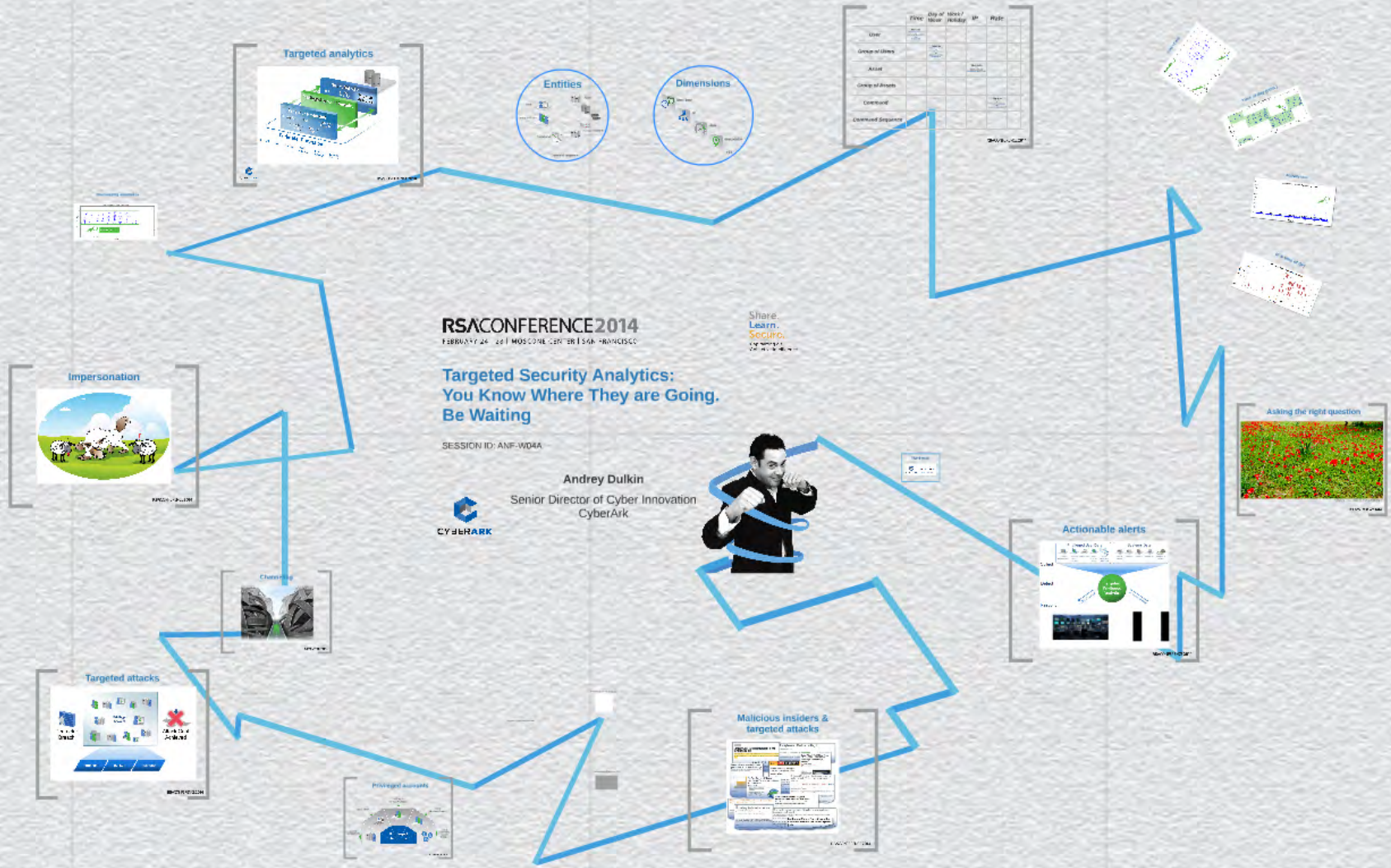
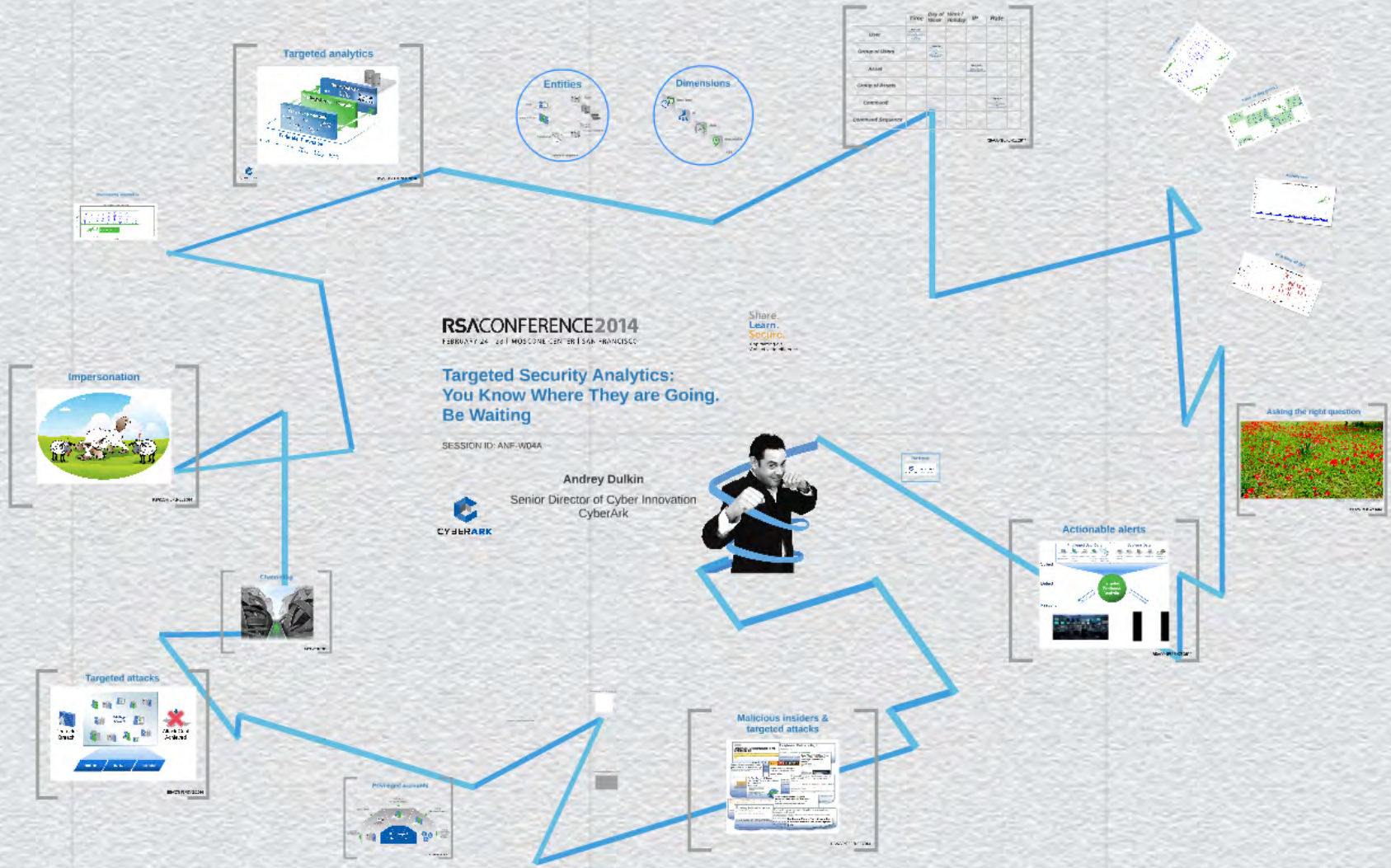
RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Targeted Security Analytics: You Know Where They are Going. Be Waiting

