Symantec
A Division of Broadcom

Product Brief

Integrated Cyber Defense Exchange

Symantec ICDx TIPP Partner Integrations

Key Features

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

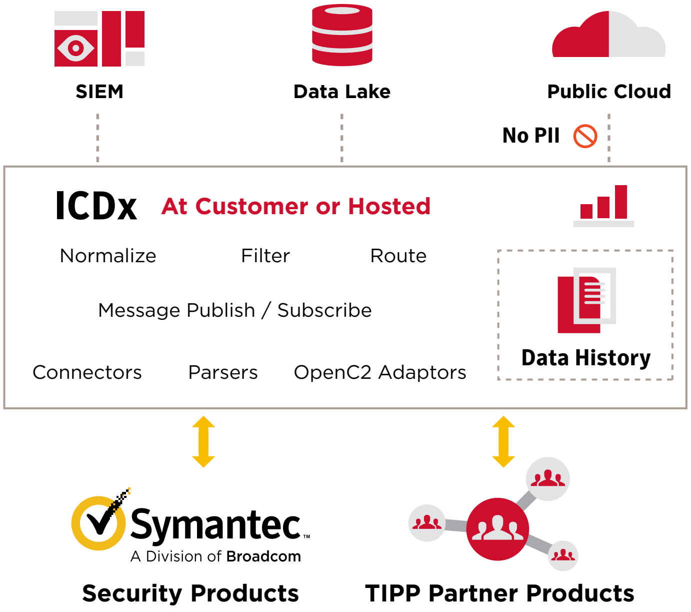
Key Partners

- Amazon Web Services
- Anomali
- Elastic
- Exabeam
- Fortinet
- IBM Resilient
- Microsoft
- ServiceNow
- Smart Hive
- Splunk

Introduction

Symantec Integrated Cyber Defense Exchange (ICDx) bridges Symantec and Partner applications and addresses the complexity that Symantec Customer and Technical Partners face when attempting to integrate multiple Symantec products. Broadcom provides various Symantec Security Operations Center (SOC) applications for partners integration.

ICDx Accelerates the Integration of Symantec and Third-Party Products



Symantec SOCView App for Splunk

Splunk is the market leader in analyzing machine data to deliver Operational Intelligence for security, IT and the business. With ICDx, Symantec provides comprehensive visibility for Splunk across an integrated portfolio of security solutions that covers Secure Web Gateways, Network Forensics, DLP, Endpoint Detection and Response and Email Security. The Symantec ICDx-based SOCView app supports curated investigator views creating greater visibility across domain, file, email and threat intelligence. The unified dashboard view gives security analysts the ability to quickly see the global distribution of threats. SOCView highlights the highest priority malicious URLs, sources and files. In addition, SOCView details the most affected endpoints and email sender and recipients. Finally, SOCView reports security events statistics by product.

Symantec Enterprise Connect Community

Symantec SOC Response App for ServiceNow

ServiceNow makes work, work better for people. Transforming old, manual ways of working into modern digital workflows, so employees and customers get what they need, when they need it—fast, simple, easy. Symantec ICDx integration with ServiceNow gives ServiceNow Security Operations users the ability to visualize ICDx created security incidents. Empowering them to enrich the incidents in ServiceNow using ICDx native event searching capability. Workflow actions let ServiceNow users automate different actions across various Symantec products covering: Investigation Search, Third Party Enrichment, Incident Management, and Response.

Symantec SOC Investigator App for Elastic

Elastic builds self-managed and SaaS offerings that make data usable in real time and at scale for search, logging, security, and analytics use cases. Symantec Integrated Cyber Defense Exchange (ICDx) provides the SOC Admin/end user a holistic view to troubleshoot security issues and improve the overall security posture of the organization. Integration with Elastic Stack allows users the ability to visualize ICDx created security incidents.

Anomali

Anomali Match integrates with your existing log sources, maintaining historical visibility without duplicating logs. This data is continuously correlated against new and existing threat intelligence to uncover evidence of breaches. The integration between Symantec ICDx and the Anomali Threat Platform offers a powerful mechanism to aggregate, enrich, and analyze existing data from the entire Symantec security suite. Anomali Match matches Symantec product events against validated threat intelligence to determine which events are malicious and merit further human investigation. Security analysts gain additional insight through threat bulletins, vulnerability information, and other indicators of compromise. Joint customers save a significant amount of time and effort, deal with less complexity, and take action more quickly.

Fortinet

Fortinet FortiSOAR (formerly CyberSponse CyOPs) is a holistic and enterprise-built security orchestration and security automation workbench that empowers security operation teams to work smarter and respond in near real time to the security alert influx. FortiSOAR integrates with Symantec ICDx to search and get data from multiple control points such as Endpoint security, Network security, Email security and Cloud security, which enables strengthening of the core security functions such as Threat Protection, Information protection and compliance protection.

Symantec Information Centric Analytics (ICA)

The combination of Symantec Information Centric Analytics and Symantec ICDx provides an end-to-end integrated cyber risk analytics ecosystem. Symantec ICA takes the data provided by Symantec ICDx, enriches it, and stores it in an integrated cyber risk data model that it then analyzes using proprietary behavioral and risk analytics. The end results are lists of enterprise threats, behaviors, users and entities prioritized by risk.

IBM Resilient

The IBM Resilient integration with Symantec ICDx allows security teams to automatically create incidents based on alerts from Symantec products and trigger an incident response plan appropriate to the alert type, source, and severity. Security analysts can also query ICDx from the Resilient Incident Response Platform (IRP) for additional information during the incident response workflow using a flexible set of integration functions in Resilient's powerful and robust workflow designer. Users can manually or automatically search ICDx for additional event details and previous occurrences to enrich incident data, enabling security teams to respond more intelligently to threats.

Microsoft Azure Sentinel

Microsoft Azure Sentinel, a cloud-based Security Information and Event Management (SIEM) system collects security data across your hybrid organization from devices, users, apps and servers on any cloud. Azure Sentinel brings it all together, combining information from ICDx with Office 365 and other sources to provide comprehensive visibility. Azure Sentinel machine learning algorithms cut through the reams of data to isolate real threats and in turn alleviate alert fatigue. Azure Sentinel helps speed up threat response with integrated automation and orchestration of common tasks and workflows.

Exabeam Security Management Platform Integrations

Exabeam, the Smarter SIEMTM company, empowers enterprises to detect, investigate and respond to cyber attacks more efficiently so their security operations and insider threat teams can work smarter. The integration of Exabeam and Symantec ICDx allows analysts to collect unlimited log data and alerts from Symantec products to the Exabeam Security Management Platform (Exabeam SMP), store them in a central repository with other data sources where they can use behavioral analytics to detect attacks, and then orchestrate and automate incident response actions, including direct actions through Symantec products. The availability of ICDx allows Exabeam customers to ingest content from existing supported Symantec products and will accelerate their ability to ingest content from additional products in the future, all using a single ingestion framework.

Smart Hive

Smart Hive enhances the Symantec ICDx story by enabling ICDx deployments located at different customer locations to learn from each other in real-time. Smart Hive does this by using the S3 forwarder and forwarding all events from ICDx to the HIVE. In the HIVE Smart Hive analysis, the data enriches the data and compares the data with other members in the HIVE. Based on the comparison and analysis, Smart Hive informs the customer of what threats others have identified and are stopping that the customer is not stopping. Smart Hive can also apply the controls using a SOAR tool. Once the controls are applied, ICDx gets the event and forwards it to Smart Hive to confirm the control has been applied. The Smart Hive ICDx integrations enable SmartHive customers to learn from each other in less than 90 seconds.

AWS S3

With over one million users, Amazon Web Services offers more than 212 different services. One of those services is Amazon Simple Storage Service (Amazon S3). It is an object storage service that offers industry-leading scalability, data availability, security, and performance. The integration with ICDx enables long-term storage and 3rd party integration for any service running on AWS. It makes it easy to share normalized data across an enterprise's entire infrastructure.

Current ICDx Partners

splunk> servicenow amazon web services elastic

IBM Resilient ANOMALI CYBERSPONSE ADAPTIVE SECURITY

exabeam smart hive Microsoft

Symantec
A Division of Broadcom

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

Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom.