"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

WGC12520-USEN-00