Feature Highlights of 2016

This article describes some of the features that were added to Cisco Defense Orchestrator in 2016

December 2016

December 22, 2016

NAT Policy Management

Cisco Defense Orchestrator now supports reading, editing, searching, and creating NAT policies via an easy to use navigation wizard and advanced interface-based diagram, to show a full list of NAT policies (and their order) defined on an ASA device.

December 15, 2016

Obsolete Names (Objects) conversion

Your device's configuration contains legacy (obsolete) names ? Cisco Defense Orchestrator now enables, during objects issues resolution, to investigate across objects, object groups and now names to provide consistency across all objects used in policy and to assist with the conversion of names into object.

November 2016

November 18, 2016

Fully Shadowed Rules Support

You can now filter and identify superfluous network policies that will never handle traffic intended, as all traffic is handled by a rule(s) up in rule set order. Upon making a change to network policies, CDO will alert in case rule edited or added is shadowed by a different rule.

November 8, 2016

On-Prem Secure Device Connector

Cisco Defense Orchestrator enables direct communication between CDO and supported devices and services. This communication is enabled by CDO Secure Device Connector (SDC) acting as proxy between remote location and CDO cloud services. This service is available now in two deployment models as follows:

On-Prem Secure Device Connector – On-prem Secure Device Connector is a pre-configured virtual appliance dedicated to the requested account.

Cloud Secure Device Connector – All cloud Secure Device Connectors are provisioned automatically and managed by Cisco Defense Orchestrator team.

September 2016

September 29, 2016

Change Log

Continuous capture of both application (layer7) and network (layer3) policy changes performed via Cisco Defense Orchestrator within a single view across on-boarded devices and services. New Change Log lists at-a-glance view of most recent changes, while further revisions can be sorted and filters by device, change status, user and more. New Change Log functionality enables organizations to:

- Before and after inline incremental view (diff) of a network and application policy change (new, edited, and deleted rule; on-boarded or deleted devices and services, and more)
- Detection of policy change conflicts (occurring outside of Cisco Defense Orchestrator) and overwriting to/from a device or service
- Be able to answer Who, What, and When during an incident investigation or troubleshooting
- Export to a common format or 3rd party monitoring systems

Note Devices and services currently managed by Cisco Defense Orchestrator will initiate change log event collection only after first deploy or read. For more information, see "Secure Logging Analytics for FTD Devices" in *Managing FTD with Cisco Defense Orchestrator*.

Hit Rates. Cisco Defense Orchestrator now enable network operations users to evaluate policy rules outcome, on top of secure and scalable orchestration of policies, providing simple visualization for more accurate policy analysis and immediate actionable pivot to root cause, all in a single pane from the cloud. New Hit Rates functionality enable organizations to:

- Eliminate obsolete and never matched policy rules increasing security posture
- Optimize Firewall performance by instantly identifying bottlenecks as well as correct and efficient prioritization is enforced (most triggered policy rule prioritized higher)
- Maintain Hit Rates history information even upon device or policy rule reset for configured data retention (1 year)
- Strengthen validation on suspected shadow and unused rules based on actionable information. Removing doubt about update or delete of those
- Visualize policy rules usage in context to entire policy, leveraging pre-defined time intervals (day, week, month, year) and scale of actual hits (zero, >100, >100k, etc.), to evaluate impact on packets traversing the network

September 23, 2016

User interface redesign: Change to Light Theme

Redesign Cisco Defense Orchestrator user experience with a light brand new user experience theme making it more intuitive, self-explanatory, and Cisco style aligned. Try it out!

Multiple Objects Support

Cisco Defense Orchestrator object management now enables inline editing of object and object group value(s) as well as referencing multiple objects in a single access list parameter; automatically assigning to a user-defined object group (without the need for dm_inline_* object creation).

Approve or Reject Out-of-Band Policy Modifications

Enhanced policy orchestration enforcement by not only identifying a remote change performed or what the change was (on a device or service), but the ability to approve or reject identified out-of-band changes in real-time.

August 2016

August 18, 2016

Delegated Admin Support

Delegated Admin Support. Cisco Defense Orchestrator enable managing more than a single account (tenant) per user for easier and faster pivot between assigned accounts, while maintaining account security and complete data separation between accounts (tenants).

Import & Export of Pre-Defined Templates

Enable Import Pre-defined Templates. Leverage pre-defined device configuration templates, either available in your organization or from a third-party, to enable the scalable orchestration of onboarding all devices and services in your organization.

Devices and Services Connection Status Management

Device Connection Status Evaluation. New "*Reconnect*" button added to enable continuous monitoring of devices and services availability state, and alert for any change or actions need to be taken automatically or on-demand (e.g. update device credentials, renew device certificate).

August 11, 2016

Enhanced Template Management

Manage Template Enhancements. When creating new or updating an existing device template configuration file, a Cisco Defense Orchestrator user can now easily search across a device configuration file and assign multiple values to new or existing parameters, for use across account's devices.

. For further information on creating and managing template, see "Templates" in Managing FTD with Cisco Defense Orchestrator.