SESSION ID: ANF-W04A

Andrey Dulkin

Senior Director of Cyber Innovation
CyberArk

CYBERARK

Malicious insiders & targeted attacks

CYBERARK

RSACONFERENCE2014

Cyberattacks on US banks (Aug. 2013)

AUSTRALIAN EDITION

SC MAGAZINE

SECURE BUSINESS INTELLIGENCE

HOME | NEWS | IN DEPTH | REVIEWS | EVENTS | RESOURCES | SC AWARDS

WHAT WE'RE FOLLOWING: Kiwicon 7 • Research • Vulnerabilities

Home / Security News / Networks

Millions stolen from US banks after 'wire payment switch' targeted

By Danielle Walker on Aug 21, 2013 8:00 AM
Filed under Networks

Three banks plundered with DDoS distraction.

South Korea credit card breach (Jan. 2014)

The Telegraph

Home News World Sport Finance Comment Culture Travel Life Women Fashi

Technology News | Technology Companies | Technology Reviews | Video Games | Technology V

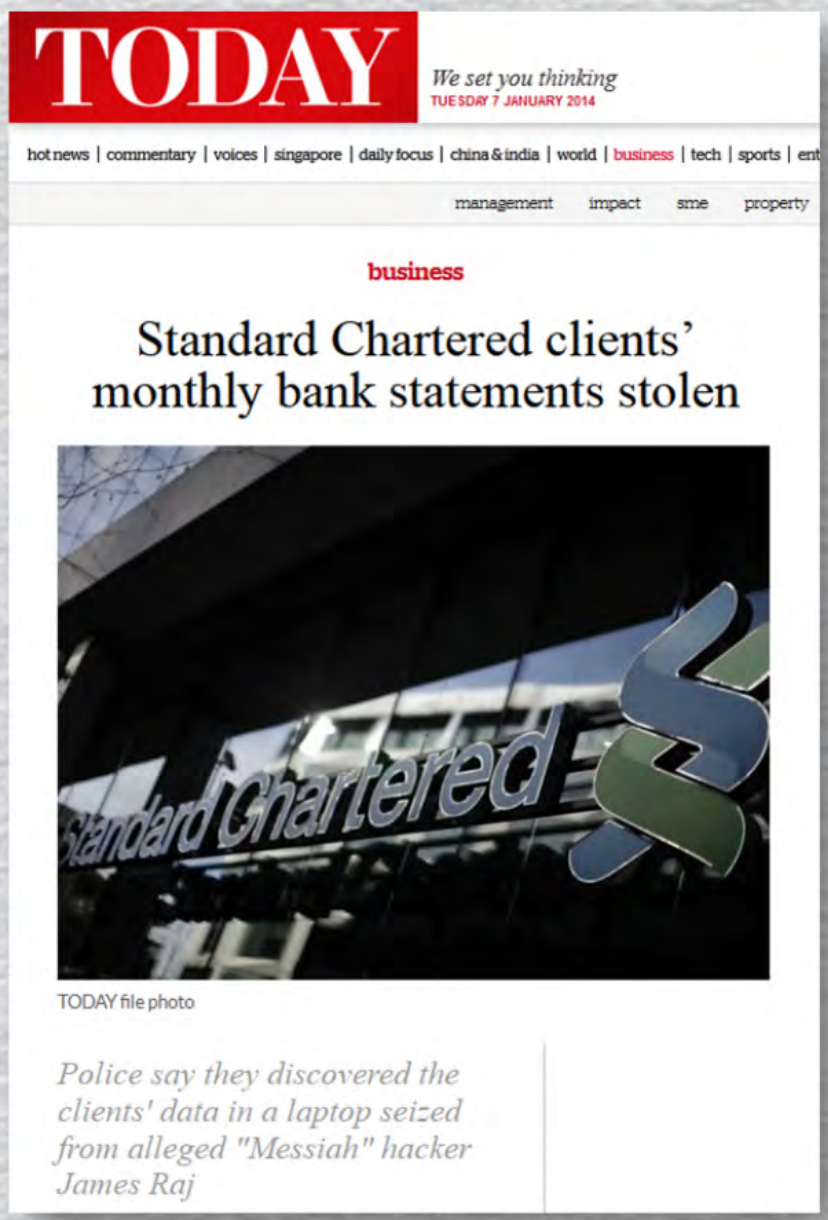
HOME » TECHNOLOGY » INTERNET SECURITY

Credit card details of 20m South Koreans leaked

Credit card details from almost half of all South Koreans may have been exposed by an employee at a credit ratings firm

The stolen data reportedly includes credit card numbers and expiration dates Photo: Alamy

Singapore bank statements breach (Dec. 2013)



TODAY

We set you thinking

TUESDAY 7 JANUARY 2014

hot news | commentary | voices | singapore | daily focus | china & india | world | business | tech | sports | ent

management impact sme property

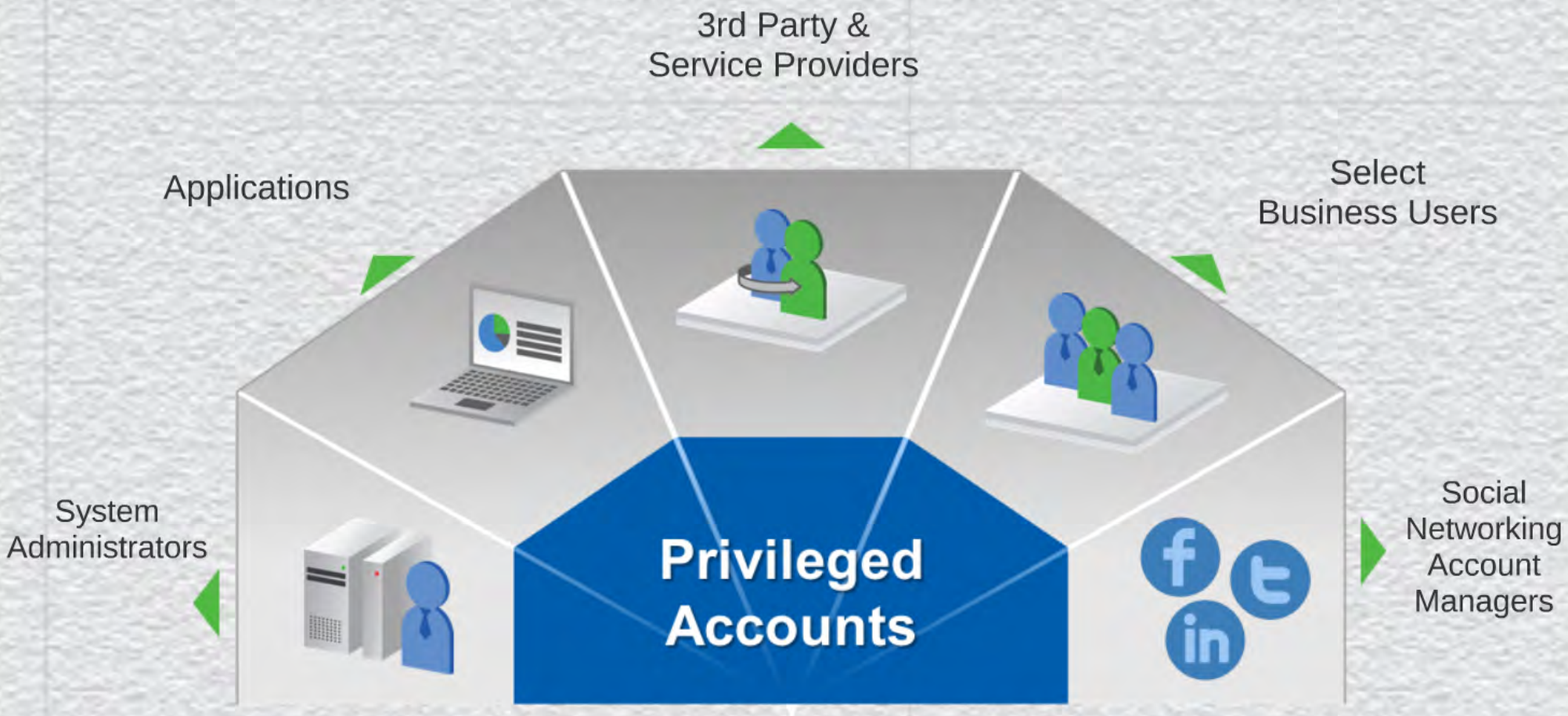
business

Standard Chartered clients' monthly bank statements stolen

TODAY file photo

Police say they discovered the clients' data in a laptop seized from alleged "Messiah" hacker James Raj

Privileged accounts



CYBERARK

RSACONFERENCE2014

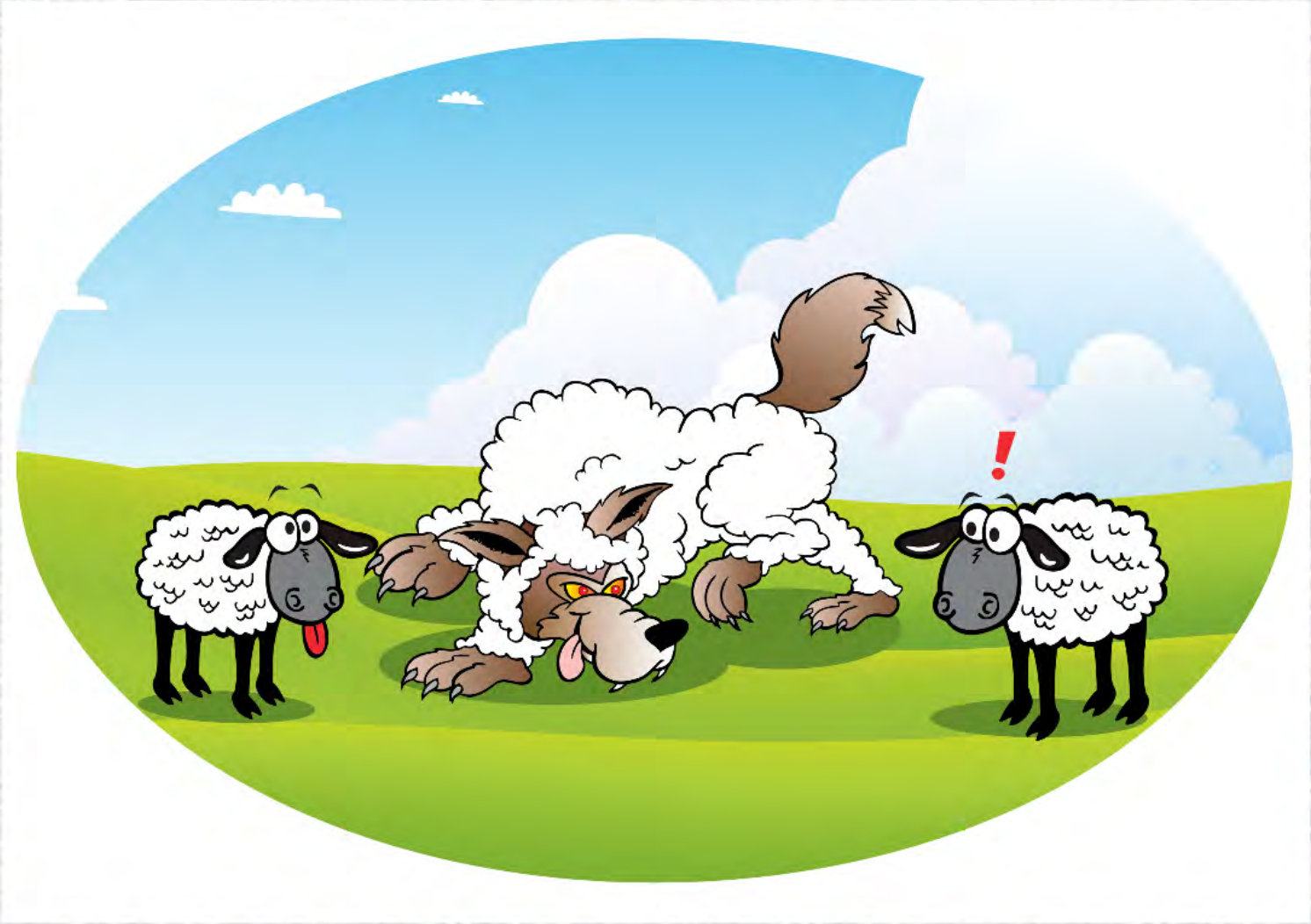
Targeted attacks

Channeling

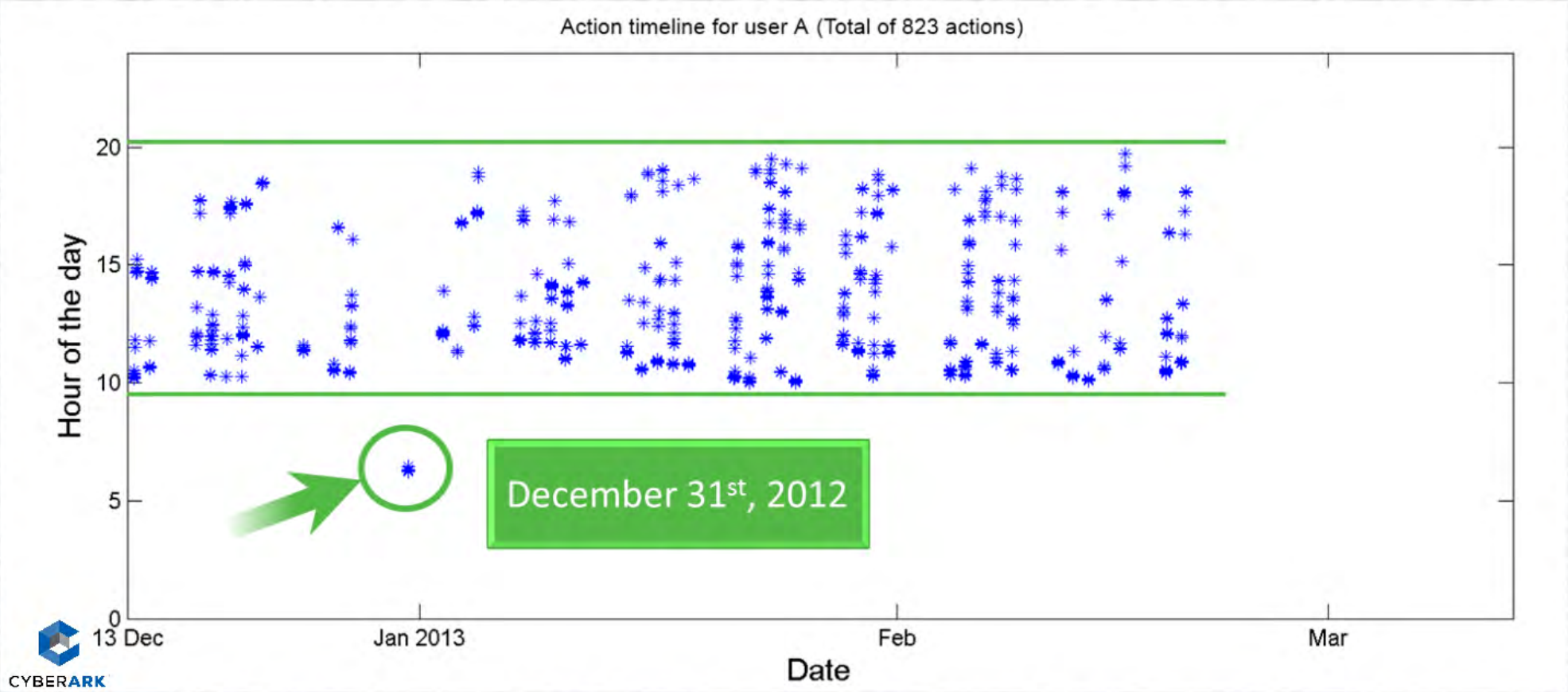
CYBERARK

RSACONFERENCE2014

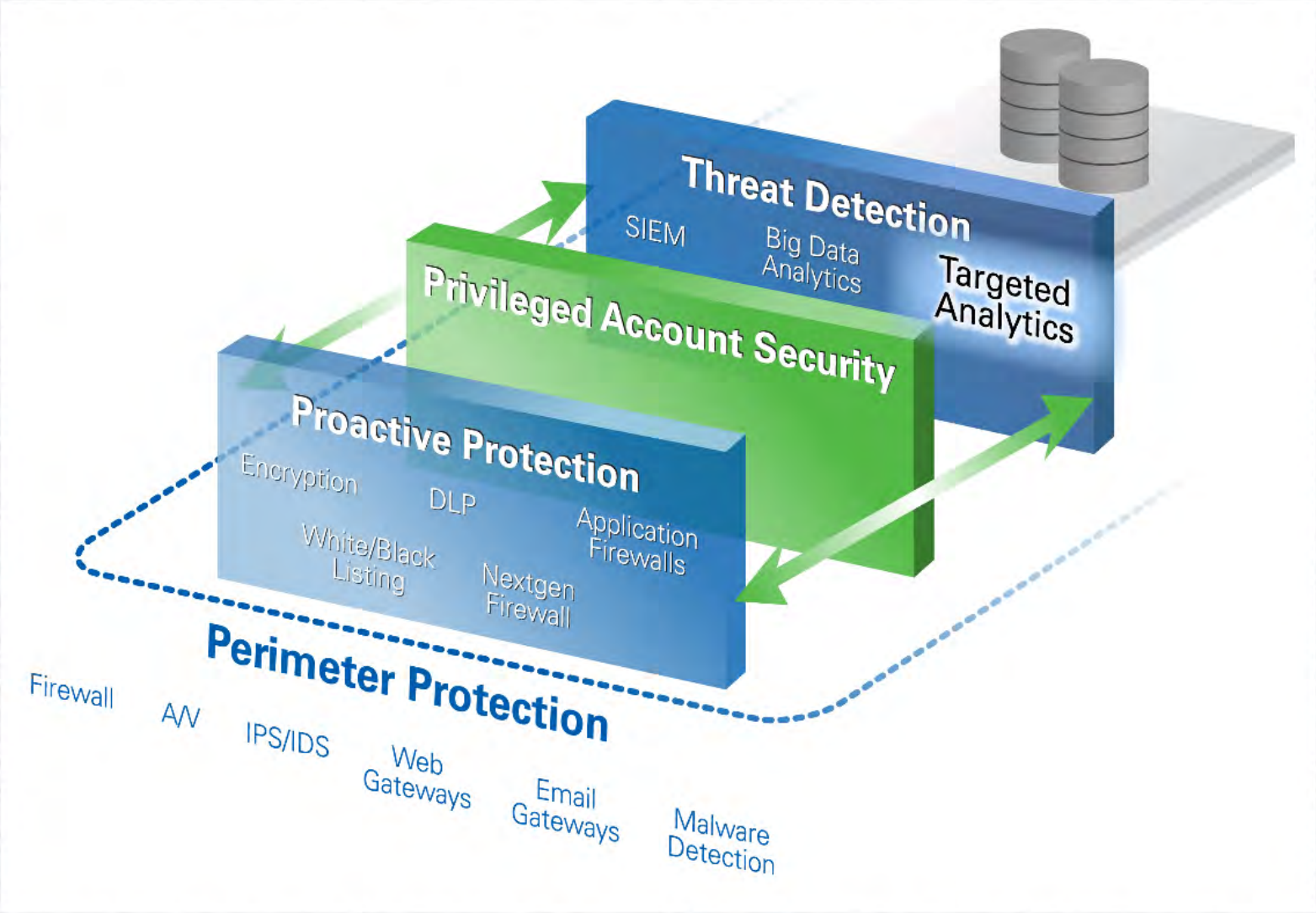
Impersonation



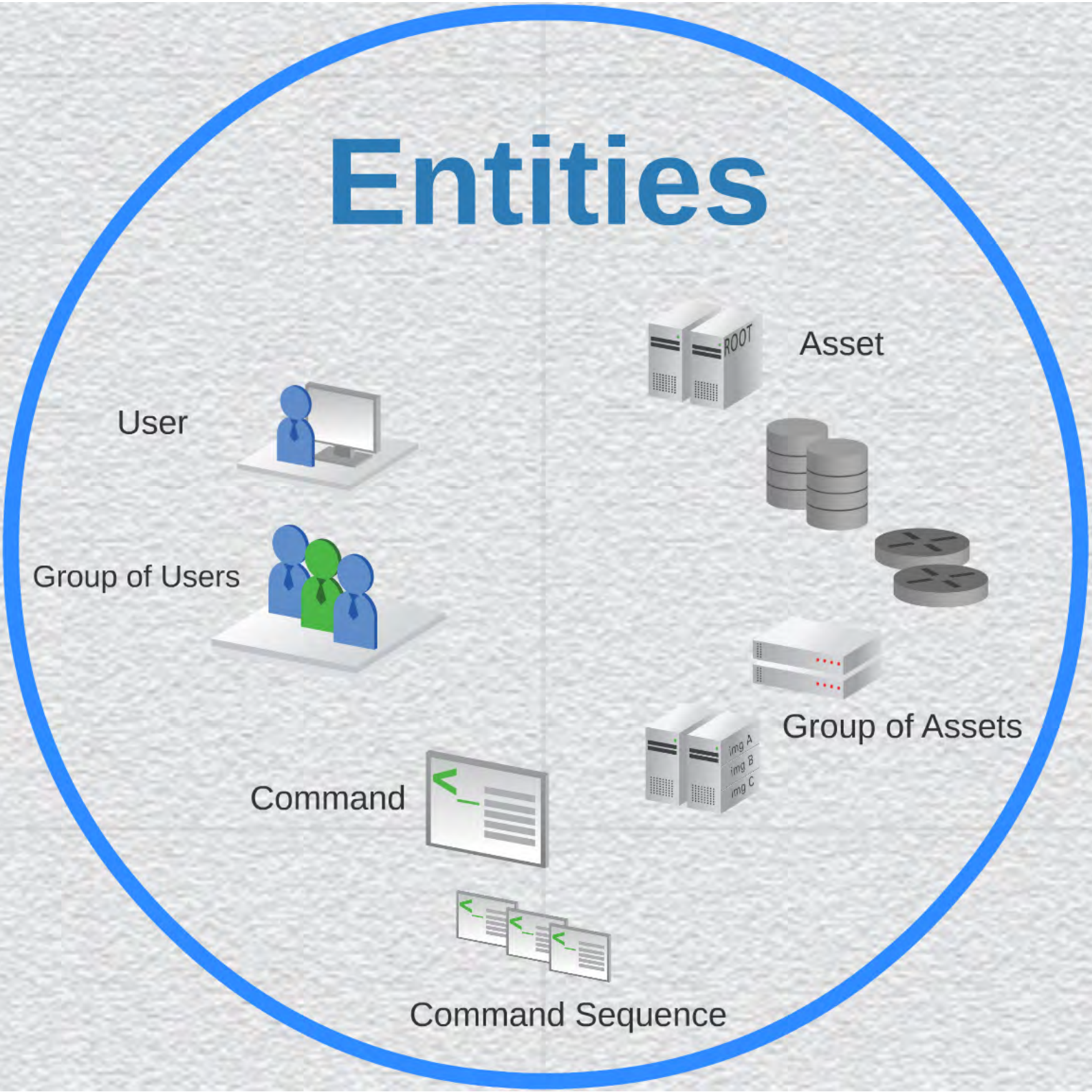
Discovering anomalies



Targeted analytics



Entities


Asset
ROOT
User
Group of Users
Group of Assets
img A
img B
img C
Command
Command Sequence

Dimensions

Time / Date

IP

Rate

GeoLocation

...

	Time	Day of Week	Work / Holiday	IP	Rate	…
User	"What is the hourly access profile of system administrator X to machine Y?"					
Group of Users		"What is the daily access profile of the UK DB admin group to DBs in the London datacenter?"				
Asset				"What are the IPs used to access Production Server 2?"		
Group of Assets						
Command					"What is the daily rate of "echo off" commands on Houston Linux servers?"	
Command Sequence						

CYBERARK

RSA CONFERENCE 2014

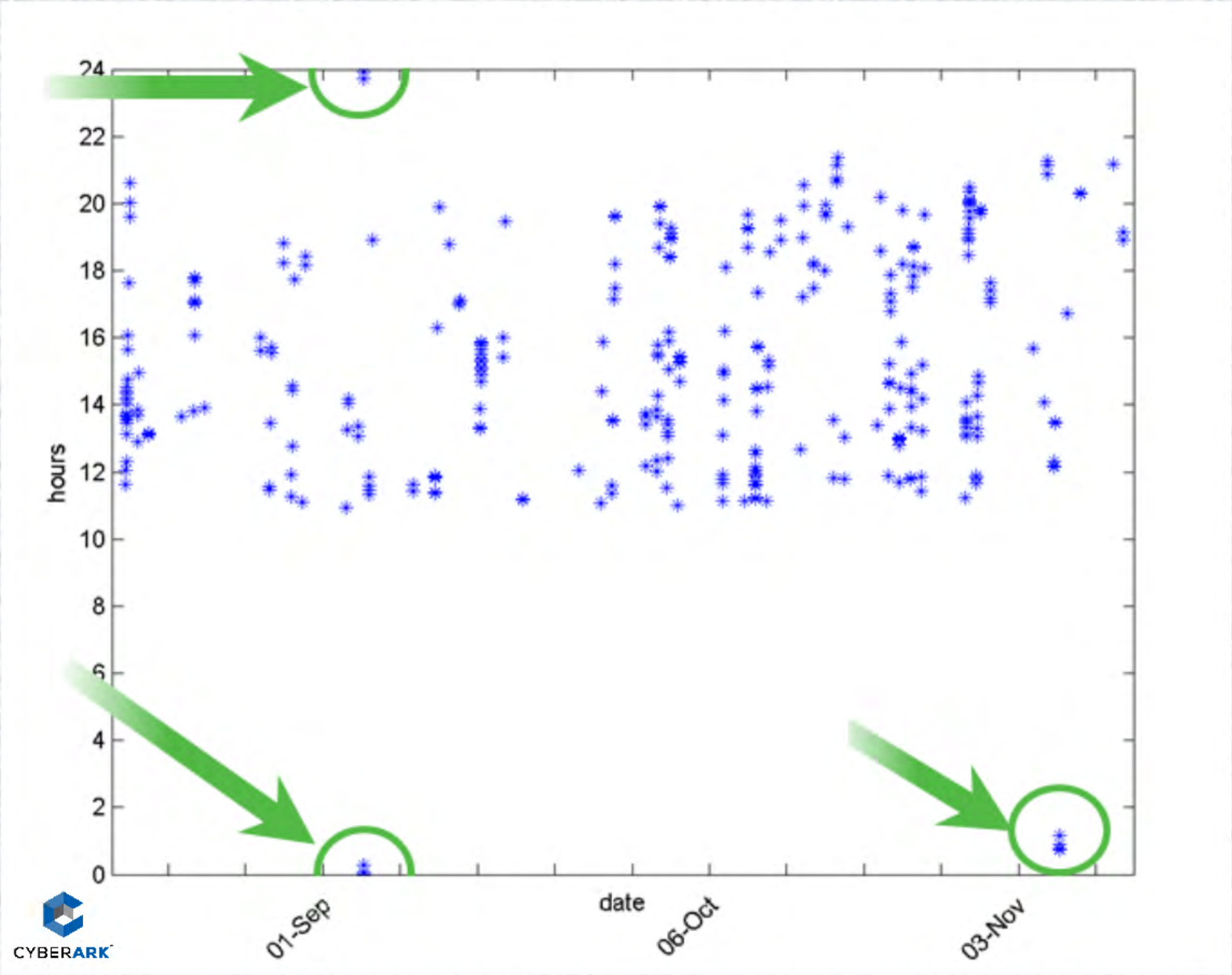
"What is the
hourly access profile
of
system administrator X
to
machine Y?"

"What is the
daily access profile
of
the UK DB admin group
to
DBs in the London
datacenter?"

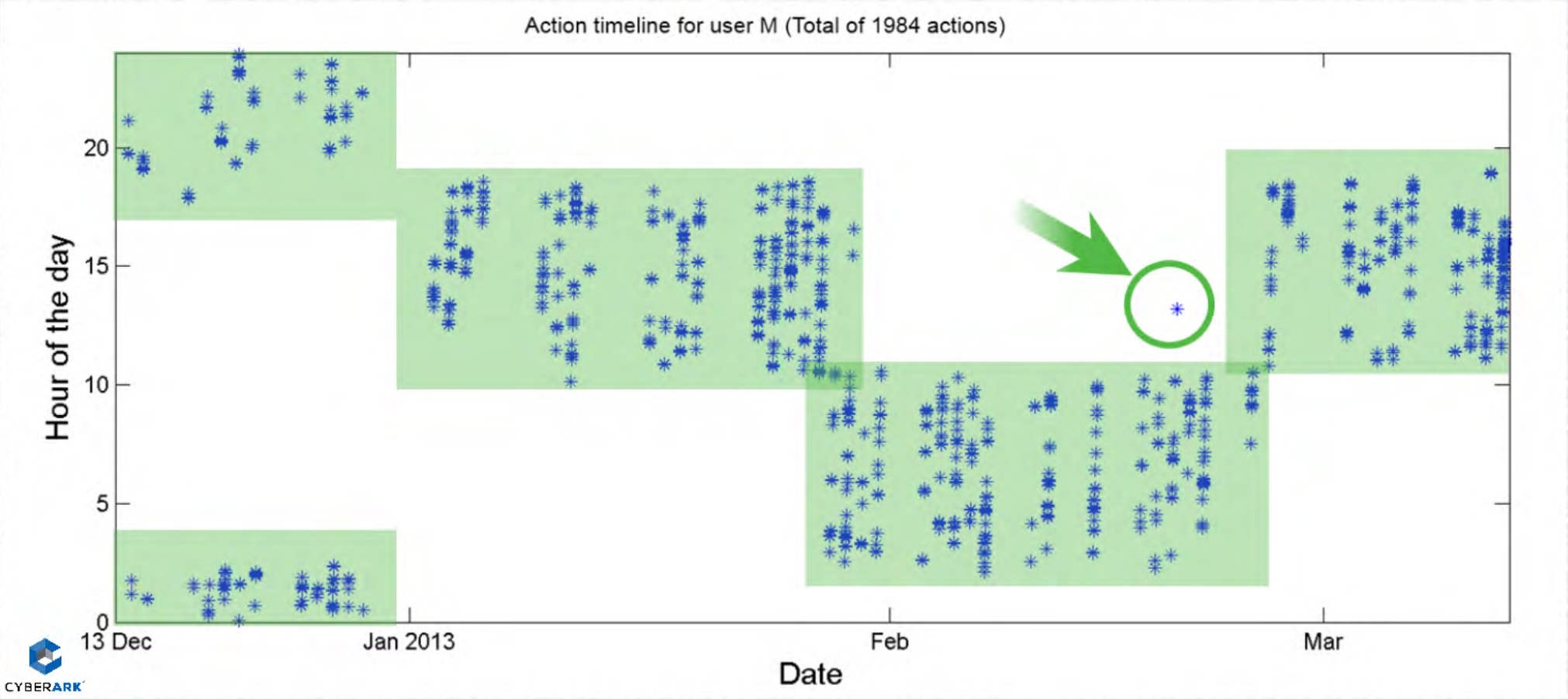
"What are the
IPs
used to access
Production Server 2?"

"What is the
daily rate
of
"echo off" commands
on
Houston Linux servers?"

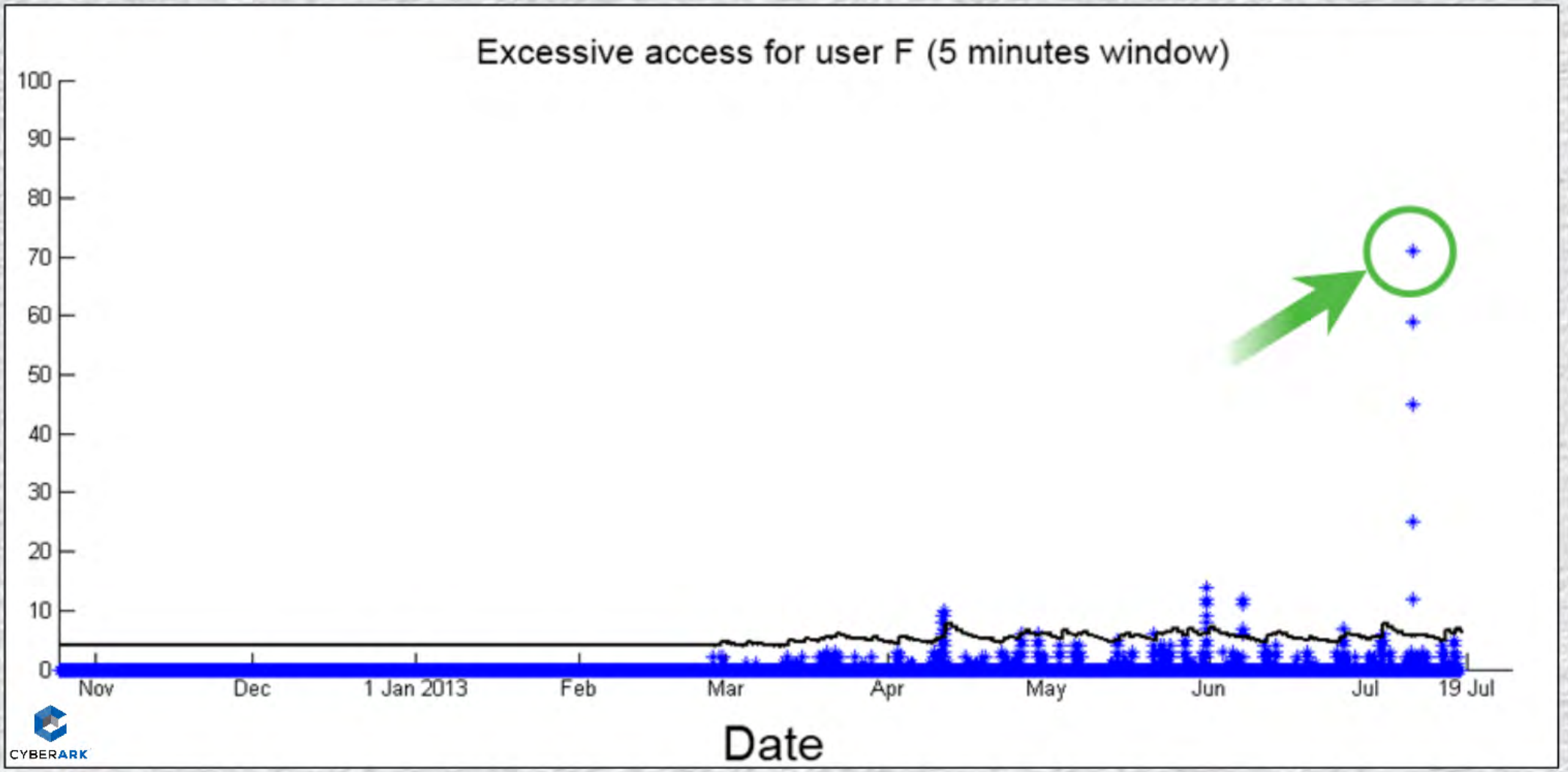
Time of day


24
22
20
18
16
14
12
10
8
6
4
2
0
hours
01-Sep
06-Oct
03-Nov
date
CYBERARK

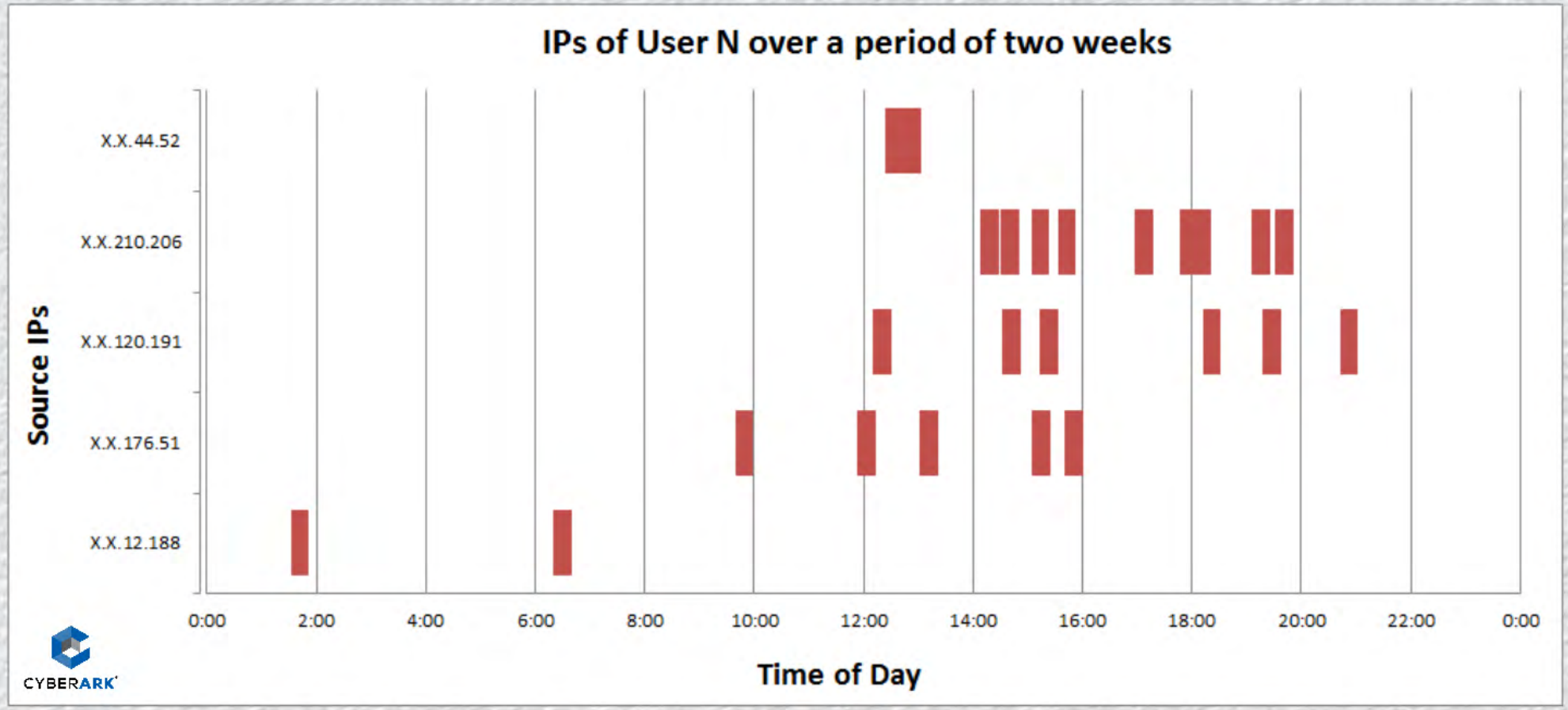
Time of day (cont.)



Activity rate



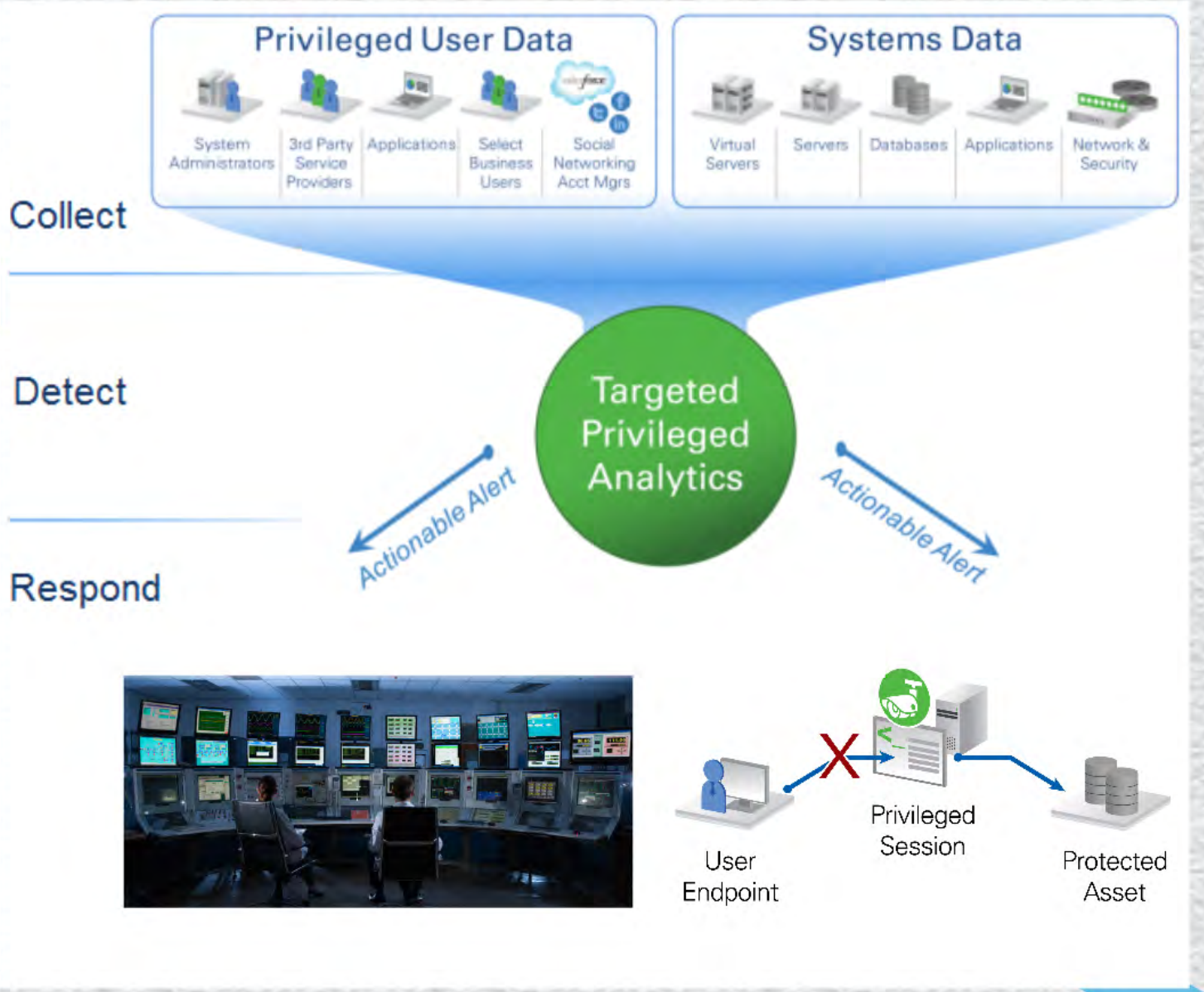
IP & time of day



Asking the right question

Photos by: Alex Gal and Shlomi Shitrit, from Pikiwiki.org.il

Actionable alerts



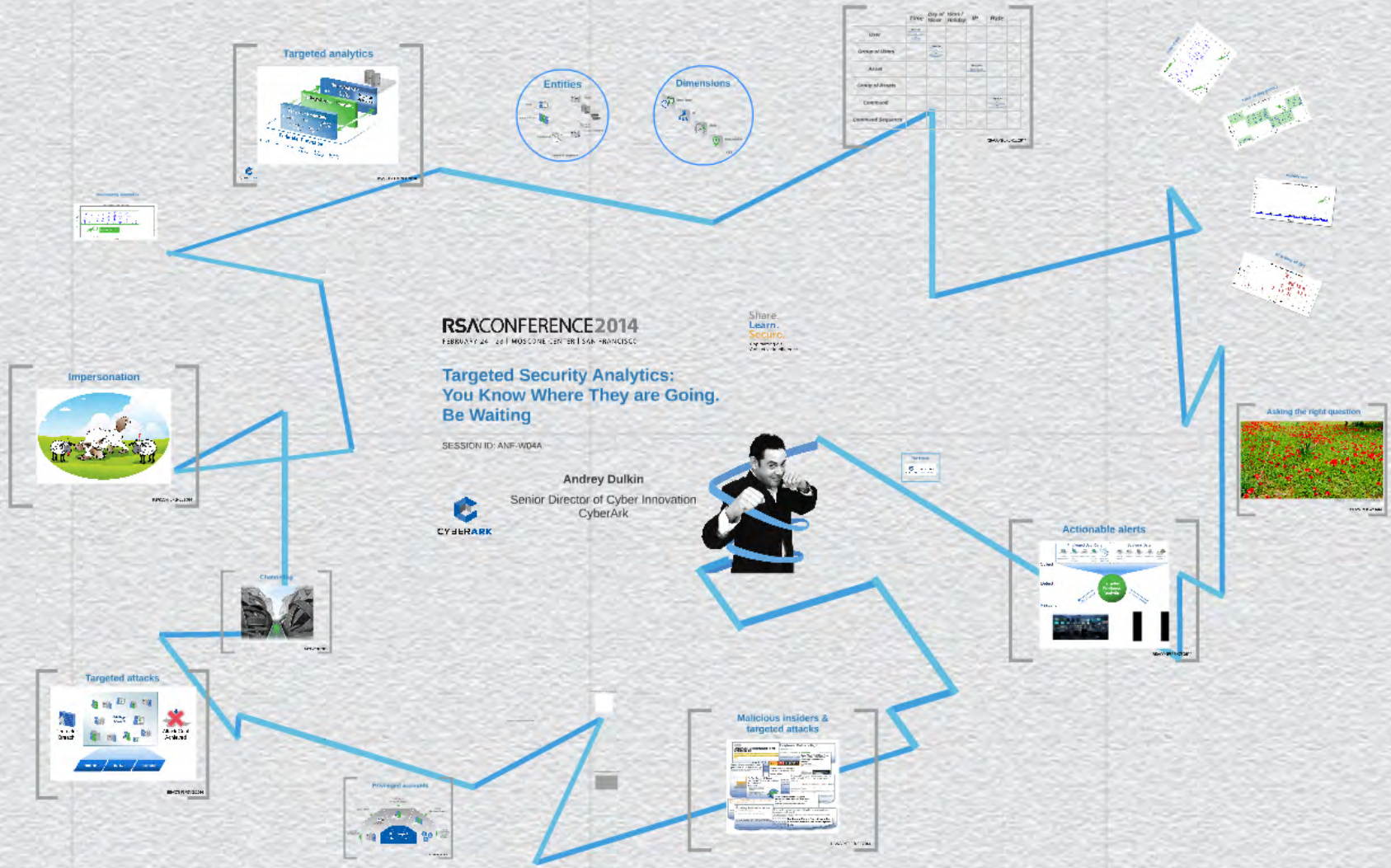
Thank you!

CYBERARK®

Andrey Dulkin

Senior Director of Cyber Innovation

andrey.dulkin@cyberark.com

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO