

A grayscale photograph of a man with short dark hair and a beard, wearing a dark jacket, sitting at a desk and looking at a computer monitor. The monitor displays a complex data table with many columns and rows. The desk is modern, with a lamp and other equipment visible in the background. The overall tone is professional and tech-oriented.

A Deeper Look at the Splunk Integration that Keeps SOC Teams on Track

Introduction

Following our recent look at the [benefits of our Splunk integration](#), we wanted to share a more detailed look at the features of the integration.

As we know, segmentation is a foundational part of modern security defense in depth practices to protect data center and cloud environments from east-west traversal attacks – and it is often managed by security operations (SecOps). Security operations teams have several challenges when executing their mission e.g. information overload, alert fatigue, event management, lack of documented process, etc. Use of technology such as SIEM (e.g. Splunk) helps alleviate the challenges faced by SecOps teams. Additionally, Splunk integrations from vendors such as Illumio can help reduce these challenges even more, by having a laser focus on their SecOps audience's needs and actively striving to reduce the noise overhead that SecOps teams face.

In other cases, Operations team are charged with managing Illumio software on workloads, but may not have access to the Illumio PCE console. By using Splunk, Operations teams can monitor the status of Illumio software and other messages generated from workloads by utilizing the Illumio integration with Splunk.

Similarly, using Illumio generated traffic flows for all communication between workloads, and leveraging Splunk as a central repository of long term workload management data, Audit teams can gather necessary information for audits such as PCI or SWIFT.

This is why we have such tight integration – and why Splunk users will gain even greater value from Illumio.

Validated by Splunk

Illumio App for Splunk and Technology Add-on for Illumio have been certified by Splunk. This provides the confidence that Splunk has examined the app for adhering to the best practices for Splunk platform development. Also, Splunk reviews the source code for security vulnerabilities and adherence to a strict set of criteria. All updates to the app are subject to the same rigor. Illumio completes this rigorous certification process to ensure that Illumio Core™ works with Splunk Enterprise Server and Splunk Enterprise Security, providing confidence in the joint solution.

How We Integrate

Let's have a deeper look at how we deliver the key benefits.

Technology Add-On for Illumio

The Technology Add-On for Illumio (TA-Illumio) for Splunk enriches Illumio Policy Compute Engine (PCE) data with Common Information Model (CIM) field names, event types and tags. This TA enables Illumio data to be generically used, either by searching directly using Splunk Query Language or with tools that utilize CIM e.g. Splunk Enterprise Security, Splunk App for PCI Compliance, and other apps in the Splunk ecosystem. By having fields extracted by TA-Illumio and available for use in search, direct searching can be done using Splunk's query language. Typical searches enabled by TA-Illumio includes:

- Top outgoing connections, by port or machine or location etc.
- Top incoming connections, by port or machine or location etc.
- Most active machines
- Most active source ports or services
- Machines communicating between Production and Development environments
- Machines with connections to/from a specific network (e.g. 10.0.0.0/8)
- Geolocating destination IPs (plot on a map)

Custom Alert Action and Adaptive Response

Splunk provides standard alert actions such as sending emails, notable events, and calling a Webhook URL. Vendors such as Illumio can provide custom alert actions, which are modular actions on top of standard alert actions. These custom alert actions let you invoke Python scripts that use APIs provided by vendors like Illumio.











The Technology Add-On for Illumio (TA-Illumio) provides a custom alert action within Splunk Enterprise for quarantining workloads managed by the PCE. On the Illumio PCE, administrators can configure a custom policy that restricts all inbound and outbound connections from a quarantined workloads, while still allowing SSH/RDP access from a management network. This policy is automatically applied to workloads which have quarantine labels. When the labels are changed on the workloads, the Illumio PCE recalculates the policy for these workloads and sends the updated quarantine policy down to the workloads in a few seconds. All of this is done while also preserving the in-memory state of the workload, logs and other information that can be utilized by forensics teams.

The Enterprise Security (ES) Suite app provides support for correlation/saved searches with notable actions. When a Splunk Enterprise Security correlation/saved

search—with notable events mapped—is executed and gets at least one event in the results, notable events are handled using a standard notable action. These notable events are visible in the Incident Review dashboard of Splunk Enterprise Security App. Splunk provides this Adaptive Response Framework in the Enterprise Security Suite by leveraging the modular action functionality provided in Splunk_SA_CIM. Illumio provides an Adaptive Response action for quarantining workloads by re-labelling workloads by calling an Illumio API to update labels on workloads. Using Splunk Enterprise Security's Adaptive Response Framework, Illumio PCE administrators can quarantine workloads managed by the PCE directly from Splunk Apps whenever the events are detected in Splunk.

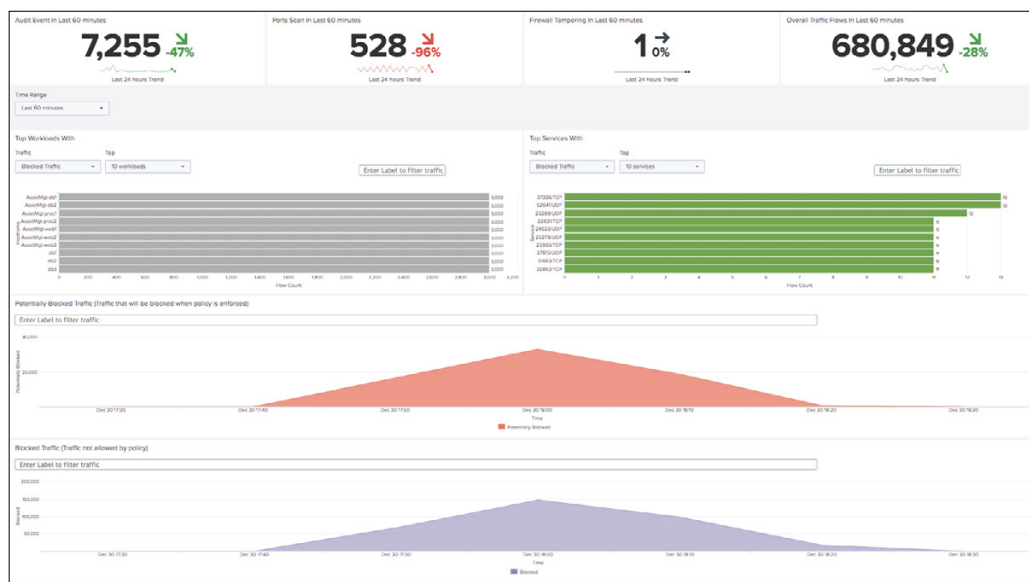
By calling Illumio APIs directly from Splunk, both Enterprise and ES, the integration provides administrator with a powerful tool. However, since labelling workloads is such a powerful tool, Illumio also provides an additional RBAC role to allow this action. Only users with this RBAC role can invoke the alerting actions. This reduces the risk of inadvertent labelling of untrained users invoking the quarantine action by accident.

CUSTOM ALERT ACTION

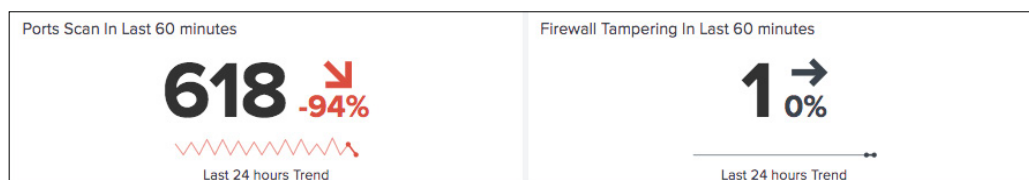
Alert action 	App 
 AWS SNS Alert Publish search result to AWS SNS	Splunk_TA_aws
 Log Event Send log event to Splunk receiver endpoint	alert_logevent
 Output results to lookup Output the results of the search to a CSV lookup file	system
 Output results to telemetry endpoint Custom action to output results to telemetry endpoint	splunk_instrumentation
 Quarantine Workload Custom action for marking a workload as quarantine.	TA-Illumio
 Run a script Invoke a custom script	system
 Send email Send an email notification to specified recipients	system
 Webhook Generic HTTP POST to a specified URL	alert_webhook

Security Operations Dashboard

The Security Operations dashboard allows admins to monitor the overall security state of the network, as determined from traffic flows reported by PCE instances. There is lot of useful functionality that underlays this dashboard that can be used by different types of users, not just Security Operations.



SECURITY OPERATIONS DASHBOARD



SECURITY OPERATIONS DASHBOARD: HEADLINE PANEL

Headline Panel

The headline panel provides a summary view of the state of the data center including traffic flows and events generated by Illumio. Useful headline items are:

- Port Scans:** These are determined by analyzing all traffic flow summaries to determine if any two hosts were communicating over 5 unique ports within a short time e.g. 1 minute. This panel also provides a drill down, which will show the list of hosts engaging in the port scan activity, their Illumio labels, and buttons to invoke both Workload Investigation and Workload Quarantine. Since port scans generally presage east-west traversal, they are an early indicator of an intruder probing the data center machines for vulnerabilities. By surfacing port scans, the machines involved and their labels, as well handy access for further investigation and taking action, security operations staff will find this panel handy.
- Firewall Tampering:** Illumio manages the firewall on hosts either iptables on Linux or WFP on Windows. One of the first actions taken by an attacker is to disable the host-based firewall. Illumio automatically detects this and will immediately restore the firewall. It also generates an event with type “agent.tampering”. This is another early indicator of an attacker on a system. The panel also provides a drill down which shows the workload information, as well as Illumio labels and buttons for both Workload Investigation and Workload Quarantine. Security operations staff will also find this headline feature very useful.

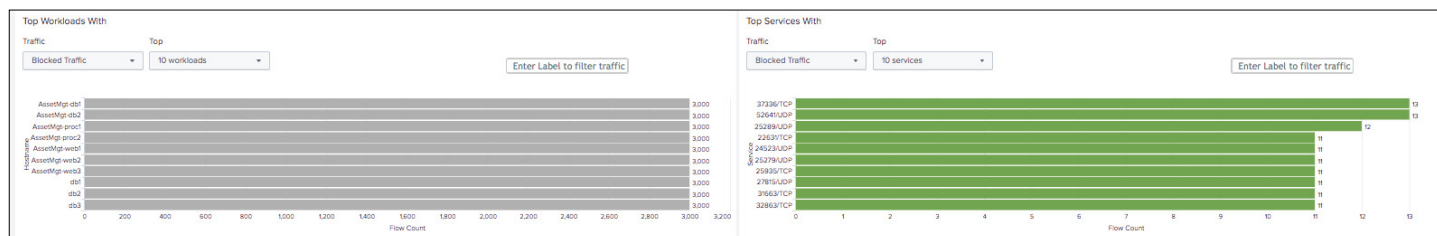
Top Hosts/Services

The “Top Hosts” panel identify the hosts that have the most blocked traffic or most potentially blocked traffic. This indicates hosts under attack. The “Top Services” panel shows services that are most blocked or potentially blocked, which indicates where policy coverage can be improved. Both of these panels can be further examined by filtering using Illumio labels.

Traffic Flow Analysis Using Labels

These charts visualize traffic flows that are potentially blocked, blocked or allowed across the entire data center. Users can apply labels to overlay traffic associated with those workloads to analyze visually relative traffic for that labels to the traffic across the data center. This can be used to prioritize efforts and allocate resources. For instance, if there is a spike in traffic in Production machines in the data center, that will require investigation. Whereas a spike in traffic in Development machines need not require the same effort.

TOP HOSTS PANEL



TRAFFIC FLOW ANALYSIS

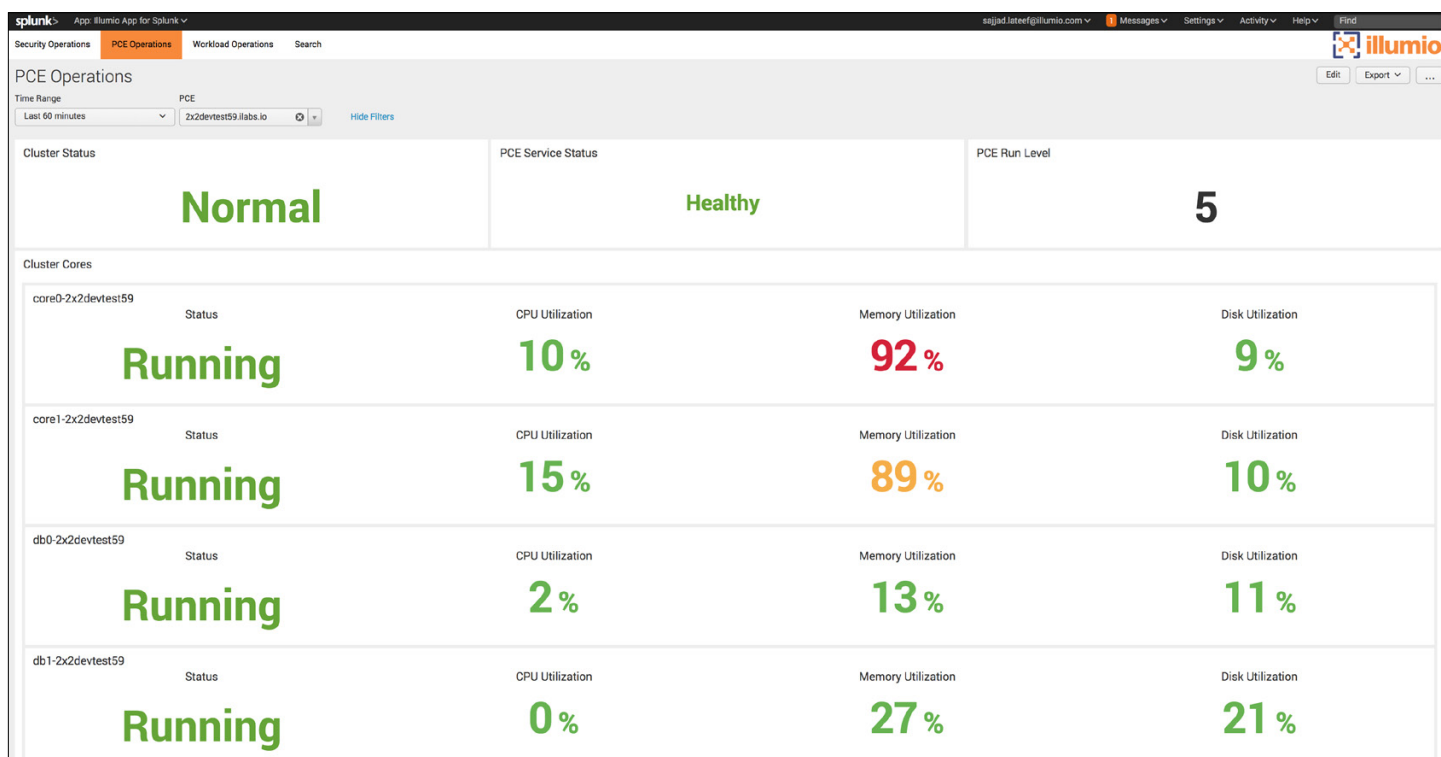


PCE Operations Dashboard

The PCE operations dashboard enables Splunk admins to monitor the health of one or more PCEs from a single screen. This includes the overall PCE cluster status, service status summary, along with the per-node service status, CPU, Memory & Disk utilization metrics. Since Splunk maintains a history, by expanding the time range through the menu, users can observe trends in system performance. Having historical system activity is useful when troubleshooting or root-causing issues.

