

Cloud Security at Scale with Trend Micro, Splunk and Chef

Hands on Lab Manual

- » This Integrated solution stack is deployed via an ARM template and designed for Microsoft Azure and Trend Micro customers and partners such as Solution Integrators (SI) and Cloud Solution Providers (CSP). This ARM template will launch a fully integrated solution stack on Azure. The extensive automation and testing of these solutions will allow you to spin up pre-production environments with minimal manual steps and customization.



TABLE OF CONTENTS

TABLE OF CONTENTS.....	1
WHAT MAKES THIS INTEGRATED STACK?	3
<i>Deep Security Manager</i>	<i>3</i>
<i>Deep Security Agent.....</i>	<i>3</i>
<i>Splunk enterprise</i>	<i>3</i>
<i>Chef Automate</i>	<i>3</i>
<i>Azure</i>	<i>3</i>
HOW TO BUILD THIS INTEGRATED STACK?.....	4
<i>Overview</i>	<i>4</i>
WHAT WILL YOU LEARN?	5
BEFORE WE START	6
<i>Tools and Information</i>	<i>6</i>
<i>Initial Steps</i>	<i>6</i>
DEPLOY STACK	11
<i>Overview</i>	<i>11</i>
<i>Launch Stack</i>	<i>12</i>
<i>Template Parameters</i>	<i>12</i>
<i>Protecting Azure Virtual Machine with Deep Security</i>	<i>14</i>
Trend Micro Azure Extension	14
Trend Micro Chef Cookbooks	14
<i>Add Protection to Test Azure Virtual Machines (Exercise)</i>	<i>14</i>
INTEGRATE	16
<i>Configure Trend Micro Deep Security for System event log forwarding (Exercise)</i>	<i>16</i>
<i>Configure Trend Micro Deep Security for Security event log forwarding (Exercise).....</i>	<i>17</i>
ANALYZE	19
<i>Generate Sample Events (Exercise)</i>	<i>19</i>
<i>Analyze Deep Security event data in Splunk's web console (Exercise)</i>	<i>21</i>
<i>Explore Chef Automate and the Chef Node(s) Installed (Optional Exercise)</i>	<i>25</i>

WHAT MAKES THIS INTEGRATED STACK?

The integrated stack consists of the Trend Micro Deep Security platform, Splunk Enterprise, and Chef Automate.



DEEP SECURITY MANAGER This is the management component of the system and is responsible for sending rules and security settings to the Deep Security Agents. The DSM is controlled using the web-based management console. Using the console, the administrator can define security policies, manage deployed agents, query status of various managed instances, etc. The integration with Splunk is done using this interface and no additional component or software is required.

DEEP SECURITY AGENT This component provides all protection functionality. The nature of protection depends on the rules and security settings that each DSA receives from the Deep Security Manager.



SPLUNK ENTERPRISE Splunk Enterprise on Azure is a high performance, scalable software server. It indexes and searches logs and other IT data in real time. Splunk works with data generated by any application, server or device. Deep Security will be integrated with Splunk to send security events to Splunk for further correlation and analytics using the Deep Security app for Splunk.



CHEF Automate Chef Automate is a highly scalable infrastructure compliance and automation platform. The Chef Automate integration with Chef Nodes (i.e. Azure VMs) is done using microservices, via a set of two Docker Containers for a Node.js app and a database. This Chef platform can be used push configuration changes and Deep Security agents to Azure Virtual Machines.



AZURE This integrated stack will be deployed on the Azure cloud platform using the provided Azure Resource Manager (ARM) template.

HOW TO BUILD THIS INTEGRATED STACK?

OVERVIEW

This integrated stack is built using a JSON template, the template is based on Microsoft Azure Resource Manager (ARM) templates. Through ARM templates, we can deploy topologies quickly and consistently with multiple services, along with their dependencies. The figure below provides an overview of the end to end tasks required to completely build the stack. Each task is discussed in detail later in this document.

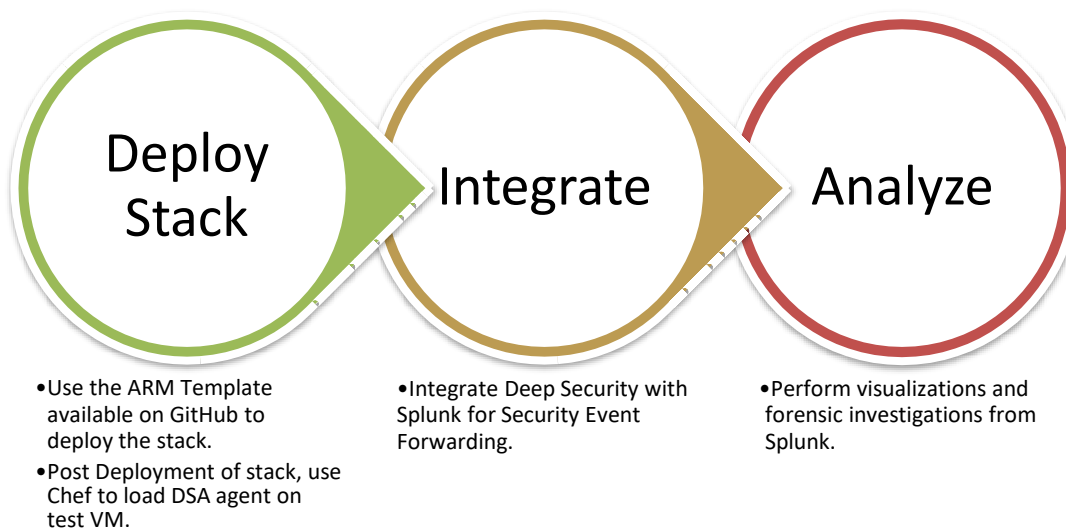
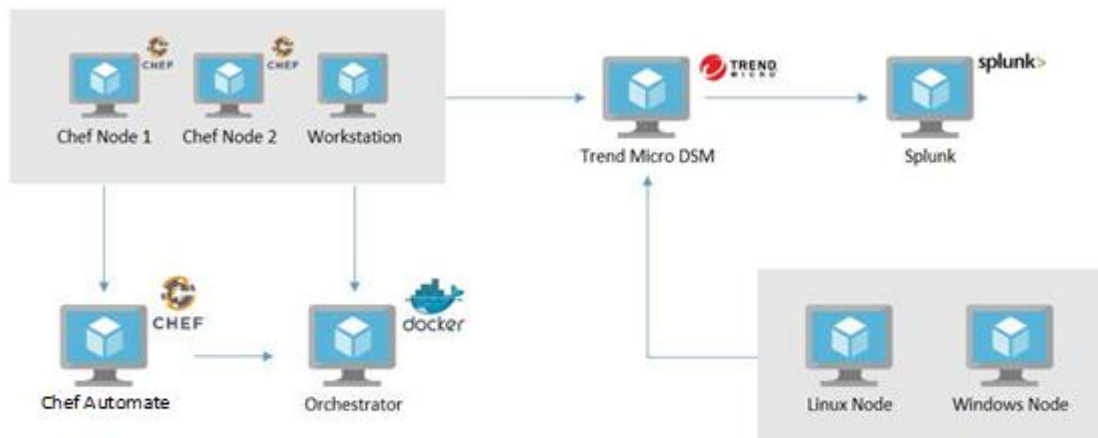


FIGURE 1 – HOW TO BUILD THIS INTEGRATED STACK?

WHAT WILL YOU LEARN?

In this hands-on lab session, you will discover what composes an ARM template and how this integrated stack was built using such templates. We will do a walk-through of this fully automated stack as a way of managing security on existing as well as new cloud workloads, with monitoring and continuous integration built in. In doing so, you will get a hands-on understanding of how Trend Micro's Deep Security Manager product can be integrated with various other cloud products to create a well-rounded and scalable cloud security solution. You will also learn how different components of this stack can be configured, and how to add protection to the test Azure virtual machines that are provisioned as part of the stack launch.



BEFORE WE START

Before we dive into the exercises, let's make sure that you have all the tools and information that you will need.

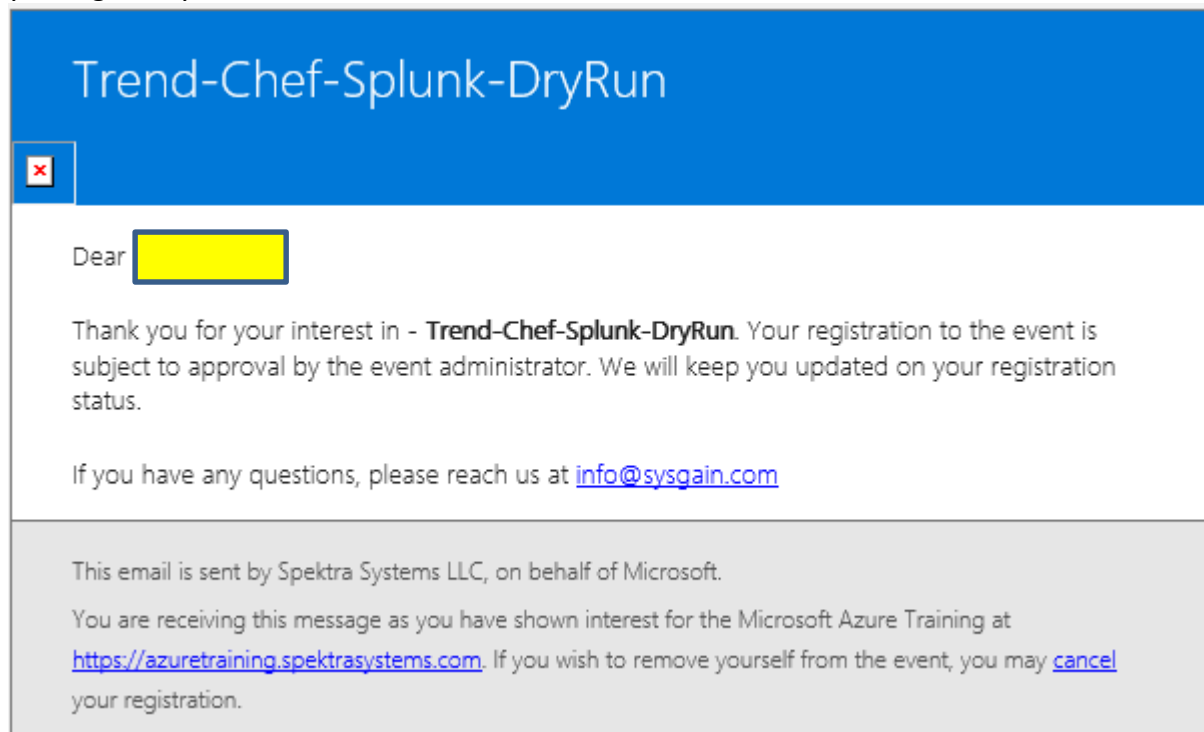
TOOLS AND INFORMATION

To successfully complete some of the exercises in this launch and learn session, you will need the following:

- A reasonably up-to-date **browser** (IE 9+, Edge, Chrome, Firefox, Safari, etc.). You will use the browser to interact with the Deep Security Manager as well as with the Splunk web console.
- **Username and password** to access Azure Portal (<https://portal.azure.com>), Trend Micro Deep Security, and the Splunk Web Console. These credentials will be provided in an email to you. For assistance, please check with the session moderators or support staff.
- **Azure Resource Group Name** that is created for you to deploy the stack.

INITIAL STEPS

You should have registered on the training portal through the link provided in the invitation. Once you register, you will have received an email like the one shown below:



After your registration is approved you will receive a confirmation:

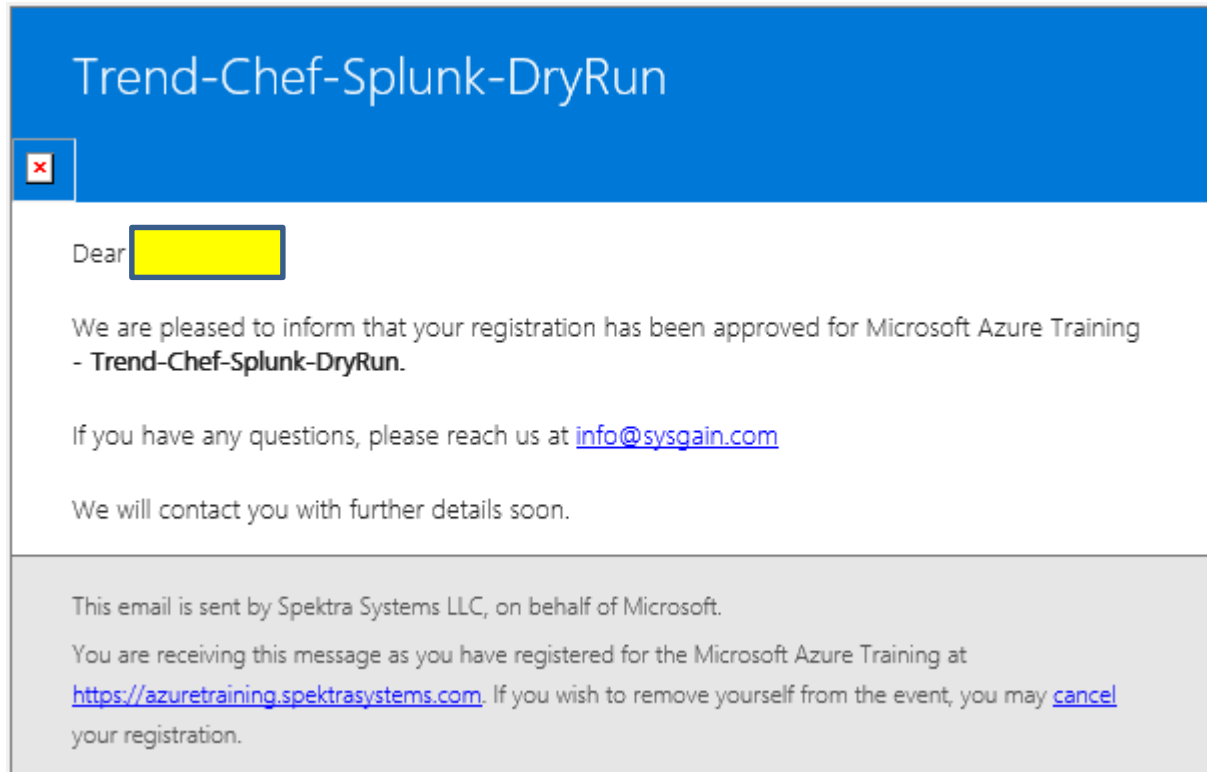


FIGURE 2 – Email acknowledgement for registration

Just before the Workshop you will receive meeting invitation:

