



“IBM’s best-in-class cognitive security portfolio will help us pre-empt threats and mitigate risk, supporting our position as a leading Digital Bank.”

—Rohan Muttiah, Chief Operating Officer, Cargills Bank

Business challenge

Cargills Bank wanted to enhance its existing defensive cyber security capabilities, improve monitoring and implement stronger preventive protocols to guard against sophisticated threats.

Transformation

With the Financial Services industry being targeted the most by cyber criminals, Cargills Bank has taken a proactive approach to better safeguard customers by deploying a cognitive security solution, IBM Watson® for Cyber Security. Now Cargills Bank analysts can readily compare external information from multiple sources with internal threat data and gain actionable insights for making decisions quickly.



Rohan Muttiah
Chief Operating Officer,
Cargills Bank

Business benefits

Speeds

The process of detecting and accurately identifying cyber threats and alerts

Guards

Against sophisticated threat incidents with stronger preventive protocols

Transforms

Millions of security documents into actionable intelligence relevant to specific threats

Cargills Bank Ltd.

Cargills Bank pioneers the use of cognitive security in Sri Lanka

Cargills Bank Ltd. is a licensed commercial bank based in Sri Lanka. Cargills is a brand that has been faithfully serving Sri Lankans for 174 years, built on a foundation of values and ethics. True to this heritage and the ethos of “Banking on the Human Spirit,” Cargills Bank is taking banking to the masses by being inclusive and accessible with offers such as the Cargills Cash Savings Account, available at over 340 Cargills Food City outlets, and the Cargills Bank Debit Card.

Solution components

- IBM® QRadar® SIEM
- IBM QRadar Advisor with Watson™
- Solution delivered by IBM Business Partners Blue Chip Engineering Co. and Secbounty Services Private Limited

Share this





© Copyright IBM Corporation 2018, IBM Security , 75 Binney Street, Cambridge MA 02142

Produced in the United States of America, March 2018. IBM, the IBM logo, ibm.com, QRadar and Watson 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. 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.



Please Recycle

97014097-USEN-00