Symantec

DATA SHEET

Symantec Integrated Cyber Defense Exchange

Unify Product Events and Actions

At a glance

Unified Event Schema

- 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
- Option to retain raw data prior to parsing, parsed fields not normalized are retained

Forwarders

- Third-party support for Splunk, ServiceNow, Elasticsearch, AWS S3 and RabbitMQ.
- 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, ServiceNow, Kibana (for Elastic Stack)

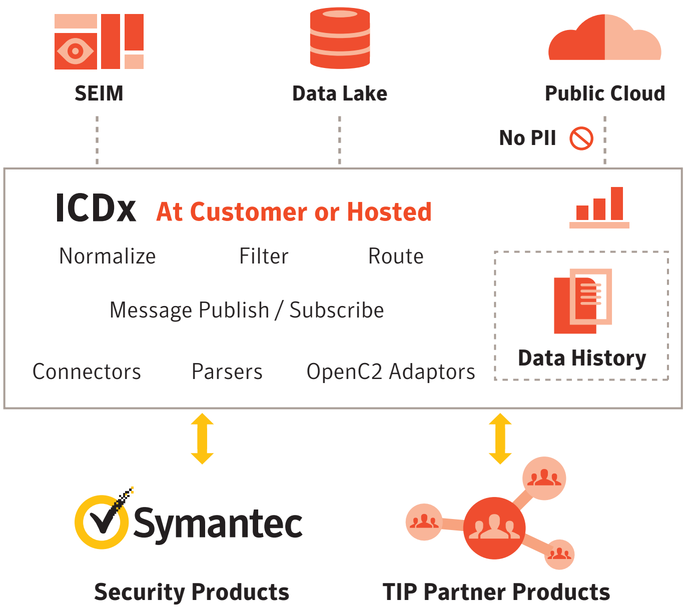
Introduction

Symantec is introducing a new software layer that bridges Symantec and Partner applications and addresses the complexity that Symantec Customer and Technical Partners face when attempting to integrate into multiple Symantec products.

Integrated Cyber Defense Exchange (ICDx) standardizes the interfaces across the Symantec products and provides technology partners and. customers a central point for:

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

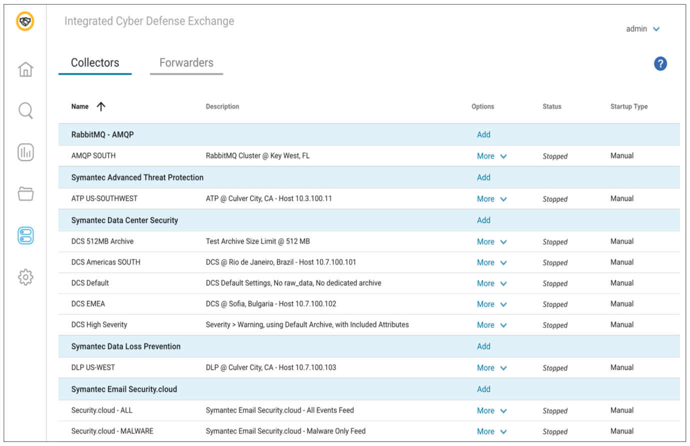
ICDx accelerates the integration of Symantec and third-party products



ICDx Admin Console

Symantec ICDx console is web 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 console showing configured collectors:



Name	Description	Options	Status	Startup Type
RabbitMQ - AMQP		Add		
AMQP SOUTH	RabbitMQ Cluster @ Key West, FL	More	*Stopped*	Manual
Symantec Advanced Threat Protection		Add		
ATP US-SOUTHWEST	ATP @ Culver City, CA - Host 10.3.100.11	More	*Stopped*	Manual
Symantec Data Center Security		Add		
DCS 512MB Archive	Test Archive Size Limit @ 512 MB	More	*Stopped*	Manual
DCS Americas SOUTH	DCS @ Rio de Janeiro, Brazil - Host 10.7.100.101	More	*Stopped*	Manual
DCS Default	DCS Default Settings, No raw_data, No dedicated archive	More	*Stopped*	Manual
DCS EMEA	DCS @ Sofia, Bulgaria - Host 10.7.100.102	More	*Stopped*	Manual
DCS High Severity	Severity > Warning, using Default Archive, with Included Attributes	More	*Stopped*	Manual
Symantec Data Loss Prevention		Add		
DLP US-WEST	DLP @ Culver City, CA - Host 10.7.100.103	More	*Stopped*	Manual
Symantec Email Security.cloud		Add		
Security.cloud - ALL	Symantec Email Security.cloud - All Events Feed	More	*Stopped*	Manual
Security.cloud - MALWARE	Symantec Email Security.cloud - Malware Only Feed	More	*Stopped*	Manual

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 actions
- Administrative settings for Active Directory, API keys and archive management

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 (currently in beta).

Symantec SOC Response App powered by ServiceNow

SOC Response enables incident management and automated workflows and orchestrated actions across the Symantec product portfolio (currently in beta).

Symantec SOC Investigator, a Kibana based front-end and Data Lake for Elastic

SOC Investigator like the SOC View app for Splunk, SOC Investigator provides curated investigator views creating greater visibility across the Symantec product portfolio for our customers who have deployed an an Elastic Stack.

ICDx Collector Support

Symantec ICDx currently supports collectors for:

- Symantec Endpoint Protection Manager version 14.0.1 (14 RU 1, 14.1, 14.2)
- Symantec Advanced Threat Protection 3.2 and later
- Symantec Data Loss Prevention versions 14.6 and later
- Symantec Secure Web Gateway (ProxySG) versions 6.6 and later
- Symantec Critical System Protection 6.5 and later
- Symantec Data Center Security database (versions 6.5 and later) via Symantec Critical System Protection collector
- Symantec Email Security.cloud
- Symantec Web Security Service
- RabbitMQ (AMQP)

ICDx Forwarder Support

Symantec ICDx currently supports the following forwarders:

- Splunk version 7.0 (via HTTPS)
- ServiceNow
- Raw JSON
- Kafka
- Symantec Information Centric Analytics 6.5
- Elasticsearch version 6.x
- RabbitMQ (AMQP)
- Amazon Web Services S3
- Syslog CEF

Software Requirements

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

About Symantec: Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.