

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: STR-W10

Deep Modernization of a Corporate IT Security Infrastructure

John Tolbert

Lead Analyst
KuppingerCole, Inc.
@john_tolbert_kc

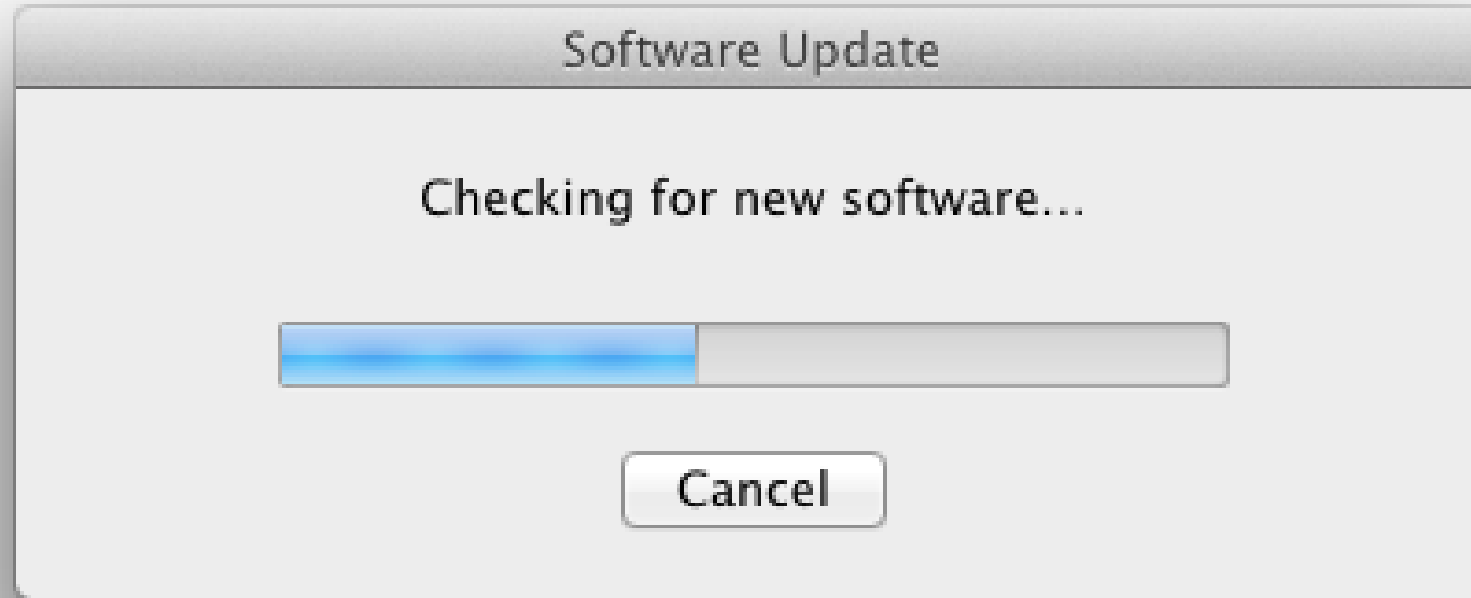


#RSAC

RSA®Conference2019

- Why modernize?
- What to modernize? Endpoint management & security, IAM
- How to modernize? Zero trust and ML-enhanced tools
- Cutting through the hype
- Case Studies sprinkled in
- Apply it – How to determine what is the best course for your organization? What are the first steps to getting your infrastructure up-to-date?

Aren't we up-to-date already?



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

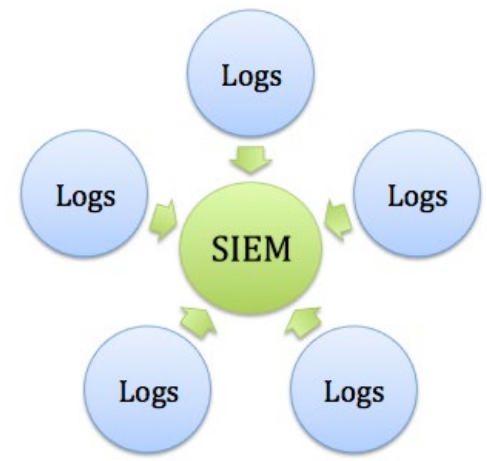
But we already have



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Now let's make your account even more secure

What's the name of your favourite pet?

What's the place of birth of your mother?

What's your favourite book?

What's your favourite destination?

What's your favourite movie?

Some mind-boggling stats from the 2018 HIMSS Cybersecurity Survey

- 13% have no dedicated cybersecurity staff
- 17% are not using a security framework
- 20% don't pen test
- 24% have no insider threat programs
- 27% have no specific cybersecurity budget set aside

Top concerns:

- Data leakage
- Ransomware
- Credential stealing malware

https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf

You can't modernize what you don't have

75%

of respondents rate the maturity of their vulnerability identification as very low to moderate.



35%

describe their data protection policies as ad-hoc or non-existent.



48%

of respondents do not have a SOC.

12%

have no breach detection program in place.



38%

have no identity and access program or have not formally agreed such a program.



57%

do not have, or only have an informal, threat intelligence program.

[https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/\\$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf](https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf)

Poll question 1

- STR-W10
- Do you think your infrastructure security and IT security services are as up-to-date as they should be?
 - A. Yes
 - B. No
 - C. Not sure

<https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3836>

Why modernize? The ever-evolving threatscape

Evolving

- Malware
 - Polymorphic
 - File-less
 - Android
 - Mac & Linux too
 - IoT
- Phishing and Vishing

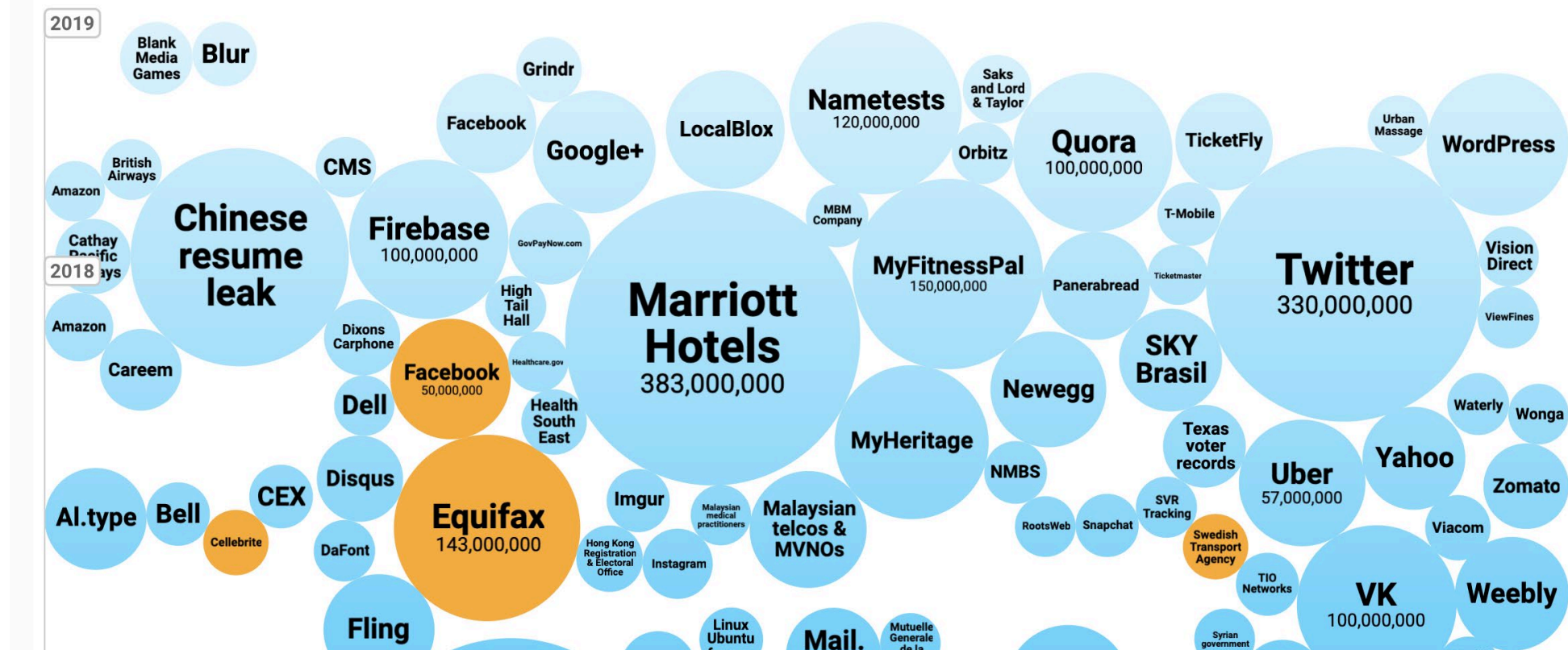
New

- Ransomware (sort of new)
 - RWaaS
- Crypto-jackers
- Account takeovers
- New account fraud
- Vaporworms?

Select losses greater than 30,000 records
(updated 1st Feb 2019)

(updated 1st Feb 2019)

Search...



<https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

**Main point: Strategic upgrades of
core security technologies can
improve your security posture***

****Caveats ahead***

Facts and myths about IT Security

Part 2. Facts and myths about technology, personnel and governance

Please rate the following statements using the five-point scale provided below each item. **Strongly Agree and Agree responses combined.**

Technology	Total
Q1a. The cloud is diminishing the need for on-premise IT security.	56%
Q1b. The cloud is cost effective because it is easier and faster to deploy new software and applications than on-premise.	74%
Q1c. As organizations re-write their apps to be cloud-enabled they are less secure than on-premises apps.	51%
Q1d. Data breaches occur because of poor patch management.	68%
Q1e. Security patches can cause greater risk of instability than the risk of a data breach.	53%
Q1f. Patching vulnerabilities is difficult because it leads to costly business disruptions and downtime.	45%
Q1g. Our organization is investing in tools to increase visibility into all applications data and devices and how they are connected.	45%

<https://www.bmc.com/content/dam/bmc/collateral/third-party/Ponemon%2bReport.pdf>, Ponemon Institute study commissioned by BMC

Perceived barriers to effective cybersecurity

Too many application vulnerabilities	54	28.6%
Too many endpoints (e.g., user devices, computers, etc., connected to the network)	52	27.5%
Too many new and emerging threats	51	27.0%
Not enough cyber threat intelligence to stay ahead of threats	44	23.3%
Network infrastructure too complex to secure	39	20.6%
Sufficient cyber threat intelligence, but lack of technologies/tools for effective use and deployment	32	16.9%
Sufficient cyber threat intelligence, but lack of know-how for effective use and deployment	27	14.3%
Too many users for timely and effective provisioning and de-provisioning of accounts	26	13.8%

New tools can help
orgs overcome
these barriers

None of the above	9	4.8%
-------------------	---	------

Q. What are the biggest barriers your organization faces to remediating and mitigating cybersecurity incidents? Please select all that apply.

https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf

Perceived barriers to effective cybersecurity – case study

FUD in management

Mediocre IT team, no security experts

Outdate perspective on security

- 30 days of patch testing before deployment
- Centralized network services

Too many tools to manage, no integration

Poll question 2

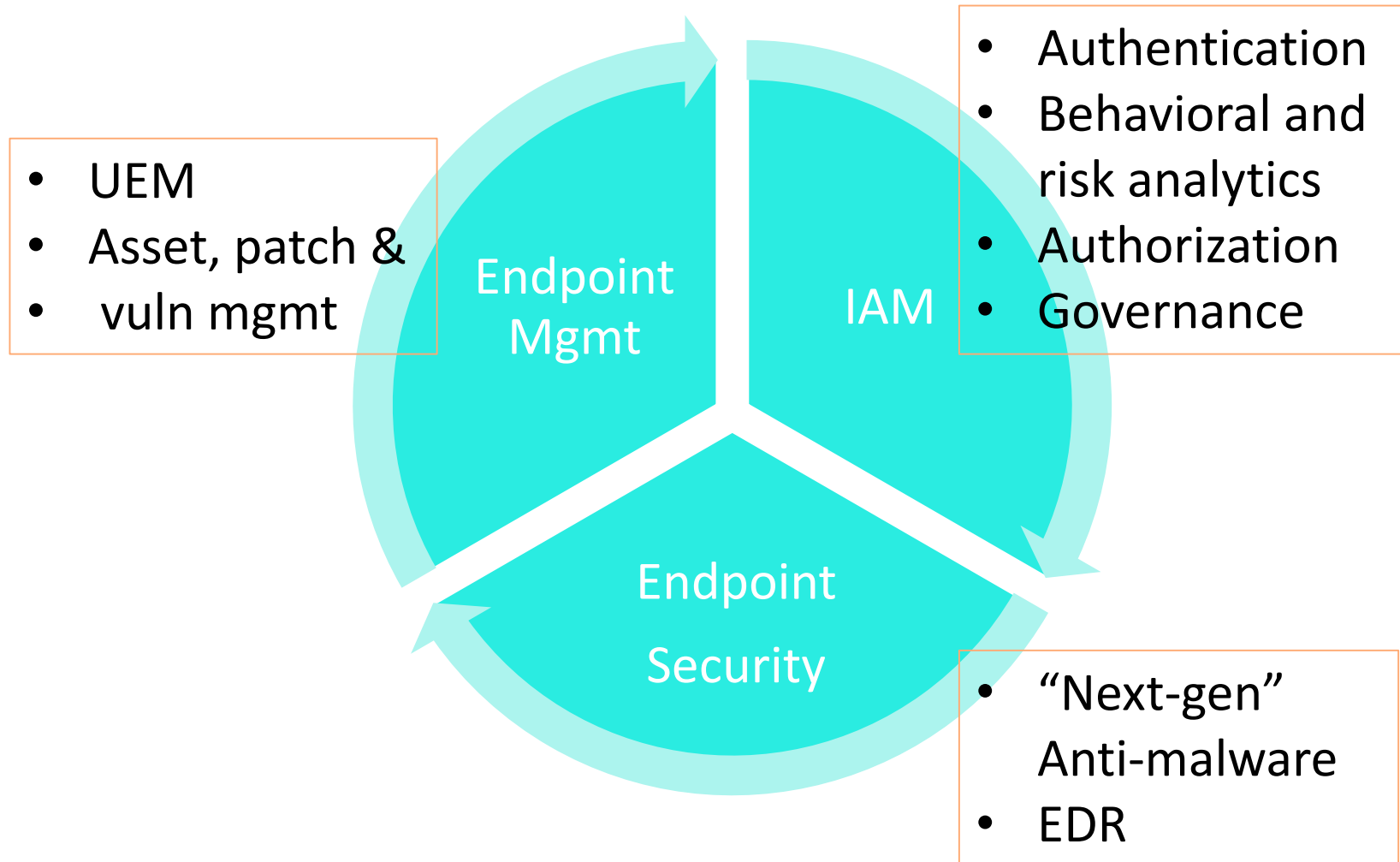
- STR-W10
- What kinds of cybersecurity events has your organization experienced?
 - A. PII theft
 - B. Corporate data theft
 - C. Ransomware /crypto-miners

<https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3838>

**What needs to be modernized in
infrastructures to deal with new
threats?**

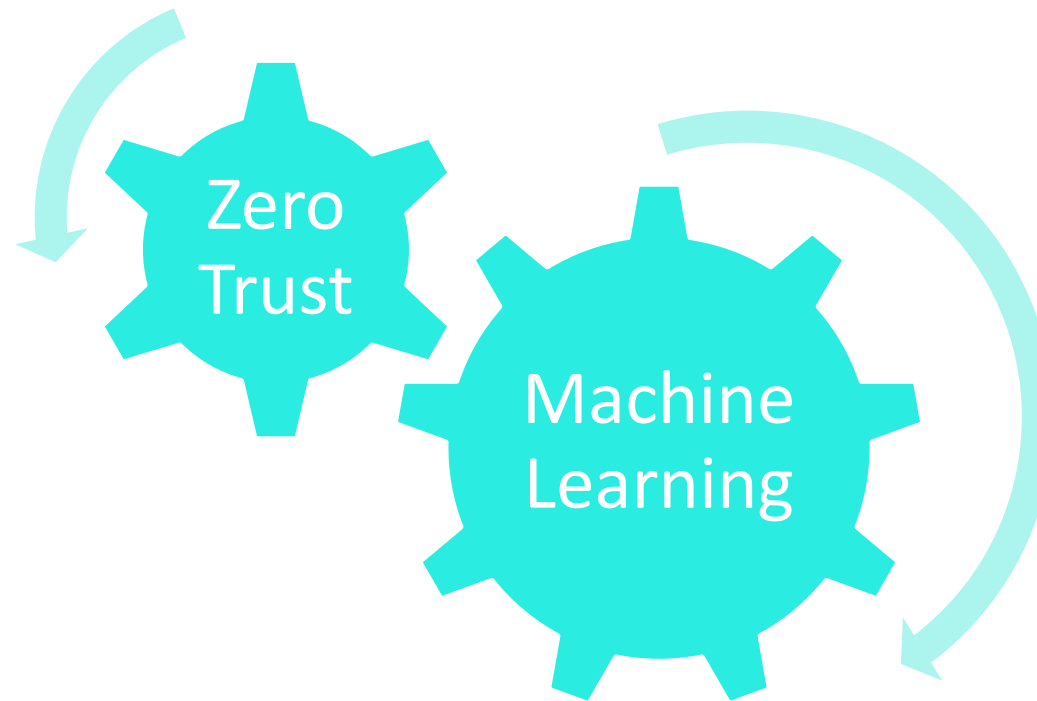


Top 3 things to modernize in your security infrastructure



How to modernize

The foundation of the
modern security
paradigm



RSA®Conference2019

Zero Trust



Zero Trust



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

What Zero Trust is (and isn't)

Is

- Concept and architectural model
- Combination of processes and technologies
- Restricted movement – greater security
- Unified experience - greater flexibility and productivity for staff and partners

Isn't

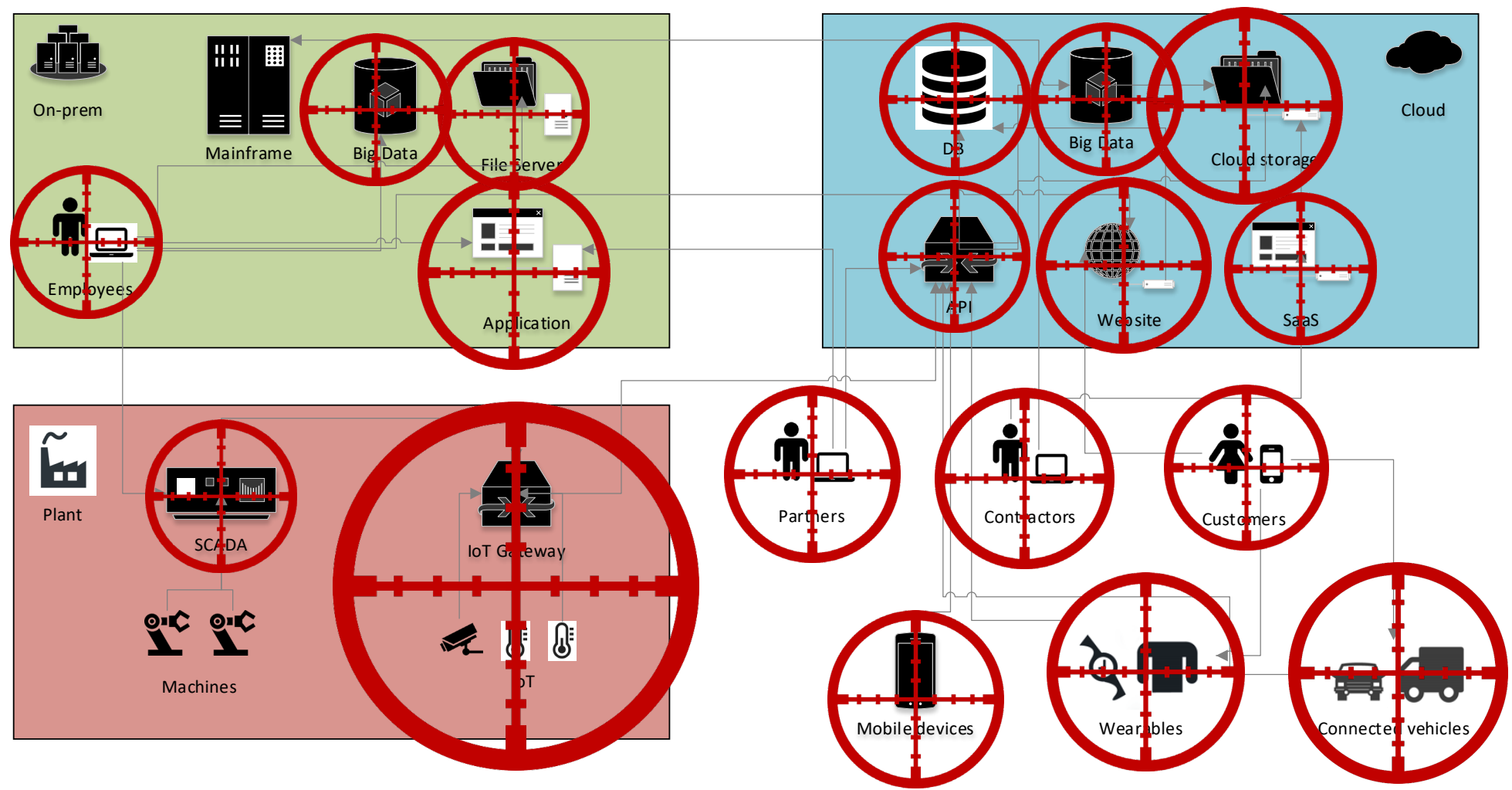
- Not about “trusting no one”
- Not a “next-generation perimeter”
- Not network segmentation
- Not a “VPN modernization”
- Not an off-the-shelf product
- Not an IT-only job



Why Zero Trust?

- Attacks come from inside and outside corporate networks
- There is no “inside” anymore anyway
- User credentials, especially passwords, are often compromised
- In the era of BYOD, devices are often not secured properly

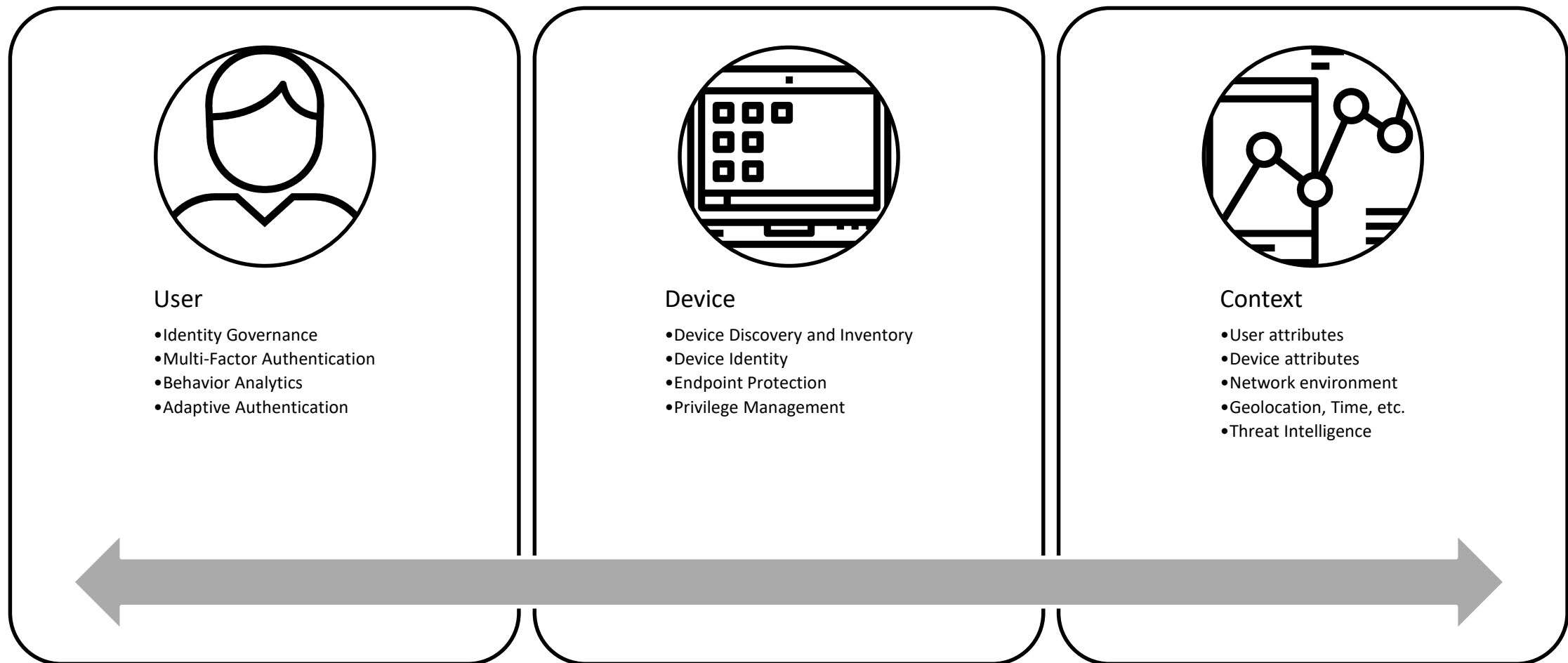
Targets



What Zero Trust means for Data

- Asset Discovery
 - You cannot protect what you don't even know exists
- Data Discovery & Classification
 - Not all data is created equal, and every organization has its own data taxonomy
- Data Flows
 - Identifying sensitive data flows between apps, users, devices is the foundation for securing them
- Data Protection
 - All sensitive data must be encrypted at rest and in transfer
- Data Security Analytics
 - Minimizing time for breach and incident response

What Zero Trust means for Identity



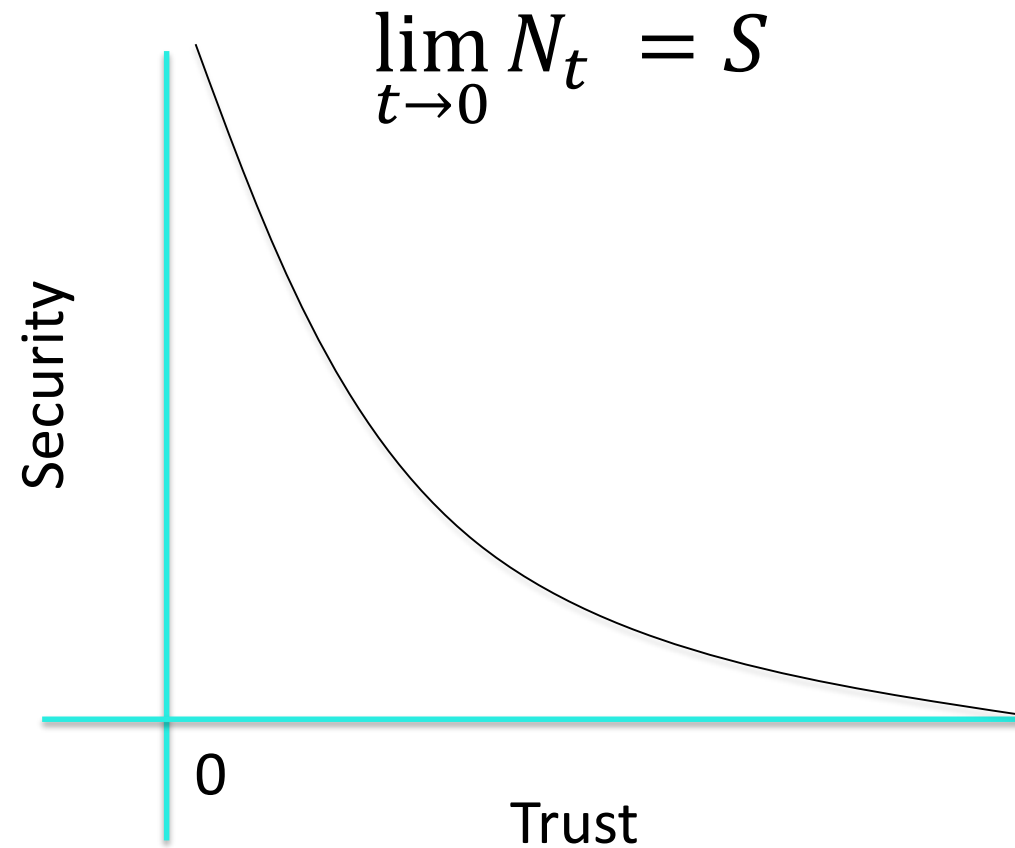
What Zero Trust means for Network

- Stop thinking in terms of “Intranet”, “DMZ”, or “VPN”
- It’s application- and user-centric, not infrastructure-centric
- No network session without authentication and authorization
- Mandatory network traffic encryption
- Monitor everything

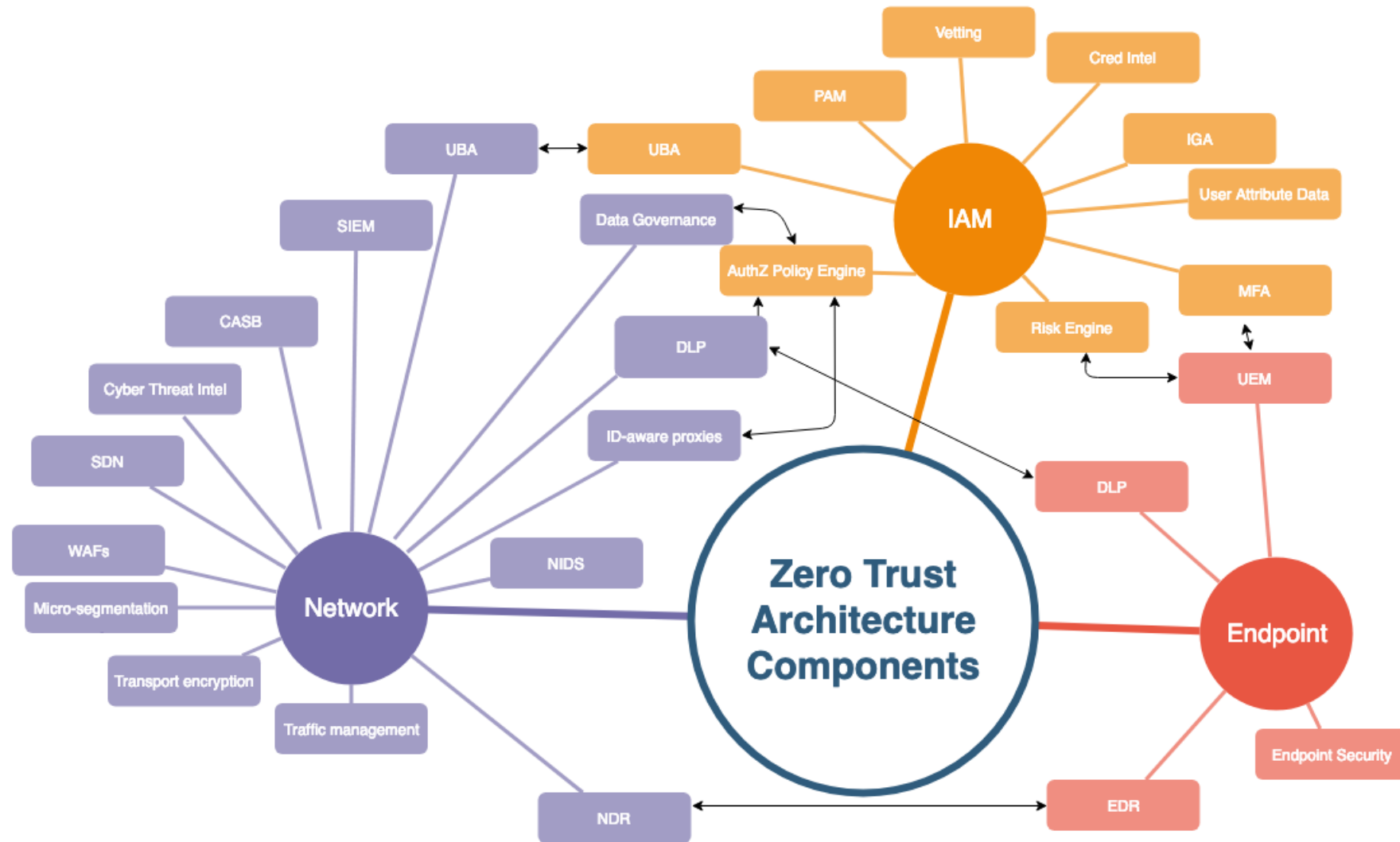
What Zero Trust means for Access Management

- Least Privilege
 - every access limited to a specific user, device, and app or resource only
 - Just enough privilege to get the job done, (if admin - revoke afterwards)
- Centralized
 - access control policies are managed centrally
 - policies are standardized across heterogeneous IT systems
 - policies are defined in uniform notation for both business and IT
- Dynamic
 - access / authorization decisions are made in real-time
 - common requirements and individual attributes influence each decision
- Adaptive
 - open to support new authentication and authorization methods
 - processing relevant intel: cyber threat, fraud, compromised credentials, etc.

