QRadar XDR

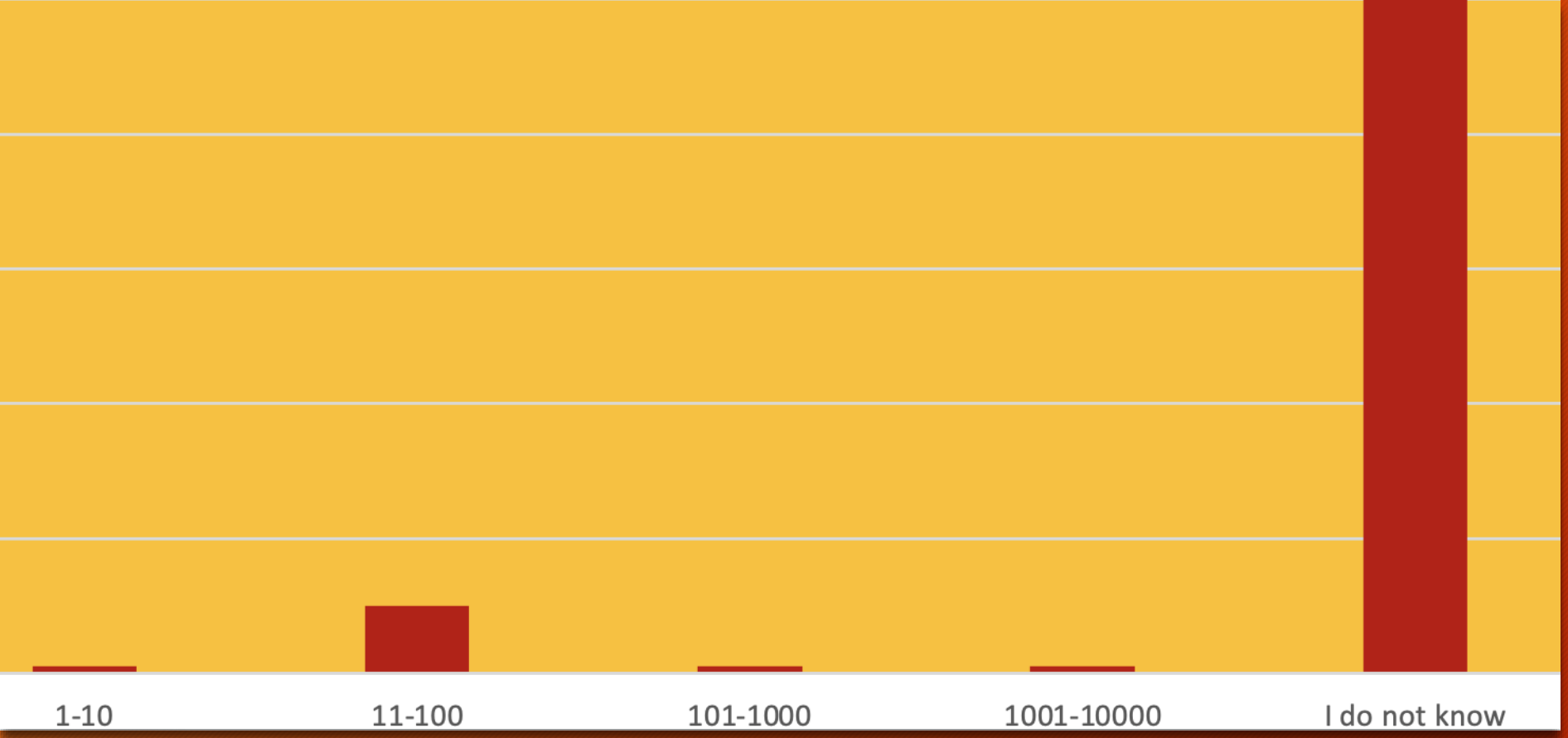
New licencing approach

tomasz.zalewski@pl.ibm.com

Licensing of Qradar Event Analytics (SIEM)

- Two approaches
  - MVS (Managed Virtual Servers)

  or
  - EPS (Events per Second)



Guess…

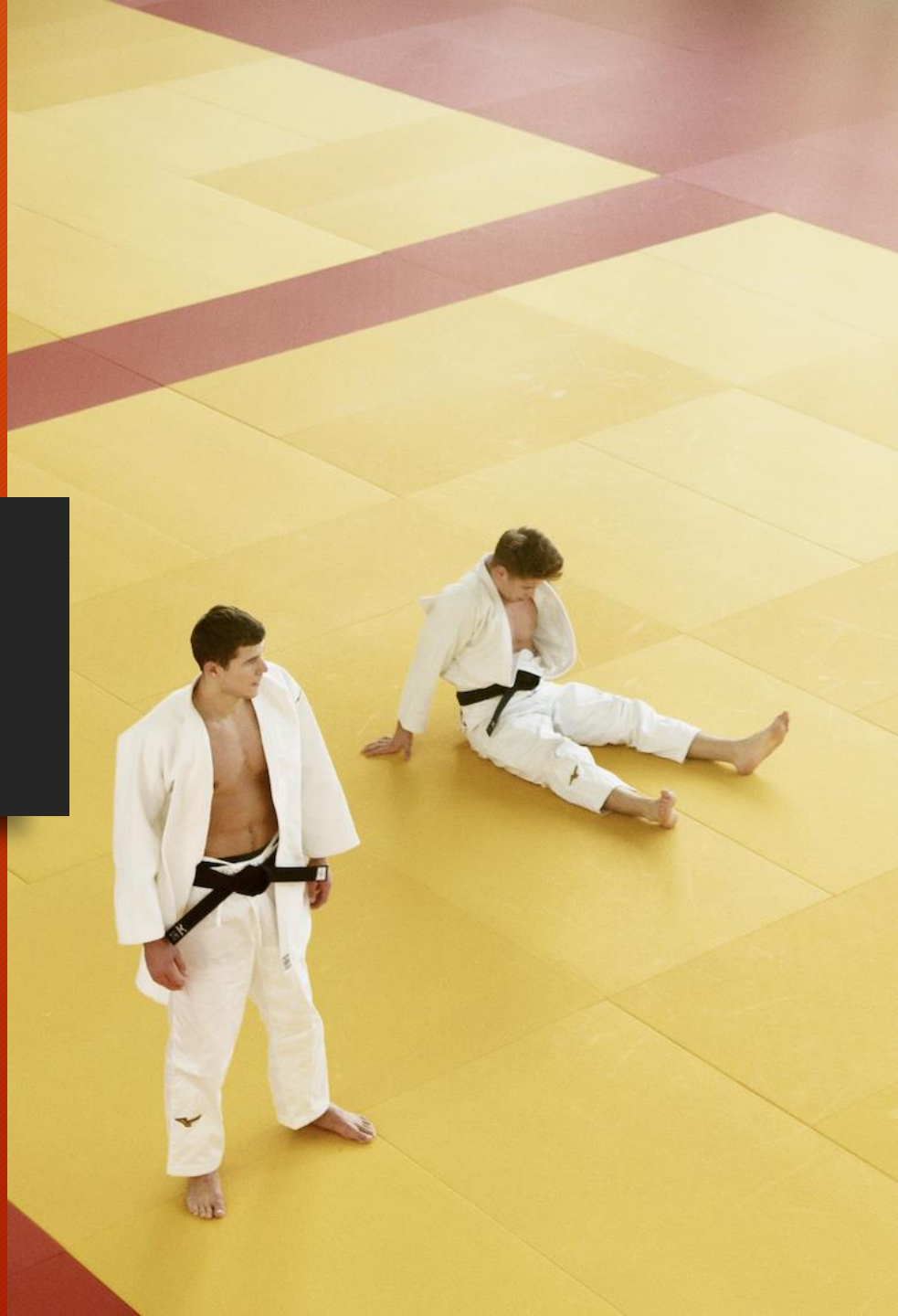
What customers say when I ask them how many servers they have?

