exabeam

CASE STUDY

BBCN BANK: DETECTING LATERAL MOVEMENT AND SERVICE ACCOUNT ACTIVITY

Headquartered in Los Angeles, for more than 30 years BBCN Bank has been serving the largest Korean community in the U.S., as well as a diverse mix of customers in over 59 full-service branches and Loan Production Offices throughout the nation.

BBCN Bank®

With more than $7.8 billion in assets, the strength of BBCN lies in its experienced management team and our focus on responsible risk management practices. The organization's expertise in small business lending, C&I lending, and international trade finance sets BBCN Bank apart from other community banks.

Security Environment

The bank has invested in a variety of security technologies and techniques, including SIEM, log management, penetration testing, and privileged account management, endpoint detection and response, etc.

Security Concerns

BBCN had concerns that were typical in the current environment, and primarily related to credential-based threats. Of primary concern was the use of service account credentials to move laterally across the corporate network to access sensitive data. A related concern is the use of account switching to avoid detection during lateral movement. BBCN wanted to ensure that it had an effective solution in place to detect lateral movement and to monitor and understand behavior from service and privileged accounts, as well as a means to detect users switching identities across accounts – including service accounts.

Existing Environment

BBCN has a broadly-deployed SIEM solution in place. The SIEM solution is a Leader in the Gartner Magic Quadrant and is considered to be a market-leading technology. However, it required excessive human oversight, especially to create and update correlation rules. The effort to create new rules was significant and complex. In addition, even this market-leading SIEM solution had challenges detecting compromised accounts; the SIEM simply wasn't designed to detect complex credential-based attacks.

With a small team, BBCN required a solution for detecting lateral movement and credential based attacks that did not place an undue burden on the security operations staff. To solve this challenge, BBCN piloted and selected Exabeam.

COPYRIGHT 2016 EXABEAM, INC. ALL RIGHTS RESERVED.

Exabeam-Enhanced Environment

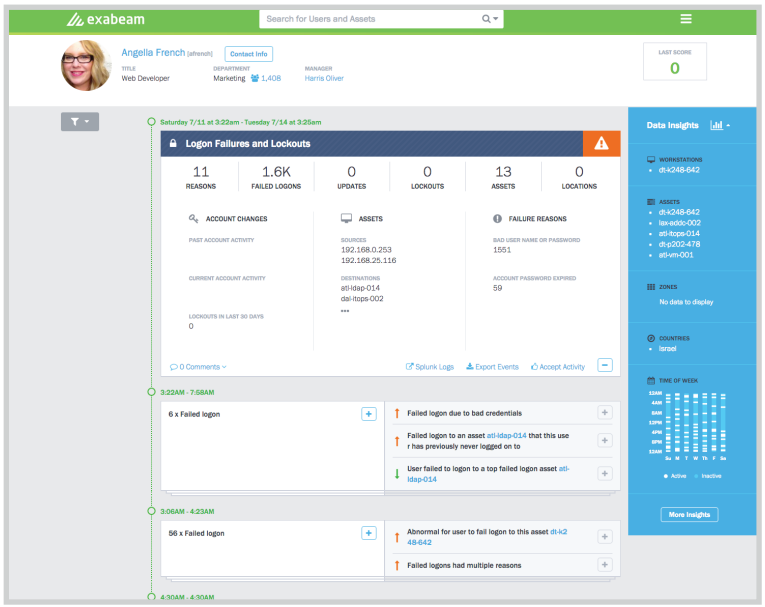
Exabeam was selected to perform user and entity behavior analytics within the BBCN environment and to enhance the capabilities of the firm's SIEM solution. BBCN confirmed Exabeam capabilities during a short pilot, and selected Exabeam based on several key criteria:

- ***Easy to use, with low administrative overhead*** – BBCN found the Exabeam solution to be easy for its security team to use. The solution required very low effort to add new rules, as it automatically learns about the customer environment.
- ***Agentless design*** – BBCN already maintains multiple types of endpoint agents and did not wish to manage any more. Exabeam's agentless design made it easy to deploy and manage.
- ***Increased activity visibility*** – Exabeam's detection and timeline capabilities provided increased visibility into lateral movement and service account activity, as well as a better understanding of user risk scoring.
- ***Platform extensibility*** – The ability to change risk scoring easily enabled the BBCN team to make Exabeam compatible with BBCN's own models.
- ***Account-switch detection*** – Hackers typically switch accounts as they move laterally through a network, as a means of avoiding detection. Tracking activity as users change accounts, devices, and IP addresses is key to identifying lateral movement. BBCN used Exabeam's Stateful User Tracking™ capabilities to track user behavior across account switches.

Benefits

BBCN has seen specific benefits from its Exabeam deployment::

- ***Reduction in false positives***
- ***Improved visibility of user and system activity***
- ***Decreased workload on security personnel***



Exabeam: Detecting Lateral Movement and Account Switches

For more information, please contact Exabeam at info@exabeam.com

COPYRIGHT 2016 EXABEAM, INC. ALL RIGHTS RESERVED.