Limits to Trust and Security



Zero Trust Architecture



Zero Trust Case Study # 1

- US financial services company
- Relatively weak authentication methods for online transactions: Username/password + KBA
- Externally developed mobile app built on SDK which utilized Android/iOS biometrics
- Recommendation: integrate online/mobile and use mobile push notifications for HVT authorization

Zero Trust Case Study # 2

- High-tech hardware supply chain
- Critical IP assets identified, classified, protected on-prem with MFA and ABAC.
- BU participating in joint venture copied certain critical IP assets to cloud-based collaboration service; protected only with username/password.
- Recommendation:
 - Deploy CASB, synchronize authentication and access control policies as well as data.
 - Deploy data governance and DLP to prevent users from doing an end-run around other controls.

Poll question 3

- STR-W10
- Which areas concern you most in terms of security? (choose all that apply)
 - On-premises/cloud infrastructure
 - Endpoint/mobile
 - Consumer-facing systems
- <https://rsa1-live.eventbase.com/polls?event=rsa2019&polls=3837>

RSA®Conference2019

Machine Learning Enhanced Tools



The Cyber Kill Chain®, an older but still valid approach for security tools

#RSAC

Recon	Weaponize	Deliver	Exploit	Install	C2	Actions
Prevent	Prevent	Prevent	Prevent	Prevent, Detect	Detect, Respond	Detect, Respond

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Mitre ATT&CK™ Framework

Initial Access	Execute	Persist	Escalate Privileges	Evade Defense	Get Credentials	Discover Data	Move Laterally	Collect	Exfiltrate
Prevent	Prevent, Detect	Detect, Respond	Detect, Respond	Detect, Respond	Detect, Respond	Detect, Respond	Detect, Respond	Detect, Respond	Detect, Respond

<https://attack.mitre.org/>

Detection is hard

Too many logs, FPs,
malware variants, etc. to
do it manually

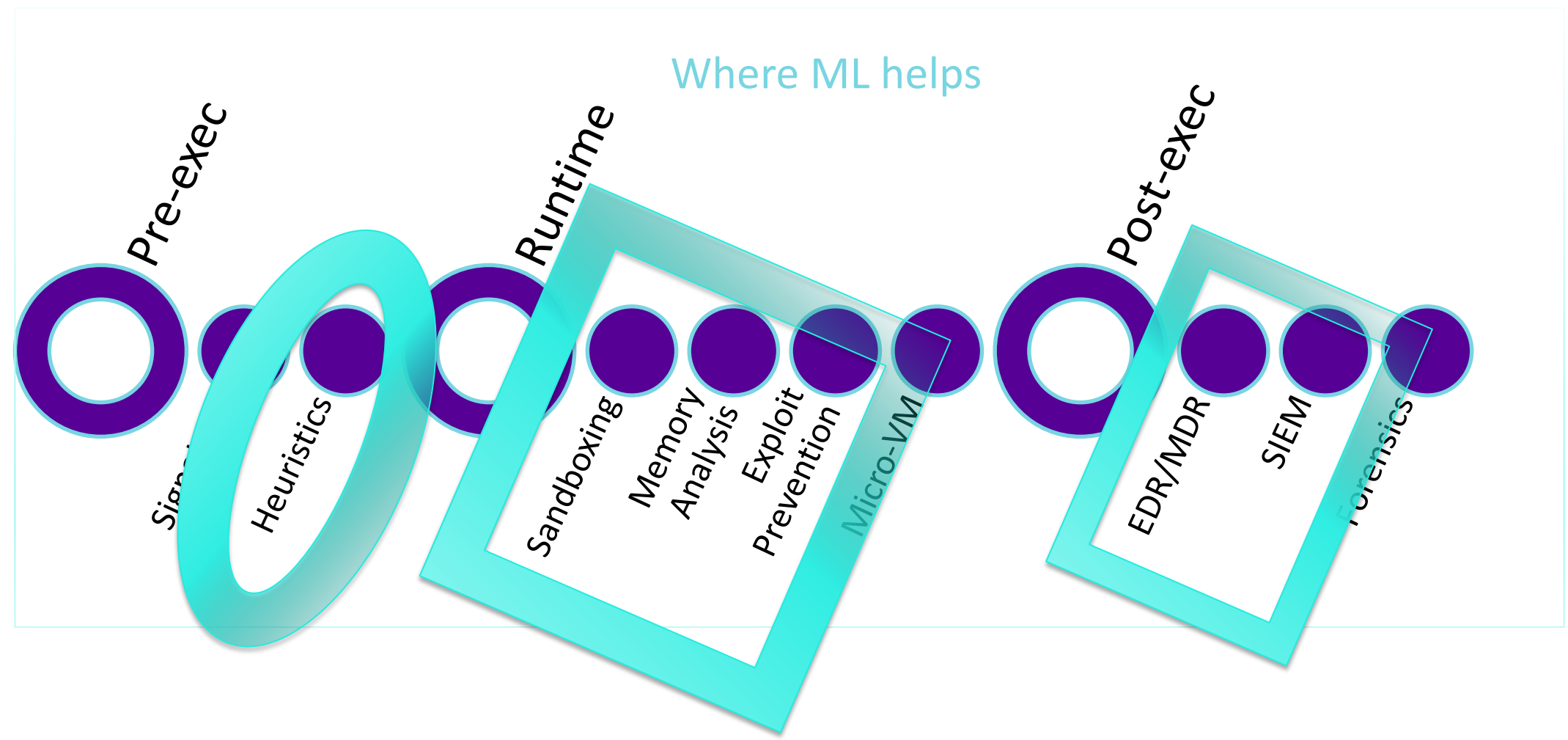


[This Photo](#) by Unknown Author is licensed
under [CC BY-NC-ND](#)


Where does ML come into play for cybersecurity and IAM?

Firewalls, WAFs, API Gateways	Analysis of traffic patterns
Anti-Malware	Millions of malware variants
Threat Hunting	Volume of data across thousands of nodes
Data Governance	Auto-classification of data objects
AuthZ & Access Control Policies	Analysis of access patterns and regulations to auto-generate rules and policies
Advanced Authentication	Evaluation of potentially large volumes of user/env data
SIEM/UBA	Efficient user access baselining and anomaly detection

Malware Detection Timeline

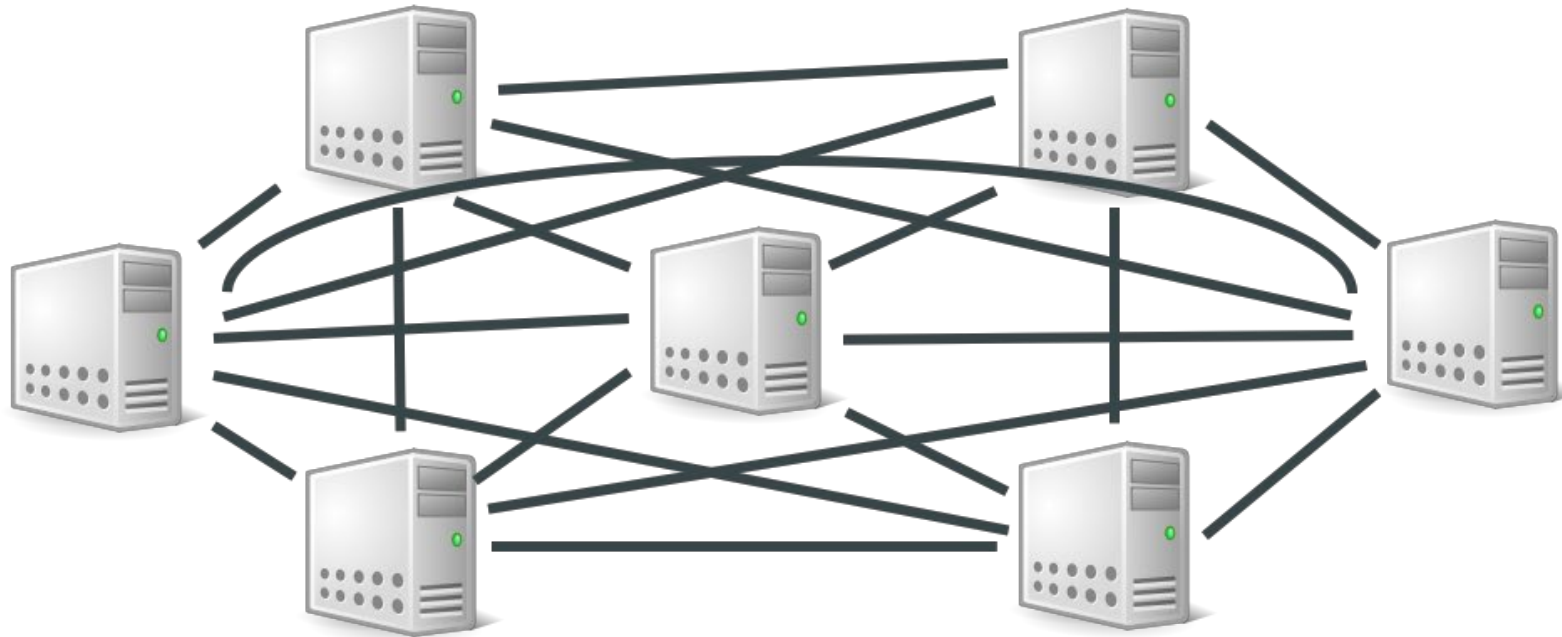


AI & ML Buzzwords explained

Artificial Intelligence (AI): Science of making computers solve tasks that usually require human intelligence				
Strong AI, General AI: Computer that has a "mind" in exactly the same sense human beings have minds 	Weak AI, Applied AI: Software focused on solving specific problems			
	AI Research: Areas of ongoing research	Cognitive Solutions: Practical Applications of AI research		
		Information Security	Self-driving vehicles	Psychological Profiling
		Postal Mail Address Detection		
		And more...		
		Cognitive Technologies		
	AI Research: Areas of ongoing research	Computer Vision	Language Processing	Knowledge Representation
		And more...		
		Machine Learning Methods		
		Pattern Recognition	Outlier Detection	Genetic Algorithms
		Deep Learning		
		And more...		
	AI Research: Areas of ongoing research	Algorithms & Methods		
		Neural Networks	Cluster Analysis	Regression Analysis
		And more...		

Not Machine Learning	
Everything only based on predefined rules	And more...
Other Algorithms & Methods	
Pattern Matching	And many more...

ML techniques can improve threat modeling

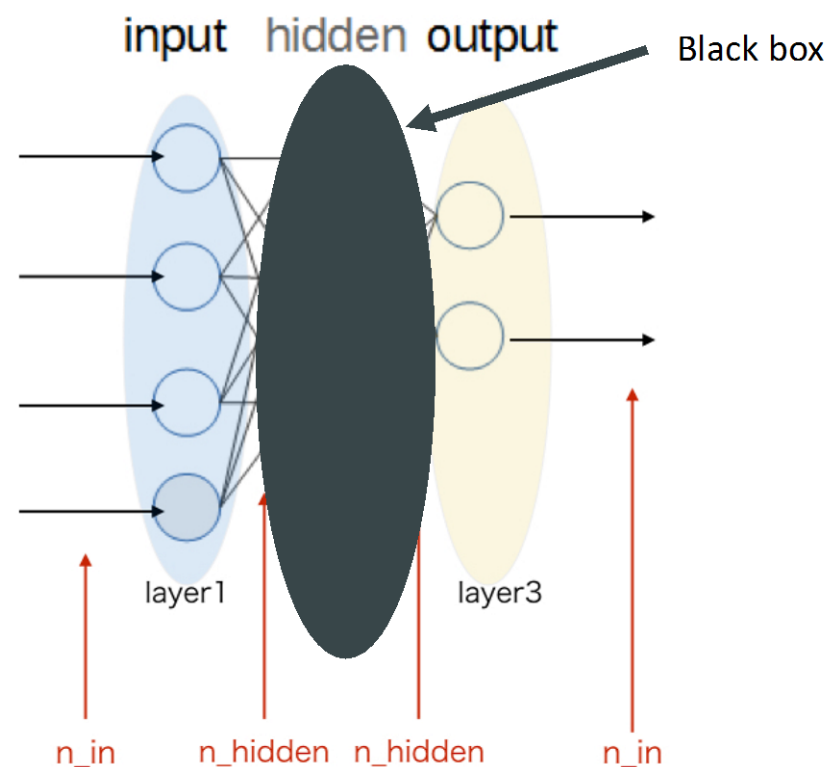


- Enumerate all nodes and details of services running
- All possible connections
- Known vulnerabilities
- Exploit probabilities
- Iterate all permutations over time

Markov chain modeling for automated intrusion detection / threat modeling and hunting

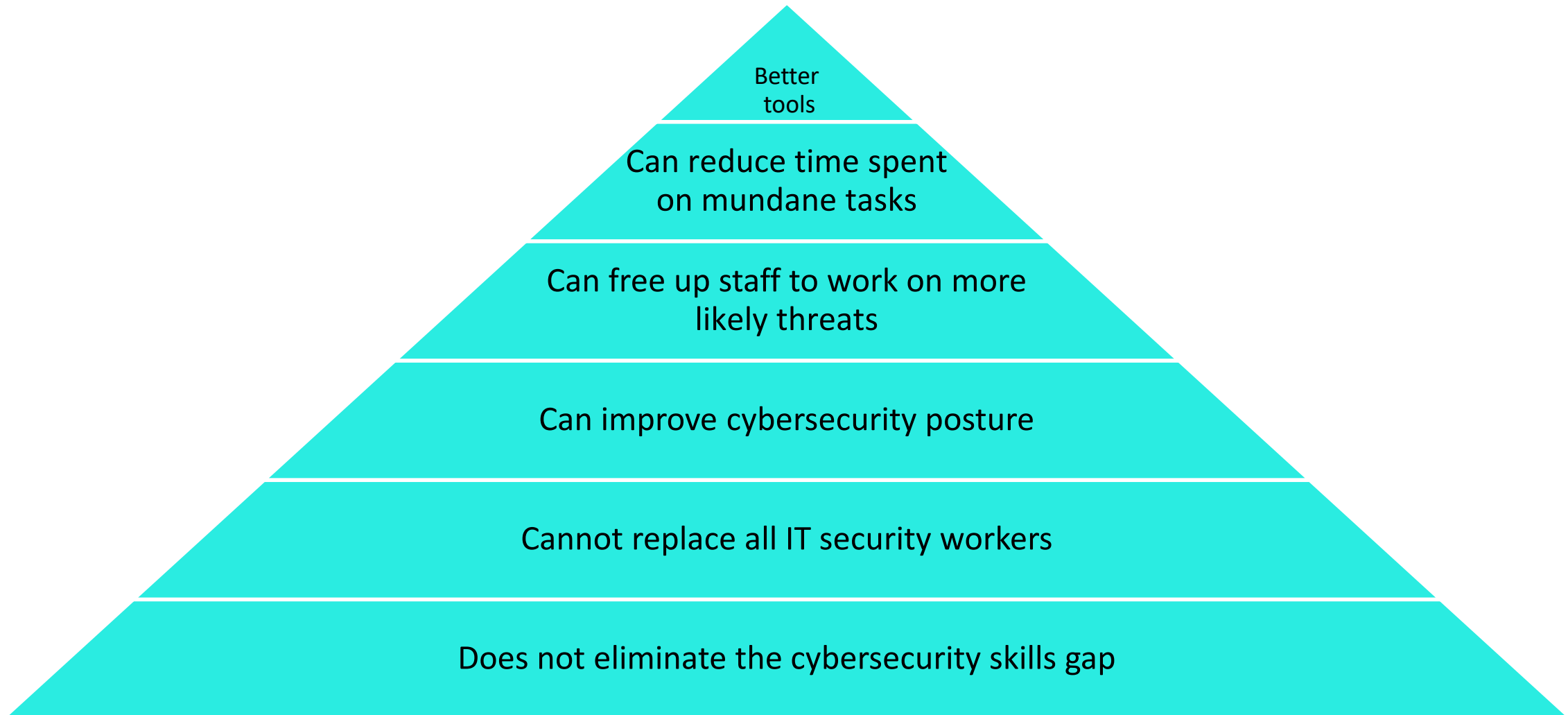
Deep Learning for rapid and automated malware analysis

```
layer1=L.Linear(n_in, n_hidden),  
layer2=L.Linear(n_hidden, n_hidden),  
layer3=L.Linear(n_hidden, n_out),
```

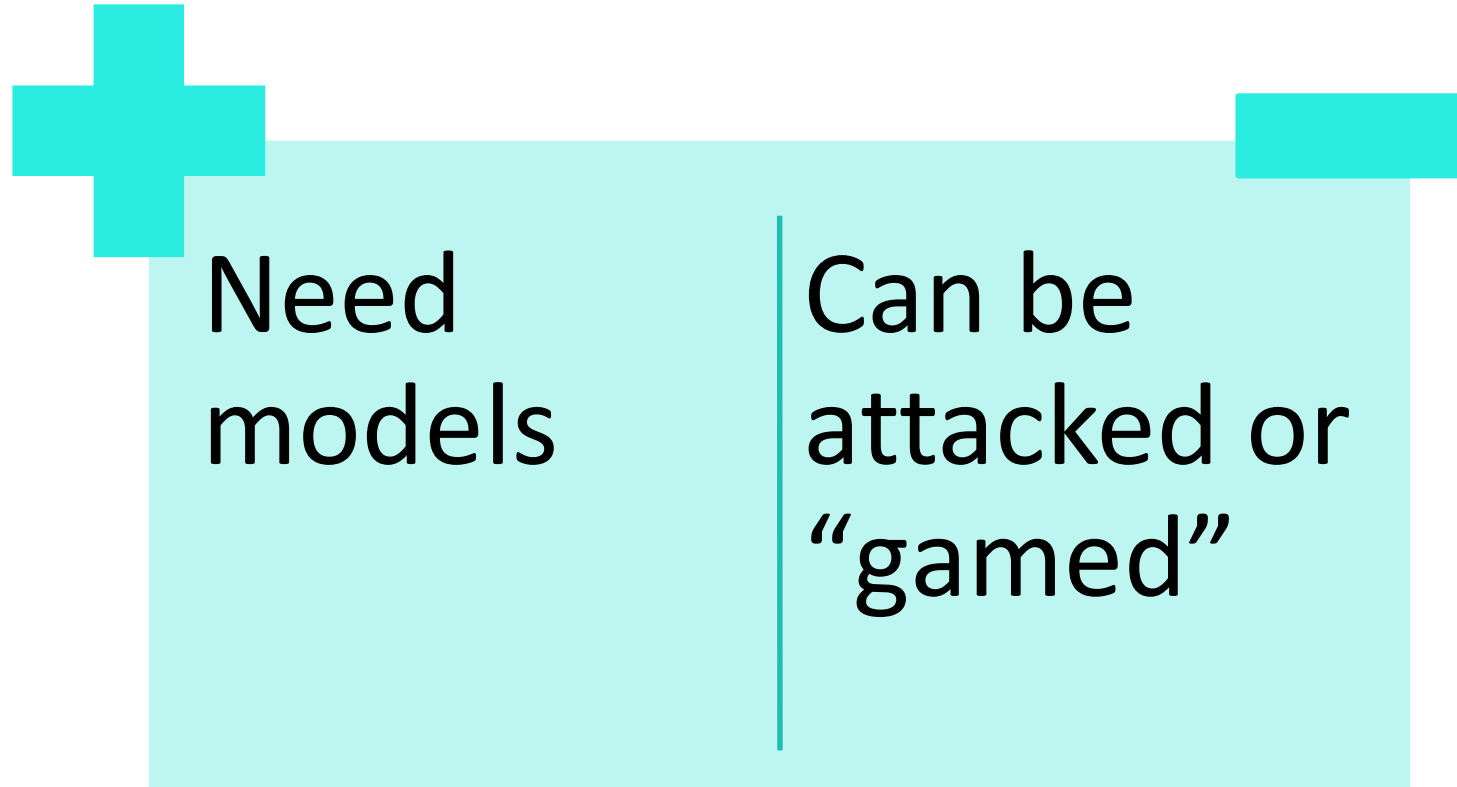


By Richmanokada - Own work, CC BY-SA 4.0,
<https://commons.wikimedia.org/w/index.php?curid=49716901>

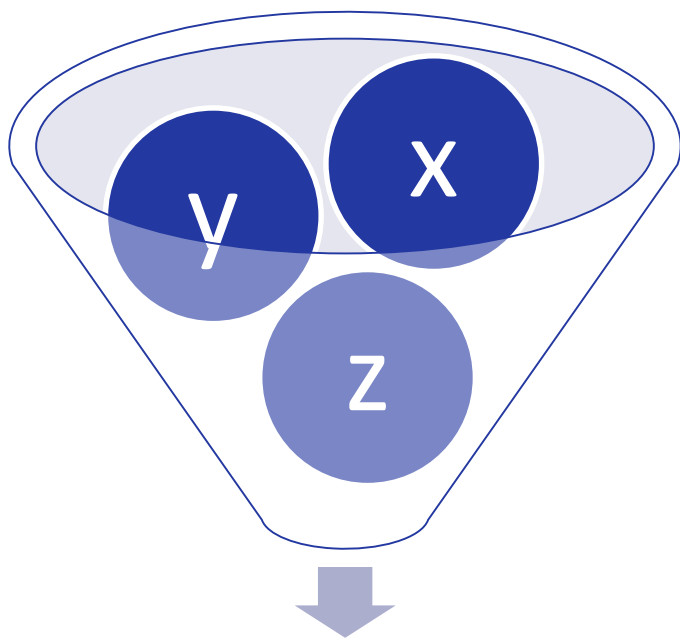
Summary: ML-enabled tools



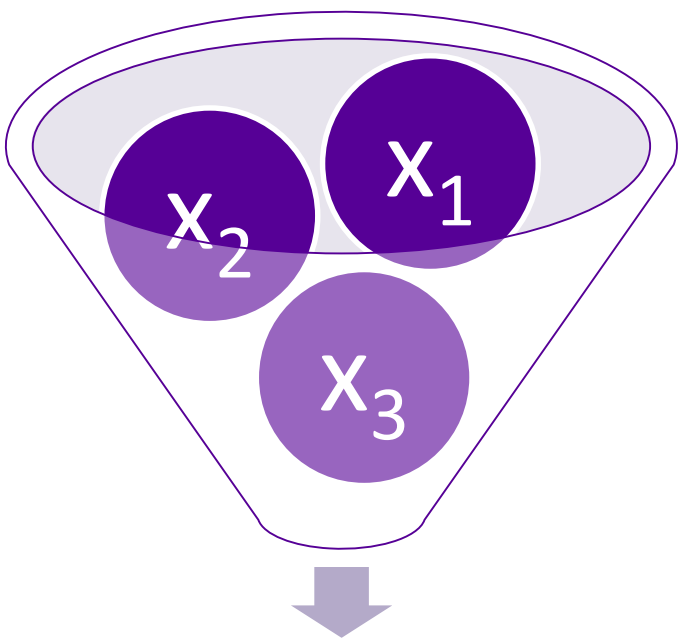
However, ML augmented tools...



