Business challenge

This public sector organization was the unknowing victim of an attacker that was attempting to test stealthy exfiltration of confidential information from a highly sensitive asset not considered at risk.

Transformation

Using the IBM® QRadar® Sense Analytics engine for advanced threat detection, along with other QRadar security software products, IBM Business Partner CarbonHelix was able to quickly determine how the attacker had gained access to the internal network and the sensitive asset as well as the tools used to capture and move data.

Business benefits

Detected
the stealth attack that was not caught by log-based SIEM analysis alone

Prevented
loss of confidential data and further undiscovered activity by the attacker

Reduced risk
with new security controls and a process to identify and patch vulnerabilities

Public sector organization

Detecting and stopping a stealth attack

Operating in the public sector, this organization found out the hard way that the log-based security information and event management (SIEM) solution from its managed security services provider was incapable of detecting stealth attacks.

Solution components

- IBM® QRadar® QFlow Collector
- IBM QRadar Sense Analytics
- IBM QRadar Vulnerability Manager
- Delivered by IBM Business Partner CarbonHelix

Share this

WGC12521-USEN-00