Since multiple PCEs can be monitored from a “single pane of glass”, it saves time and effort by operations teams.

PCE OPERATIONS DASHBOARD



Workload Operations Dashboard

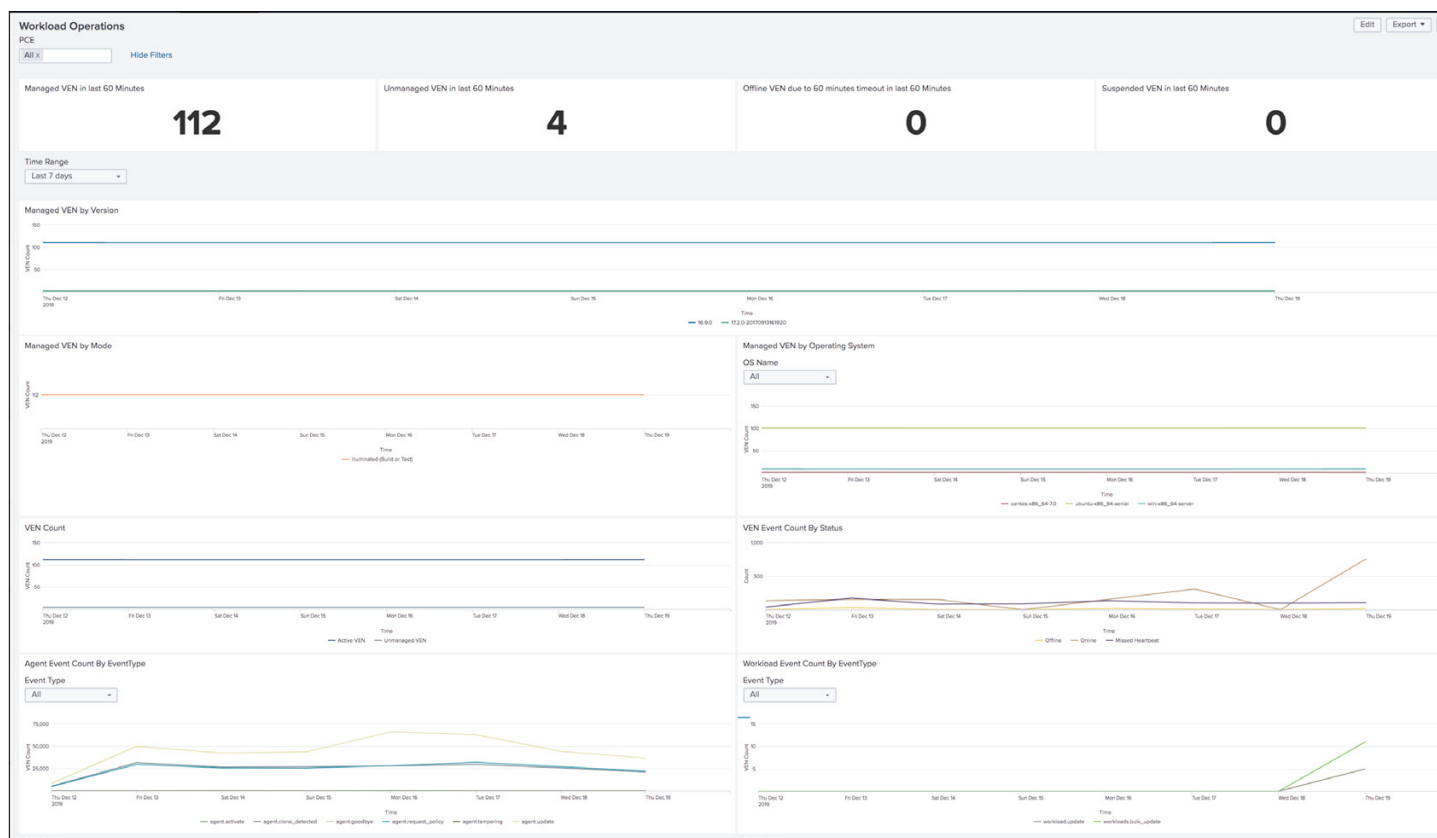
The Workload Operations dashboard enables Splunk admins to monitor the Workloads managed by one or more PCE instances. The dashboard displays VEN deployment statistics as well as VEN-reported events.

