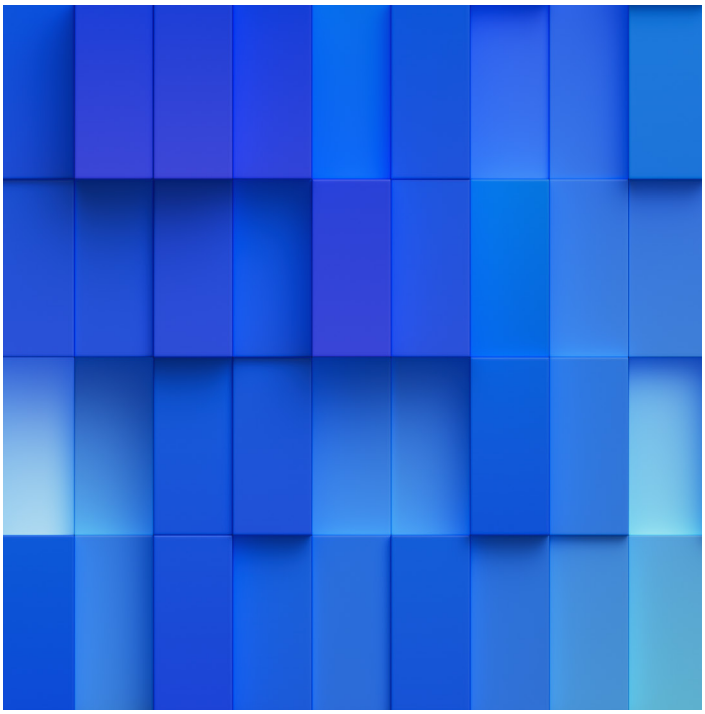
How to boost detection rates and save time hunting for threats

Reveal hidden patterns and connections to investigate and remediate cyberthreats faster



According to the Cost of a Data Breach Report 2023, the global average cost of a data breach was USD 4.45 million, a 15% increase over 3 years.[1] Enterprise businesses today rely on hybrid cloud environments that are evolving and scaling at an exponential rate. Growing IT footprints, siloed technologies, manual searches and an overload of alerts make it harder to find real threats and create clear context or visualizations. These challenges often allow attackers to lurk for weeks, or even months, before discovery. An effective threat-hunting approach can help greatly reduce the time from intrusion to discovery, decreasing the amount of damage attackers can inflict.

A successful threat-hunting program is based on the quantity of relevant data available for use in a security environment. In other words, an organization must first have an enterprise security system in place that can collect all relevant data. However, the information gathered can provide valuable clues for threat hunters only if the security information and event management (SIEM) solution can quickly and precisely query all that data while using AI to help surface signs of a real attack.

The IBM Security® QRadar® SIEM solution normalizes event data to provide a structure of event properties that allows simple queries to find related attack activity across disparate data sources. QRadar SIEM offers context and prioritization to threats by using mature AI capabilities that have been pretrained on millions of alerts from IBM's vast network of clients, helping analysts hunt for threats faster and more accurately.

Proactively target high-value threats
Hunt for malicious actors seeking to execute harmful code with the Kestrel threat-hunting language.

Find hidden threats faster
Use multiple layers of AI and automation to uncover hidden patterns and connections to drastically ease threat hunting for overtasked security teams.

Take advantage of federated search
Quickly access your siloed data from where it resides to enrich your investigations with proactive threat hunting and eliminate the costs of ingesting data into QRadar SIEM.

Stop threat actors in their tracks. Proactively speed up and improve the success of your security team's threat-hunting efforts with the cloud-native edition of IBM Security QRadar SIEM.

Learn how it works →
See an interactive demo →

1. Cost of a Data Breach Report 2023, IBM Security, July 2023.