IBM Cloud Pak for Security

Version 1.0

Data Explorer

Investigate threats and indicators of compromise (IOCs) across multiple siloed solutions, from a single, unified interface

Security teams today face the challenge of identifying insights from hundreds of thousands of events every day from disparate security tools, cloud environments, and data lakes. Effective investigations and threat hunting require analyzing insights from all the tools. Analysts today waste precious time in attempts to individually log into different tools, perform a search in the tool's native language or chase the subject matter experts of each of these tools in order to gather the needed information. This ineffective manual process often slows down investigations, and often analysts are forced to make decisions based on partial information. A strong and efficient cybersecurity posture requires broad and deep investigation of potential risks and threats, which is a challenge for today's overburdened security analysts.

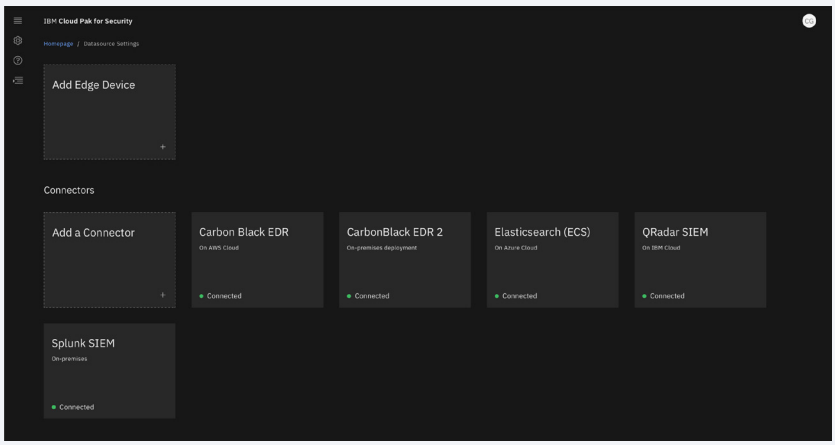
What if you could search all your data sources with one tool, and using one language?

IBM Security Data Explorer, part of Cloud Pak for Security, enables analysts to perform federated investigations across IBM and third-party data sources. Connect insights from security tools, such as security information and event management (SIEM) and endpoint detection and response (EDR), and data stored in data lakes, such as Elastic. [Figure 1]

Additionally, get insights from multicloud environments that your SIEM tools like QRadar and Splunk are monitoring. Significantly reduce time to investigate by querying multiple data sources using a simple query builder and one workflow. Enable your security operation center (SOC) to do more, faster, and empower analysts to search for IOCs and threats across all data sources.

IBM Security Data Explorer can expedite IOC investigations from hours to minutes and remove blind spots with federated search and investigation. Simply connect your data sources and run a query from the unified interface.

Figure 1 | Connectors



Learn more at
ibm.com/products/cloud-pak-for-security/data-explorer

Solution highlights

Extract more value out of your existing security tools

Improve analyst productivity with the power to do more

Leave the data where it is by federating data without having to move it, no additional data lake required

Uncover hidden threats faster by searching across your disparate data set from one screen

Reduce privacy risks from duplicating your data to data lakes

Avoid building costly product integrations in house by leveraging pre-built integrations

Break down data silos: Data is increasingly siloed across different tools and different cloud and on-prem environments, which makes visibility across all your data sources a challenge. IBM Security Data Explorer can access all of your data no matter where it resides.

Make threat hunting and incident investigations more efficient: SOC analysts have to search through multiple tools when hunting for a threat or investigating a security incident. With IBM Security Data Explorer, it takes one query from one interface to get insights and information you need. [Figure 2]

Streamline operations: Once an IOC is found, SOC analysts have to open a case in their Security Orchestration, Automation and Response (SOAR) tool. With the case management functionality built in to Cloud Pak for Security, SOC analysts can take these actions from one single user interface.

Manage multiple clients easily: If you are an Managed Security Services Provider (MSSP), you can search multiple client environments and data repositories from one interface.

Figure 2 | Query Builder