The top headline panel of this dashboard provides a summary view of the Workloads in the datacenter – how many are under management currently, workloads that are unmanaged but used in Illumio policy, and how many agents went offline or were suspended. This gives users a pulse into the datacenter by having the most useful information up front and center.

Additional panels show a time-series chart of various useful metrics for workloads: The default time range shown is 72 hours, but, can be increased to show a longer duration if necessary.

- Managed agents by agent version
- Managed agents by mode – either Enforced or Illuminated
- Managed agents by operating system of the workload
- Workloads that are managed or unmanaged,
- Workloads that have been taken offline or suspended
- Agent events by event type – these are messages generated regarding the state of the Illumio VEN, e.g tampering, updates, goodbye (VEN graceful shutdown)
- Workload events by event type – these are messages generated regarding the state of the workload itself, e.g. workloads online, label updates, interface changes, updates

WORKLOAD OPERATIONS DASHBOARD



Workload Investigation Dashboard

Workload investigation dashboard is used to correlate all known information about the workload, from multiple sources into a single panel. By having all of this information in one handy panel, an administrator has all needed information for multiple use-cases – Auditing, Compliance, troubleshooting, security, etc.

A user can specify a workload to investigate by specifying a hostname. Wildcards can also be used in hostnames to search for a set of workloads. An Auditor can use this dashboard for a specific time range to get most of the necessary evidence for auditing the security posture of a workload. By utilizing this data, PCI auditors will get necessary evidence for the CDE (Cardholder Data Environment) as well as the Connected Systems.

This dashboard has three panels:

- Workload Details – this provides hostname, IP address, OS information, workload state, policy state, labels
- Workload Audit Events – all events that apply to the selected workloads. This includes events related to policy.
- Workload Traffic Flows – all traffic flow summaries that either originated from or terminated at the specified workloads

WORKLOAD INVESTIGATION DASHBOARD

Workload Investigation

Time Range: Last 24 hours | PCE: All | Hostname/IP: *

Workload Details

Host Name	Public IP	OS Name	Online	Status	Policy Applied At	Policy Sync State	Mode	Log Traffic	App Label	Role Label	Env Label	Loc Label	PCE
null		null	true	-	-	-	illuminated	false	-	Web	Production	Amazon	poc1.illum.io
peter-test-4		null	true	-	-	-	illuminated	false	-	Database	Production	Amazon	poc1.illum.io
peter-test-ven		linux	true	-	-	-	illuminated	false	-	Web	-	-	poc1.illum.io
s3test1	103.66.112.226	centos x86_64 7.0	true	active	2019-11-16T01:18:50.292815Z	applied	illuminated	false	-	Web	Production	Amazon	poc1.illum.io
s3test2	203.88.139.34	centos-x86_64-7.0	true	active	2019-11-19T19:07:40.151768Z	applied	illuminated	true	-	Database	Staging	Azure	poc1.illum.io

Audit Events

Include Event Type: All | Exclude Event Type: None

Timestamp	Event Type	Host Name	Source IP	Notification Type	Severity	Status	PCE
2019-11-26T14:02:20.269Z	workload_service_report.update	s3test2	203.88.139.34	-	info	success	poc1.illum.io
2019-11-26T12:56:01.943Z	workload_service_report.update	s3test1	103.66.112.226	-	info	success	poc1.illum.io

