DISRUPTING CREDENTIAL-BASED ATTACKS

SLAIT Consulting

MARYLAND EDUCATION MEEC ENTERPRISE CONSORTIUM

paloalto NETWORKS®

STATE OF CREDENTIAL PHISHING

63%

of breaches use stolen credentials*

90%

phishing success rate with just 10 emails**

1m40s

average time until the first response*

3%

of victims contacted security*

*Sources: * Verizon 2016 Data Breach Investigation Report; **Verizon 2015 Data Breach Investigation Report; *** Vanson Bourne/Cloudmark Survey 2016*

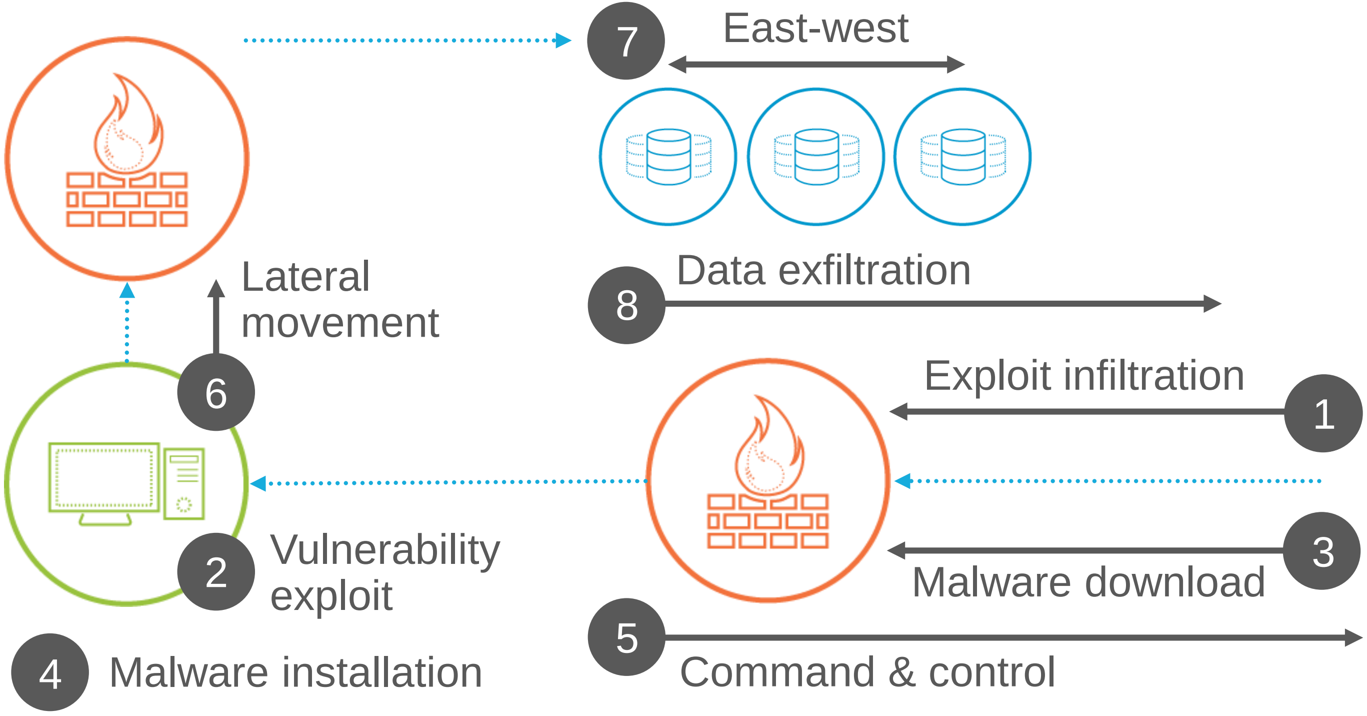
Observed Targeted Staff

44%	IT Staff
43%	Finance Staff
27%	CEO
17%	CFO

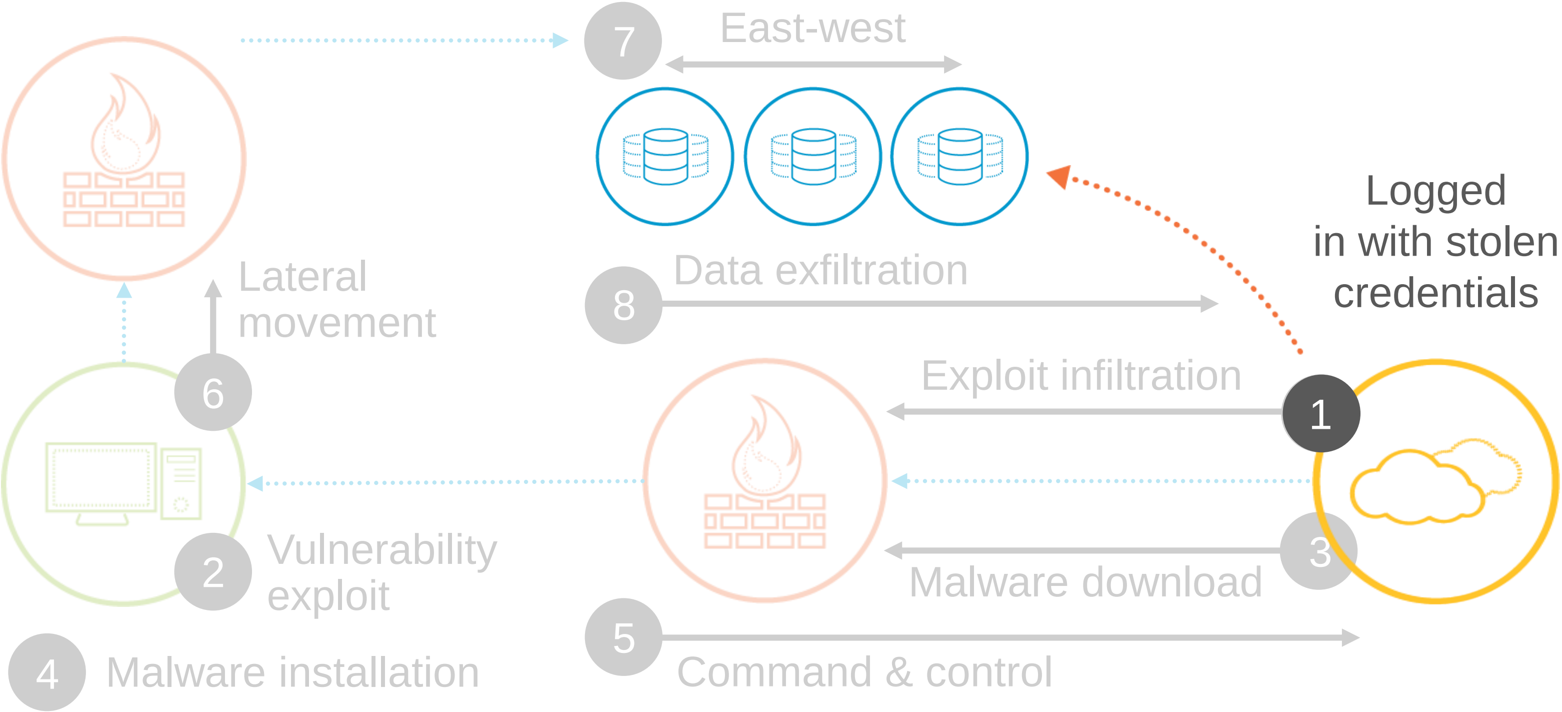
Observed delivery mechanisms ***

90%	Email
48%	Mobile
40%	Social Media

CREDENTIAL PHISHING IS EASIER THAN ZERO DAY EXPLOITATION



CREDENTIAL PHISHING IS EASIER THAN ZERO DAY EXPLOITATION



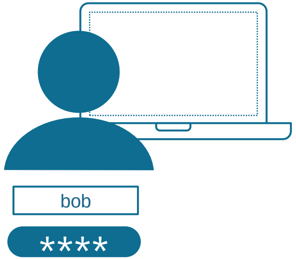
STATE OF CREDENTIAL PHISHING

IF WE COULD COLLECTIVELY ACCEPT A SUITABLE REPLACEMENT, IT WOULD'VE FORCED ABOUT 80% OF THESE ATTACKS TO ADAPT OR DIE.

Verizon DBIR on the role of passwords in breaches

* Verizon 2016 Data Breach Investigation Report; **Verizon 2015 Data Breach Investigation Report

WHY ARE PASSWORDS STILL A PROBLEM?

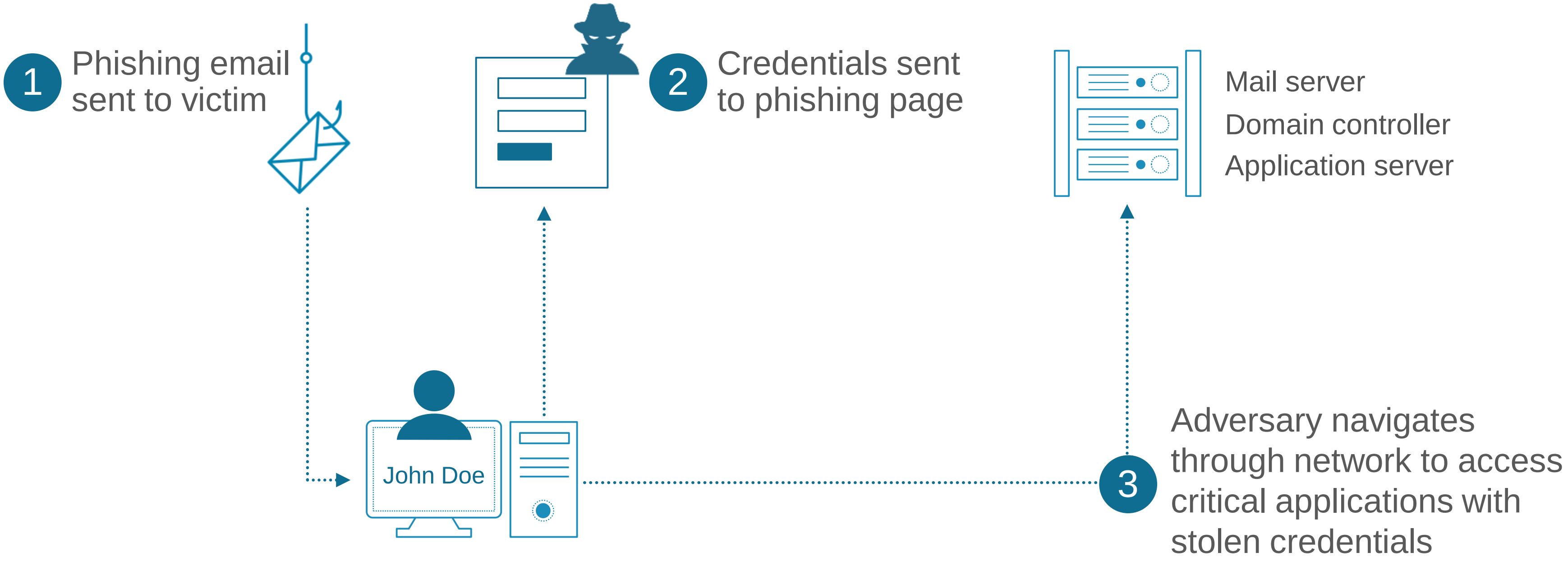


Passwords provide weak security

Credential phishing is rampant

Multi-Factor Auth is difficult

ANATOMY OF A CREDENTIAL THEFT-BASED ATTACK



1 Phishing email sent to victim

2 Credentials sent to phishing page

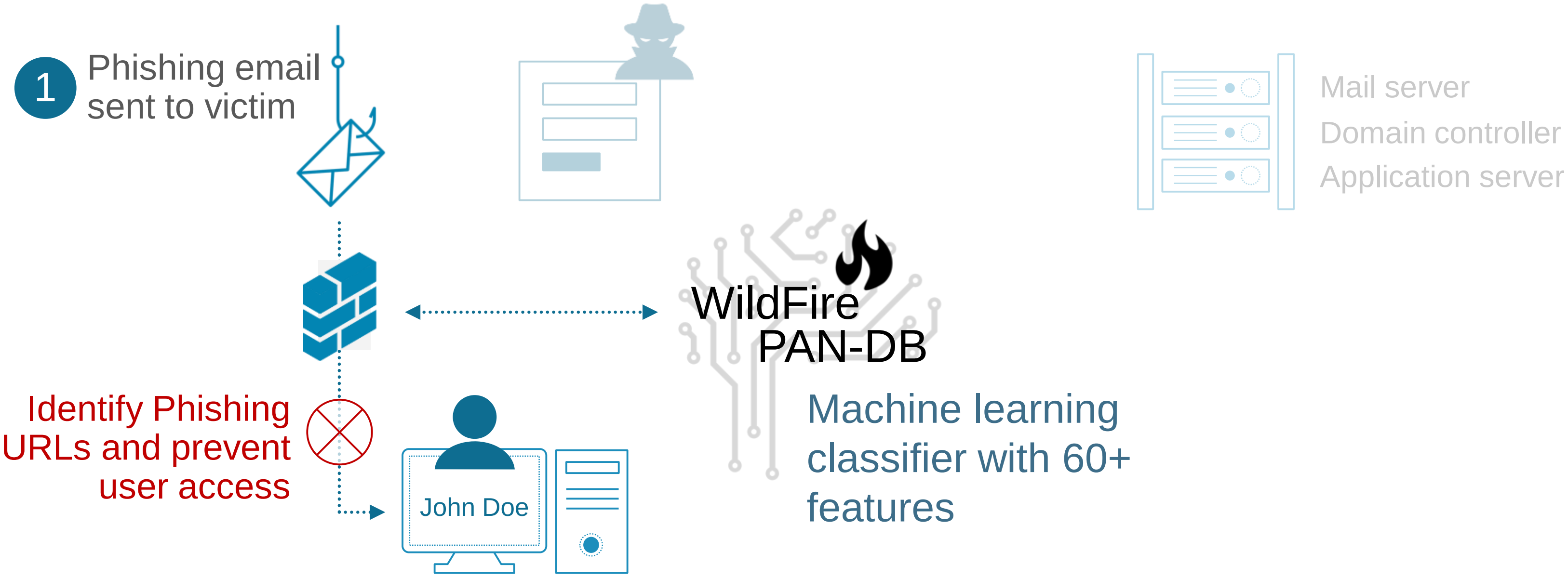
Mail server

Domain controller

Application server

3 Adversary navigates through network to access critical applications with stolen credentials

IDENTIFY AND BLOCK THE PHISHING PAGE



1 Phishing email sent to victim

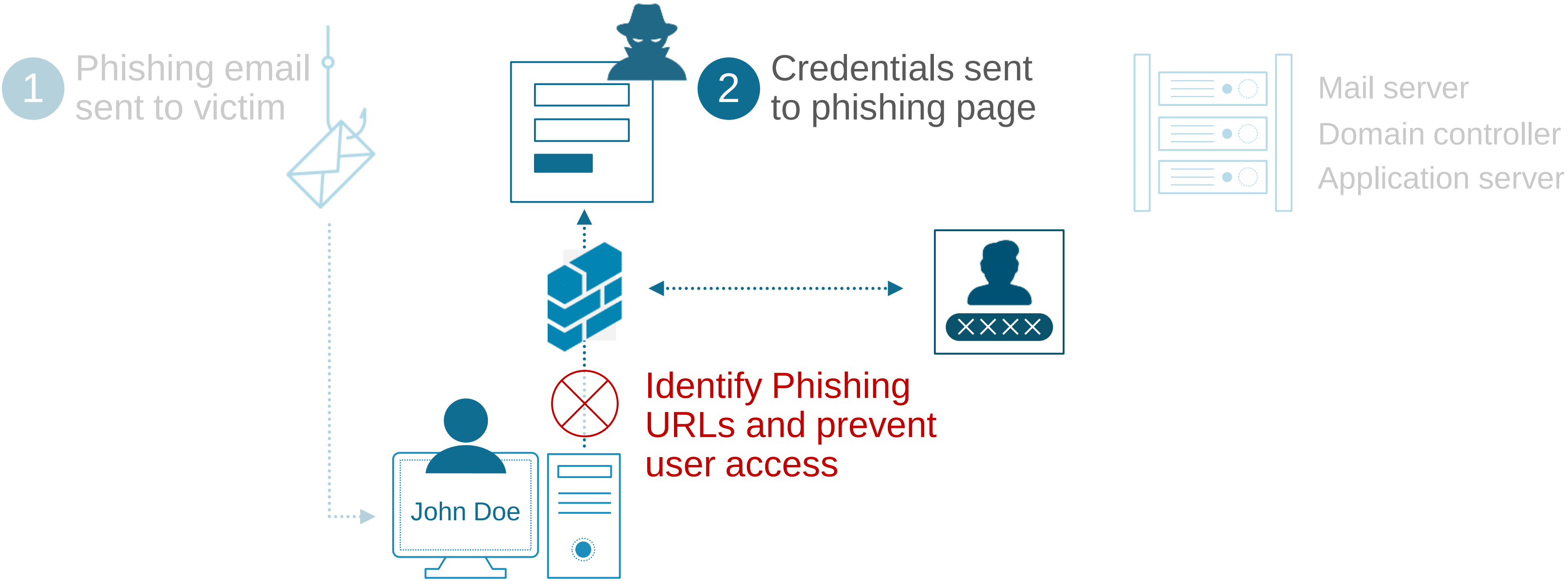
Identify Phishing URLs and prevent user access

Machine learning classifier with 60+ features

BLOCKING KNOWN BAD URLS ISN’T ENOUGH

- Targeted credential phishing is difficult to identify
  - Sophisticated cloaking techniques make pages invisible to everyone but the targeted victim
  - Links to credential phishing pages delivered through non messaging channels
- Attackers have to be successful once, defenders all the time
  - One missed phishing page can set an attack in motion that is difficult to detect

IDENTIFY AND BLOCK ACTUAL CREDENTIAL PHISHING ATTEMPTS


1
Phishing email sent to victim
2
Credentials sent to phishing page
Mail server
Domain controller
Application server
XXXX
John Doe

Identify Phishing URLs and prevent user access

CREDENTIAL DETECTION EXPLAINED

Known user names

- Detect submission of valid users names.

- Uses information retrieved from a connected LDAP directory to detect uniquely created user identifiers that don’t resemble real names.

Known logged in users

- Detect submissions of user names for logged in users for visibility and user education.

- Uses information available in User-ID to detect the known user name for the source IP of a session.

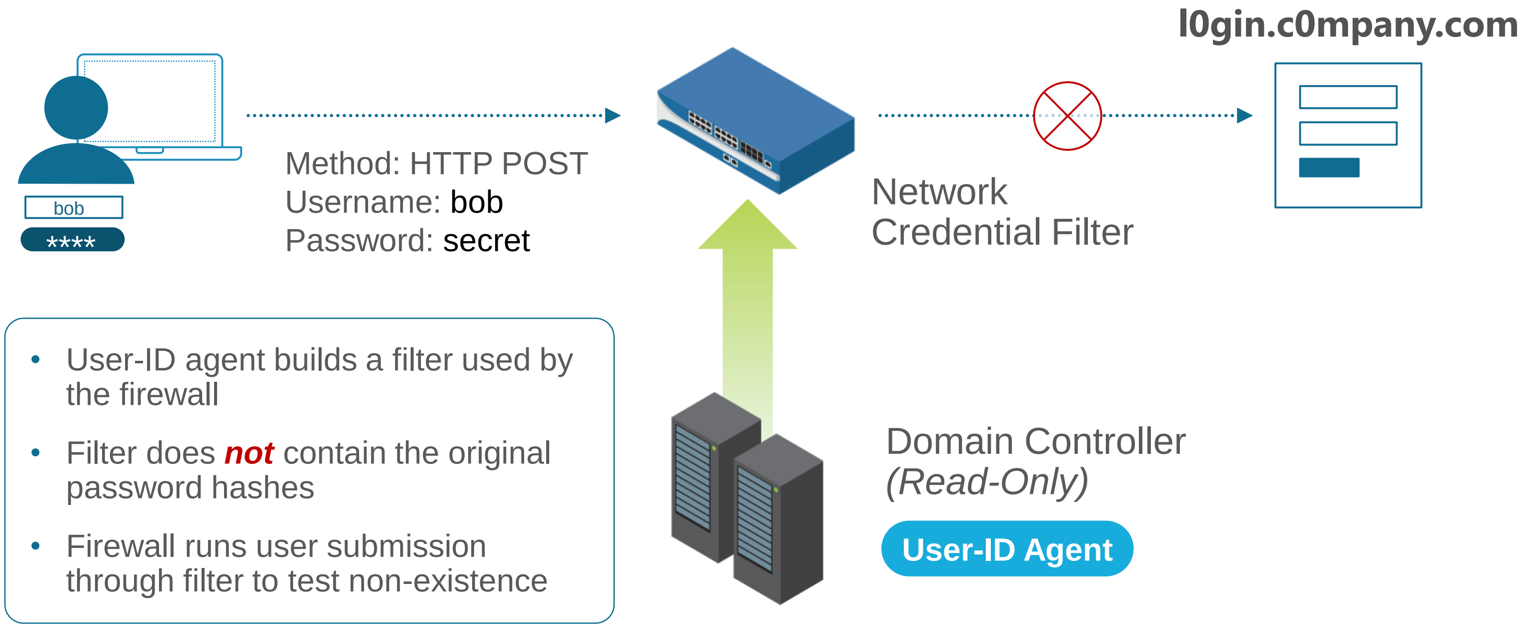
Known user credentials

- Exact credential submission to prevent credential leakage with zero false negatives.

- Used to detect the known user name and password for the source of a session, by using the User-ID Agent and the User-ID Credential Agent add-on.

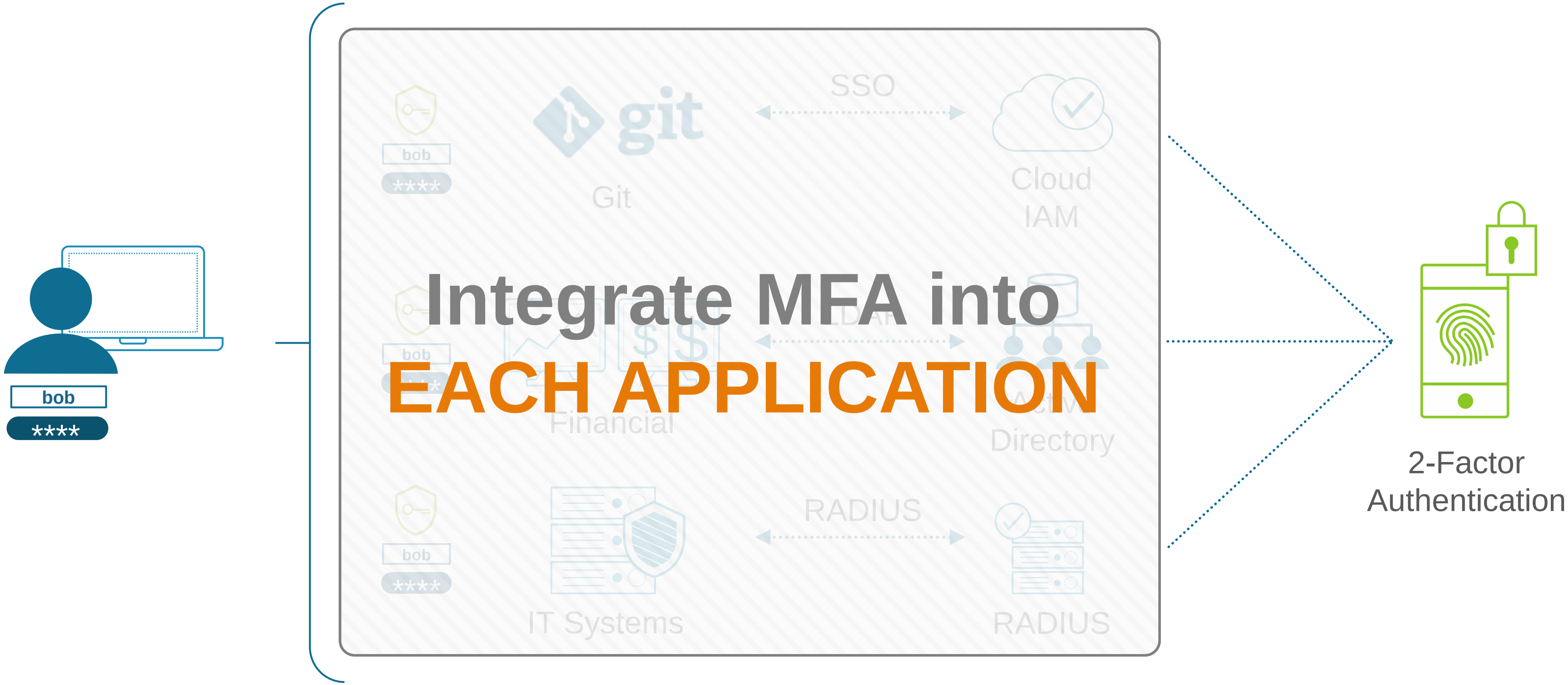
Prevent credential re-use ← | → Prevent credential theft

HOW CREDENTIAL FILTERING WORKS



- User-ID agent builds a filter used by the firewall
- Filter does ***not*** contain the original password hashes
- Firewall runs user submission through filter to test non-existence

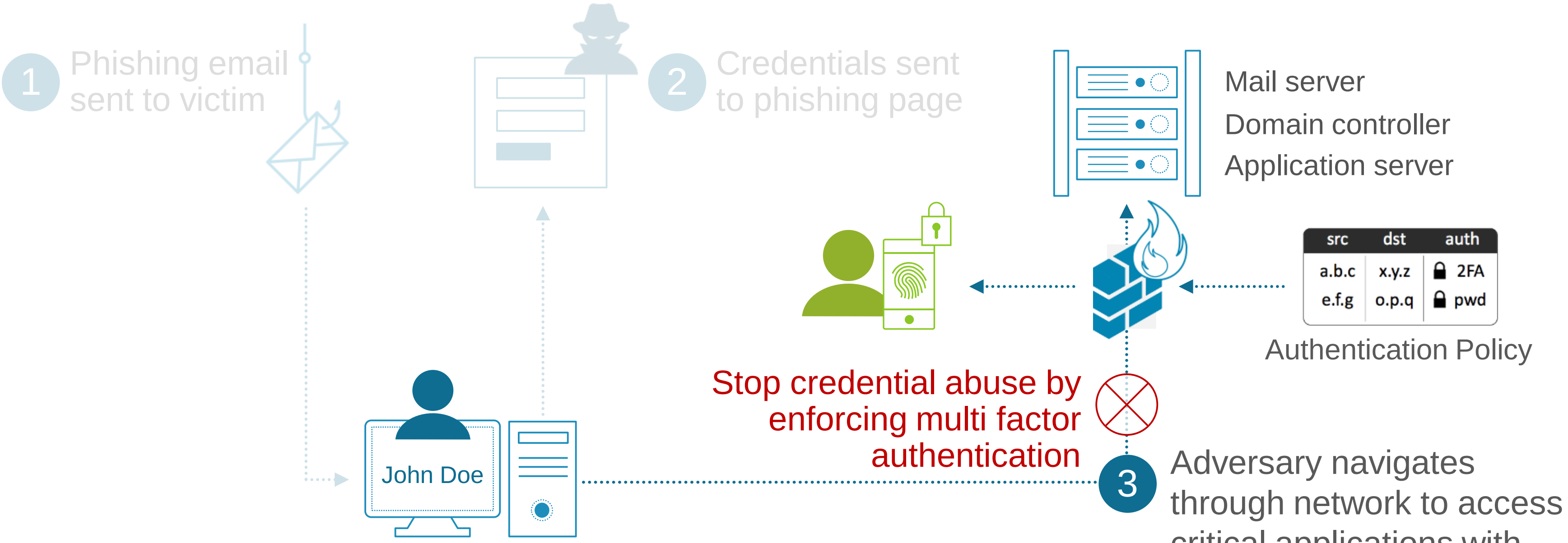
MFA – CHALLENGES WITH THE CURRENT SOLUTION



Integrate MFA into

EACH APPLICATION

PREVENT USE OF STOLEN CREDENTIALS ON THE NETWORK



1 Phishing email sent to victim

2 Credentials sent to phishing page

Mail server

Domain controller

Application server

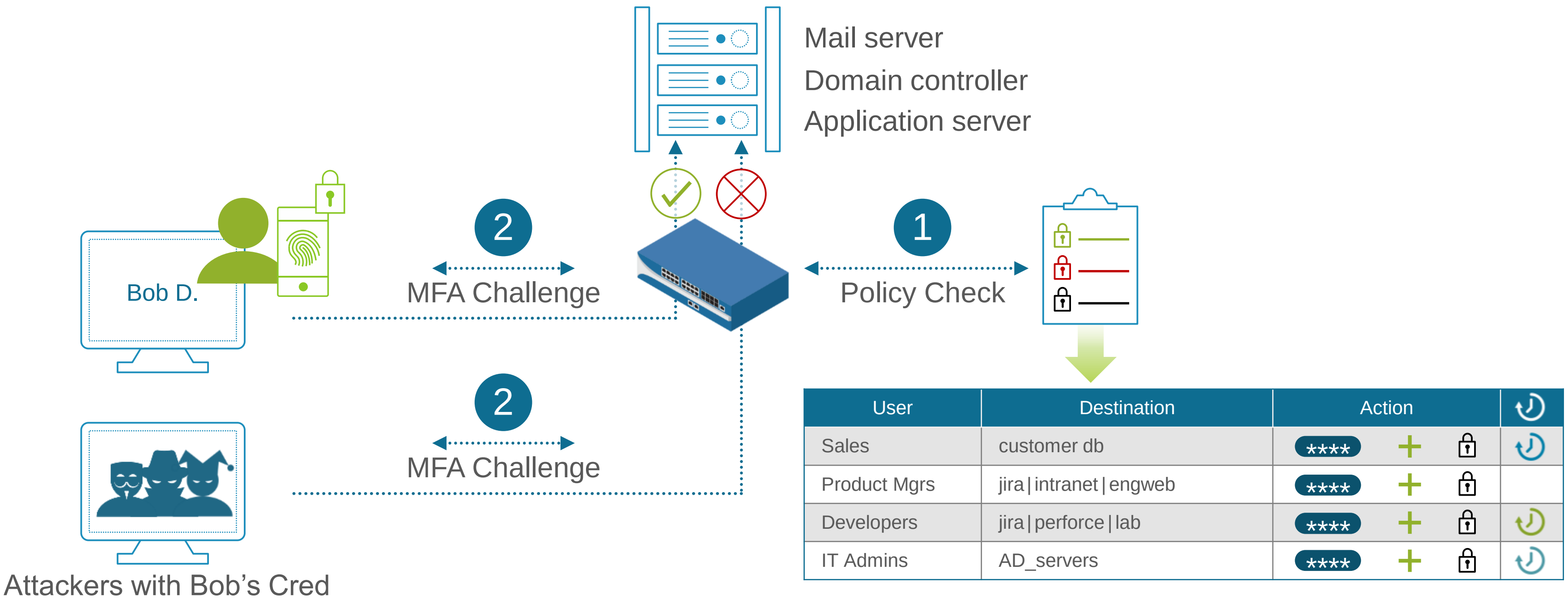
src	dst	auth
a.b.c	x.y.z	🔒 2FA
e.f.g	o.p.q	🔒 pwd

Authentication Policy

Stop credential abuse by enforcing multi factor authentication

3 Adversary navigates through network to access critical applications with stolen credentials

PREVENT USE OF STOLEN CREDENTIALS ON THE NETWORK



User	Destination	Action	⟲
Sales	customer db	**** + 🔒	⟲
Product Mgrs	jira | intranet | engweb	**** + 🔒	
Developers	jira | perforce | lab	**** + 🔒	⟲
IT Admins	AD_servers	**** + 🔒	⟲

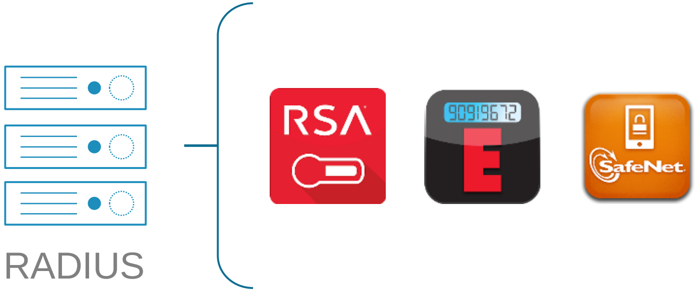
WORKS WITH YOUR EXISTING IAM SOLUTION

IDENTITY & PRIMARY AUTH

SAML | KERBEROS | TACACS+

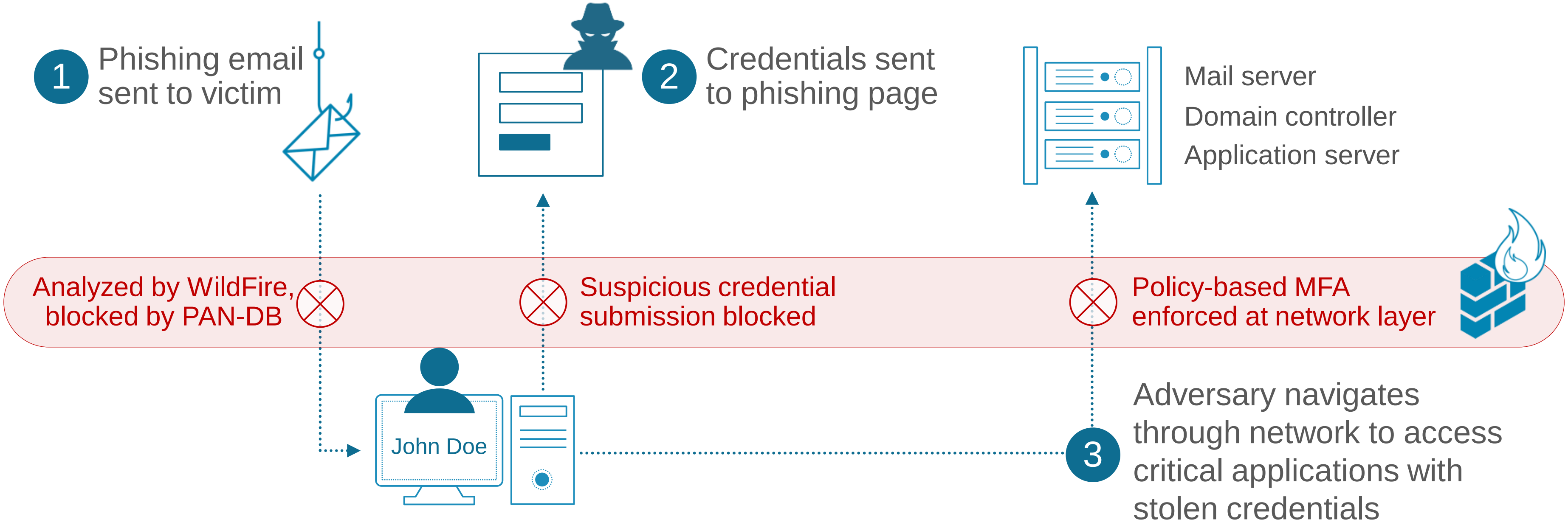
RADIUS | LDAP

SECONDARY AUTH



RADIUS

BREAKING CREDENTIAL THEFT ATTACK CYCLE



1 Phishing email sent to victim

2 Credentials sent to phishing page

Mail server

Domain controller

Application server

Analyzed by WildFire, blocked by PAN-DB

Suspicious credential submission blocked

Policy-based MFA enforced at network layer

3 Adversary navigates through network to access critical applications with stolen credentials

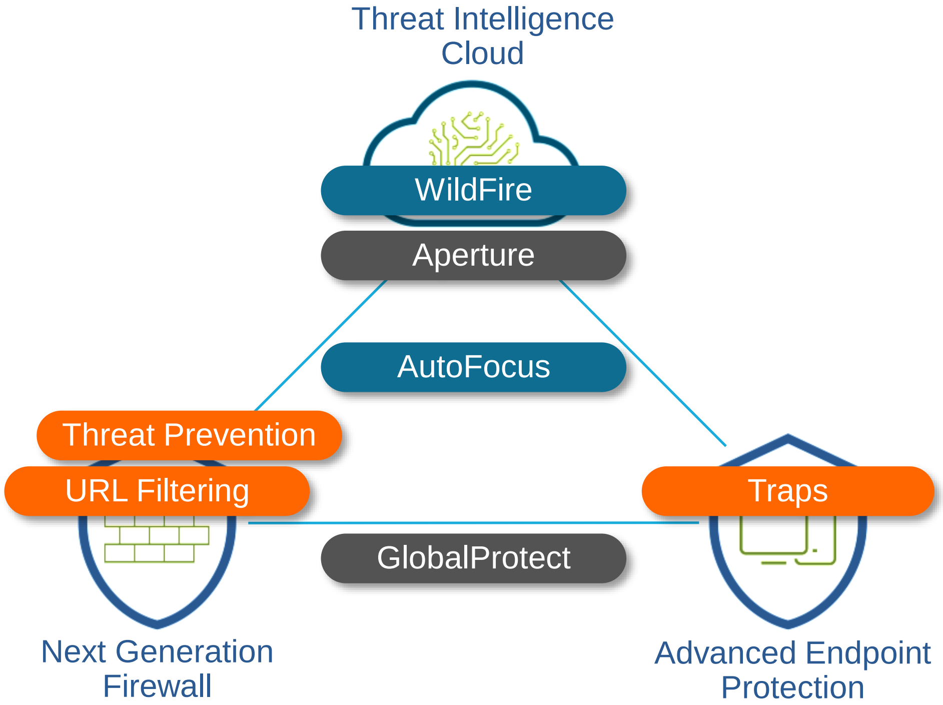
THE PLATFORM APPROACH TO THREAT PREVENTION

Detect & prevent new threats

Prevent all known threats

Reduce attack surface area

Complete visibility



Threat Intelligence Cloud

WildFire

Aperture

AutoFocus

Threat Prevention

URL Filtering

GlobalProtect

Traps

Next Generation Firewall

Advanced Endpoint Protection

Questions contact:

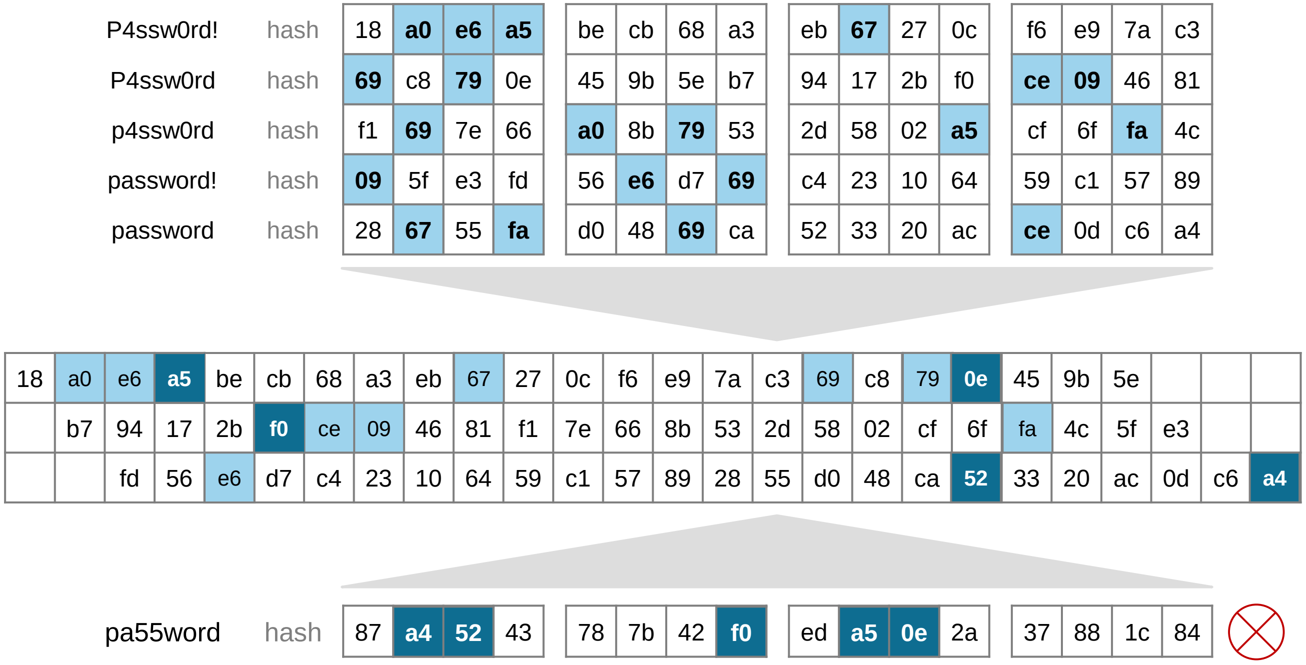
Ashley Hess
Marketing Events Manager
ashley.hess@slaitconsulting.com

HOW DOES A BLOOM FILTER WORK?

1 Collect data and create a table of hashes.

2 Deconstruct into stream of individual de-duplicated byte groups.

3 Hash data and match byte groups with Bloom Filter entries.



P4ssw0rd!	hash	18	**a0**	**e6**	**a5**	be	cb	68	a3	eb	**67**	27	0c	f6	e9	7a	c3
P4ssw0rd	hash	**69**	c8	**79**	0e	45	9b	5e	b7	94	17	2b	f0	**ce**	**09**	46	81
p4ssw0rd	hash	f1	**69**	7e	66	**a0**	8b	**79**	53	2d	58	02	**a5**	cf	6f	**fa**	4c
password!	hash	**09**	5f	e3	fd	56	**e6**	d7	**69**	c4	23	10	64	59	c1	57	89
password	hash	28	**67**	55	**fa**	d0	48	**69**	ca	52	33	20	ac	**ce**	0d	c6	a4

18	a0	e6	a5	be	cb	68	a3	eb	67	27	0c	f6	e9	7a	c3	69	c8	79	0e	45	9b	5e			
	b7	94	17	2b	f0	ce	09	46	81	f1	7e	66	8b	53	2d	58	02	cf	6f	fa	4c	5f	e3		
		fd	56	e6	d7	c4	23	10	64	59	c1	57	89	28	55	d0	48	ca	52	33	20	ac	0d	c6	a4

pa55word	hash	87	**a4**	**52**	43	78	7b	42	**f0**	ed	**a5**	**0e**	2a	37	88	1c	84	⊗