CEO CFO

ceocfointerviews.com
All rights reserved!
Issue: May 1, 2017

CEOCFO Magazine

vericlouds

# Seattle Threat Intelligence Company helps Organizations Detect Compromised Credentials before Attackers Do

**Steve Tout**
**Chief Executive Officer**

**VeriClouds**
**www.vericlouds.com**

**Contact:**
**Steve Tout**
**(650) 352-3740**
**info@vericlouds.com**

**Interview conducted by:**
**Lynn Fosse, Senior Editor**
**CEOCFO Magazine**

**CEOCFO:** ***Mr. Tout, what is the idea behind VeriClouds?***
**Mr. Tout:** The idea behind VeriClouds is simple. VeriClouds is a threat intelligence company that helps organizations detect compromised credentials before attackers do. Many companies don't allow their employees to monitor activities or obtain data from the dark web, and as such they can outsource the legal risks and liabilities of working with compromised account data to us. Working with VeriClouds, organizations can significantly reduce the time it takes to detect and remediate data breach on their network. Thus, they can shorten the window of opportunity that attackers have to steal data or gain escalated privileges on a company's network or infrastructure.

**CEOCFO:** ***Do companies look at this part of security as something separate and apart from other measures? Where does it integrate? Should it integrate? What is the lay of the land surrounding what you are doing?***
**Mr. Tout:** Security monitoring has been around for a very long time. Just a few years ago, ingesting log files into large data bases and reporting, sort of clearing the data base and filtering by key words, tends to be how all of this gets started. You could look for and report on events such as authentication errors and then apply analytics on top of that to see trends and failed login attempts. That seems to be the earliest attempts at gaining insight into anomalous user behavior trying to attack a web application. Where the industry is today is that many companies look to Cloud Access Security Brokers (CASBs) to provide visibility into user activities within third party applications, such as Software as a Service or SaaS applications. They offer services commonly referred to as User & Entity Behavior Analytics, or UEBA. That tends to be based on signatures for risk monitoring. It looks at user activity logs. However, the challenge with that is that it does not allow an organization to always distinguish between a real user and a potential hacker. There are things like IP reputation services or other things that a company can look at, like IP addresses or the speed at which users are typing on a keyboard, all of which can be indicators of whether a user is indeed a real user or an attacker. However, it relies emerging data sciences applied to this field such as machine learning and artificial intelligence. It is looking for patterns that emerge and is more reactive to the patterns. This approach can be valuable, but it can lead to a large volume of calls or tickets in a company's help desk which turn out to be false positives.

**CEOCFO:** ***How do you accomplish this security at VeriClouds? What do you do that is different?***
**Mr. Tout:** What companies are doing today with UEBA, machine learning, artificial intelligence, security incident and event management tools, are static indicators and algorithms based upon user activity and other known threats. What VeriClouds is doing differently is that we take the guesswork out of security monitoring. The data that we have is the same data that attackers are leveraging from the dark web to perform their attacks and succeed. Therefore, VeriClouds is not