QRadar XDR

New licencing approach

IBM Randori

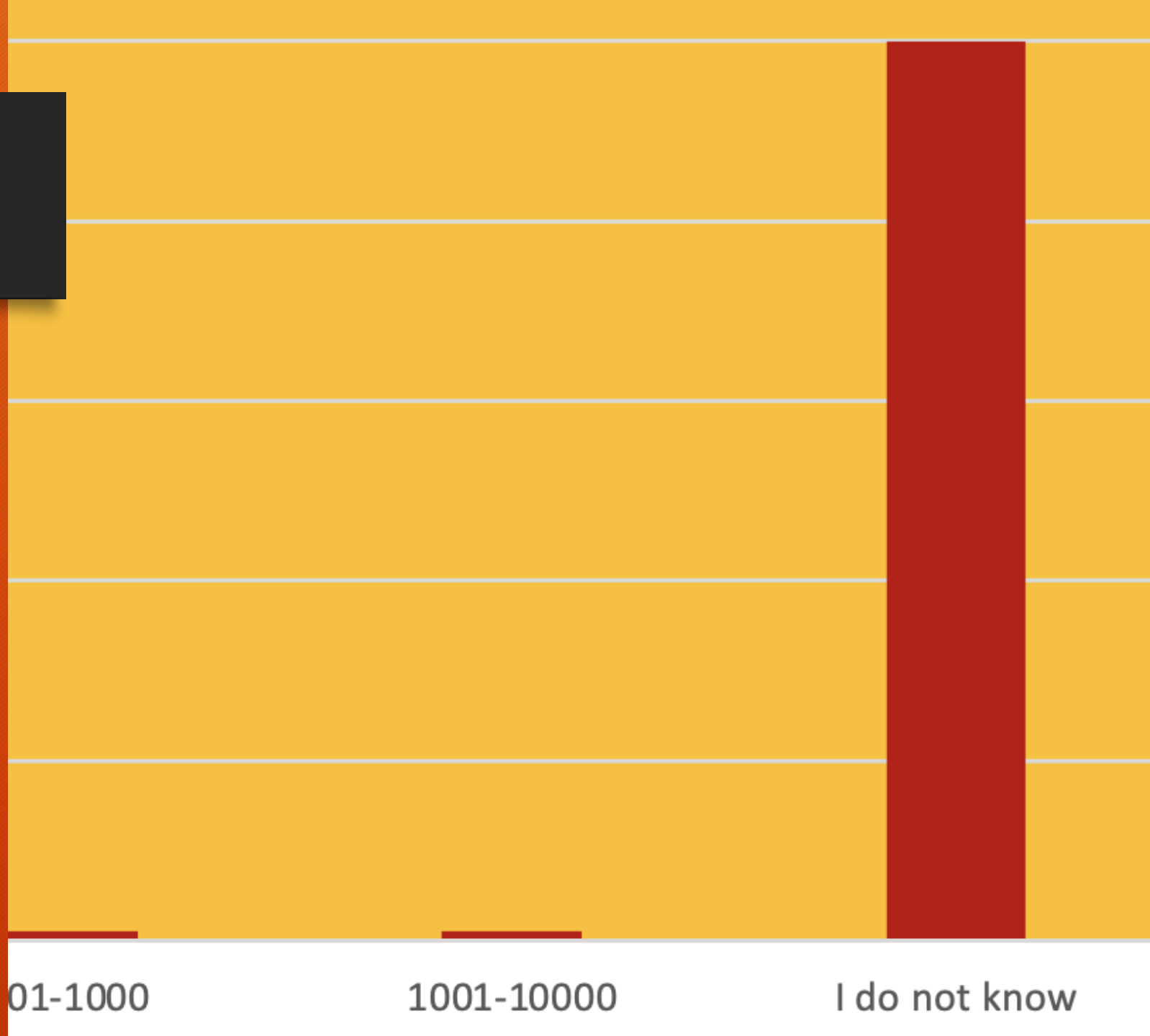
What is External Attack Surface Management and why you need it



And I am only asking about usefull servers!

No shadow IT

No zombie servers



How many servers you do not know about?

30%

of assets are *unknown* or *unmanaged* to an organization due to rapid transformation.

FORRESTER

Is shadow and zombie dangerous?

7 in 10

organizations have been compromised by an *unknown* or *unmanaged* asset in the past year.

ESG

What Randori does?

First:

It finds all external targets – as seen by attacker

Wait!
My external vulnerability scanner does this!

- No.
- You need to enter targets to vulnerability management system, so it can scan them
- First Randori finds targets
- Then you enter them to VM
- You need both!

But what if I give whole subnet to VM?

- Same IP serves multiple services – based on a name
- Are you sure this is the only subnet?
- How about M&A?
- How about cloud?

How “find” works in Randori

- Just enter an e-mail of somebody in company
- Randori uses:
  - Business intelligence databases
  - DNZ zones
  - IP topology
  - Whois
  - Certificates
  - etc

What Randori does?

Second:

Prioritizes targets by how tempting they are

What would look into as attacker?

- (Applicability) Windows or Banyan Vines?
- (Criticality) Production server or test server?
- (Enumerability) Apache 2.2.24 or Apache 2.x.x?
- (Exploitability) Log4J or no Log4J?
- (Research potential) QNI 1940 or CentOS?
- (Post Exploit Potential) Branch VPN or coffee maker?

What Randori does?

Third:

Act!

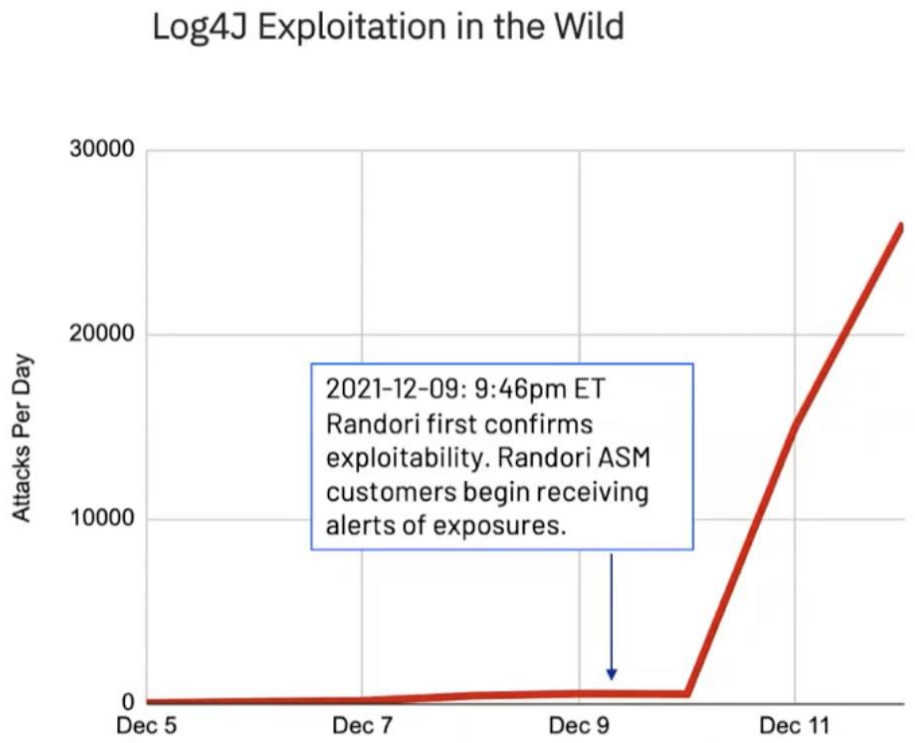
What can I do with results?

- Report it
- Enrich it
- Tune it
- Send to TT/SIEM/VM

meijer

" In the case of Log4j, Randori's real-time visibility was the difference between being ahead of attackers or having to react to attacks. That first weekend we saw 4,000 log4j related attacks against our environment...that we were already ahead of and had mitigated. Continuous monitoring and real time alerting was the key here."

— Philip Keibler, CISO



Practical example

Interested?

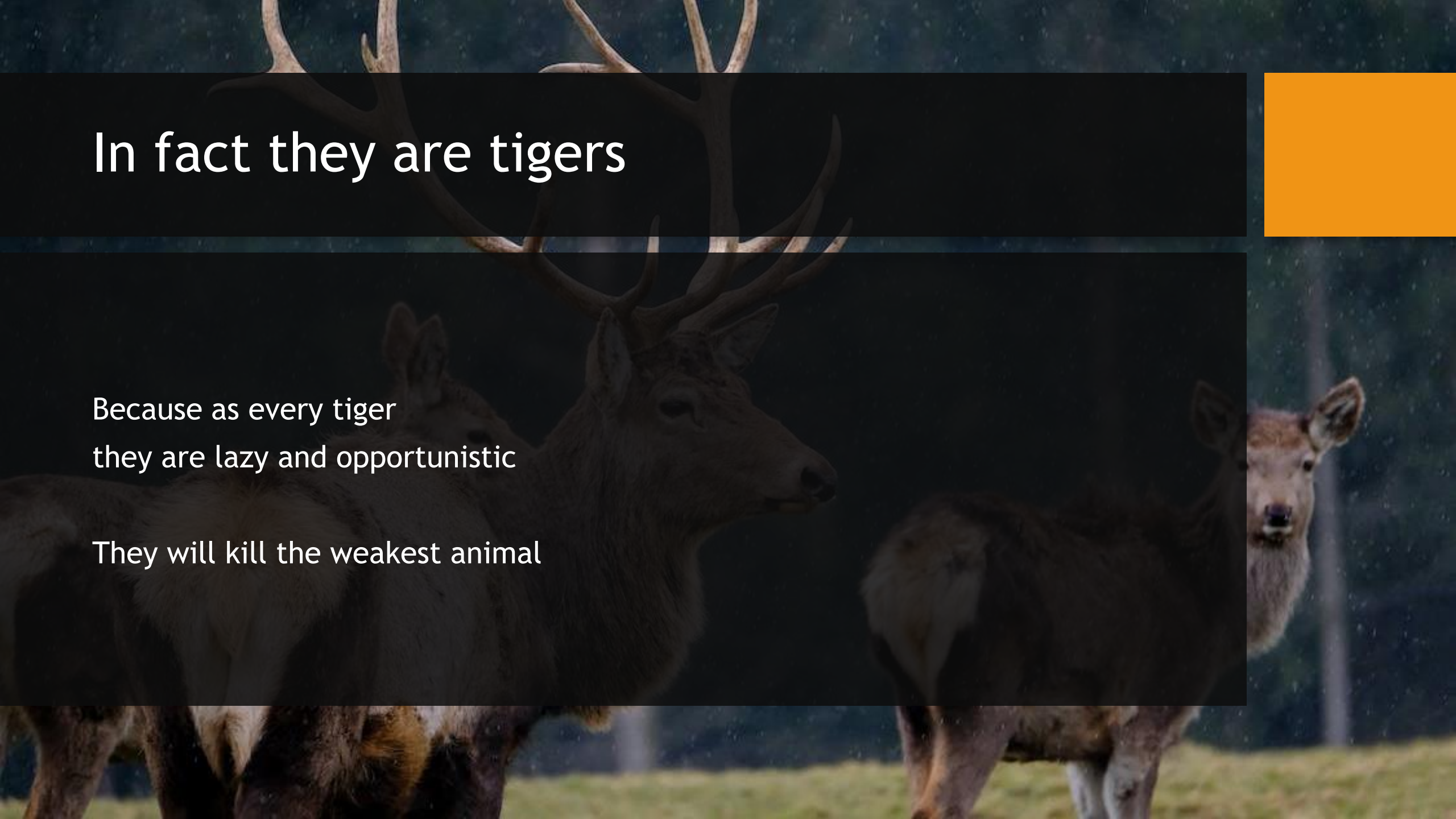
Set up a meeting where we present what Randori found in your network

Summary before demo – what will Randori find?

- Vulnerable targets – if you have them
- Unknown targets – at initial scan, for sure
- New targets – on regular basis
- BAD IT HYGIENE – MOST IMPORTANT

Cybercriminals see themselves as tigers

And they see us as prey

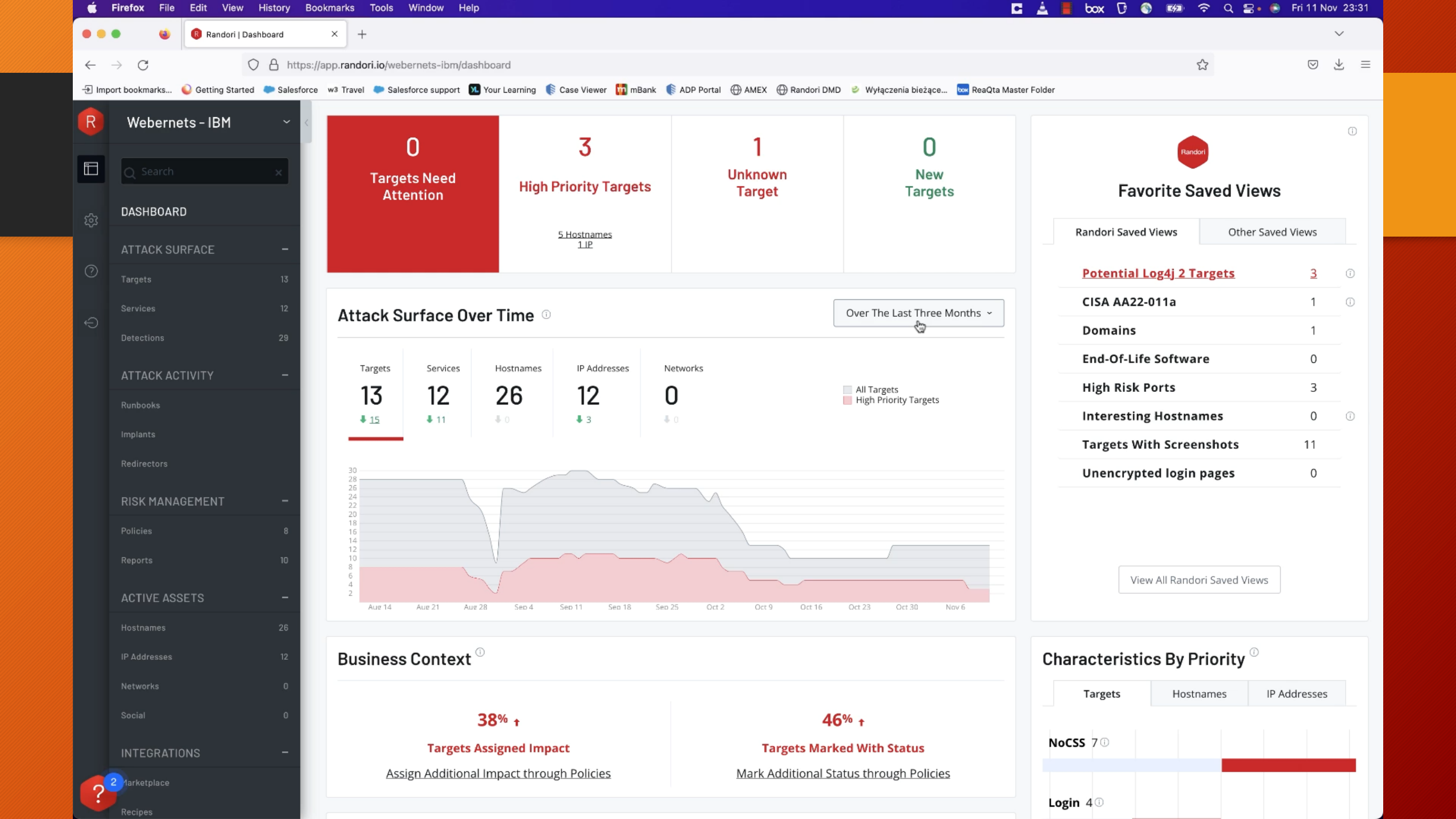


In fact they are tigers

Because as every tiger
they are lazy and opportunistic

They will kill the weakest animal

Demo!


Webernets - IBM
DASHBOARD
ATTACK SURFACE
Targets 13
Services 12
Detections 29
ATTACK ACTIVITY
Runbooks
Implants
Redirectors
RISK MANAGEMENT
Policies 8
Reports 10
ACTIVE ASSETS
Hostnames 26
IP Addresses 12
Networks 0
Social 0
INTEGRATIONS
Recipes
0
Targets Need Attention
3
High Priority Targets
5 Hostnames
1 IP
1
Unknown Target
0
New Targets
Attack Surface Over Time
Over The Last Three Months
Targets 13 15
Services 12 11
Hostnames 26 0
IP Addresses 12 3
Networks 0 0
All Targets
High Priority Targets
Aug 14
Aug 21
Aug 28
Sep 4
Sep 11
Sep 18
Sep 25
Oct 2
Oct 9
Oct 16
Oct 23
Oct 30
Nov 6
Favorite Saved Views
Randori Saved Views
Other Saved Views
Potential Log4j 2 Targets 3
CISA AA22-011a 1
Domains 1
End-Of-Life Software 0
High Risk Ports 3
Interesting Hostnames 0
Targets With Screenshots 11
Unencrypted login pages 0
View All Randori Saved Views
Business Context
38% ↑
Targets Assigned Impact
Assign Additional Impact through Policies
46% ↑
Targets Marked With Status
Mark Additional Status through Policies
Characteristics By Priority
Targets
Hostnames
IP Addresses
NoCSS 7
Login 4

Do not be the weakest animal