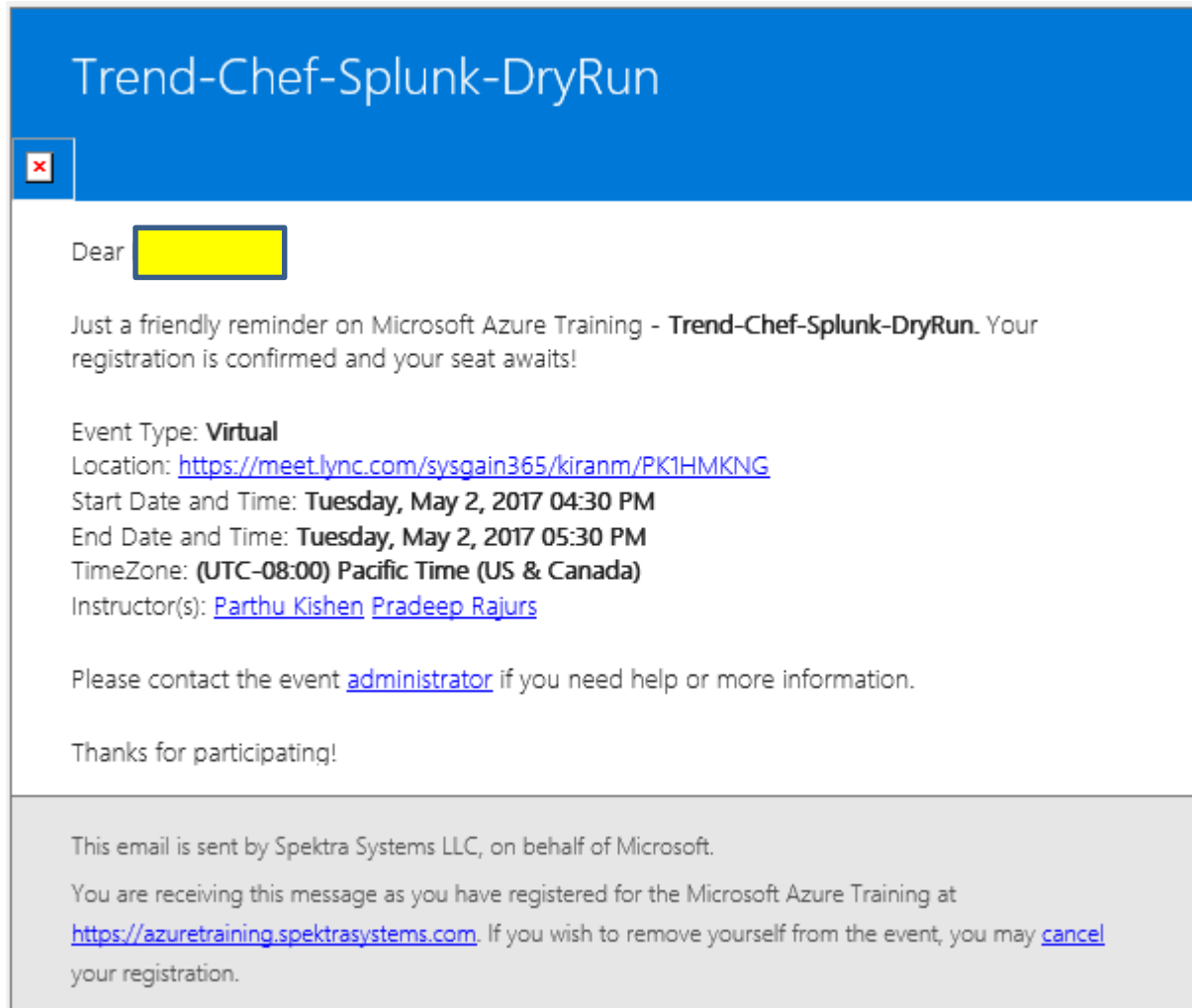


FIGURE 3 Email confirmation for the registration

The Lab for Trend Chef and Splunk will be provisioned, and you will receive an email like the one below with the URI's, usernames and passwords. **Keep these credentials handy, as you will use them to proceed through the lab steps.**

Testing2-trend-chef-splunk

Dear hi there

We are delighted to have you as a part of Microsoft Azure Training - **Testing2-trend-chef-splunk**.

Here are your credentials to login to [Microsoft Azure](#).

Username: kiram.sysgain.com@sysgainqlabsoutlook.onmicrosoft.com
 Password: zrys26LMM!SO
 Lab Guide: <https://github.com/Azure/azure-quickstart-templates/blob/master/trend-chef-splunk-security/images/TrendMicro2pManualSteps.pdf>

Please note that the credentials in this email were generated the first time you registered with us. If you have since changed your password you should use the most recent password.

Please use the below details for future use in your labs:

Name	Value
trendAdminUserName	trend
trendAdminPassword	tdoh49WMS!Y9
splunkAdminUserName	admin
splunkAdminPassword	tdoh49WMS!Y9
chefAutomateAdminUserName	trend
chefAutomateAdminPassword	tdoh49WMS!Y9
trendMicro DSM URI	https://csdfa423cb39934504vigcfnek5oi26.westus.cloudapp.azure.com
chef Automate URI	https://csb143046b04754feavigcf.westus.cloudapp.azure.com
splunk Server URI	https://cs6e0a986cd7f14ea5vigcfnek5oi26.westus.cloudapp.azure.com

If you have any questions, please contact us at kiranm@sysgain.com

See you soon!

This email is sent by Spektra Systems LLC, on behalf of Sysgain Inc.

You are receiving this message as you have registered for the Microsoft Azure Training at <https://azuretraining.spektrasystems.com>. If you wish to remove yourself from the event, you may [cancel](#) your registration.

FIGURE 4 URI's, user names and passwords

Navigate to the URIs and login to Trend Micro Deep Security Web Console and Splunk Enterprise Server Web Console using the username(s) and password(s) provided to ensure you have access to each application (as in above fig 4).

Instructions continued on next page.

DEPLOY STACK

OVERVIEW

The template provides automated provisioning, configuration and integration of Trend Micro's Deep Security product on Azure. The figure below depicts the stack details once it is deployed;

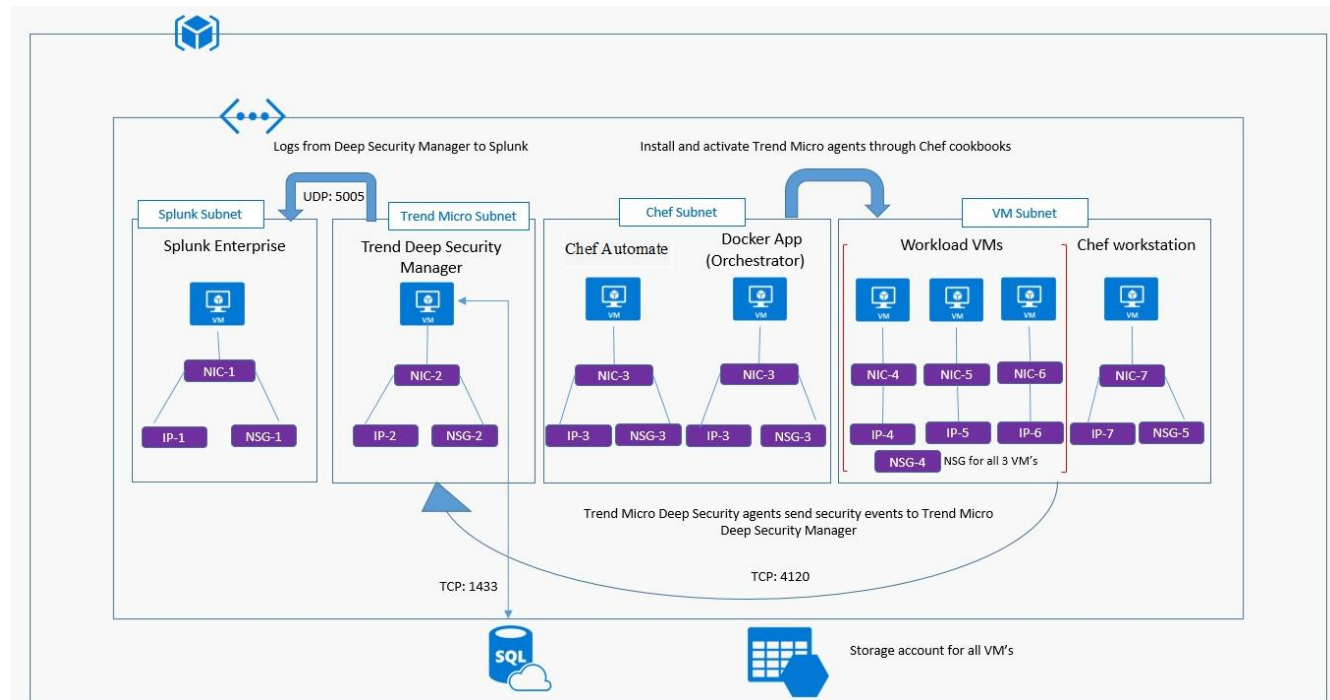


FIGURE 5 – INTEGRATED STACK ARCHITECTURE

As a part of stack deployment, the template launches the following:

- A **storage account** in the resource group.
- A **Virtual Network (vNet)** with four subnets.
- **Virtual Machines** to host solution components.
- **Network security groups** to control what communication paths are allowed.
- **Azure SQL DB** to host Deep Security persistent data.
- **Three test Virtual Machines**; 2 VMs (Linux, Windows) with bootstrap scripts to install TrendMicro agents (through Azure VM extensions) and 1 VMs (Linux) with bootstrap scripts to install Chef Agents.

LAUNCH STACK

The stack deployment can be started by accessing the ARM template at GitHub ([here](#)). You can simply click the "**Deploy to Azure**" button on this GitHub repository or use PowerShell, Azure CLI etc. to start the deployment. The deployment takes about **30-45 mins**.



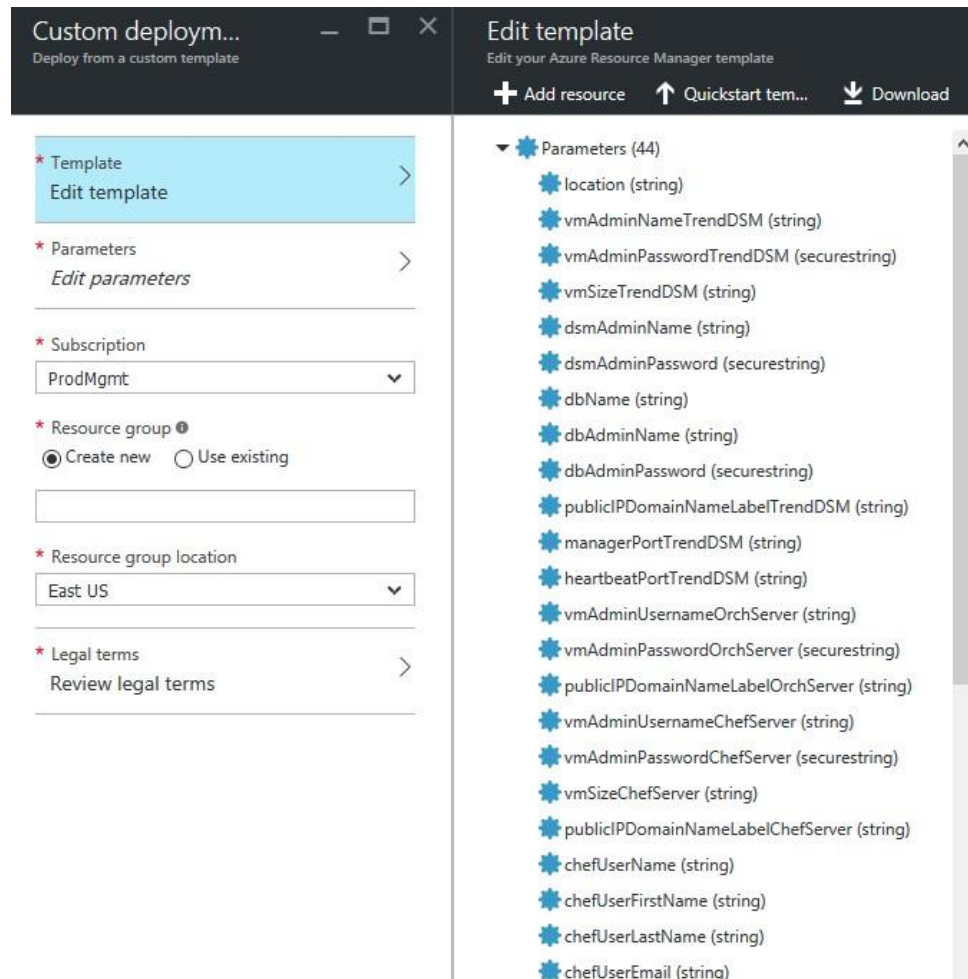
For this Hands-on Lab session, the stack is pre-launched for you, and you will receive all credentials and URLs via email. Review the instructions later in this document on how to access the pre-provisioned stack environment in Azure for this session.

TEMPLATE PARAMETERS

The template provides a list of parameters. Some parameters are defined with default values but some require your input during stack launch. In the parameters section of the template, we specify which values you can input when deploying this stack. These parameter values enable us to customize the stack deployment which is tailored to your requirements.

(Note: If the template is pre-launched, you will not be required to provide input parameters.)

Below is what the parameters would look like in a manual deployment of this solution template. For this lab, this step has already been done.



The screenshot shows the 'Edit template' interface in the Azure portal. On the left, there are deployment options: Template (Edit template), Parameters (Edit parameters), Subscription (ProdMgmt), Resource group (Create new / Use existing), Resource group location (East US), and Legal terms (Review legal terms). On the right, a list of 44 parameters is displayed, including location, vmAdminNameTrendDSM, vmAdminPasswordTrendDSM, vmSizeTrendDSM, dsmAdminName, dsmAdminPassword, dbName, dbAdminName, dbAdminPassword, publicIPDomainNameLabelTrendDSM, managerPortTrendDSM, heartbeatPortTrendDSM, vmAdminUsernameOrchServer, vmAdminPasswordOrchServer, publicIPDomainNameLabelOrchServer, vmAdminUsernameChefServer, vmAdminPasswordChefServer, vmSizeChefServer, publicIPDomainNameLabelChefServer, chefUserName, chefUserFirstName, chefUserLastName, and chefUserEmail.

FIGURE 6 - ARM TEMPLATE - PARAMETERS

The parameters sections can be summarized into these logical areas:

- Where you want to deploy this stack.
- Web application administrators account and Virtual machine administrator account credentials for the various stack components.
- Communication ports for Deep Security.
- Virtual machine size and number of test virtual machines.

PROTECTING AZURE VIRTUAL MACHINE WITH DEEP SECURITY

This solution stack provides two ways of deploying deep security agents on an Azure VM to add various security controls:

TREND MICRO AZURE EXTENSION

The Azure Virtual Machines Agent (VM Agent) is a secured, light-weight process that installs, configures, and removes VM extensions on instances of Azure Virtual Machines. The VM Agent acts as the secure local control service for your Azure VM. ([Source](#))

As a part of this stack deployment, we provide two test virtual machines (Windows and Linux) that have Deep Security agents already installed via Trend Micro Deep Security VM extensions on Azure.

TREND MICRO CHEF COOKBOOKS

Configuration Management is a key aspect in configuring servers, configuring server applications, and handling security. Chef can also be used to install and configure Trend Micro agents. As part of the stack launch, we deploy Chef Automate and a framework that allows any VM's to bootstrap to Chef Automate when they get provisioned.

ADD PROTECTION TO TEST AZURE VIRTUAL MACHINES (EXERCISE)

Deep Security Agents are already installed on these test Azure Virtual Machines as a part of the stack launch. The next step is to enable protection and assign security policies to the Azure VMs from Deep Security Manager. Deep Security provides out-of-the-box security policies based on various Operating Systems. To assign a policy to the test VM:

- Login to the **Deep Security Manager Web Console** using the URL and credentials provided via email.
- Click on the “**Computers**” tab from the top main menu.
- There should be two VMs listed here: One **Microsoft Windows** based and the second one **Linux Ubuntu** based.



