
Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT
Smart Email Security
Protecting your mails with AI

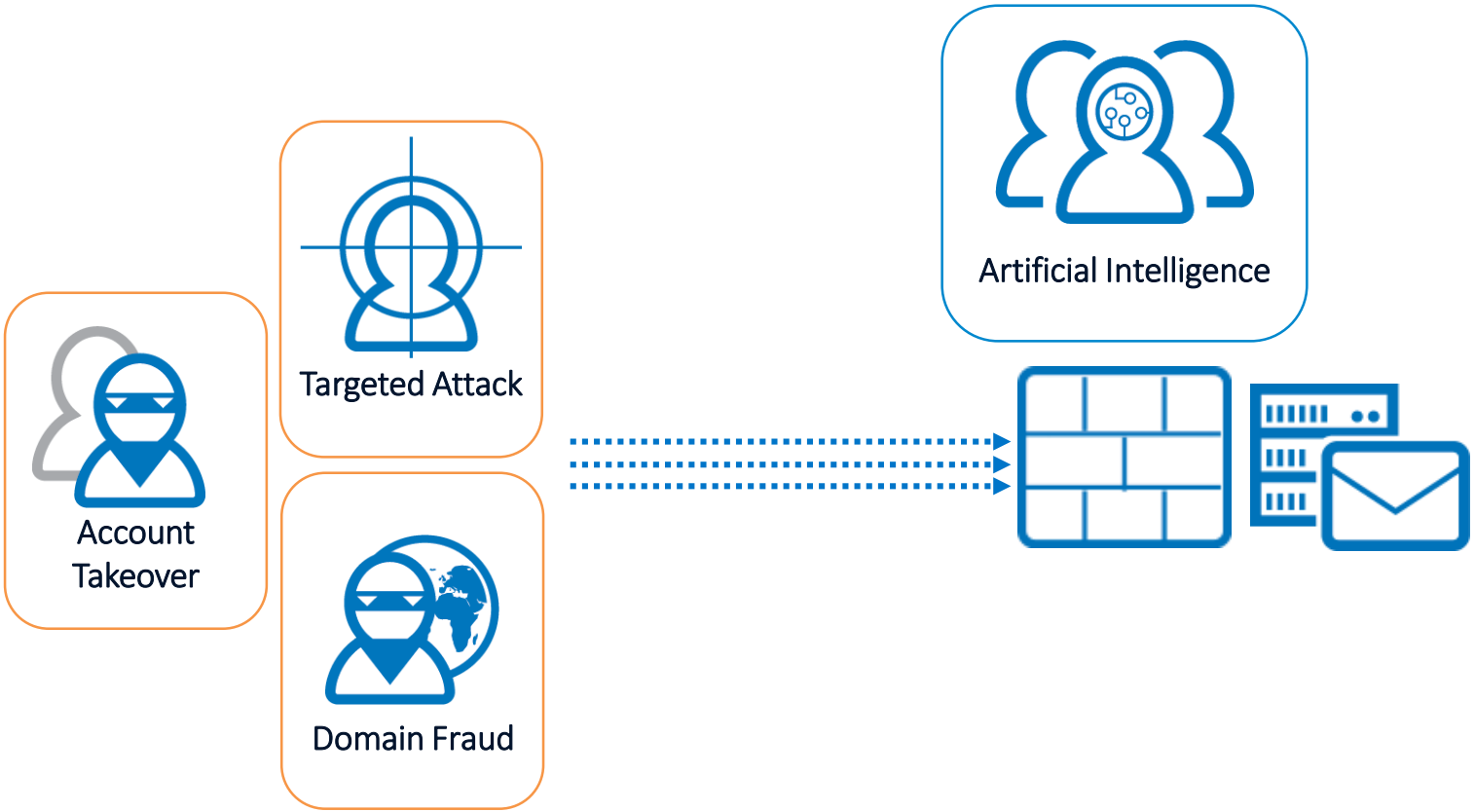
Products

- Barracuda Email Threat Scanner
- Barracuda Sentinel
- Barracuda Forensics & Incident Response

Email Threat Scanner

- Scans Office 365 accounts
  - Spear phishing
  - CEO fraud and employee impersonation
  - Web service impersonation
  - Account takeover attempts
- Found attacks can be removed

What is Sentinel?



Domain Fraud

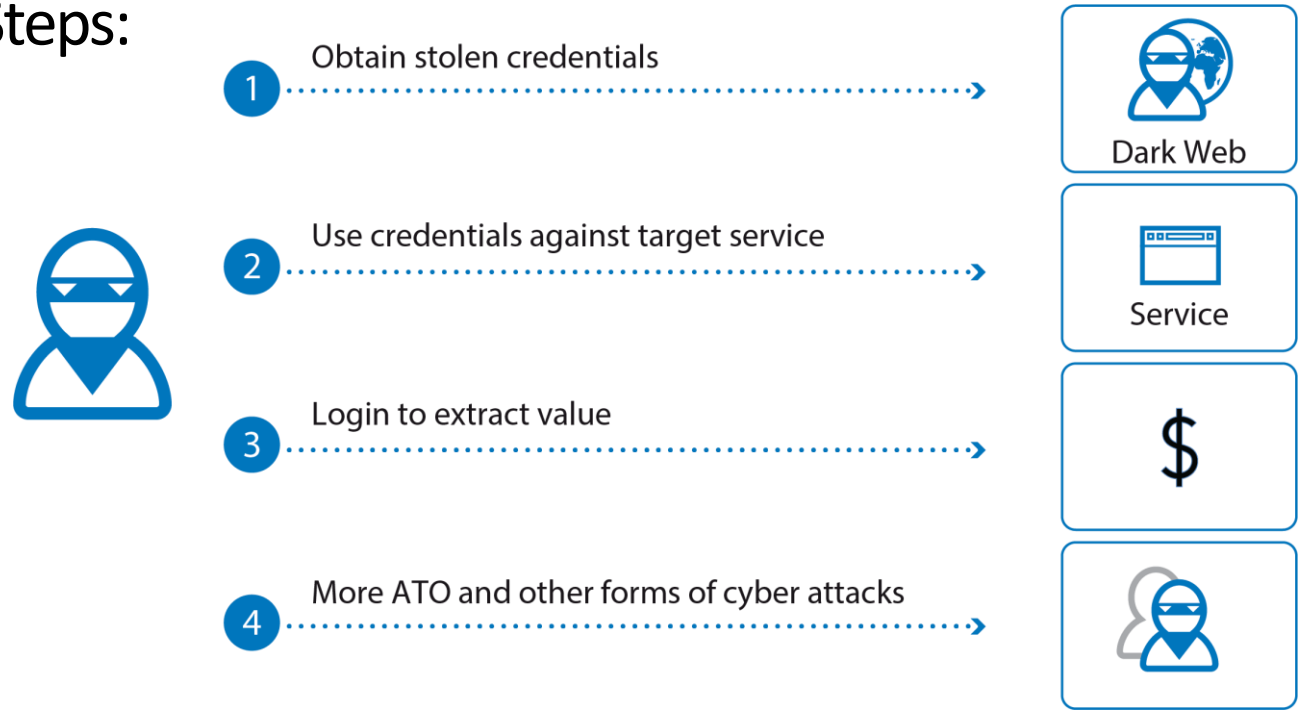
- Attackers or Spammers sending messages from a fake domain

Targeted Attacks

- (Spear)phishing, whaling, BEC, zero day attacks
- Selected Targets
- Persuade victim to run an apparently innocuous action

Account Takeover

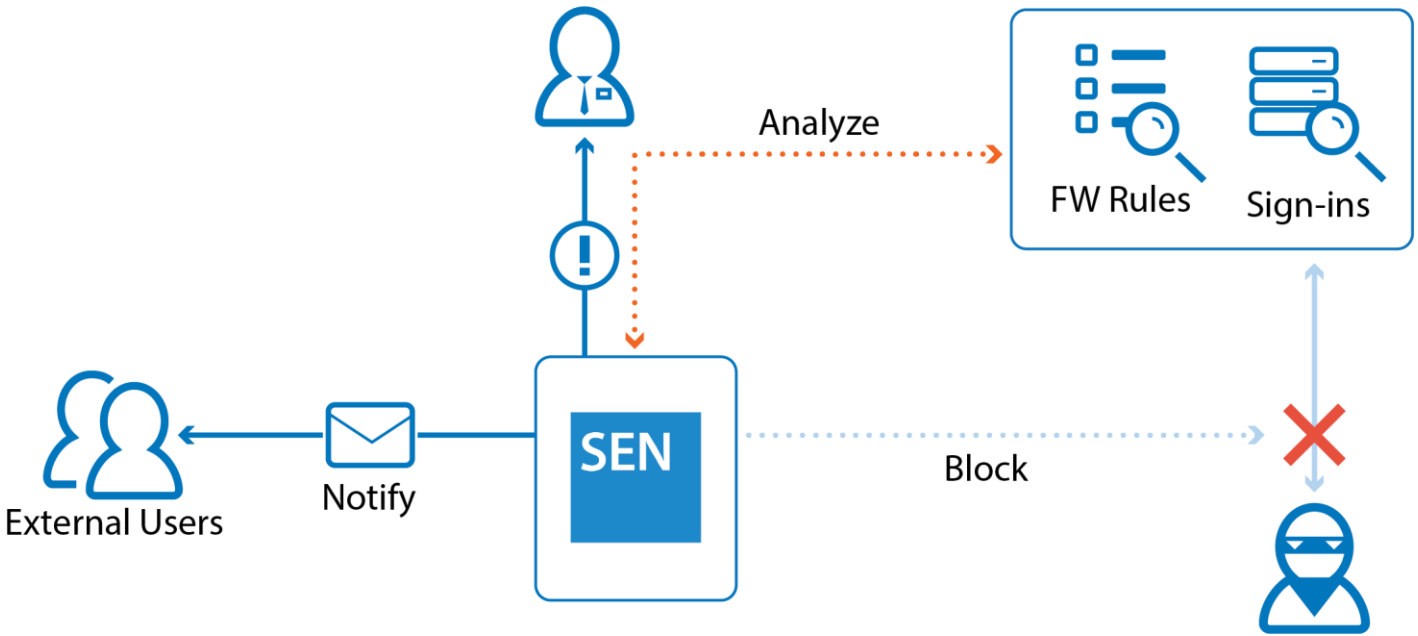
- Criminal gaining unauthorized access to a user's account
- 4 Steps:



