"By understanding the complexities of our network and our users, CarbonHelix was able to help improve our SOC efficiency very quickly."

—IT Security manager, service provider

Business challenge

Because the company's network users produced a wide range of unclassifiable behaviors, IBM® QRadar® SIEM generated an average of 400 valid alerts per day, many of them low priority and unactionable.

Transformation

By understanding the client's complexity and using tuning techniques to optimize QRadar, IBM Business Partner CarbonHelix was able to filter out the noise and move the low-priority issues into actionable reports. Improved data visibility and data quality allowed CarbonHelix to detect a wider range of threats and enhanced SOC analysts' efficiency.

Business benefits

Optimizes
the service provider's investment in the IBM QRadar system

Reduces
time spent on incident investigations, freeing up resources for higher-value work

Increases
the visibility of real threats, helping analysts use QRadar for proactive threat hunting

Service provider

Optimizing security data and SOC operations by fine-tuning SIEM

This service provider operates a diverse, complex and extensive network that supports many different types of user communities. Their diverse interactions and behaviors are difficult to baseline as "normal" for network activity.

Solution components

- IBM® QRadar® SIEM
- IBM Security App Exchange
- IBM X-Force® Threat Intelligence
- Delivered by IBM Business Partner CarbonHelix

Share this

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.

Please Recycle

WGC12522-USEN-00