Using machine learning to unlock the potential of your network security data

Fabien Guillot and Kevin Sheu
Vectra AI

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

.conf19

splunk>

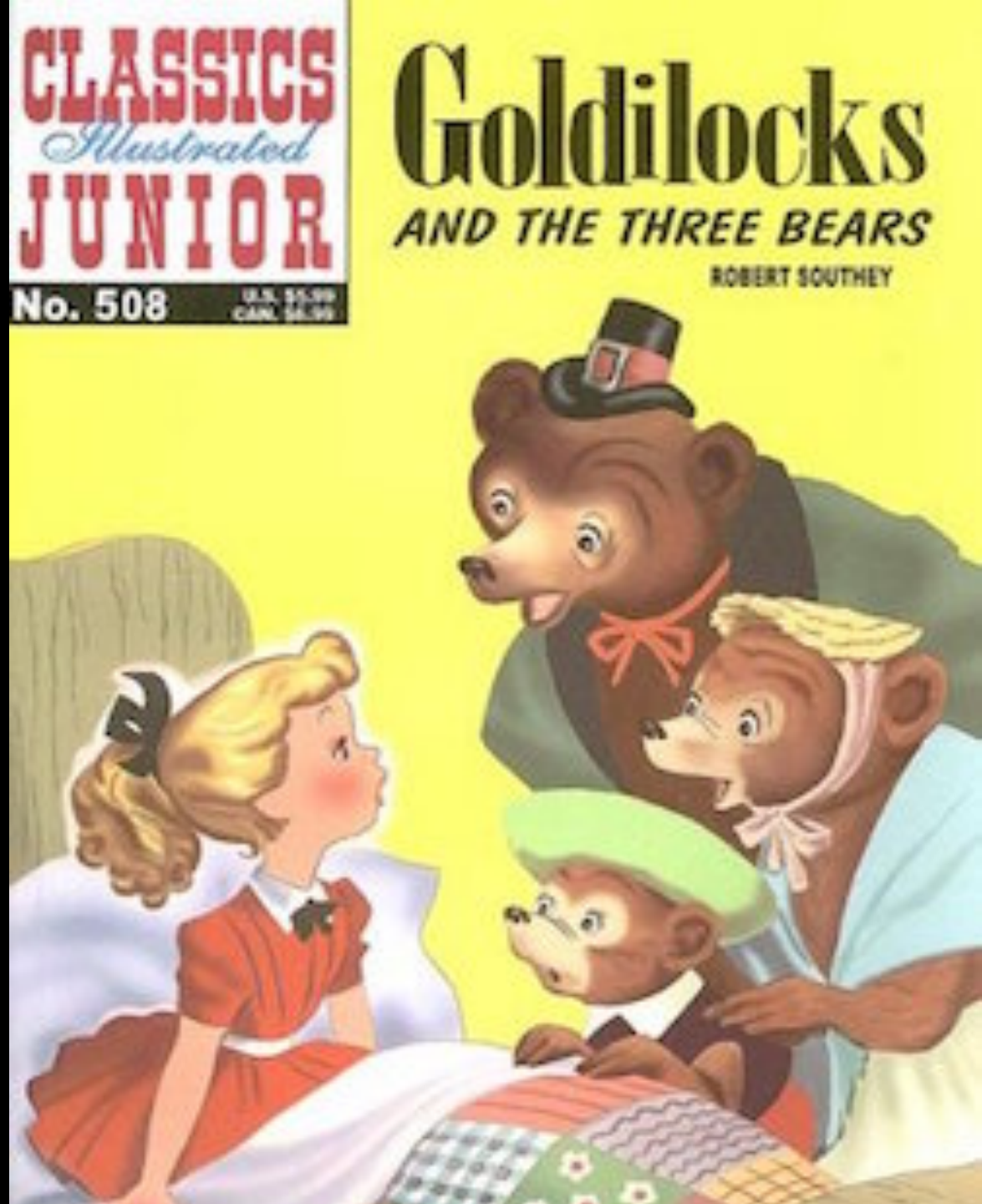
Fabien Guillot

Senior Technical Marketing Engineer | Vectra AI

Kevin Sheu

Vice President of Product Marketing | Vectra AI

The foundation for security begins with the data



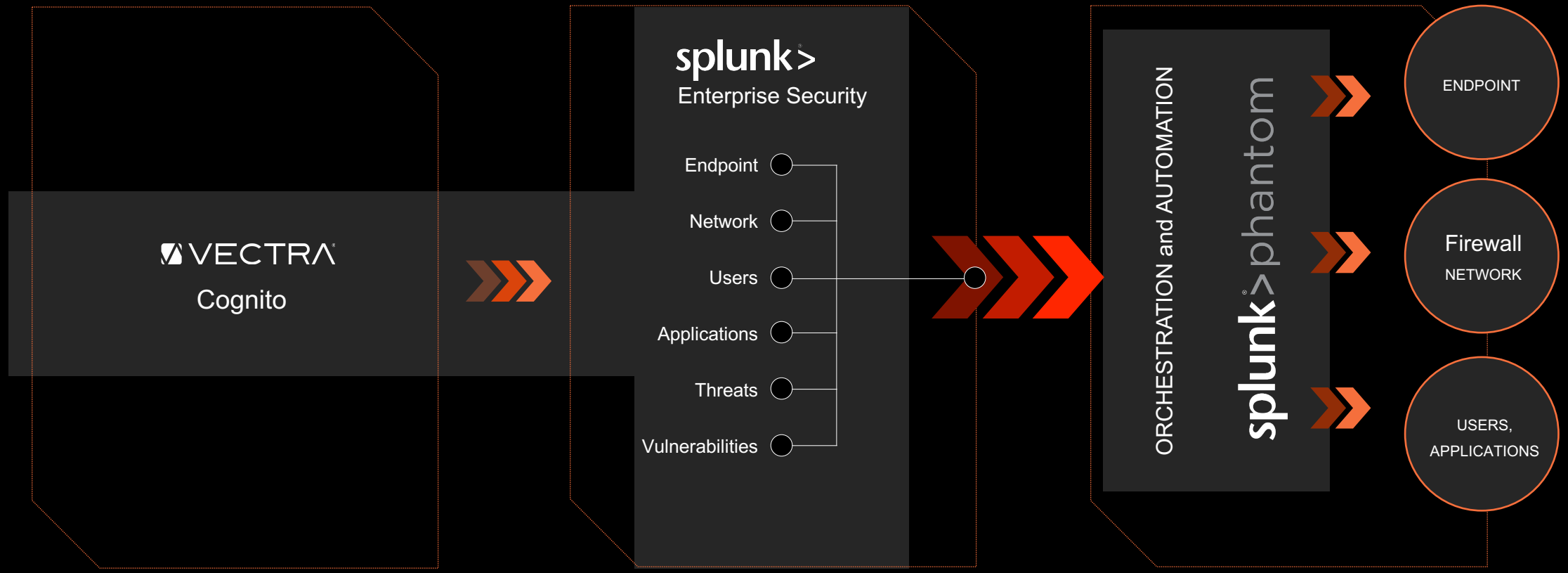
The data chasm

- Zeek network data
- 100X the richness of NetFlow
- 100X smaller than PCAP

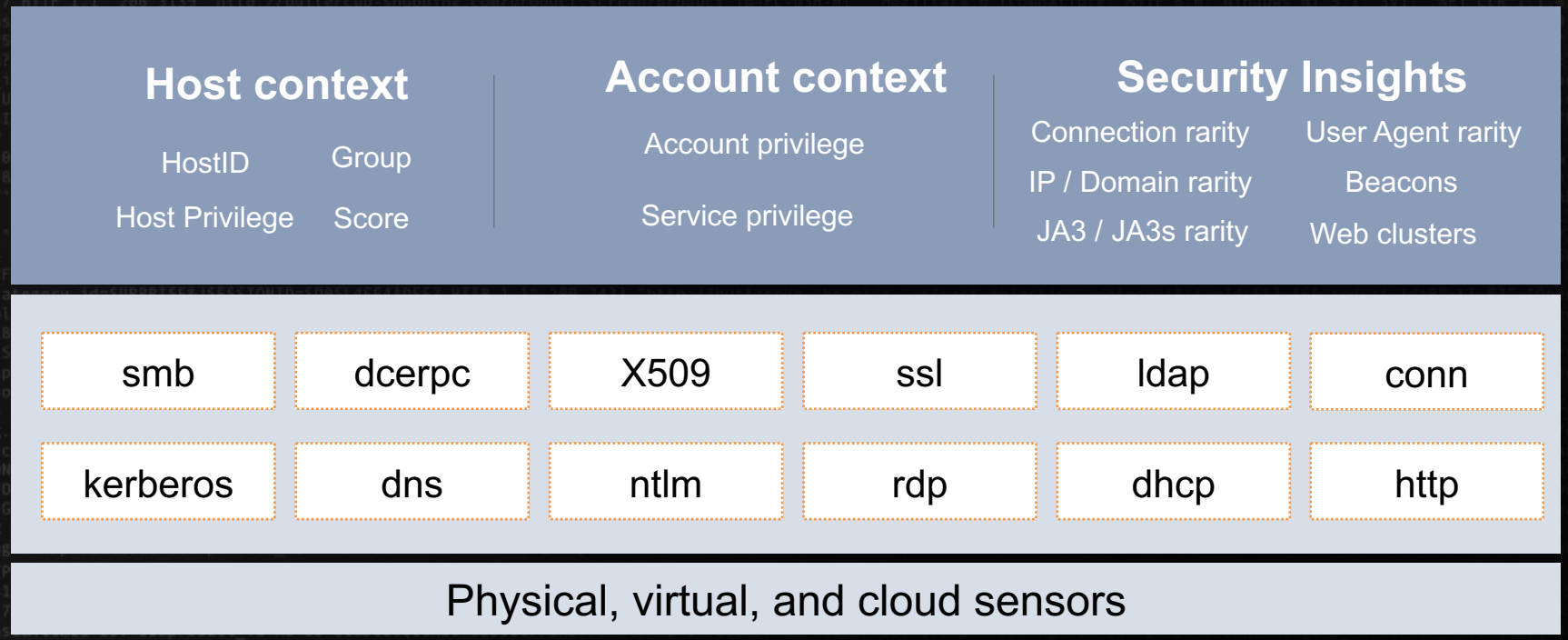
Scalability
Operational complexity
Data science

- Faster investigation
- Effective hunting
- Improved security posture
- Compliance

Empowering Splunk deployments