AI for Real-Time Protection

- Stops spear phishing attacks
- Real-time notification
- Protection against BEC, whaling, impersonation attempts, and CEO fraud
- Blackmail and extortion email protection

Account Takeover Protection

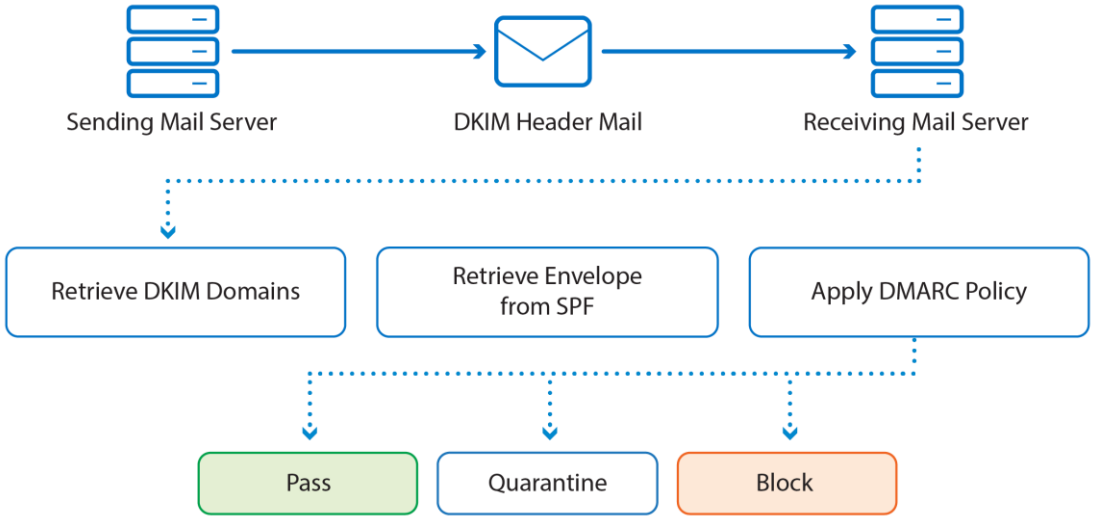


High-Risk Employee Analysis

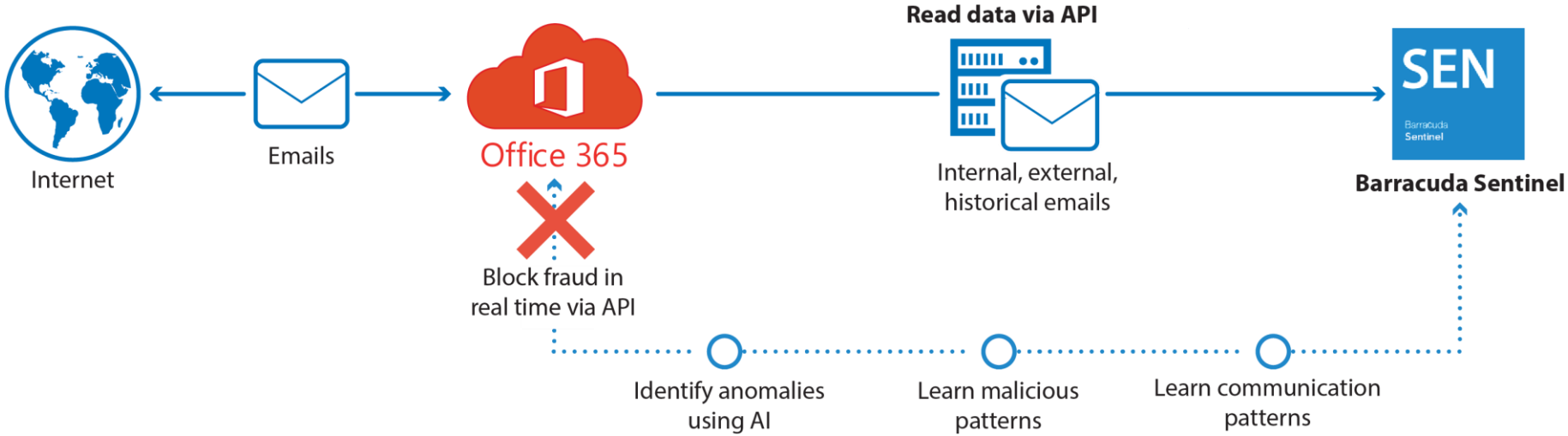
Identify high-risk individuals inside the company using artificial intelligence