Name	Platform	Policy	Status	Send Policy Successful
104.45.145.72	Ubuntu Linux 14 (64 bit)	None	Update of Configuration Pending (Heartbeat)	N/A
104.45.152.166	Microsoft Windows Server 2012 R2 (64 bit)	None	Update of Configuration Pending (Heartbeat)	N/A
publicdnstrendsm6x3x17pgq4nu.eastus.cloudapp.azure.com	Red Hat Enterprise 7 (64 bit)	Deep Security Manager	Update of Configuration Pending (Heartbeat)	5 Minutes Ago

- Double click on the **Windows test Azure VMs** one by one and then under “**General**” select **Policy** in the “Policy” dropdown list.
 - **Linux Ubuntu test VM:** Select the Linux policy
 - **Windows test VM:** Select the Windows 2012 policy

Computer: 40.121.143.158 Help

Overview
Anti-Malware
Web Reputation
Firewall
Intrusion Prevention
Integrity Monitoring
Log Inspection
Interfaces
Settings
Updates
Overrides

General Actions Events

General

Hostname: 40.121.143.158 (Last IP Used: 40.121.143.158)
Display Name:
Description:
Platform: Microsoft Windows Server 2012 R2 (64 bit) Build 9600
Group: Computers
Policy: Base Policy > Windows > Windows Server 2012 Edit
Asset Importance: None Edit
Download Security Updates From: Default Relay Group Edit

Status

Agent

Status: Managed (Online)
Anti-Malware: Off, not installed, no configuration
Web Reputation: Off, not installed
Firewall: Off, not installed, no rules
Intrusion Prevention: Off, not installed, no rules
Integrity Monitoring: Off, not installed, no rules
Log Inspection: Off, not installed, no rules
Online: Yes

Save Close

FIGURE 7 - ASSIGN POLICY TO TEST AZURE VM



The Deep Security Agent and Deep Security Manager communicate with each other at a regular time interval. By default, it is set to 10 minutes. If you notice the status of the VM is reported as “Update of Configuration Pending (heartbeat)”, that just means the agent has not performed a heartbeat yet. There is no action required, as the policy update will be pushed to the agent once the heartbeat occurs.

INTEGRATE

Most of the integration steps are already handled by the solution stack template. The only integration step that is required to be performed post deployment is to configure Trend Micro Deep Security to send system and security events to Splunk.

CONFIGURE TREND MICRO DEEP SECURITY FOR SYSTEM EVENT LOG FORWARDING (EXERCISE)

The integration of Trend Micro Deep Security for system events forwarding to Splunk Enterprise is done via the system settings (**Administration System Settings SIEM**) configuration, as shown below:

- Login to **Deep Security Manager Web Console** using the URL and credentials provided via email.
- Click **Administration** from the top menu.
- Click **System Settings** from the left pane.
- Click on the **SIEM** tab under System Settings and then specify the following details:
 - **FQDN** (fully qualified domain name) of the Splunk server. The FQDN for the Splunk can be retrieved from the stack credentials sent to you via email earlier.
 - “Forward System Events to a remote computer” is **enabled**.
 - In **UDP port** textbox, enter port **5005**.
 - Syslog Format is set to “**Common Event Format**.”

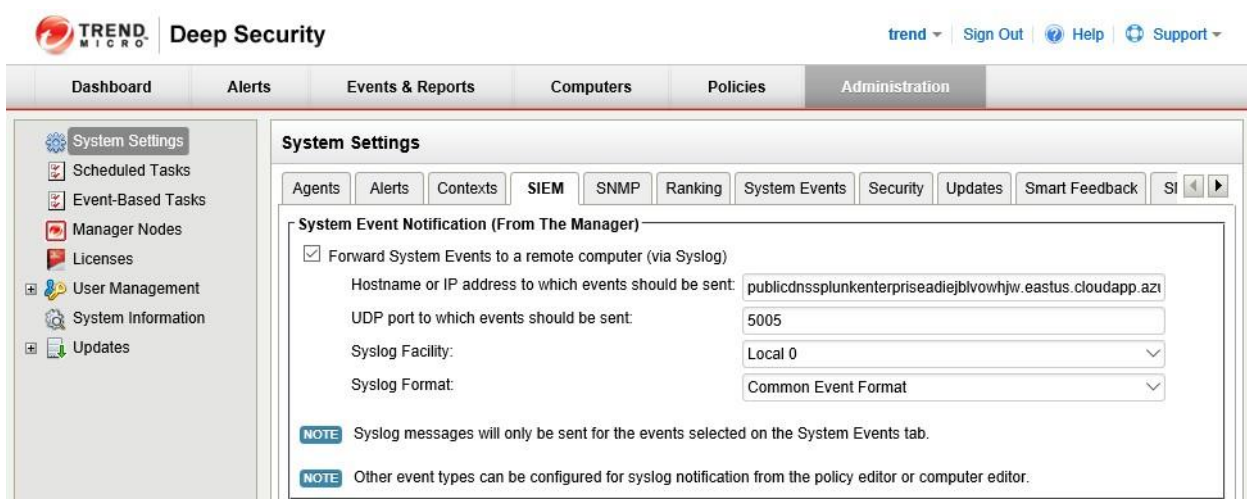


FIGURE 8 - SYSTEM EVENT FORWARDING TO SPLUNK

CONFIGURE TREND MICRO DEEP SECURITY FOR SECURITY EVENT LOG FORWARDING (**EXERCISE**)

The integration of Trend Micro Deep Security for security event forwarding to Splunk is done via Policy configuration. Deep Security allows Policy inheritance, where child policies inherit their settings from their parent Policies. This way, you can create a policy tree that begins with a top/base parent policy configured with settings and rules that will apply to all computers. It is recommended to set the integration details at the Top (root/base) policy **as shown below (and in the image on the next page)**.

Select “**Policies**” in the menu bar - Click on the “**Base Policy**” which opens a pop-up. In the pop-up screen, go to settings and select “**SIEM**,” then specify the following details:

- **FQDN** (fully qualified domain name) of the Splunk server. The FQDN for the Splunk server can be retrieved from the credentials sent to you via email earlier.
- Ensure the “**Forward Events to**” and “**Relay Via Manager**” options are selected.
- In the **UDP** port textbox enter port **5005**.
- Syslog Format is set to “**Common Event Format**.”

Policy: Base Policy

Overview

Anti-Malware

Web Reputation

Firewall

Intrusion Prevention

Integrity Monitoring

Log Inspection

Interface Types

Settings

Overrides

Computer

Network Engine

Scanning

SIEM

Anti-Malware Event Forwarding (From The Agent/Appliance)

Use Default Settings:

Forward Events to a remote computer (via Syslog): No

Forward Events To:

Direct forward

Relay via the Manager

Hostname or IP address to which events should be sent:

publicdnssplunkenterpriseadiejblvowhjlw.eastus.cloudapp.azure.com

UDP port to which events should be sent:

5005

Syslog Facility:

Local 0

Syslog Format:

Common Event Format

Do Not Forward Events

Web Reputation Event Forwarding (From The Agent/Appliance)

Use Default Settings:

Forward Events to a remote computer (via Syslog): No

Forward Events To:

Direct forward

Relay via the Manager

Hostname or IP address to which events should be sent:

publicdnssplunkenterpriseadiejblvowhjlw.eastus.cloudapp.azure.com

UDP port to which events should be sent:

5005

Syslog Facility:

Local 0

Syslog Format:

Common Event Format

Do Not Forward Events

Firewall and Intrusion Prevention Event Forwarding (From The Agent/Appliance)

Use Default Settings:

Forward Events to a remote computer (via Syslog): No

Forward Events To:

Direct forward

Relay via the Manager

Hostname or IP address to which events should be sent:

publicdnssplunkenterpriseadiejblvowhjlw.eastus.cloudapp.azure.com

UDP port to which events should be sent:

5005

Syslog Facility:

Local 0

Reset

Save

Close

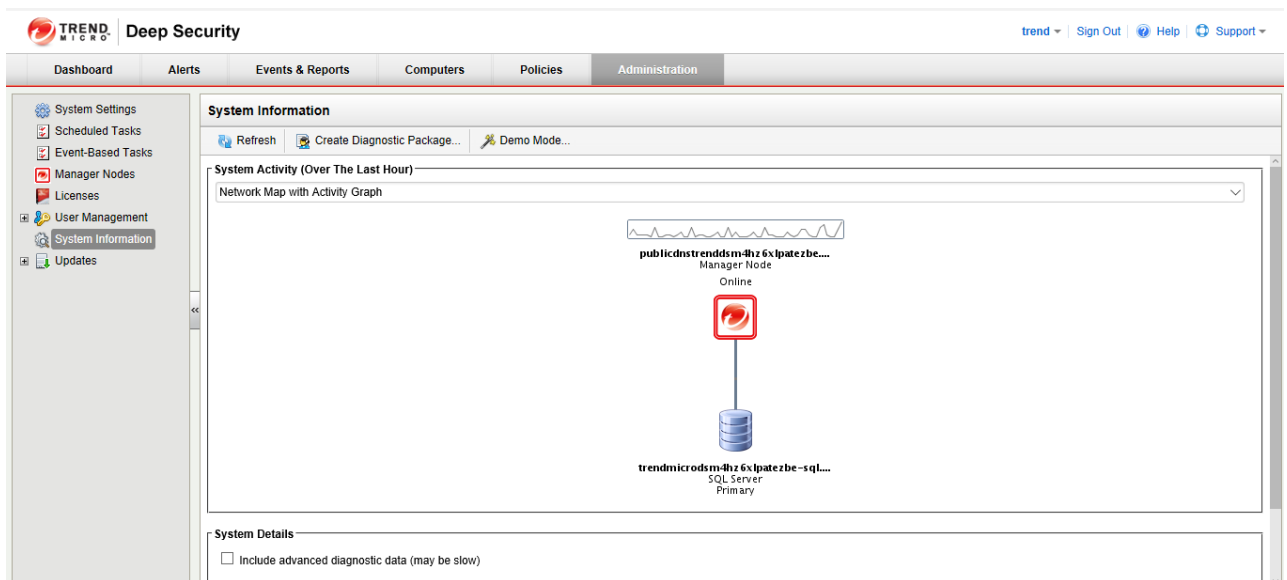
FIGURE 9 - SECURITY EVENT FORWARDING TO SPLUNK

ANALYZE

GENERATE SAMPLE EVENTS (EXERCISE)

Now that the integration piece is completed, we are all set to analyze security events in the Splunk Web Console. For this hands-on lab session, we will leverage the Trend Micro Deep Security Demo mode setup to generate sample data for us.

- Login to **Deep Security Manager Web Console** using the URL and credentials provided via email.
- Click **Administration** from the top menu.
- Click **System Information** from the left pane.
- From the System Information page, click **Demo Mode** to start the wizard.



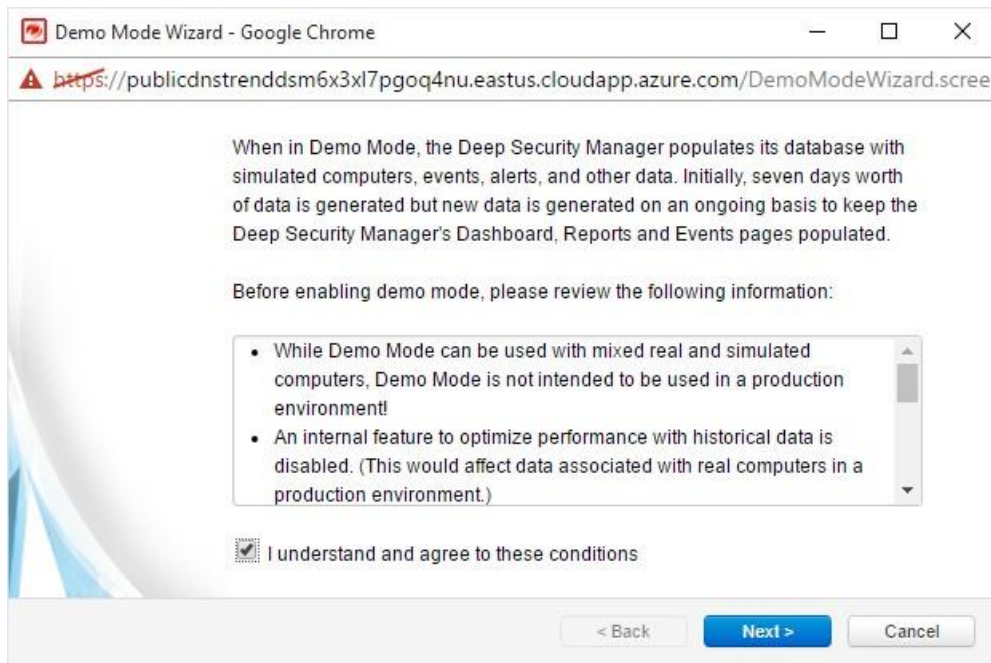


FIGURE 10 - DEEP SECURITY DEMO MODE

- Check **I understand and agree to these conditions** and click **Next**. Then click **Finish**.



The Demo mode will take roughly 20-30 minutes to complete, but as the task is being completed you can start visualizing the event data in Splunk.

ANALYZE DEEP SECURITY EVENT DATA IN SPLUNK’S WEB CONSOLE (EXERCISE)

Once the installation and integration steps are done, you are all set to analyze Deep Security event data in Splunk’s web console. You can run searches, identify anomalies, and correlate events across your protected workloads. The Splunk platform offers many options for data analysis and visualization. As a part of stack launch, we will deploy the Deep Security App for Splunk. This app contains parsing logic, saved searches, and dashboards for monitoring.

- Login to the **Splunk Web Console** using the URL and credentials provided via email.
- From the **Apps** panel on the left, select the **Trend Micro Deep Security for Splunk** app.



FIGURE 11 - TREND MICRO DEEP SECURITY FOR SPLUNK

- From the top menu bar, expand **Saved Searches** using the drop-down option and then select **System Events** and search for “**Deep Security – System Events.**” You will notice the raw data is coming through as part of the integration exercise we did previously.

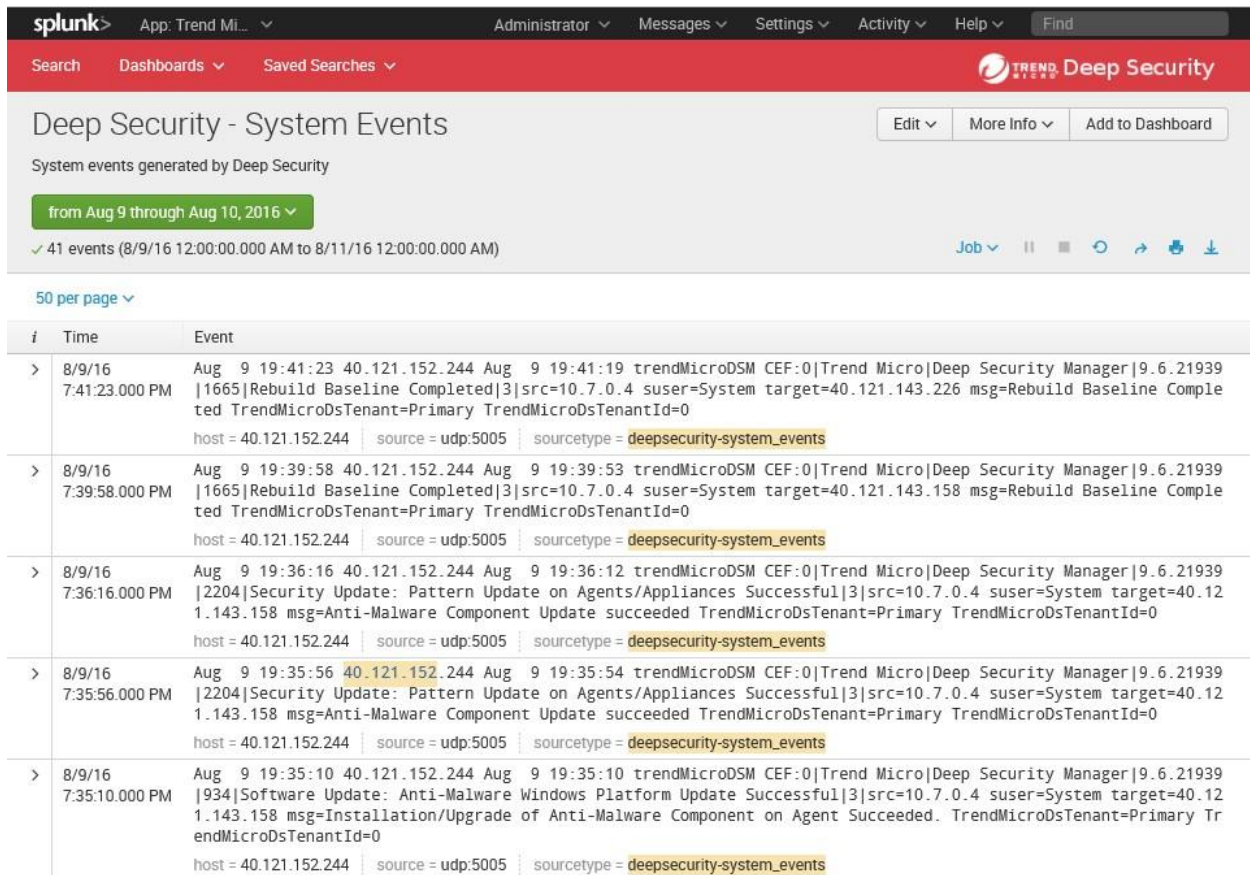


FIGURE 12 SPLUNK WEB CONSOLE WITH TREND MICRO DEEP SECURITY SYSTEM EVENTS

Again, from the top menu bar, expand **Saved Searches** using the drop-down option and then select **Security Events** and search for “**Deep Security – All Security Events.**” You will notice that the raw data is coming through and there are various security events reported, such as firewall traffic that is not allowed by our set firewall policy.

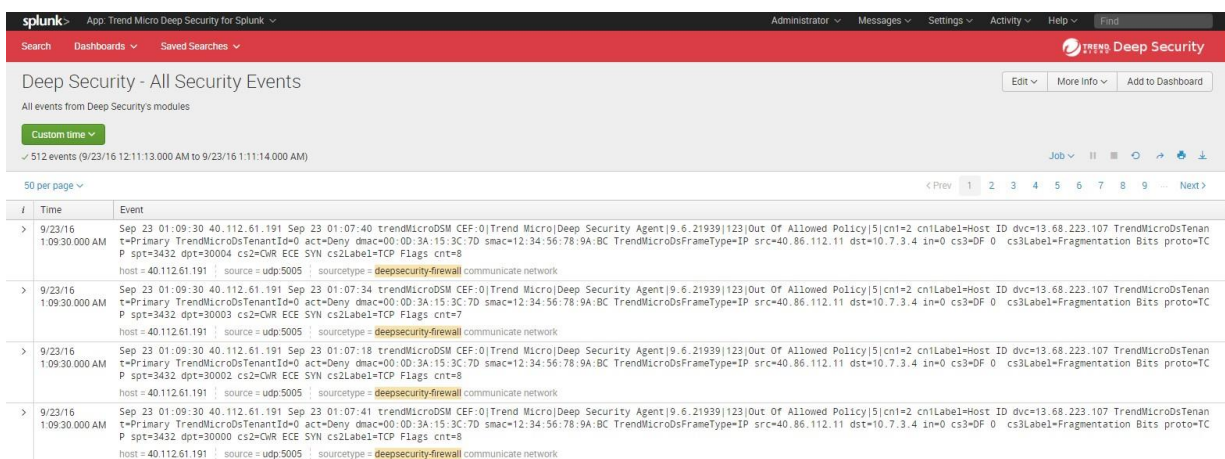


FIGURE 13 DEEP SECURITY – ALL SECURITY EVENTS



If you don't see any event data, then try reloading the search from the refresh button on the right few times.

Now that you have the event data coming into Splunk, it's time to observe some pre-built dashboards from the Trend Micro Deep security app for Splunk.

Dashboards are a powerful visualization tool to help accelerate the time to identify anomalies and indicators of compromise (IOC). The saved searches powering these dashboards can also be leveraged for forensic investigations, and to reduce the time it takes for root cause analysis and remediation.

- From the top menu bar, expand **Dashboards** using the drop-down option and then pick available dashboards one by one to observe and analyze security data:

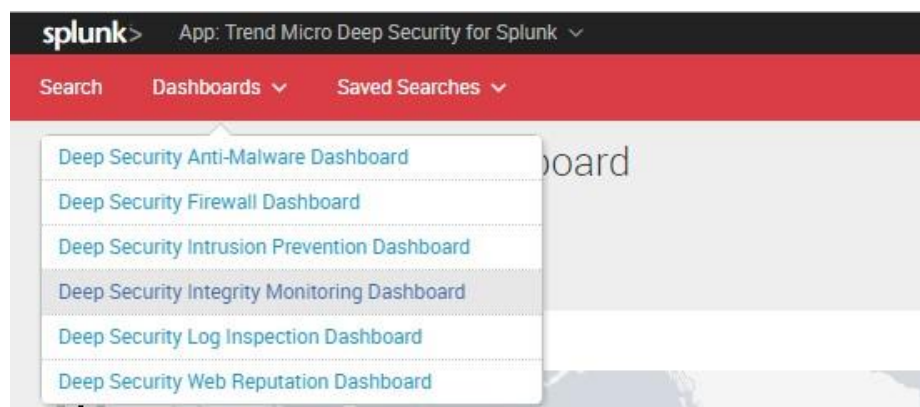
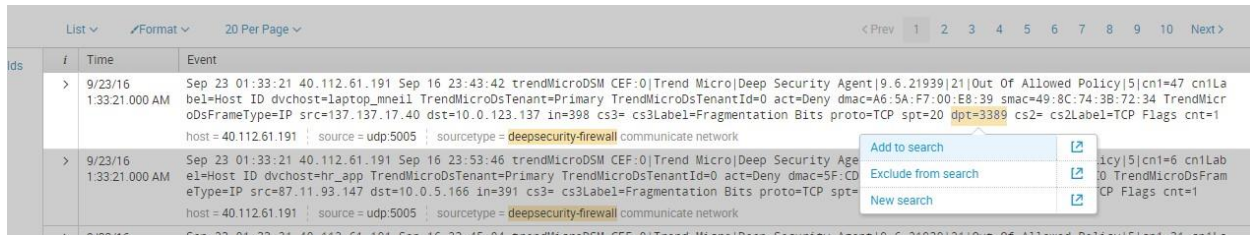


FIGURE 14 TREND MICRO DEEP SECURITY FOR SPLUNK DASHBOARD

For example, picking a firewall dashboard will show you that there are many “out of allowed policy” events being generated. These are generated because our Azure VMs are being hit by traffic that is not specifically allowed. You can further click on the “Event Name” and start the search / query screen.

From this search screen, you can easily expand your search criteria and start filtering data for your analyses, etc. Expanding the search filter is as easy as picking a data field in the search results by clicking on it and selecting to add it to the search (such as “dpt” is 3389). Now the search will filter all the events where the destination port is the RDP port.



ids	i	Time	Event
>	9/23/16 1:33:21.000 AM	Sep 23 01:33:21 40.112.61.191 Sep 16 23:43:42 trendMicroDSM CEF:0 Trend Micro Deep Security Agent 9.6.21939 21 Out Of Allowed Policy 5 cn1=47 cn1La	bel=Host ID dvchost=laptop_mnell TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dmac=A6:5A:F7:00:E8:39 smac=49:8C:74:38:72:34 TrendMicroDsFrameType=IP src=137.137.17.40 dst=10.0.123.137 in=398 cs3= cs3Label=Fragmentation Bits proto=TCP spt=20 dpt=3389 cs2= cs2Label=TCP Flags cnt=1 host = 40.112.61.191 source = udp:5005 sourcetype = deepsecurity-firewall communicate network
>	9/23/16 1:33:21.000 AM	Sep 23 01:33:21 40.112.61.191 Sep 16 23:53:46 trendMicroDSM CEF:0 Trend Micro Deep Security Agent 9.6.21939 21 Out Of Allowed Policy 5 cn1=47 cn1La	el=Host ID dvchost=hr_app TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dmac=5F:CD eType=IP src=87.11.93.147 dst=10.0.5.166 in=391 cs3= cs3Label=Fragmentation Bits proto=TCP spt= host = 40.112.61.191 source = udp:5005 sourcetype = deepsecurity-firewall communicate network

FIGURE 15 EXPANDING THE SEARCH

Similarly, you can observe other dashboards such as Log Inspection. The Log Inspection module lets you set alerts on specific log entries that are of concern from a security perspective. For example, it is useful to track specific user logins to a system. In the demo data you will find various activities such as:

Event Description	Event Count	Percent of Total
Successful login during weekend	101	1.219218
Detected an error in the protocol stream and has disconnected the client	101	1.219218
Successful login during non-business hours	84	1.014003
Exceeded maximum allowed failed logon attempts	83	1.001931
Multiple connection attempts from same source.	50	0.603573

FIGURE 16 LOG INSPECTION EVENT

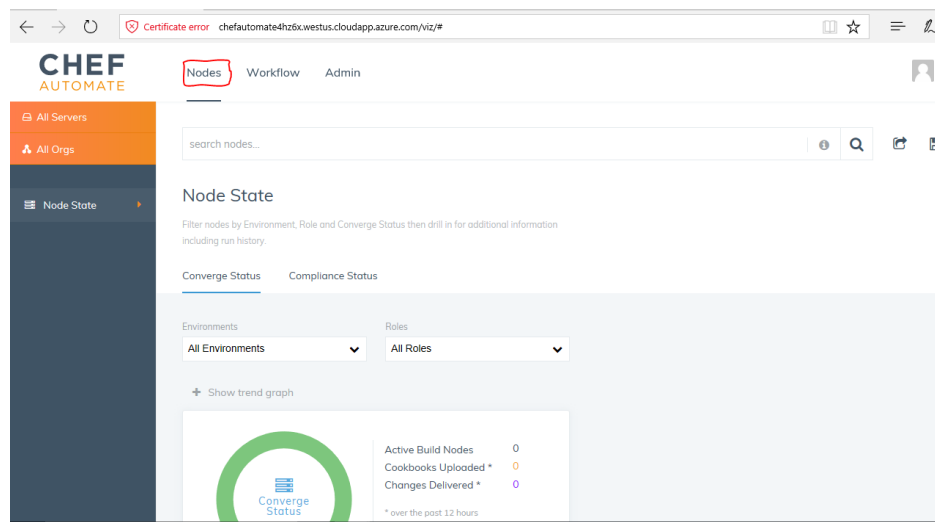
- Click any one of the events of your interest and observe the raw event data, and spend some time with the search filters to do analyses and correlation with other security event data.

Explore Chef Automate and the Chef Node(s) Installed (OPTIONAL EXERCISE)

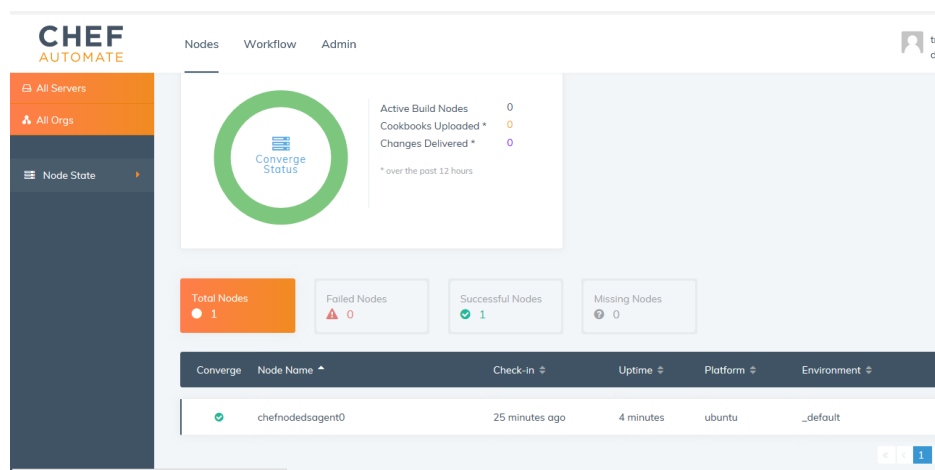
We have provisioned one test virtual machine as part of stack launch that is registered as a node for Chef Automate. As an additional exercise, if you are familiar with the Chef orchestration tool, you can go ahead and explore and experiment with the Chef node(s).

- Access the **Chef Automate Web Console**. The URL to access the Chef Web Server console is provided in the email sent to you earlier.
- Login to the **Chef Automate Web Console** using the credentials provided to you in that same email. If asked to "Please enter your VM Name to continue to the web interface," type "**ChefAutomate.**"

Below is screen capture of the navigation in the Chef Automate web console:



Scroll down, and you should be able to see the installed Chef node:



Click on the node agent to view more details:

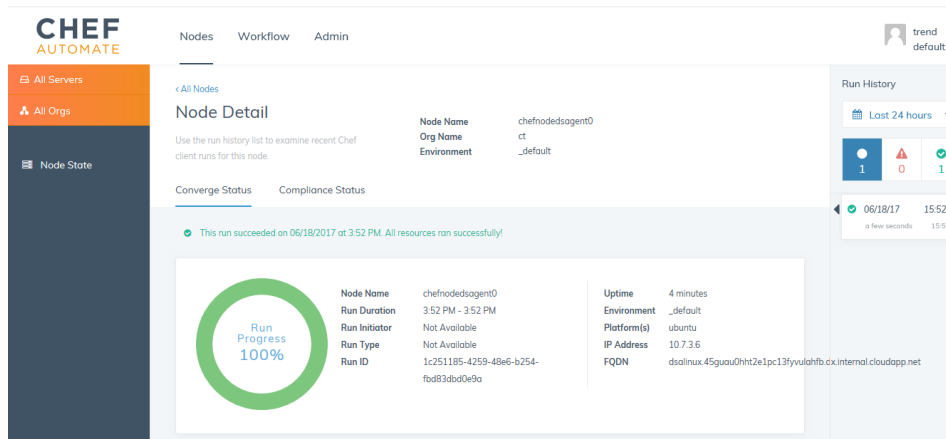


FIGURE 17 - REGISTERED NODE IN CHEF