Unlock the potential of your security data



Security-targeted context

Record of what happened

Enriching your data

Security Research

Fundamental attacker behaviors sourced from securing the world's most sensitive assets

Data Science

Team of **PhD data scientists** who codify behaviors across unsupervised, supervised and deep learning models

"Is this a "privileged" host?"

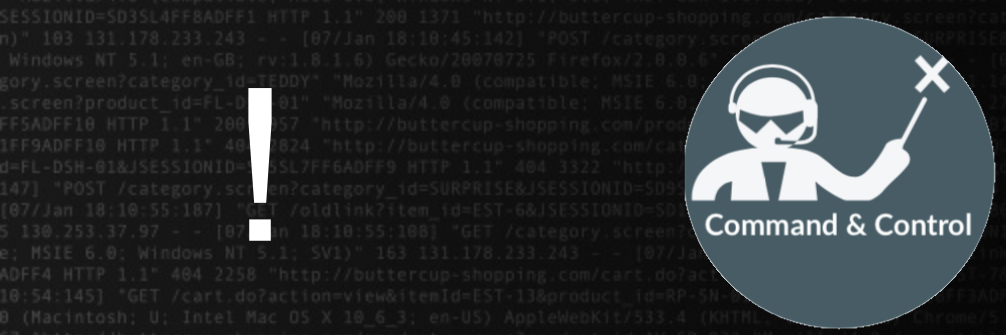
"Is this part of a larger infrastructure?"

"Is this accessing a privileged asset?"

"What's the Host ID (not IP address)?"

"Does the beacon have an unusual JA3?"

A simple example



Spear phishing email sent to several hosts

Escalate privilege
Extract local admin credentials

Stolen admin credentials also work on other hosts

Scan for file shares

Access domain controller
Copies files locally
Exfiltrate through C2

Cognito Stream

Cognito Detect

“What did the attacker target?”

“What is the scope and scale?”

“What do I prioritize?”

“Where did the attacker move?”

“Who else is communicating to the same C2 server?”

“What data was stolen and how?”

“Who is patient zero?”

The ultimate network detection and response platform

Cognito Stream

Send security-enriched metadata to data lakes and/or SIEM

Cognito Recall

Investigate and hunt in a cloud-based application

Cognito Detect

Detect and prioritize hidden threats at speed using AI

Cognito platform

- Cloud, user, datacenter
- Security-enriched
- Real time and historical
- Scalable architecture

splunk> .conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION