



Other



“Without fast action by CarbonHelix and their use of QRadar, we would have joined the list of data breach victims.”

—IT Security manager, public sector organization

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





© Copyright IBM Corporation 2017. IBM Security, 75 Binney Street, Cambridge MA 02142

Produced in the United States of America, December 2017. IBM, the IBM logo, ibm.com, and QRadar are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml. This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

