Symantec
A Division of Broadcom

Product Brief

Integrated Cyber Defense Exchange

Unify Product Events and Actions

At A Glance

Integrated Cyber Defense Schema

- An event model covering threat detection, response, information protection, system and application activity, audit, and more
- Common event objects covering file, process, session, user, email, network connections, and more

Collectors

- Parse, normalize, filter, and store event data
- Built-in collectors for many Symantec products
- Options to retain raw data prior to parsing, parsed fields not normalized are retained

Forwarders

- Third-party support for Splunk and AWS S3.
- Generic support for Syslog CEF, Kafka, RabbitMQ, and JSON

Action Orchestration

- Actions based on the OpenC2 standard
- Invoke actions on multiple targets simultaneously

SOC Front-Ends

- Splunk

Overview

Integrated Cyber Defense Exchange (ICDx) is a software layer that bridges Symantec and partner applications and addresses the complexity that customers and technical partners face when attempting to integrate multiple Symantec products.

ICDx standardizes the interfaces across Symantec products and provides technology partners and customers a central point for the following actions:

- Data collection, normalization, and archiving
- Data filtering and forwarding
- Action orchestration for platform functions through OpenC2 APIs
- Information exchange through messaging bus APIs

ICDx Admin Console

The Symantec ICDx console is browser-based and provides user interfaces to configure the overall system, collectors, forwarders, actions, and threat feeds. The console capabilities are intended to verify and monitor that event data is collected and forwarded correctly. Symantec ICDx has the following console operations:

- Dashboard with summary metrics
- Search and display event details by attribute
- Top N views by attribute and time span
- Configuration of collectors, forwarders, and action adapters
- Administrative settings for Active Directory, API keys, and archive management

Figure 1: ICDx Accelerates the Integration of Symantec and Third-Party Products

SOC Front-Ends

Symantec SOC View App Powered by Splunk

SOC View supports curated investigator views creating greater visibility across the Symantec product portfolio. The unified dashboard view gives security analysts the ability to quickly see the global distribution of threats.

Anomali Match

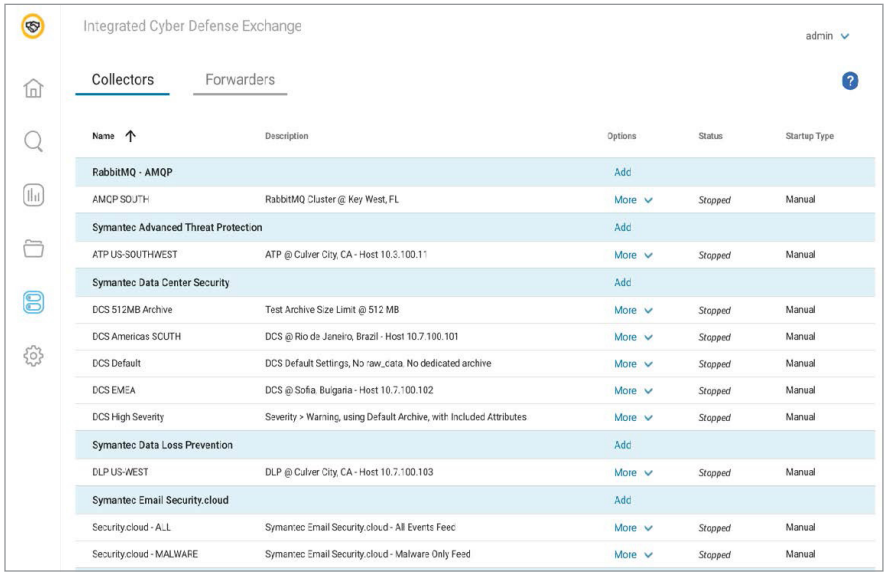
Anomali Match matches Symantec product events against validated threat intelligence to determine which events are malicious and merit further human investigation. The data is continuously correlated against new and existing threat intelligence to uncover evidence of breaches.

ICDx Collector Support

Symantec ICDx currently supports the following collectors:

- Symantec CloudSOC Cloud Access Security Broker (CASB) version 2.0
- Symantec Control Compliance Suite versions 11.x and later
- Symantec Endpoint Detection and Response versions 4.0 and later
- Symantec Advanced Threat Protection 3.2 and later
- Symantec Security Analytics version 8.1
- Symantec Endpoint Protection Manager version 14.0.1 (14 RU 1, 14.1, 14.2)
- Symantec Data Loss Prevention versions 14.6 and later
- Symantec Secure Web Gateway (ProxySG) versions 6.6 and later
- Symantec Data Center Security database (versions 6.5 and later)
- Symantec Email Security.cloud
- Symantec Web Security Service
- RabbitMQ (AMQP)

Figure 2: Symantec ICDx Console Showing Configured Collectors



ICDx Forwarder Support

Symantec ICDx currently supports the following forwarders:

- Amazon Web Services S3
- Apache Kafka
- Elasticsearch versions 6.x and 7.x
- Raw JSON
- Microsoft Azure Sentinel (Log Analytics)
- Symantec Information Centric Analytics 6.5
- Splunk versions 7.0 and 8.0
- Anomali Match
- RabbitMQ (AMQP)
- Syslog
- Syslog Common Event Format (CEF)

Software Requirements

- Ubuntu Server 16.04 LTS or 18.04 LTS
- Red Hat Enterprise Linux 7.4, 7.6, and 7.7
- Red Hat 7.6

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-ICDx-EN-PB101 June 12, 2020