XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva

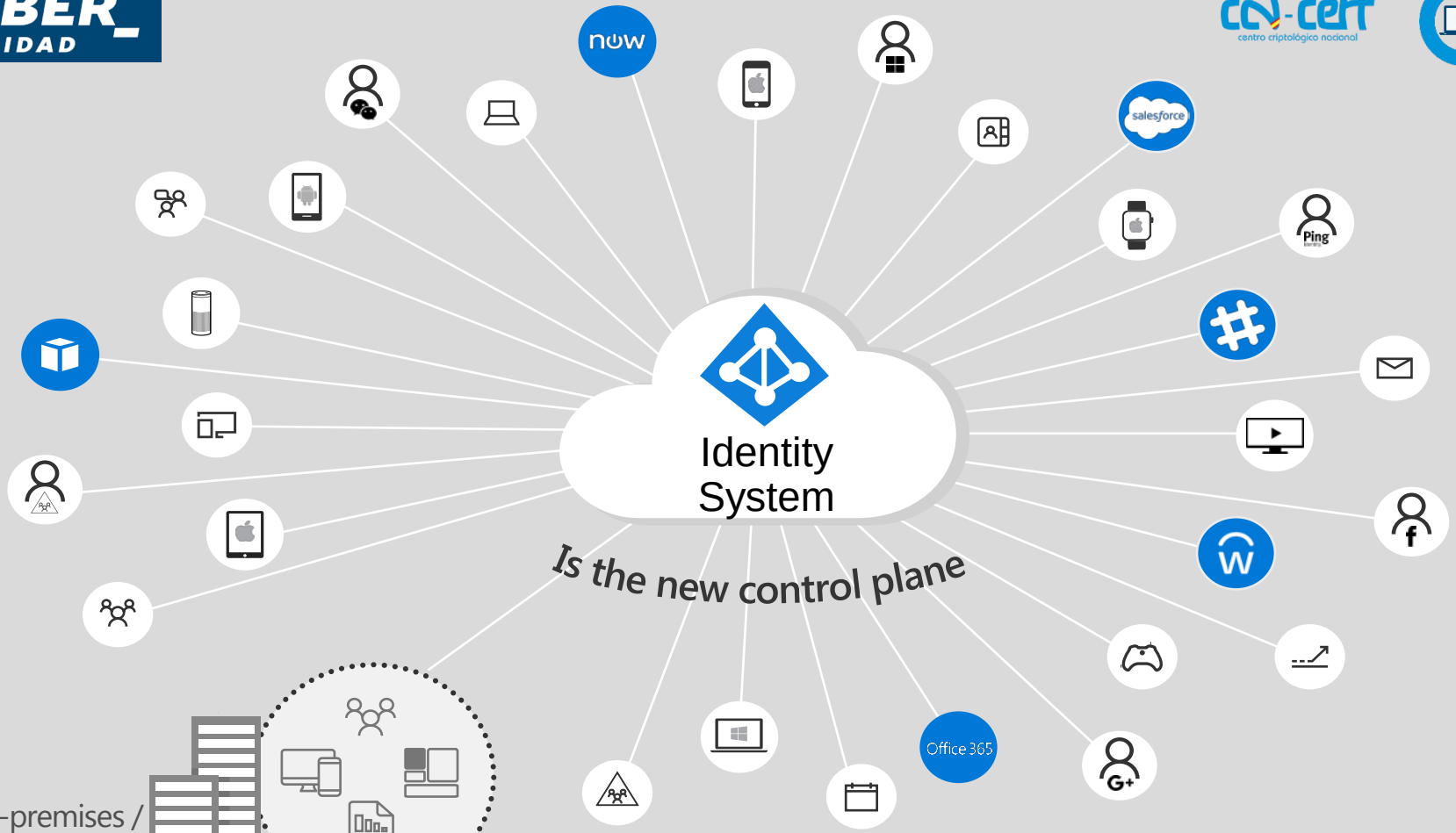
Cómo Microsoft aplica Machine Learning para la protección de cuentas de usuario en tiempo real

CCN-CERT
centro criptológico nacional

Maria Puertas Calvo
Senior Data Scientist - Microsoft
maria.puertas@microsoft.com

Sergio Medina Vallejo
Senior Consultant - Microsoft
sergio.medina@microsoft.com

On-premises / Private cloud


now
salesforce
Ping
Office 365
Identity System
Is the new control plane
On-premises / Private cloud

Microsoft Identity Systems at a Glance

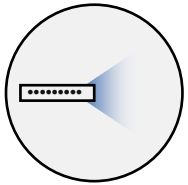
~10B MAU
Between MSA and AAD

~10B daily authentications

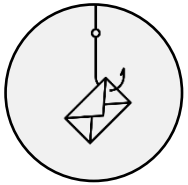
ML protection systems processes >20TB of data daily

automatically deflect 20M attacks per day

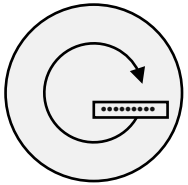
Top Attacks



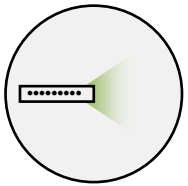
Password Spray



Phishing



Breach Replay

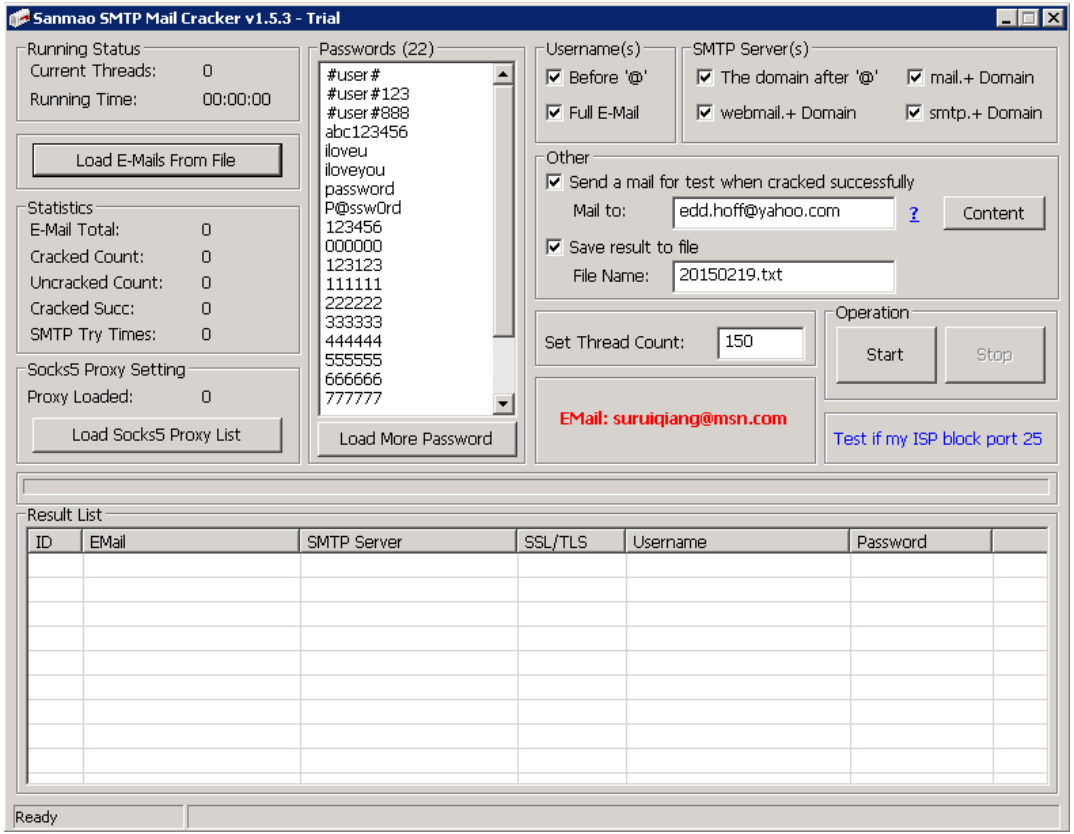


Password Spray

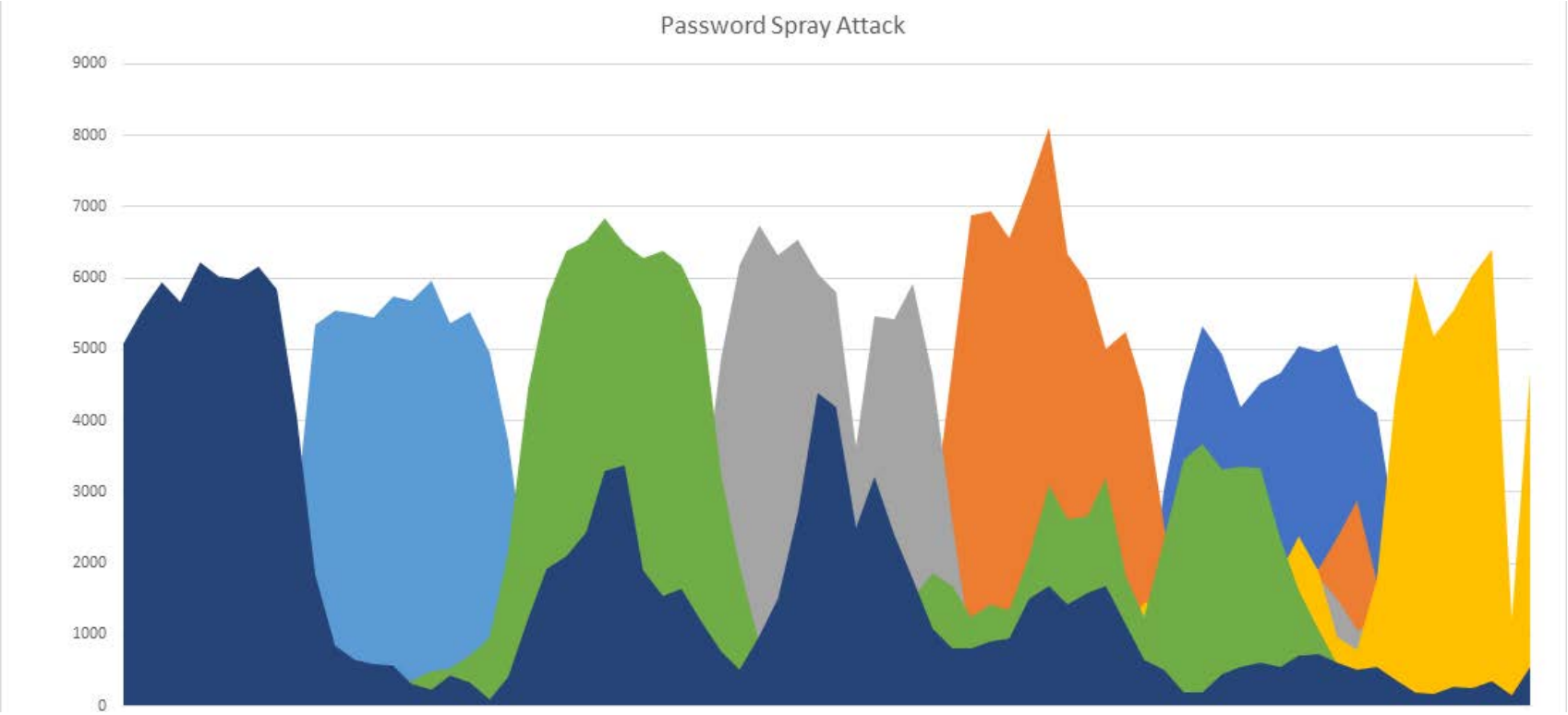
Josi@contoso.com	RedSox2018
Chance@wingtiptoys.com	RedSox2018
Rami@fabrikam.com	RedSox2018
TomH@cohowinery.com	RedSox2018
AnitaM@cohovineyard.com	RedSox2018
EitokuK@cpandl.com	RedSox2018
Ramanujan@Adatum.com	RedSox2018
Maria@Treyresearch.net	RedSox2018
LC@adverture-works.com	RedSox2018
EW@alpineskihouse.com	RedSox2018
info@blueyonderairlines.com	RedSox2018
AiliS@fourthcoffee.com	RedSox2018
MM39@litwareinc.com	RedSox2018
Margie@margiestravel.com	RedSox2018
Ling-Pi997@proseware.com	RedSox2018
PabloP@fineartschool.net	RedSox2018

Password Spray

- One common password used against many, many accounts.
- Below account lockout threshold
- After successful login, dump the GAL.
- Start pivoting in environment.



Password Spray Attack Instances



Phishing

Evolving Threat Landscape | Phishing

$12B

BEC attributed loss since 2013

5B

Phish mails blocked in Office 365 in 2018

300K

Phish Campaigns analyzed in 2018

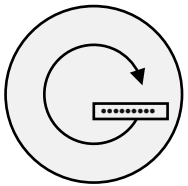
20% in 5 mins

Clicks in first 5 mins

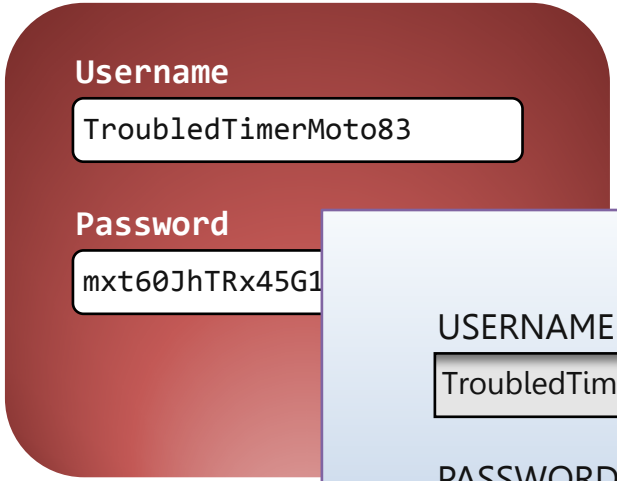
8M

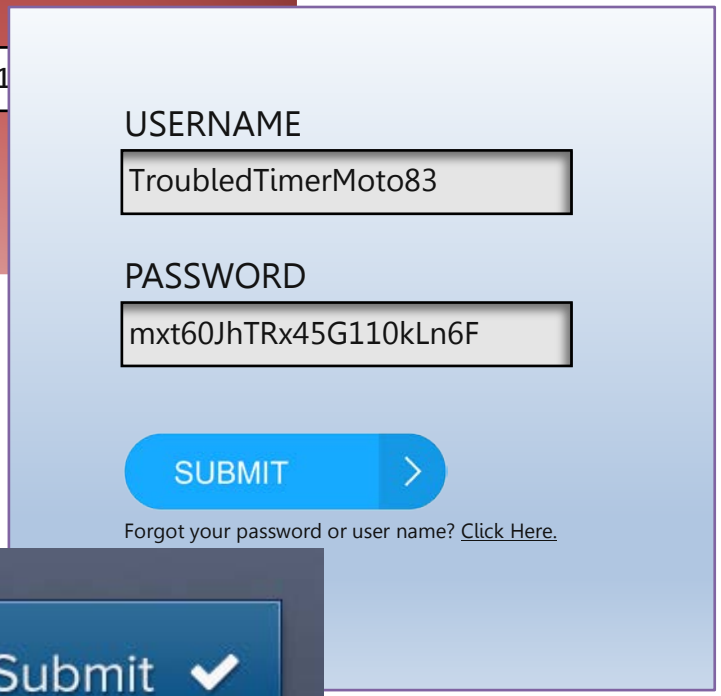
Suspicious BEC attempts in 2018

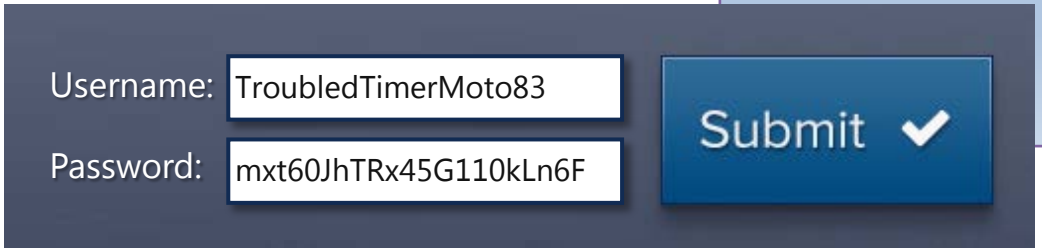
Polymorphic Parallel Attacks | Short Span Attacks | Serial Variant Attacks | Shared Cloud/SaaS Infrastructure



Breach replay







15,000 government em

thehill.com/policy/cybersecurity/251431-ashley-madison-leak-appears-real-includes-thousands-of-government-emails

News Policy Opinion Events Jobs HILL.TV

THE HILL

15,000 government emails revealed in Ashley Madison leak

BY CORY BENNETT - 08/19/15 09:55 AM EDT

525 COMMENTS

6,290 SHARES

SHARE TWEET PLUS ONE

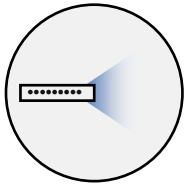
Just In...

Jimmy Fallon responds to Trump: I'll donate to pro-immigrant nonprofit in his name
IN THE KNOW — 44M 47S AGO

South Carolina GOP candidate expected to make full recovery after car accident
CAMPAIGN — 1H 3M AGO

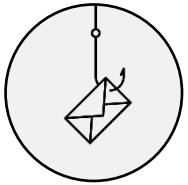
Melania Trump tells kids to embrace kindness,

Attack Impact



Password Spray

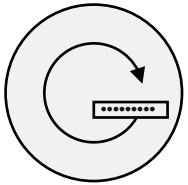
200,000 accounts compromised in Aug 2018



Phishing

5B emails blocked in 2018

44M risk events in Aug 2018



Breach Replay

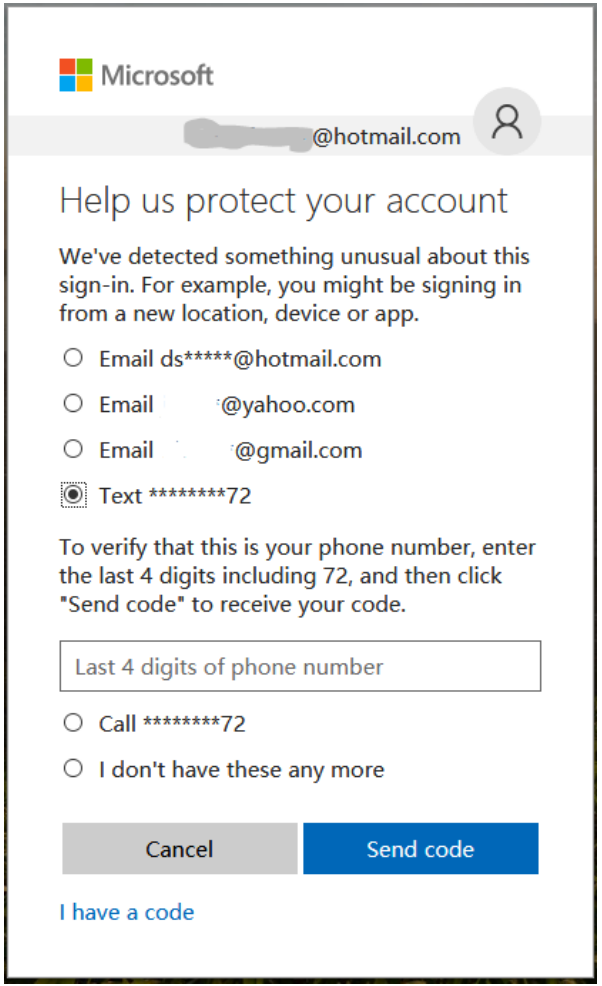
650,000 accounts with leaked credentials in 2018

Real time machine learning risk detection

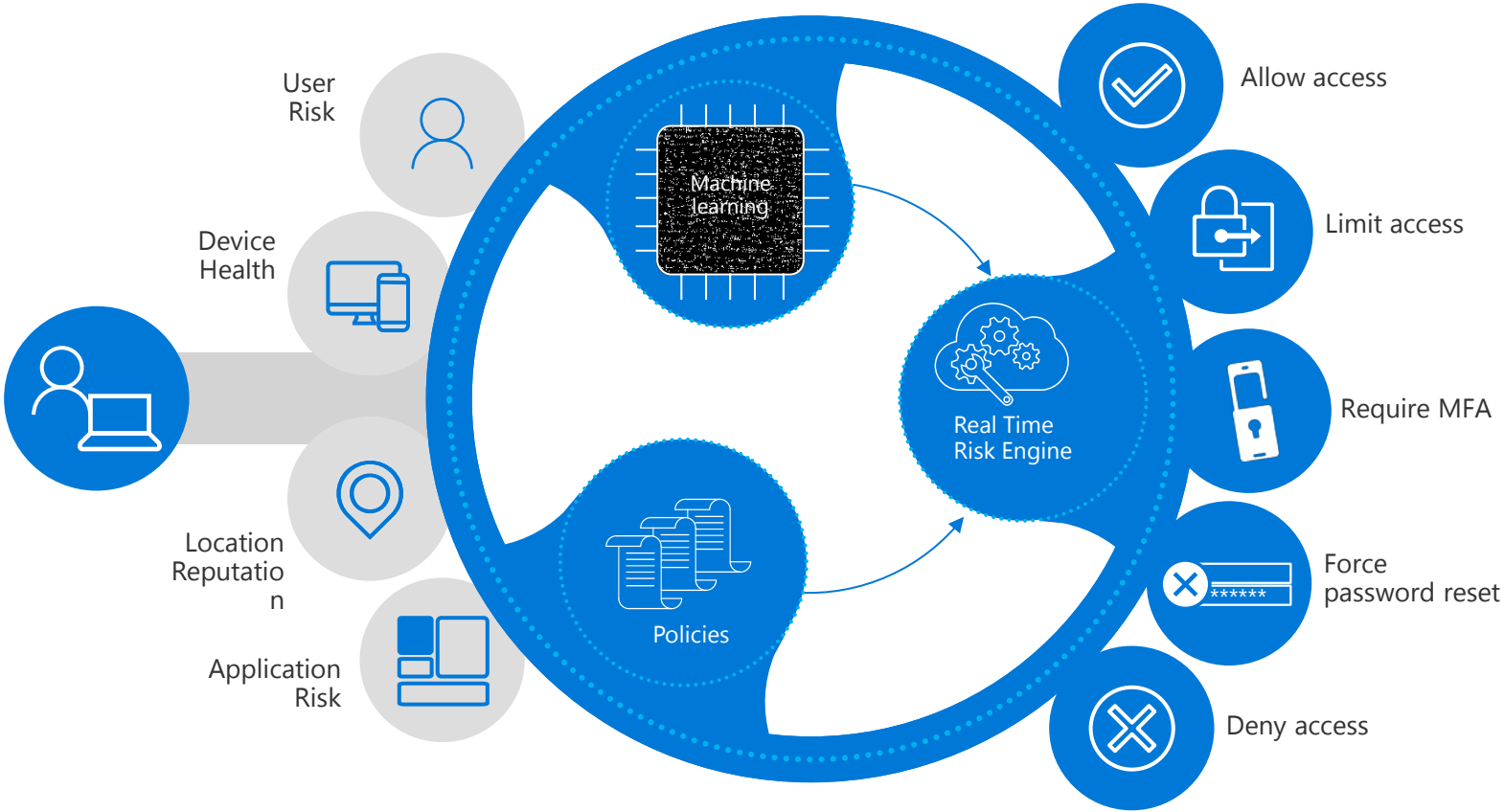
Risk based MFA stops

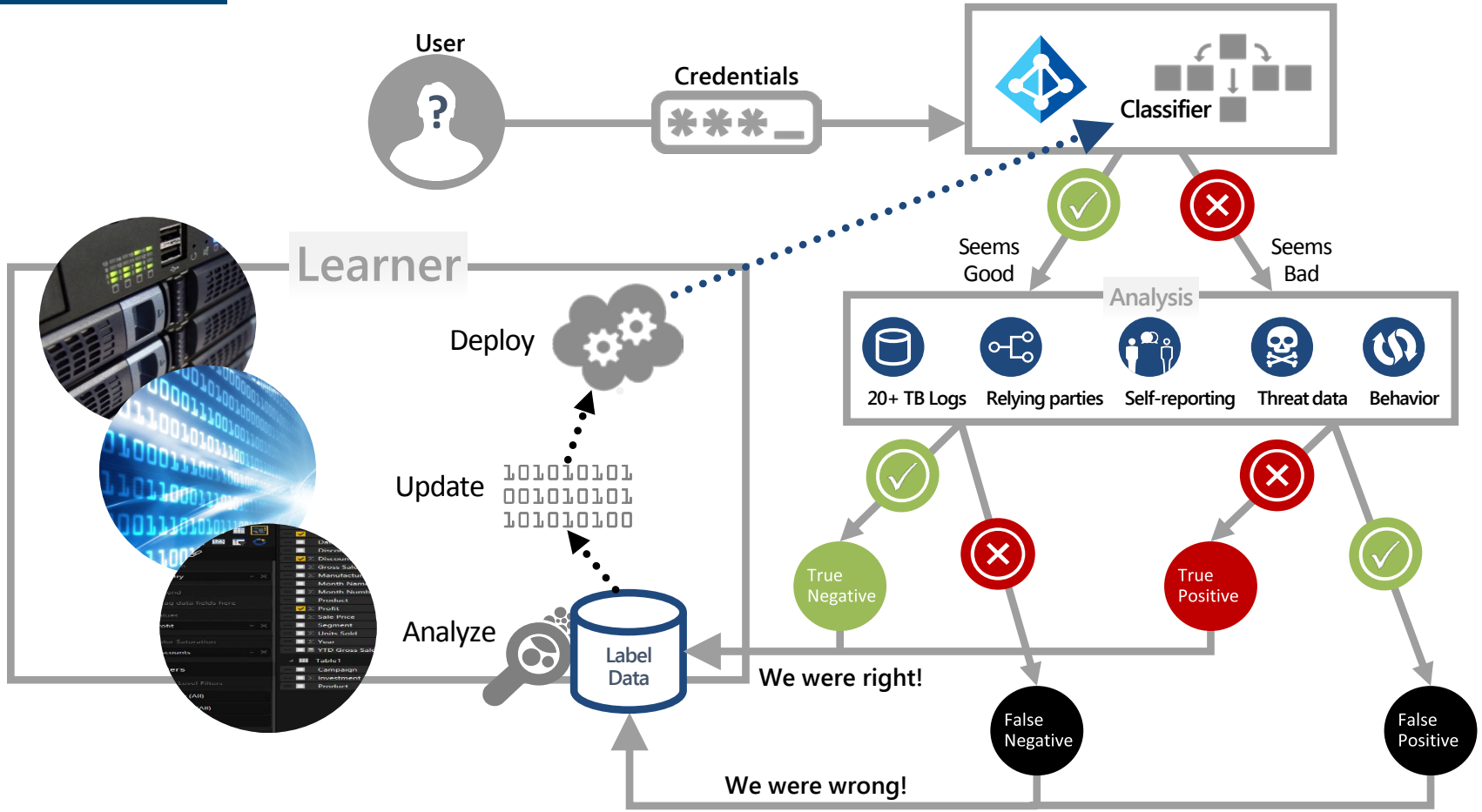
95% of attacks

with correct password



Maximize security. Maximize Productivity.

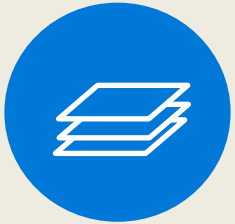



User
Credentials
Classifier
Learner
Seems Good
Seems Bad
Analysis
20+ TB Logs
Relying parties
Self-reporting
Threat data
Behavior
Deploy
Update
Analyze
Label Data
True Negative
True Positive
We were right!
False Negative
False Positive
We were wrong!

BE A DOMAIN EXPERT

Know your data

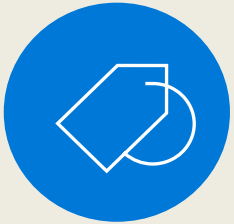
Build smart features



BUILD DEFENSE IN LAYERS

Start simple

Build ML on top



INVEST IN LABELS

User generated

Heuristic auto generated

First/third party inputs

KNOW THE NUMBERS

Measure detection performance

Measure attack volume

Be a domain expert

Understand your data. Know good vs bad when you see it.

Date	Time	User	Session	Device	Application	IP Address	Country
3-Mar	10:05	Alice	1	iPhone 8	Exhange	1.2.3.4	US
3-Mar	15:07	Alice	2	iPhone 8	Exchange	1.2.3.5	US
3-Mar	16:45	Alice	3	Windows 10	Salesforce	2.2.2.1	US
4-Mar	10:23	Alice	4	Windows 10	Salesforce	2.2.2.1	US
4-Mar	2:04	Alice	5	Linux	Sharepoint	13.22.12.12	RU
5-Mar	11:30	Alice	6	iPhone 8	Exhange	1.2.3.4	US

We have never seen Alice log in from Russia

There are 132 other users from different tenants using this IP address

Alice doesn't normally log in at 2 AM

This is not a familiar device for Alice

Alice doesn't normally use SharePoint

Be a domain expert

Understand your data. Know good vs bad when you see it.

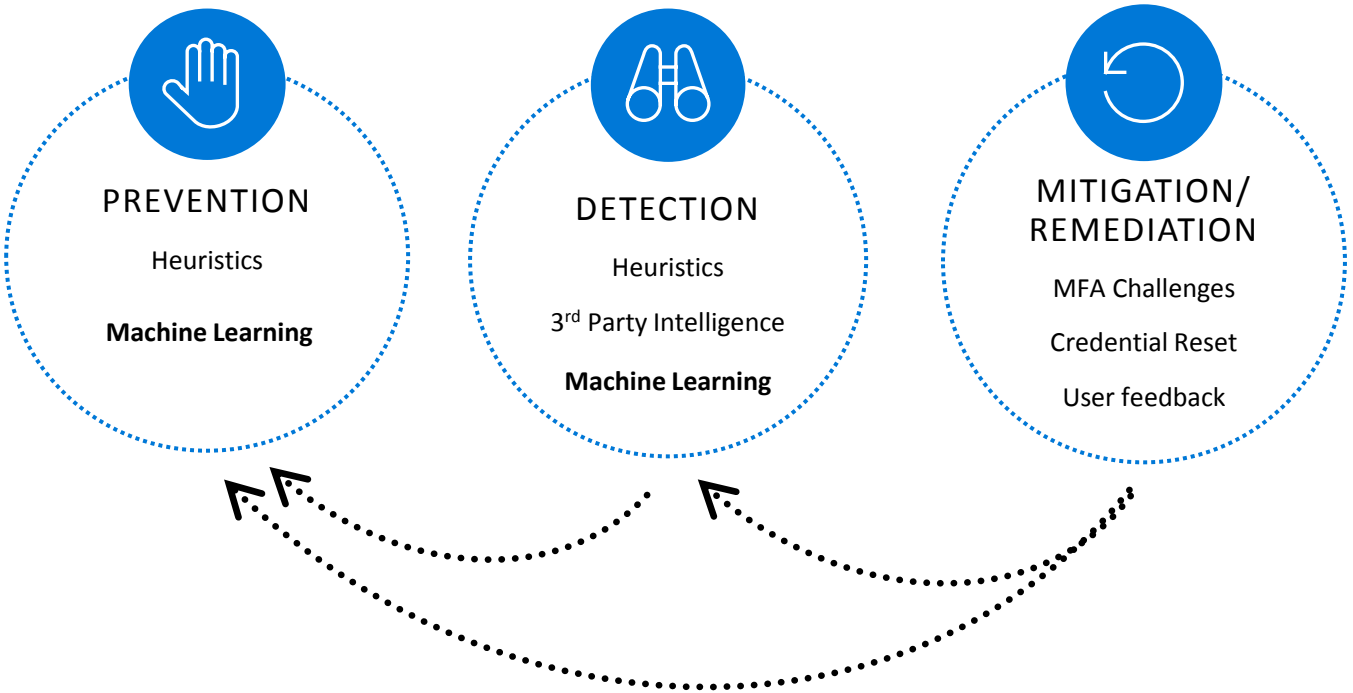
Date	Tim	User	Session	Device	Application	IP Address	Country
3-Mar	10:05	Alice	1	iPhone 8	Exhange	1.2.3.4	US
3-Mar	15:07	Alice	2	iPhone 8	Exchange	1.2.3.5	US
3-Mar	16:45	Alice	3	Windows 10	Salesforce	2.2.2.1	US
4-Mar	10:23	Alice	4	Windows 10	Salesforce	2.2.2.1	US
4-Mar	2:04	Alice	5	Linux	Sharepoint	13.22.12.12	RU
5-Mar	11:30	Alice	6	iPhone 8	Exhange	1.2.3.4	US

Feature Engineering

IsNormalTimeOfDay	IsFamiliarDevice	IsFamiliarApp	IsFamiliarIP	IsFamiliarCountry	IPRiskScore	UserRiskScore	DeviceHealth
FALSE	FALSE	FALSE	FALSE	FALSE	0.2	0	unknown

Build defense in layers

Start with the easy things. Build the ML on top.



Invest in labels.

Labels tell your ML what to look for. Get there wherever you can.

Train supervised ML models

Measure model quality

End user generated

- Build feedback loops
- End users/admins/secops
- Remove errors

Expert generated

- Security researchers
- Customer support
- Dedicated labelers

Autogenerated

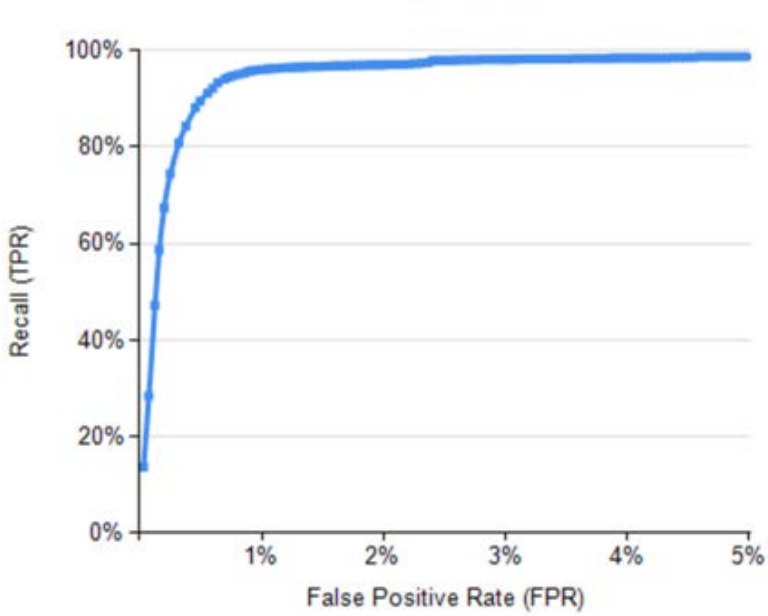
- High quality heuristic based detections
- Detections from other first parties

Know your numbers

So you know where you need to invest

Measure the performance of all detections:

- Precision
- Recall



“What % of attacks can I stop with this amount of user friction?”

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectiva

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional