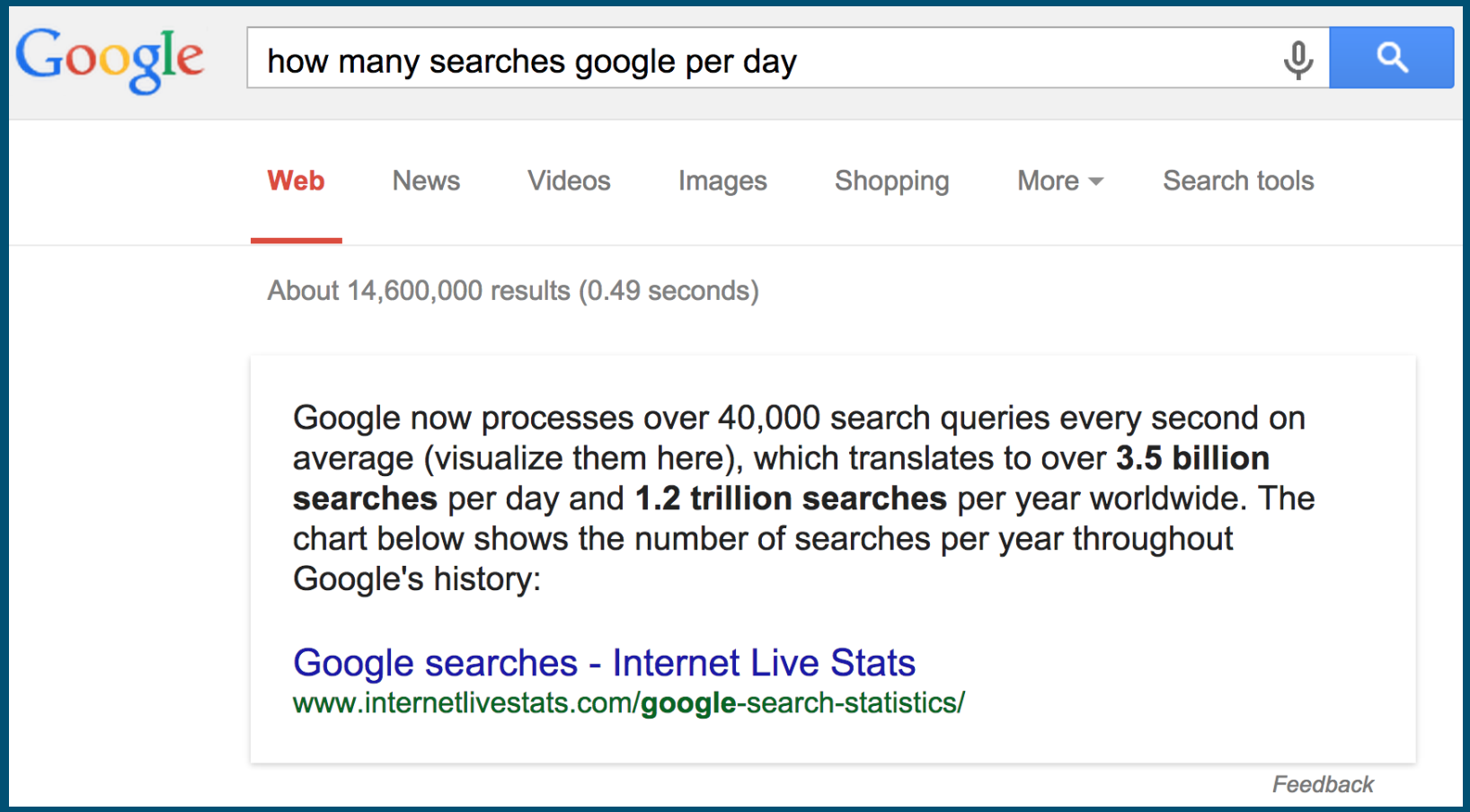
Battle between hackers and machine learning

Alexey Lukatsky
Cybersecurity Business Consultant
April 03, 2019

Google: facts and numbers



3.5 Billion

searches a day

1.2 Trillion

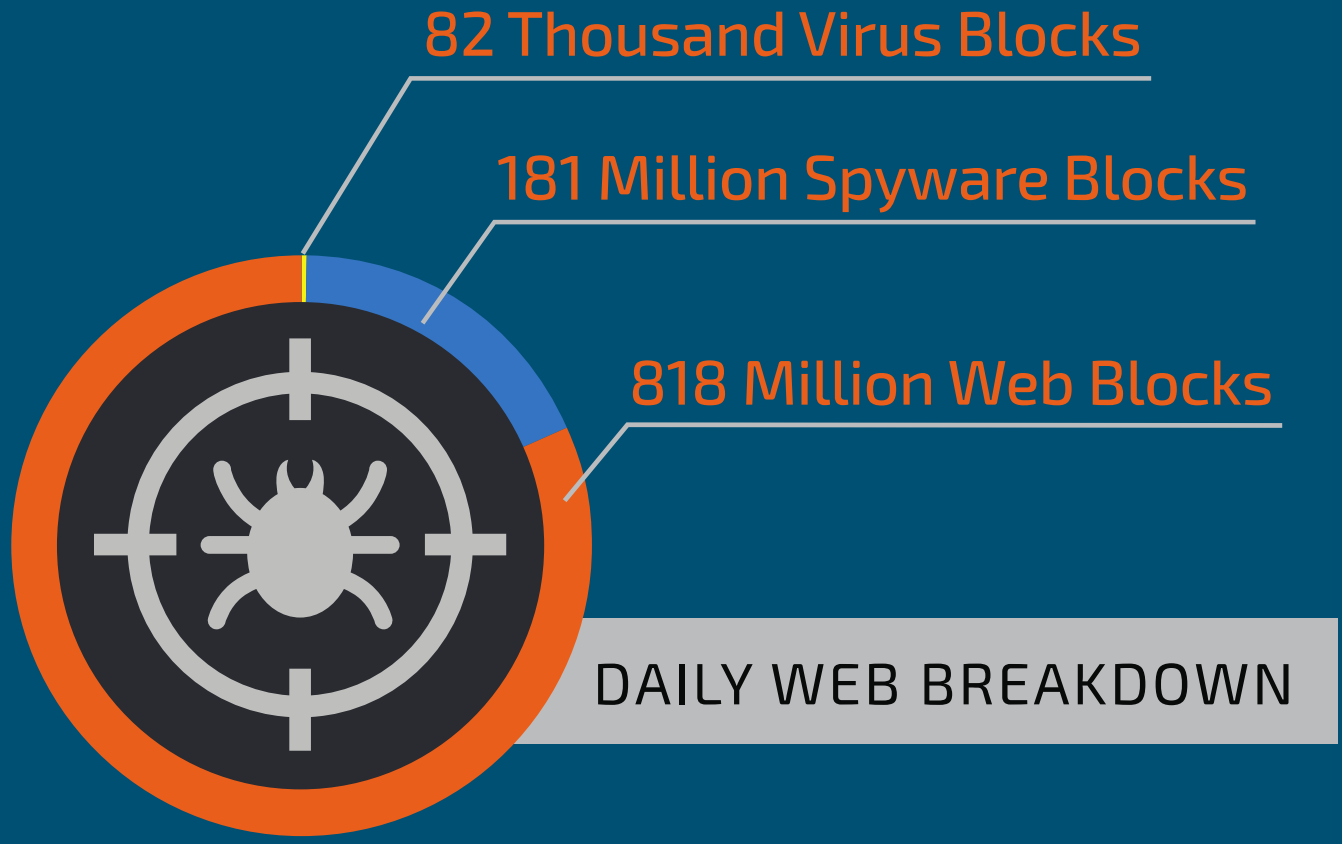
searches a year

Real Cisco Big Data for Security Training Set

19.7 Billion
TOTAL THREAT BLOCKS
DAILY

=

7.2 Trillion
YEARLY



Why is Machine Learning so useful in Security?

Static

With limited variability or is well-understood

Evolving Security

The security domain is always evolving, has a large amount of variability, and is not well-understood

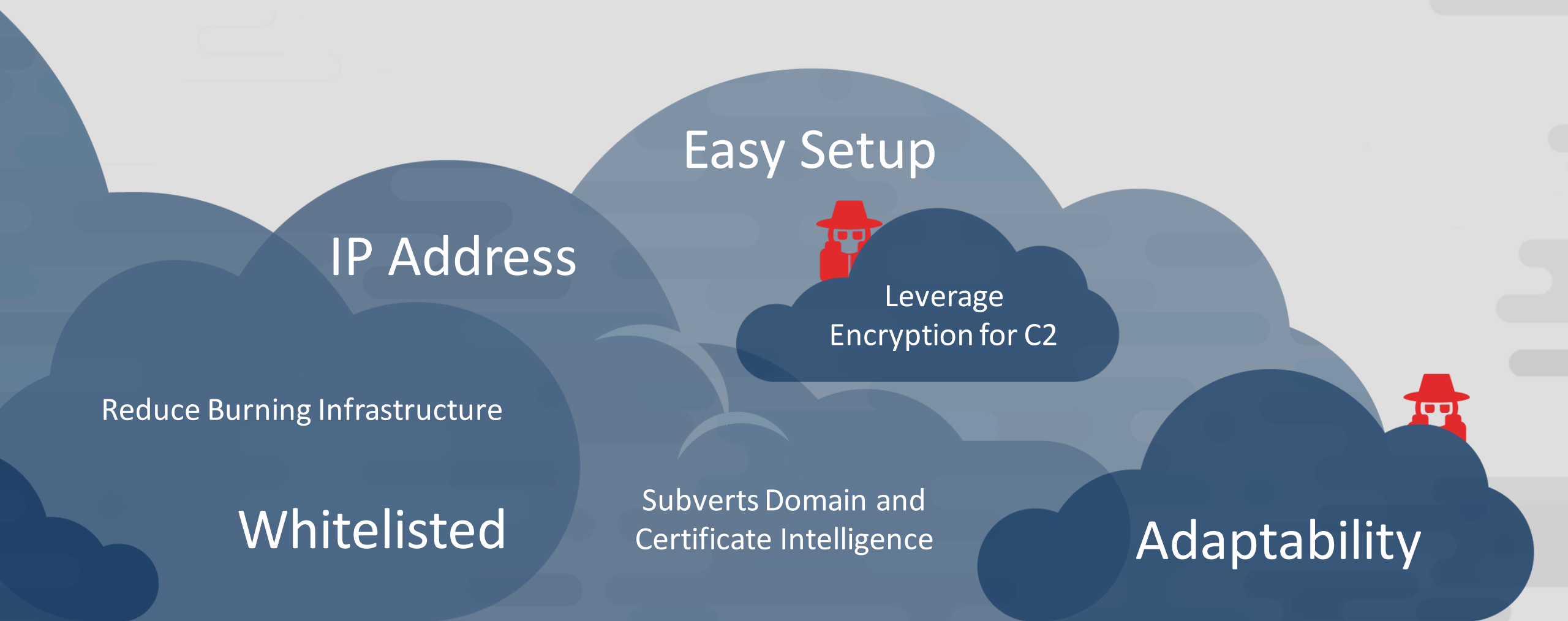
Finding Malicious Activity in Encrypted Traffic

Leveraged network	Faster investigation	Higher precision	Stronger protection
Enhanced NetFlow from Cisco's newest switches and routers	Enhanced analytics and machine learning	Global-to-local knowledge correlation	Continuous enterprise-wide compliance

* Future support coming soon for ISR and ASR systems

Malicious Use of Legitimate Resources

Cybercriminals are adopting command-and-control channels that rely on legitimate Internet services, making malware traffic almost impossible to shut down



Internet anomalies typically detected

Sample report demonstrating an advanced threat visibility gap: http://cognitive.cisco.com/preview

Insider Threat

Machine learning algorithms can greatly help detect internal malicious actors

5200
docs per user

“Data”
was the most popular keyword in doc titles

PDFs
were the most common file type

62%
occur outside of normal work hours

High*
accuracy of malicious activity detection since June 2017

Compromised Cloud Account Detection

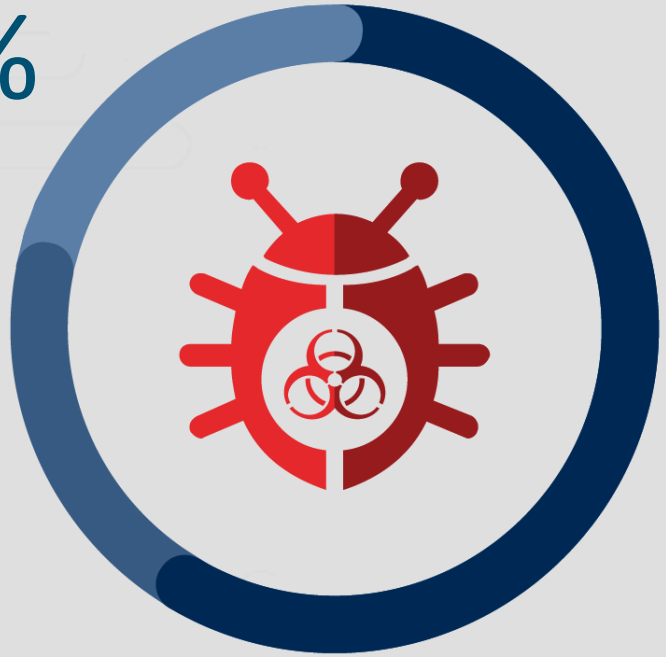
Compromised Account Risk

Showing top **14 users** out of total **14 users** that have generated activity from 3 or more locations in the past **7 days**.
Activity in one account across multiple locations may indicate use of a VPN, possibly unauthorized.
Activity from multiple and/or risky locations may indicate compromised accounts.

User	Logins	Location
There were **14** instances of users who logged in from 3+ locations.		
[redacted]	4,711	Pleasant Grove, UT, United ...
	7	Lehi, UT, United States
	6	Buenos Aires, C, Argentina
	4	Federal, E, Argentina
	1	San Francisco, CA, United S...
	1	Dallas, TX, United States
	2	Los Angeles, CA, United Sta...
	2	Parker, CO, United States
	1	Columbus, OH, United States
	1	Manhattan Beach, CA, Unite...
	1	Denver, CO, United States
	3	Hyderabad, TG, India

How Malicious Actors Leverage Domains

Type of Attack



20%
Other

60%
Spam

20%
Malvertising

RLD Registered Times

20%
Less than 1 week

80%
More than 1 week

New or Reused Domains

42%
New

58%
Reused

Organizations need to minimize access to malicious domains

cisco

DNS predictive models

2M+ live events per second

11B+ historical events

Guilt by inference

- Co-occurrence model
- Sender rank model
- Secure rank model

Guilt by association

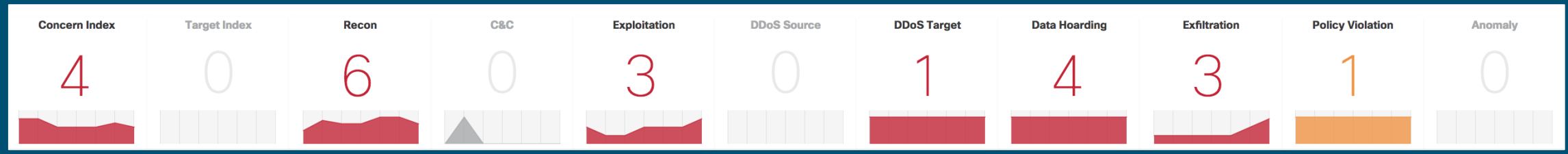
- Predictive IP Space Modeling
- Passive DNS and WHOIS Correlation

Patterns of guilt

- Spike rank model
- Natural Language Processing rank model
- Live DGA prediction

Suspicious events in internal network

Source or target of malicious behavior	Reconnaissance	Command and Control	DDoS Activity	Insider threats
Scanning, excessive network activity such as file copying or transfer, policy violation, etc.	Port scanning for vulnerabilities or running services	Communication back to an external remote controlling server through malware	Sending or receiving SYN flood and other types of data floods	Data hoarding and data exfiltration



Market Expectations: Modern Workplace

The modern workplace will continue to create conditions that favor the attackers

- The footprint security executives must secure continues to expand
- Employees increasingly carry their work (and the company's data) with them wherever they go—a well-documented source of exposure
- Clients, partners and suppliers all need secure access to corporate resources
- With the increasing deployment of IoT sensors, etc., companies' interfaces to the internet will multiply dramatically

cisco

Market Expectations: AI and Machine Learning

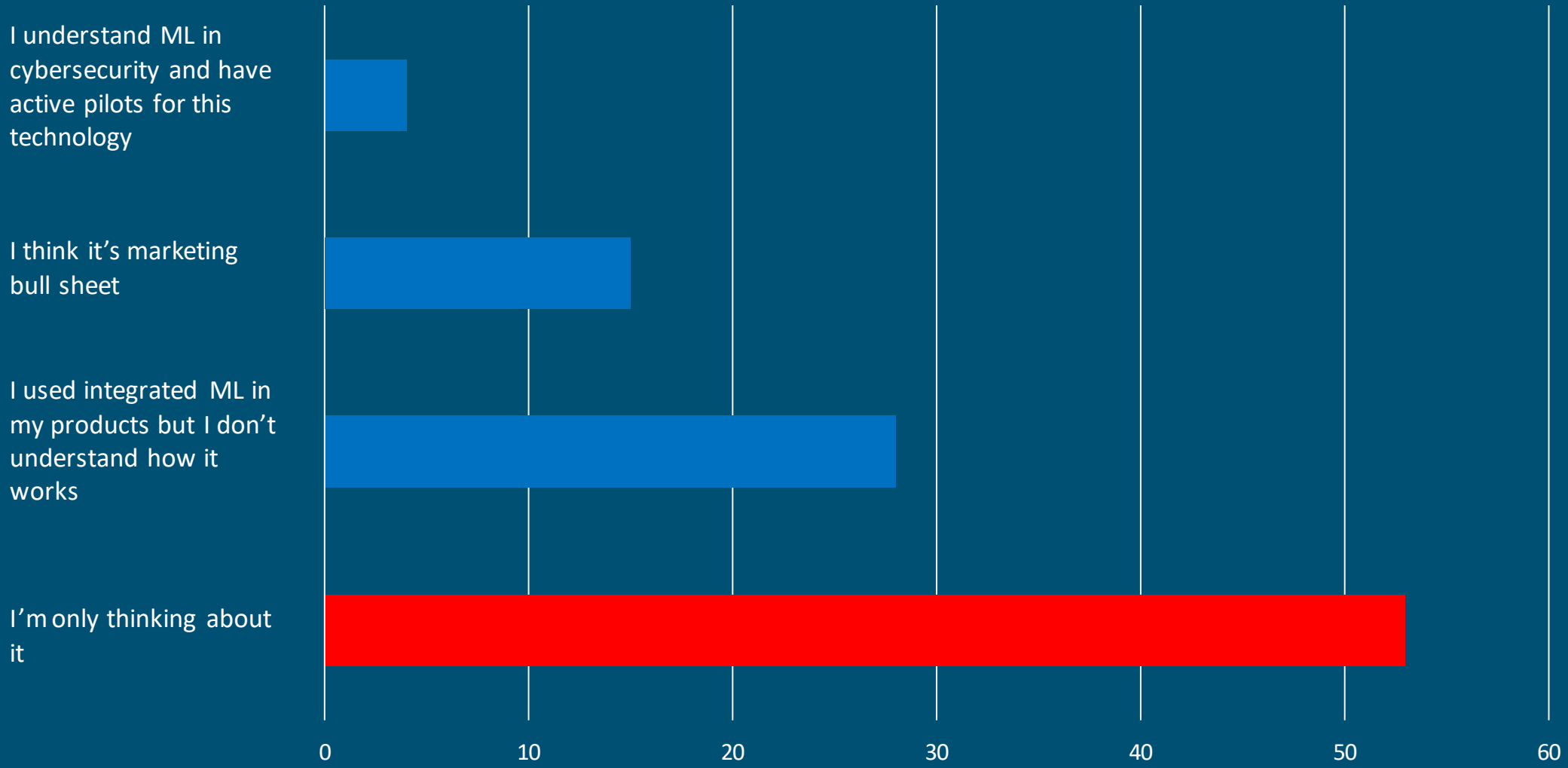
More spending on AI/ML capabilities

- AI, ML and automation increasingly desired and expected
- 83%: Reliant on automation to reduce level of effort to secure the organization
- 74%: Reliant on AI to reduce level of effort to secure the organization
- CISOs expect to take increasing advantage of AI and robotics
- 92% of security professionals say behavior analytics tools work well in identifying bad actors

cisco

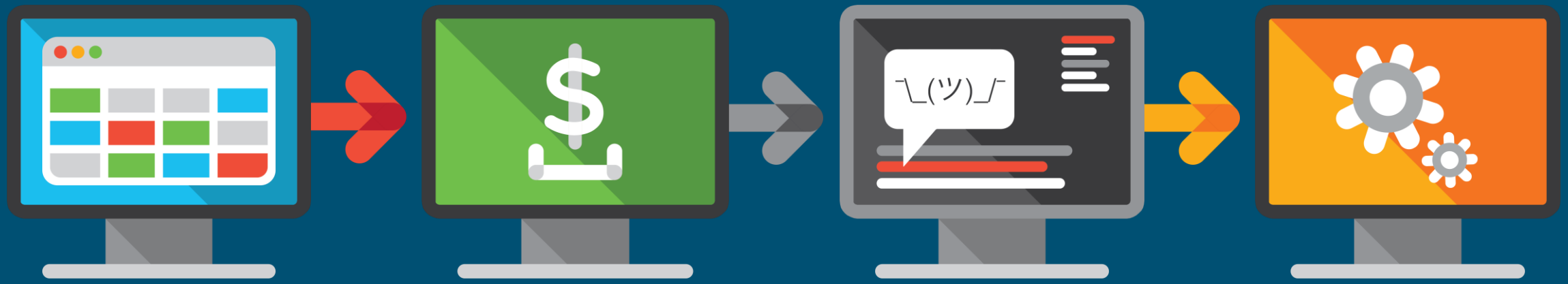
What about Russia?

How are you using AI/ML in your cybersecurity? (%)



Source: Лукацкий А.В., IDC Security Roadshow

AI in cyber security isn’t panacea but future



Signatures and IoC

IDS, AV, NGIPS, EDR, TIP

Rules

NGFW, WSA, SIEM, ESA

Statistical models

Netflow

AI algorithms

References for Cisco Cyber Security & Machine Learning

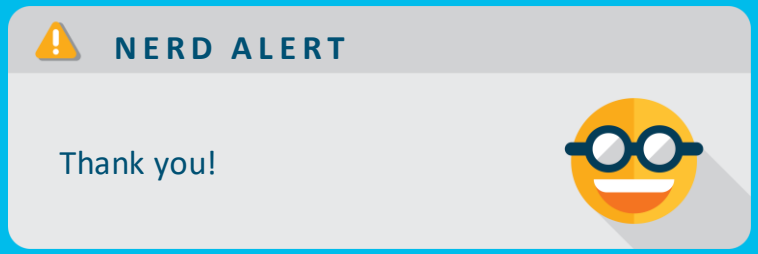
https://www.cisco.com/go/security

https://www.talosintelligence.com

https://blogs.cisco.com/tag/machine-learning

http://www.cisco-ai.com

You can test all of our Cisco Security Solutions


NERD ALERT
Thank you!