloads, and more
Call to Action
How you can get started with Phantom

Get an Account on my.phantom.us
• Account is free
• Access to documentation, product downloads, and more

Get the Free Community Edition
• Limited Functionality After 100 Actions in a Day
• Easy, Single-Server Install
Call to Action
How you can get started with Phantom

Get an Account on my.phantom.us
• Account is free
• Access to documentation, product downloads, and more

Get the Free Community Edition
• Limited Functionality After 100 Actions in a Day
• Easy, Single-Server Install

Get Trained
• A Training Investment Will Kickstart Your Productivity!
• Check Out the Splunk Training Portal
Thank You

Please provide feedback via the SESSION SURVEY