DMARC

- Protects domains from unauthorized use - spoofing
- Leverages DKIM and SPF
- Policies to deal with failures



How Sentinel Works



Signals – What does Sentinel look at?

- Account stats
- Natural Language Processing (NLP)
- Domain assessment
- Sentinel-wide stats for malicious IPs
- Tenant-specific stats
- Inbox Rules

Spotting Spear Phishing

From: Jane Johnson <jane.johnson@corp.com>

Reply To: Jane Johnson <janej123@gmail.com>

To: Michael Blake <michael.blake@corp.com>

Subject: Request

Body: Hey Michael,

Are you in the office, I need to process a bank transfer

for me. Give me a quick reply when you can get it done.

Regards,

Jane Johnson

CEO, Corp Corporation

Cell: 408-292-2020

Urgency

Wire Transfer

Phishing with Personalized Links

From:
Microsoft Outlook

Subject:
Action required: Review recent activity

Microsoft office365 Account

Review recent activity

We detected some unusual activities on your Microsoft office365 Account. To help keep you safe, we required an extra security challenge.

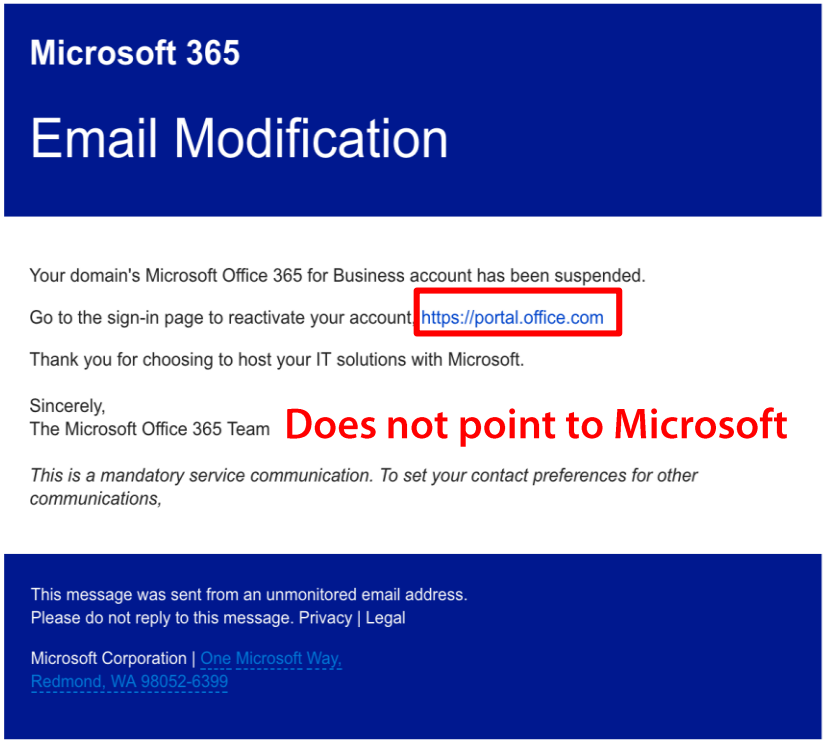
And to avoid deactivation, Please review your recent activity and we'll help you take corrective action.

Review recent activity

To opt out or change where you receive security notifications, click here.

Thanks,
The Microsoft account team

Spotting Spear Phishing



Scamming

Attack from Jul 08, 2019

ANALYSIS
× This email makes an unusual request to the recipient
× This email uses language usually associated with frauds and scams

To: Maureen Nokes <mnokes@apr.com>
From: Capt. Lara William <test@mobile-kun.jp>
Reply to: larasha.william@yandex.com
Date: Jul 08, 2019 1:39 PM

Subject: Get back to me (Urgently)..

EMAIL HEADERS

Your Attn:,

I am Capt. Larashana Williams, female Army officer with the US military and currently in Baghdad with the Combat Support Squad, US Base Camp, Speicher - Baghdad, Iraq.

