Data-driven detection and response

Better information sharing and long-view data analysis are key to improving agencies' security posture

"We're seeing a lot of uptick in activity in customer interest in cybersecurity. It's obviously a big concern across the board," said Carolyn Duby, Principal Solutions Engineer and Cyber Security SME Lead, Cloudera.

Cyberattacks are increasing in number, type, and scale, with many implications yet unknown even for attacks already discovered and stopped. "We need to take a big leap forward in our ability to effectively combat these cyberattacks," said Duby.

"We have to do better with our cybersecurity posture and we have to do better sharing across organizations to detect those threats," Duby said. Cloudera provides enterprise data solutions to federal agencies, state and local governments and in the private sector, and across environments and architectures.

> **"It's great to have a lot of data … in a consistent format, but you need to be able to effectively analyze it, to … get the answers you're looking for in terms of an incident investigation or response."**
>
> **– CAROLYN DUBY, PRINCIPAL SOLUTIONS ENGINEER, AND CYBER SECURITY SME LEAD, CLOUDERA**

The massive shift to remote work during the Covid health pandemic, nation-state attacks, and exponential growth of ransomware and other cyberattacks all were reflected in the May 2021 Executive Order on national cybersecurity. Agencies need to address consistency, normalization, scalability and cost-effectiveness—as well as security and governance.

Cloudera is well positioned to meet these challenges. Duby outlined some of the ways that Cloudera is advancing the art and science of cybersecurity.

With the massive amounts of data coming in, one challenge for agencies has been how much to retain and how to effectively retain what is needed. Finding out what

Article Source: FCW Cybersecurity Workshop | August 4, 2021

really happened in a cyberattack can require months' or years' worth of context, Duby explained. An attacker can infiltrate a network, wait until the time is right and then within seconds compromise a network; or exist under the radar while quietly exfiltrating data.

"We need long context, and we need to be able to detect quick attacks in real time, Duby advised. "We need to bring all that data together." Cloudera's mission is to enable organizations to maximize the utility of cyberdata toward improving their ability to detect and respond to cyberattacks.

"We're making realtime decisions that will affect the security and very defenses of our organizations. … In some cases the data we're using and the defenses we're taking may have legal implications. We need to make sure that the data we're collecting is secure …[and] that we have confidence in that data," Duby said.

"It's great to have a lot of data [and] to have it in a consistent format, but you need to be able to effectively analyze it, to have the tools to really break down data, aggregate it, and get the answers you're looking for in terms of an incident investigation or response," Duby said.

"We're making real time decisions that will affect the security and very defenses of our organizations. … We need to make sure that … we have confidence in that data."

– CAROLYN DUBY, PRINCIPAL SOLUTIONS ENGINEER, AND CYBER SECURITY SME LEAD, CLOUDERA

Cloudera's solution is scalable and can be deployed on premises, a data center, or the cloud or hybrid cloud. Duby outlined a potential use case: "If you want the hottest, most recent data on premises and want to push old data to the cloud so you can retain and do elastic workloads—long investigations or threat hunting or machine learning -- Cloudera has all the tools in our toolkit to do those types of flexible deployments."

Cloudera takes a two-part approach to security and governance: metadata management to tag all sensitive data; and creation of policies based on that metadata. "It is important to have unparalleled access to your data, not locked up in proprietary format [but] in a format you want with the retention you in want in the way that you want it," Duby said.

One of Cloudera's most effective strategies on the front lines of cyberdefense has been to engage in strategic partnerships.

For example, Duby said that while Cloudera's solution already improves the ability to retain context in a way that is cost effective and scalable, "Through our partnership with NVIDIA we're advancing this scalability even more, … [and] advance the state of AI in cyber as well."

"We're doing things that seem impossible, but we're making them possible," Duby said.

Yurchanka Siarhei / Shutterstock.com