Attacking ML

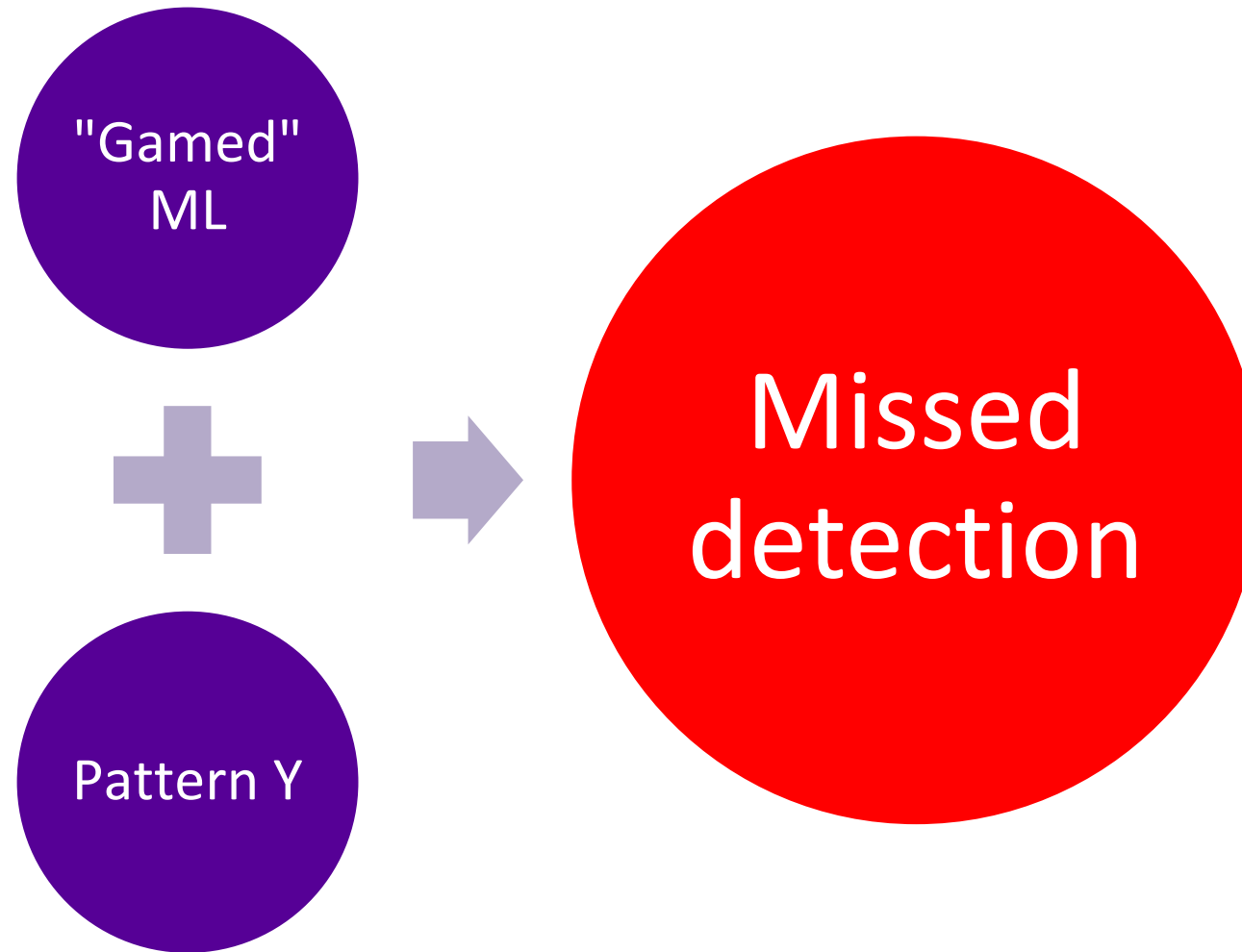


Broad detection scope

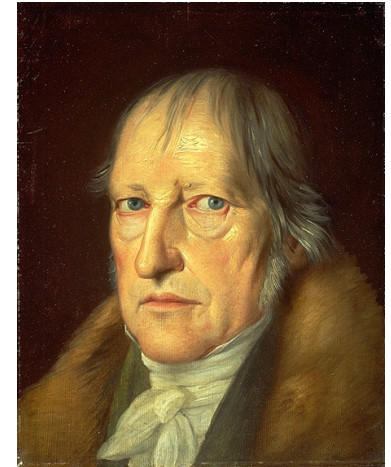
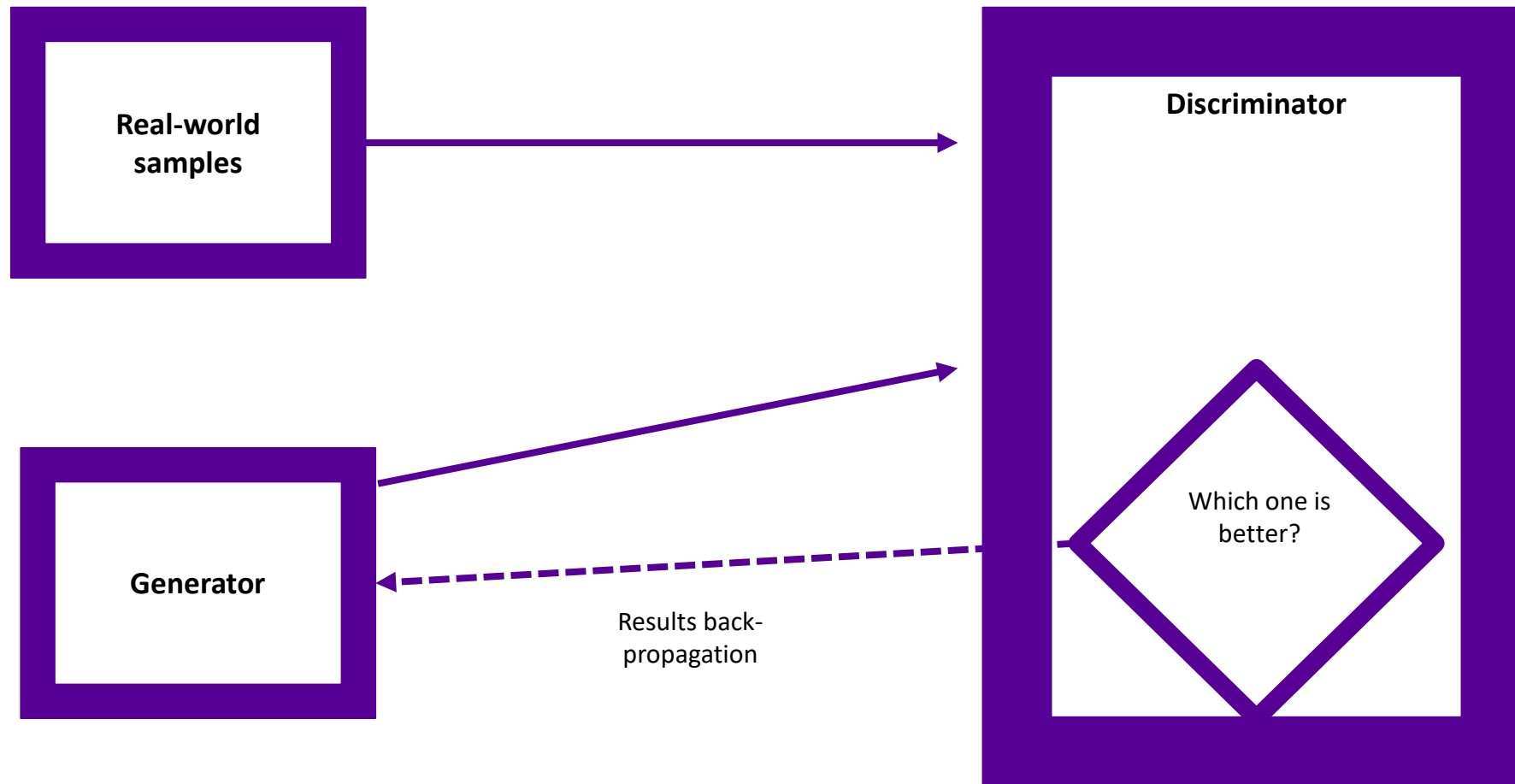


Limited detection scope

Attacking ML



Using ML for cyber attacks (GANs example)



<https://commons.wikimedia.org/w/index.php?curid=615903>

What GANs are typically used for

“Deep Fakes”



<https://commons.wikimedia.org/wiki/index.php?curid=73886038>

GAN-based cyber attack tools

Password cracking

- PassGAN

Biometric deception

- Synthetic master prints

Steganography

- SSGAN

ML-enhanced cyber tools case study

High tech manufacturer

Modern office network; “isolated” SCADA network

Missed malware detections on outdated nodes on SCADA net due to significant drop in effectiveness when agents couldn’t connect to vendor’s sandbox in the cloud

Recommendation: implement ML-enhanced endpoint agents capable of functioning autonomously / disconnected state.

Recommendations - How to apply this

- Strategic insertions or upgrades of security and identity technologies can make a positive impact, particularly those built with Zero Trust principles and/or ML augmentation
- Determine which areas you have deficiencies
- Prioritize according to risk and projected mitigation value
- Budget, plan, execute

Sample Risk-Benefit Analysis

	Technologies	Automated vulnerability scan for WebApps	Static code analysis
Metrics	Change in Risk	9	6
	Risk Mitigation Effectiveness	9	7
	Risk Mitigation Efficiency / Automation	7	5
	Types of Threats	9	3
	Cost	6	6
	Usability / Acceptance	9	8
	Performance Impact	9	10
	Interoperability / Integration	8	8
	Autonomy / Predictability	8	8



RSA[®]Conference2019

Q + A

jt@kuppingercole.com