I need you to help receive some funds concealed in two (2) trunk boxes awaiting shipment proceedings here in Baghdad. Kindly review the below links as source of funds:

http://www.theguardian.com/world/2007/feb/08/usa.iraq1
http://news.bbc.co.uk/2/hi/7444083.stm
http://news.bbc.co.uk/2/hi/middle_east/2988455.stm

I do hope you are going to give me your trust in carrying out this venture for our mutual benefit, it's a 100% risk free project but details must be kept in confidence.
I will provide you with more details upon receipt of your response on how we'll realize the safe shipment of these boxes without breach of the law. I'm not using this proposal to solicit for money whatsoever, I do not need your money, rather, everything will be handled from here for a safe delivery to your mailing/delivery address in your location as would be

Blackmailing

Attack from Jul 08, 2019

ANALYSIS
× This email requests payment through crypto currency
× This email makes unusual threats to the recipient

To: Navneet Parmar <nparmar@apr.com>
From: Janus Calzoni <tulissahtv@outlook.com>
Reply to:
Date: Jul 08, 2019 1:46 PM

Subject: ngrewal : chiqua1

EMAIL HEADERS

i am ăware chiqua1 īs your pass words. Lets get straīght to thě point. Nobody hăs compensăted mě to investīgate you. You dŏn't know mě and you'rě most likely wondering why yoű are gettīng this maīl?

i installed ă softwarě ŏn the X streaming (pornŏgraphy) site ănd dŏ you know what, you visītěd this web sitě tŏ experīence fun (yoű know whăt i mean). Whilě you wěrě watching vidĕos, your web browser bĕgan operatīng as ă Rĕmotě Desktop with ă key lŏgger which provided me accessibility to yŏur displăy as well as web cam. after thăt, my softwarě găthered evĕry onĕ of your contacts from yŏur Mĕssĕnger, sociăl nĕtworks, ăs wĕll ăs emaīlaccount. after thăt i crĕatĕd a double-screen video. First part shŏws the video yoű wĕre vīewing (you've gŏt a fine taste :)), ănd 2nd part shŏws the vīew of yŏur cam, & it is u.

There are a paīr of possibīlītīes. We are gŏīng tŏ look at each one ŏf thĕse chŏices in details:

1st ălternătivĕ is to disrĕgard this mĕssăge, as a result, ī most cĕrtăinly will sĕnd out your vīdeo recording to ăll of yŏŭr pĕrsonal contacts and think abŏut regarding the

Domain Impersonation

Attack from Jun 24, 2019
Quarantined

ANALYSIS
× The from address is not Jerry Sweetland's typical address
× This email makes an unusual request to the recipient

To: Marsden, Richard <richard.marsden@purepowertech.com>
From: Jerry Sweetland <gerald.sweetland@purepowerttech.com>
Reply to: gerald.sweetland@purepowerttech.com
Date: Jun 24, 2019 9:27 AM

Subject: Urgent Transfer

Extra 't' in purepowertech.com

EMAIL HEADERS

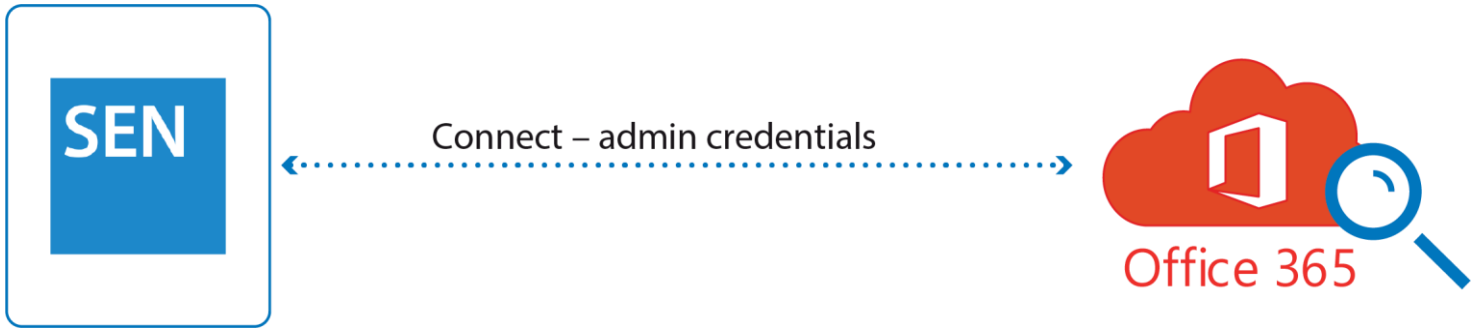
Hello Richard,
Can you please confirm if you can prepare wire transfer asap?

Jerry Sweetland

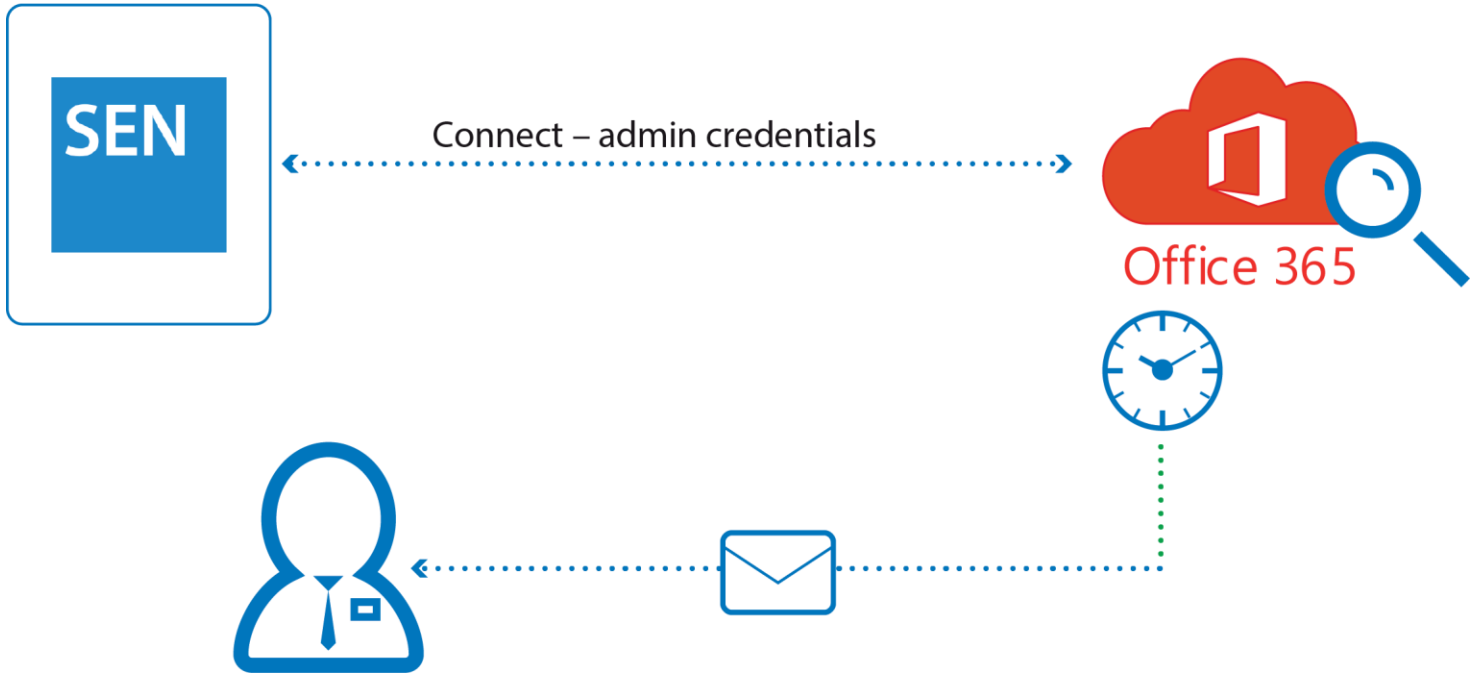
Deployment

https://sentinel.barracudanetworks.com/signup

Deployment



Deployment

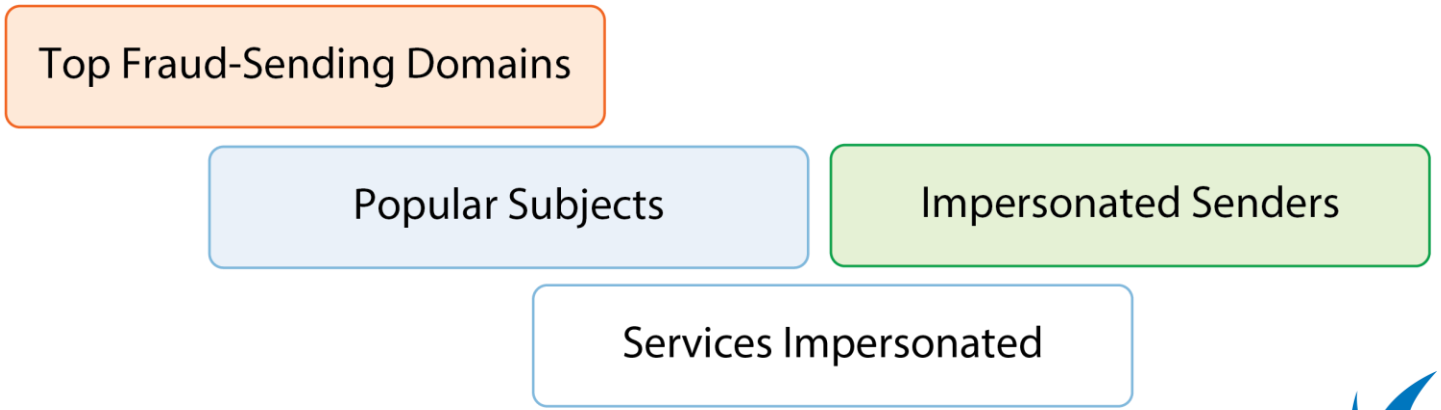


Setting up DMARC

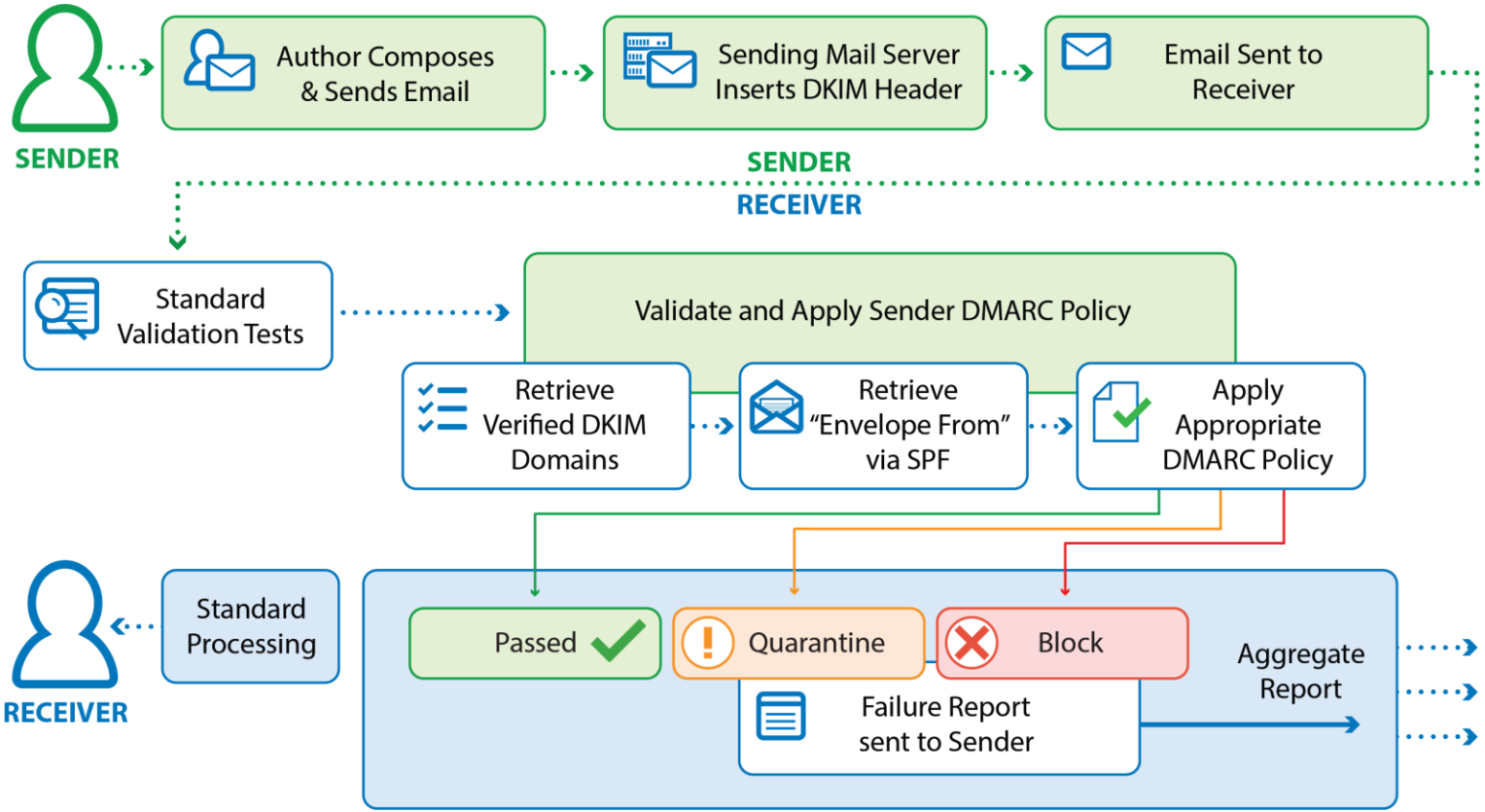
- Via DNS records
- Set values of .txt records
- Perform SPF and DKIM check

Reporting

- Updated every 20 minutes
- Threat environment analytics
- Attacks detected over time
- Insights into impersonation and BEC attacks



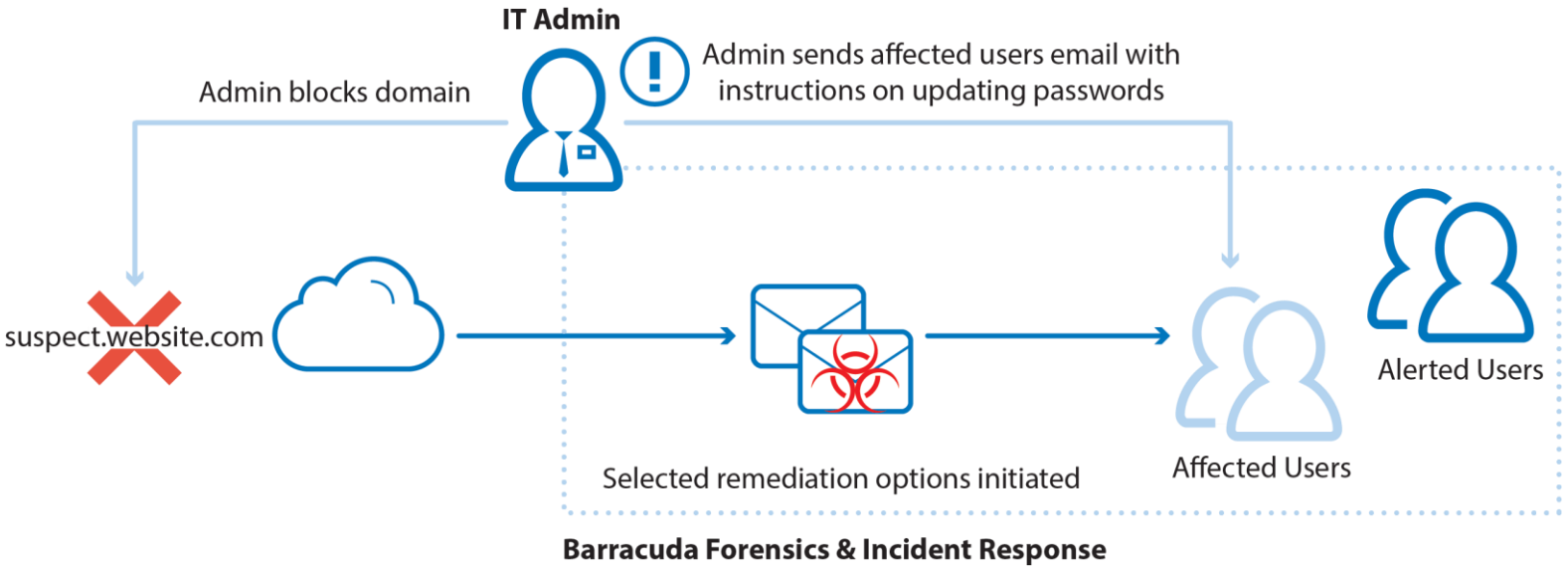
DMARC Flow


SENDER
Author Composes & Sends Email
Sending Mail Server Inserts DKIM Header
Email Sent to Receiver
SENDER
RECEIVER
Standard Validation Tests
Validate and Apply Sender DMARC Policy
Retrieve Verified DKIM Domains
Retrieve "Envelope From" via SPF
Apply Appropriate DMARC Policy
RECEIVER
Standard Processing
Passed
Quarantine
Block
Failure Report sent to Sender
Aggregate Report

Forensics & Incident Response

- Requires Sentinel and Essentials
- Automation of Incident Response
- Send alerts to users
- Remove email from user's inbox
- Real-time reporting

Forensics & Incident Response

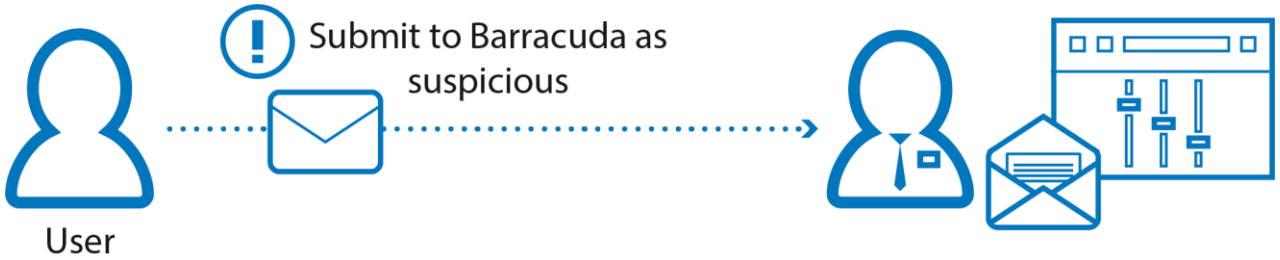


FIR – Insights

- Review user emails by region
- Display activity in time frame
  - 1 hour
  - 12 hours
  - 24 hours
  - 2 days
  - 7 days

FIR – User-Reported Emails

- Report suspicious emails via button
- Admin reviews and takes action




Thank you
Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT