## Technical Accomplishments

Developed technique on Ansible Tower to test presence of ssh keys for **ansibsplunk** user on TJX prod & non-prod servers. Ran in batches to determine list of servers which required manual remediation.

## Ansible playbook development

**Developed playbook & role to forward logging from TJX servers to syslog.** This was a time-sensitive project due to pending ArcSight license expiration. All TJX servers (prod/non-prod, Linux/AIX) needed to forward their system logs to central Syslog server.

JIRA ticket: [Ansible playbook: Enable logging to Syslog server (SECTEAM-619)](https://jira.tjx.com/browse/SECTEAM-619)

I implemented this key functionality:

* Dynamic detection of OS (Linux vs AIX)
* Edit config file (rsyslog.config) on each target server
* Dynamic search for key string in config file (os dependent search)
* Replace key value (ArcSight server to Syslog server)
* Replacement value is based on server’s OS (Linux/AIX) and location (NA/EU/AU)
* All values defined as Ansible group variables.
* Auto stop & start of Syslog service after update.

**Developed playbook & role to upgrade Splunk Universal Forwarder on Unix servers.**

**Jira ticket:** [Ansible playbook: Install/upgrade Splunk on Unix (DSOTEAM-1054)](https://jira.tjx.com/browse/DSOTEAM-1054)

I implemented this key functionality:

* Dynamic detection of install vs upgrade scenario
* Create Splunk destination path with proper access rights
* Added support for AIX servers. Allowed us to remove separate AIX playbook.

**Developed playbook & role to install Splunk Universal Forwarder on Windows servers**

**JIRA ticket:** [Ansible playbook: Install Splunk on Windows (DSOTEAM-1056)](https://jira.tjx.com/browse/DSOTEAM-1056)

I implemented this key functionality:

* Configured WinRM with CREDSSP transport for Ansible-Windows connectivity
* Pulled Splunk installer files from JFrog artifactory.
* Auto stop & start of Splunk service
* Auto clean-up of temp files upon completion.

**Developed playbook & role to install/upgrade App Dynamics**

**JIRA tickets:**

[Ansible playbook: Install AppDynamics on Linux (DSOTEAM-1063)](https://jira.tjx.com/browse/DSOTEAM-1063)

[Ansible playbook: Install AppDynamics on Windows (DSOTEAM-1058)](https://jira.tjx.com/browse/DSOTEAM-1058)

I implemented this key functionality:

* Used Ansible tags to control workflow: Install java agent vs machine agent
* Pulled AppDynamic installer files from JFrog artifactory.

**Developed playbook & role to disable log forwarding to Syslog**

**JIRA ticket:** [Ansible playbook: Disable syslog forwarding (DSOTEAM-1052)](https://jira.tjx.com/browse/DSOTEAM-1052)

This playbook stops servers from sending their logs to Syslog server. Replaced original config file entry with date-stamped comment to explain how & why the file got edited.

**Server Tracking**

I tracked & reported status of 1400 Prod & Non-prod TJX server logging to Splunk cloud.

* Used Splunk queries to determine logging success.
* Researched each failed server for firewall block or other environmental cause.
* Reached out to Security team and server owners to make necessary updates.
* I opened required ServiceNow tickets to gain access to **Unreachable** servers.

I tracked & reported status of each Prod & Non-prod TJX server for Splunk mount provisioning needed

**User Support**

**Resolve user Splunk failover issue.**

JIRA ticket: [Configure Splunk on Marshalls TM1 Prod fail-over server (DSOE-2822)](https://jira.tjx.com/browse/DSOE-2822)

Description: Resolved issue with fail-over server not logging to Splunk. Used root cause analysis to isolate server issue. Discussion with customer revealed they copied entire config tree from master server. I used text string search to confirm invalid server reference in configuration.

**Blue Prism-Splunk integration**

JIRA ticket: [Enable Splunk logging for Blue Prism servers via Http Event Collector (DSOTEAM-958)](https://jira.tjx.com/browse/DSOTEAM-958)

I created an Http Event Collector token for the Blue Prism team.  This establishes basic connectivity between Blue Prism servers and Splunk cloud.   Blue Prism team will create a dashboard in Splunk using audit log from Blue Prism servers.

**Rest API application**

**JIRA ticket:** [Create a node.js based restful service for training and demos (DSOTEAM-1467)](https://jira.tjx.com/browse/DSOTEAM-1467)

Create a REST api application as a sample for training TJX development teams on BDD development. This application serves as a model for teams to learn Behavior Driven Design practices.

**Other accomplishments:**

JIRA ticket: [Set up Visual Studio Code IDE for Ansible development (DSOTEAM-1311)](https://jira.tjx.com/browse/DSOTEAM-1311)

Installed & configured Visual Studio Code for developing in Ansible and Node.js

**Jira Stories**

[Enable Splunk logging for Blue Prism servers via Http Event Collector (DSOTEAM-958)](https://jira.tjx.com/browse/DSOTEAM-958)

[Configure Splunk on Marshalls TM1 Prod fail-over server (DSOE-2822)](https://jira.tjx.com/browse/DSOE-2822)

[Ansible playbook: Disable syslog forwarding (DSOTEAM-1052)](https://jira.tjx.com/browse/DSOTEAM-1052)

[Ansible playbook: Install/upgrade Splunk on Unix (DSOTEAM-1054)](https://jira.tjx.com/browse/DSOTEAM-1054)

[Ansible playbook: Install Splunk on Windows (DSOTEAM-1056)](https://jira.tjx.com/browse/DSOTEAM-1056)

[Ansible playbook: Install AppDynamics on Linux (DSOTEAM-1063)](https://jira.tjx.com/browse/DSOTEAM-1063)

[Ansible playbook: Install AppDynamics on Windows (DSOTEAM-1058)](https://jira.tjx.com/browse/DSOTEAM-1058)