Traffic Events

Policy Decision: All

Timestamp	Source IP	Source Host	Direction	Destination IP	Destination Host	Destination Port	Protocol	Policy Decision	Source App Label	Source Role Label	Source Env Label	Source Loc Label	Destination App Label	Destination Role Label	Destination Env Label	Destination Loc Label	PCE
2019-11-27T04:09:57+05:30	10.0.0.23	-	I	10.0.15.255	s3test2	138	UDP	potentially-blocked	-	-	-	-	-	Database	Staging	Azure	poc1.illum.io
2019-11-27T04:09:55+05:30	10.0.0.140	-	I	10.0.15.255	s3test2	137	UDP	potentially-blocked	-	-	-	-	-	Database	Staging	Azure	poc1.illum.io
2019-11-27T04:09:54+05:30	10.0.0.47	-	I	10.0.15.255	s3test2	137	UDP	potentially-blocked	-	-	-	-	-	Database	Staging	Azure	poc1.illum.io
2019-11-27T04:09:48+05:30	10.0.11.144	-	I	10.0.15.255	s3test2	138	UDP	potentially-blocked	-	-	-	-	-	Database	Staging	Azure	poc1.illum.io
2019-11-27T04:09:39+05:30	10.0.9.92	-	I	10.0.15.255	s3test2	138	UDP	potentially-blocked	-	-	-	-	-	Database	Staging	Azure	poc1.illum.io
2019-11-27T04:09:29+05:30	10.0.12.91	-	I	10.0.15.255	s3test2	137	UDP	potentially-blocked	-	-	-	-	-	Database	Staging	Azure	poc1.illum.io

Alert Configuration & Alerts

By using alert configurations, administrators can leverage the power of the Splunk platform to automate alerting on events that are of interest and taking an action automatically. Using the Illumio App for Splunk, an administrator can create or update alert configurations using the Alert Configuration page.

In the Illumio App for Splunk, you can configure a few different types of alerts

PCE system health events, choose which level of event severity (warning, error, or critical) to alert on. For details on conditions that trigger severity of warning or above, see section on PCE Health Monitoring with Syslog in the PCE Operations Guide.

Changes to draft rules or draft rulesets on the PCE. For example, a draft rule might be created that affects all workloads or a draft ruleset changed for a very large scope or to a scope for highly secure workloads. Since this is a very wide-ranging effect, an automated alerted can trigger an user to investigate and confirm the change was correct or intentional.

A policy provision event. In PCE 19.1.0 and above, the policy provision event contains the number of workloads affected by a policy provision. If this number is greater than a specified threshold of affected workloads, an automated alert can trigger an administrator to investigate.

Changes to workload like label adds or changes. These events indicate a change in a workload security posture. Highly secure workloads with secure labels changed could indicate a reduction in security for that workload. Lower security workloads acquiring secure labels could indicate a privilege escalation on that workload, allowing it access to higher security workloads. Alerting on changes to sensitive labels can help an administrator keep track of these type of security posture changes.

The actions associated with the event can be any Splunk Alerting Action – from sending an email to calling a webhook. Alerts can be configured for a variety of useful Illumio data. After creating alert configurations, users can access the Alerts page to set up the usage of the alerts, such as sending emails whenever an alert is triggered.

Getting Started

Download the latest versions of the Illumio App for Splunk and Technology Add-On for Illumio from splunkbase.splunk.com. Quick start instructions are available from the details section on splunkbase.

Detailed documentation on installation and configuration is available on the Illumio Support site's Documentation section.



Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com/what-we-do.



See what customers have to say about Illumio.

The GARTNER PEER INSIGHTS Logo is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences and do not represent the views of Gartner or its affiliates.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085, Tel (669) 800-5000, www.illumio.com. Copyright © 2020 Illumio, Inc. All rights reserved. This document is protected by U.S. and international copyright and intellectual property laws. Illumio's products and services are protected by one or more U.S. and international patents listed at <https://www.illumio.com/patents>. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. To review a list of Illumio's trademarks, go to <https://www.illumio.com/trademarks>. Third-party trademarks mentioned in this document are the property of their respective owners.