



"It became evident to us very quickly that we needed visibility into our own network as well as to external events."

— Security manager, regional US bank

Business challenge

The bank's need for an advanced solution that could detect insider threats was revealed when its existing managed security services provider misidentified an attack as a "high" external network threat.

Transformation

The original investigation consumed 3 hours and produced 300 alerts, 100 emails, 3 phone calls—and no resolution. Using IBM® QRadar® SIEM, IBM Business Partner CarbonHelix security professionals were able to identify the cause in 5 minutes as a non-threat resulting from a common network configuration problem caused by an unscheduled network change.

Business benefits

5 minute

investigation to resolve cause of security attack, compared to 3 hours

360-degree

view of network, internally and externally, with IBM QRadar and CarbonHelix

Improved

security posture with a more advanced managed SIEM solution

Regional bank

Reclassifying a false positive security event triggers a service provider change

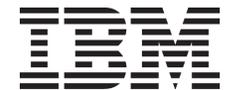
This regional bank located in the United States operates 60 branches and manages security with a small internal team augmented by managed security services.

Solution components

- IBM® QRadar® SIEM (Security Information and Event Management)
- Delivered by IBM Business Partner CarbonHelix managed security services

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. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. 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.

