Barracuda

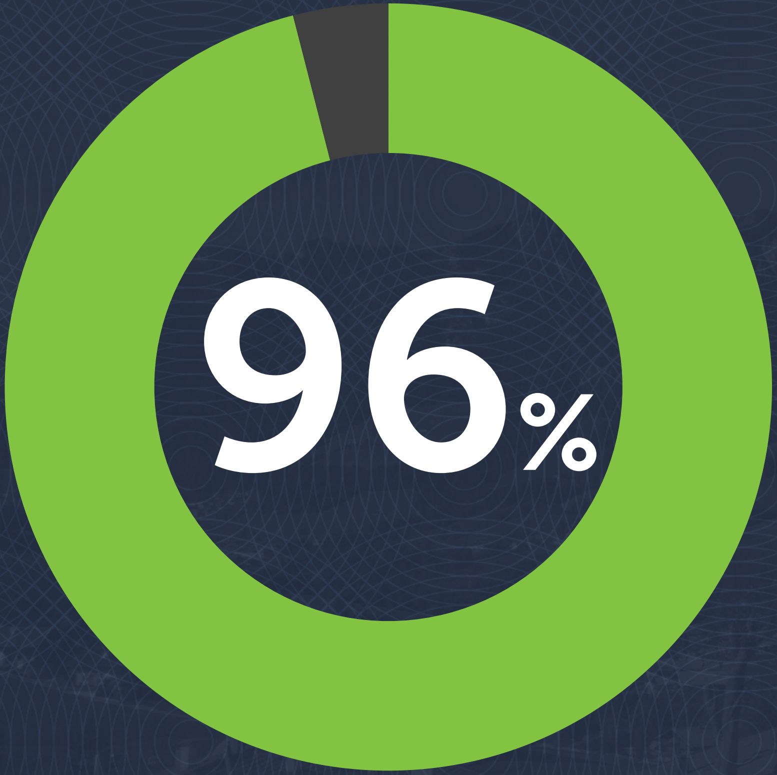
TECHSUMMIT19

BARRACUDA TECHNICAL SUMMIT

Forensics & Incident Response

Nishant Taneja & Aseem Asthana

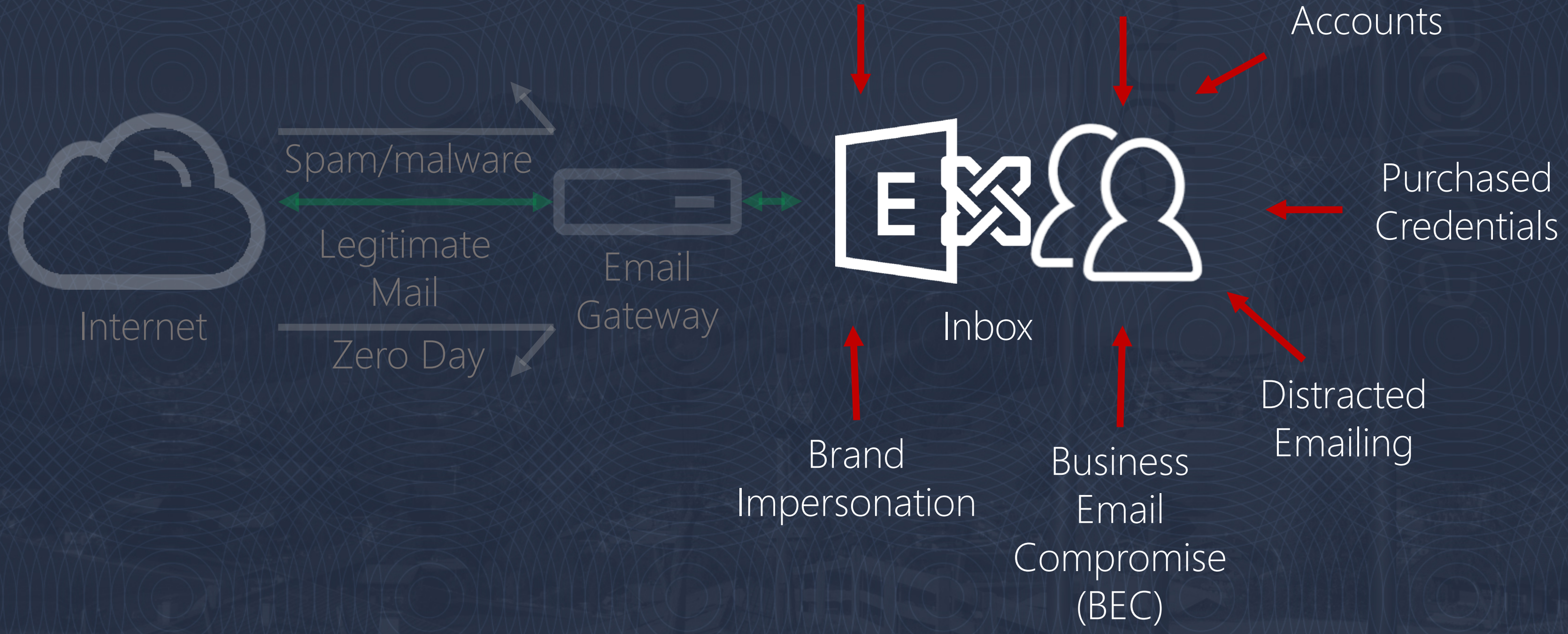
Most data breaches start with email



Email continues to be **the most common vector** for breaches.

- 2018 Verizon DBIR

Email threats 2.0



Account Takeover (ATO)

Conversation Hijacking

Personal Accounts

Purchased Credentials

Distracted Emailing

Business Email Compromise (BEC)

Brand Impersonation

Inbox

Internet

Spam/malware

Legitimate Mail

Zero Day

Email Gateway

Invest in detection and response

Prevention

- Email Gateway
- Archiving
- Inbox BEC Prevention
- Service Impersonation Prevention
- User Training
- User Simulation

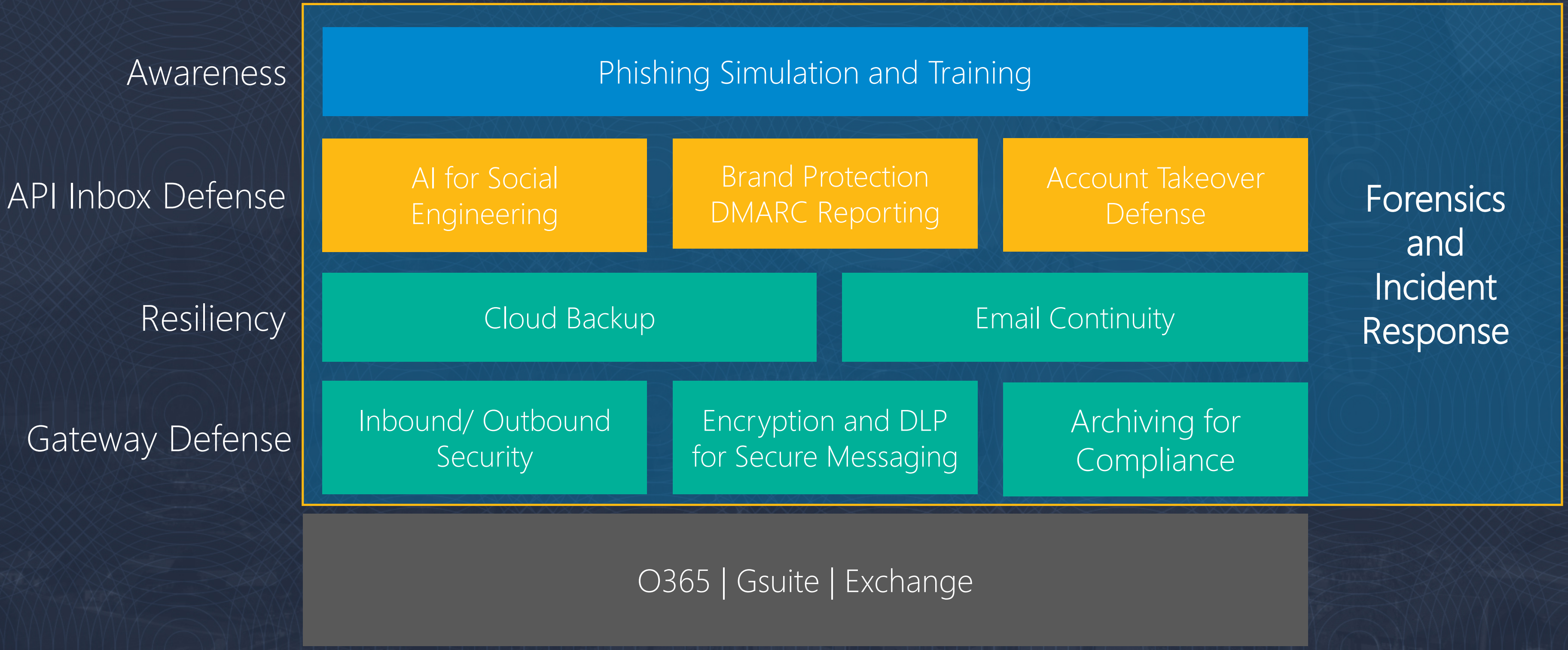
Detection

- ATO Detection
- Conversation Hijacking Detection
- Brand Spoofing Detection

Response

- Post Delivery Cleanup
- Threat Hunting
- User Reported Message Triage

Critical Part of Total Email Protection



Awareness

Phishing Simulation and Training

API Inbox Defense

AI for Social Engineering

Brand Protection DMARC Reporting

Account Takeover Defense

Resiliency

Cloud Backup

Email Continuity

Gateway Defense

Inbound/ Outbound Security

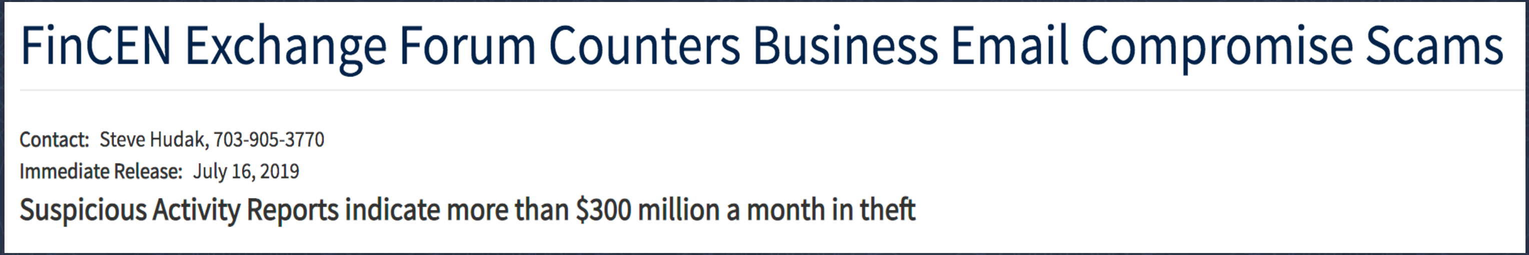
Encryption and DLP for Secure Messaging

Archiving for Compliance

Forensics and Incident Response

O365 | Gsuite | Exchange

No protection is 100% guaranteed

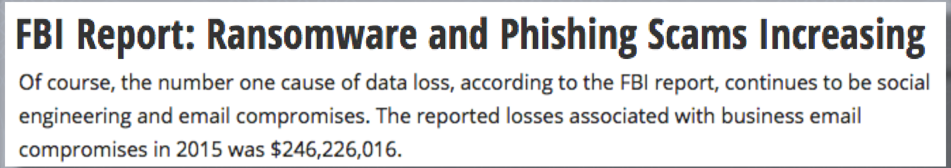


FinCEN Exchange Forum Counters Business Email Compromise Scams

Contact: Steve Hudak, 703-905-3770

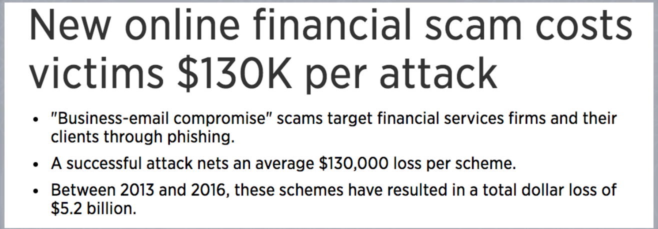
Immediate Release: July 16, 2019

Suspicious Activity Reports indicate more than $300 million a month in theft



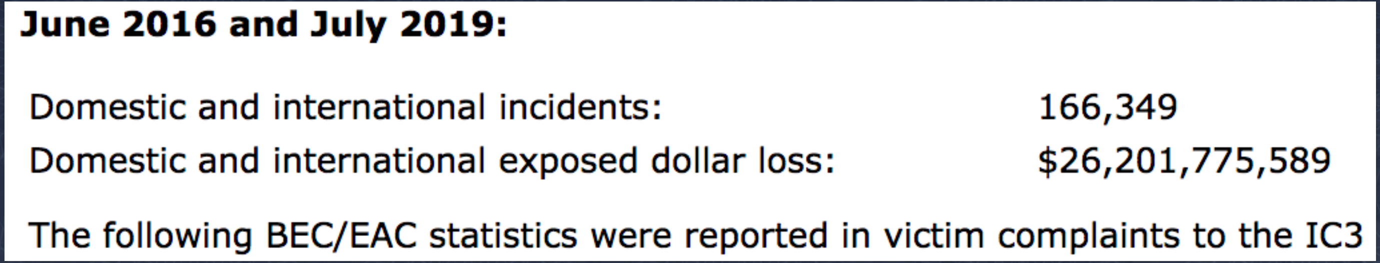
FBI Report: Ransomware and Phishing Scams Increasing

Of course, the number one cause of data loss, according to the FBI report, continues to be social engineering and email compromises. The reported losses associated with business email compromises in 2015 was $246,226,016.



New online financial scam costs victims $130K per attack

- "Business-email compromise" scams target financial services firms and their clients through phishing.
- A successful attack nets an average $130,000 loss per scheme.
- Between 2013 and 2016, these schemes have resulted in a total dollar loss of $5.2 billion.



June 2016 and July 2019:

Domestic and international incidents:	166,349
Domestic and international exposed dollar loss:	$26,201,775,589

The following BEC/EAC statistics were reported in victim complaints to the IC3

According to Gartner

Technical professionals must understand end user’s role in phishing detection and the human role of the incident responders during phishing response.

- Mario De Boer, Gartner

Gartner also says..

The email security market is starting to adopt a continuous adaptive risk and trust assessment (CARTA) mindset and acknowledge that perfect protection is not possible. As a result, vendors are evolving or emerging to support new detect and response capabilities by integrating directly with the email system via API.

Incident response today

IDENTIFY

- Users don't always report attacks
- IT investigations take too long

> 30 min

INVESTIGATE

- Manual search for other recipients of malicious mail
- Unconnected systems lead to tedious manual checks

2-4 hours

RESPOND

- Manually remediation
- Quarantining malicious mail takes too long

1-4 hours

Incident response scenario

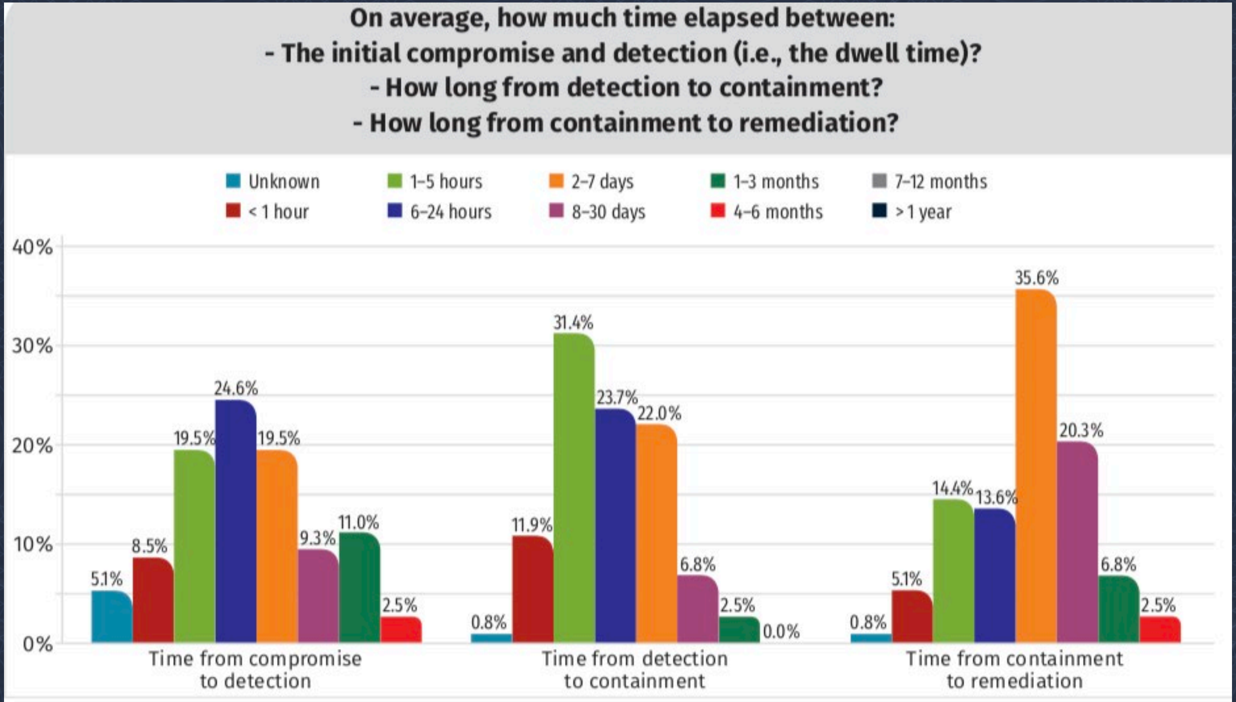
Manual incident response can take **3-8 hours** per incident

This could add up:

5 incidents x 8 hours = **40 hours per incident**

Lack of information and tools result in a manual, inefficient, time consuming process that often can lead to further spread of attacks

Time from compromise to remediation



On average, how much time elapsed between:
- The initial compromise and detection (i.e., the dwell time)?
- How long from detection to containment?
- How long from containment to remediation?

Source: SANS Incident Response 2019

Who is the clicker?

16 min

First click in most campaigns

28 min

First savvy individual to report

Never a single attack

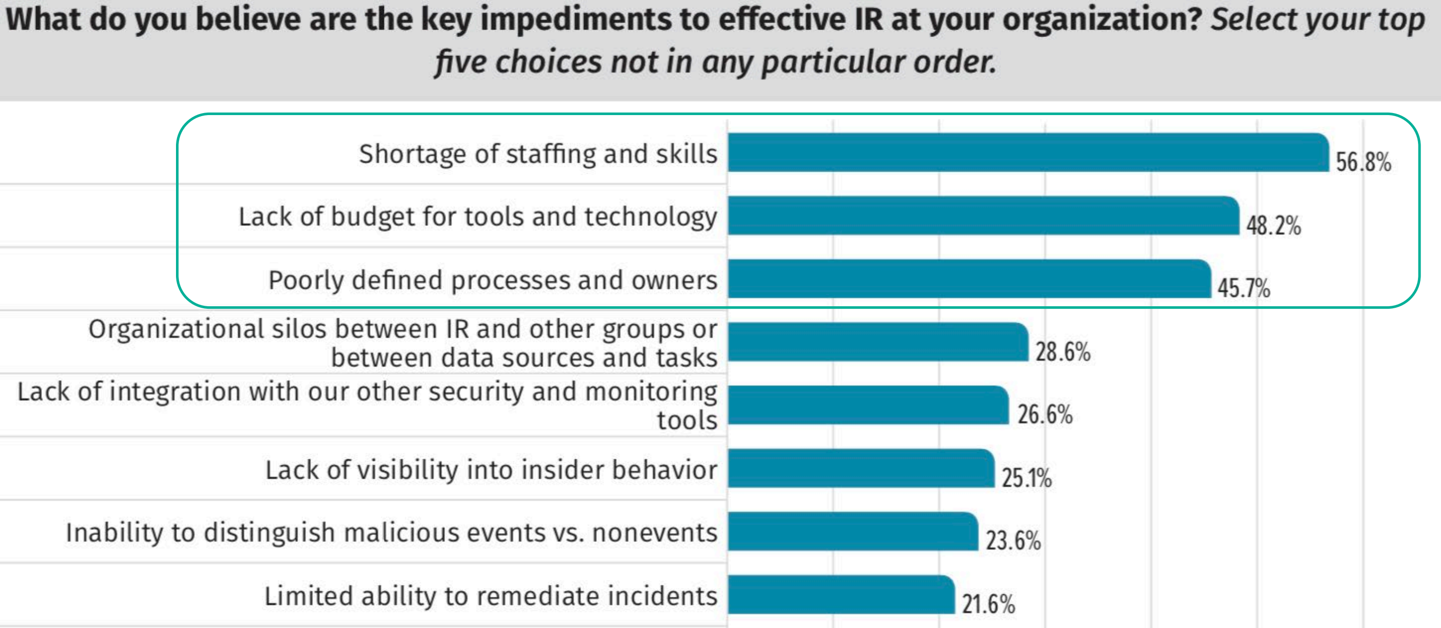
- Search through mail server logs

4% of people in any given phishing campaign will click

- Hackers only need one

Remember LOFT?

Blockers to effective incidence response



What do you believe are the key impediments to effective IR at your organization? ***Select your top five choices not in any particular order.***

Source: SANS Incident Response 2019

Manual incident response pain points

"There is no way to determine the scope and size of email-based attacks"

“There is no easy way to remove malicious and phishing emails from users' inboxes"

“It takes a very long time to deal with remediating email attacks"

“There is no reporting on past attacks and resolved incidents "

“There is no way to identify which users clicked on malicious URLs"

“End users can't easily report phishing emails to us"

IT, we have a BEC

Business Email Compromise Attack

A BEC attack steals funds or sensitive data by exploiting normal business processes using pure social engineering tactics (*not* malicious URLs or attachments).

Why it works:

Bypasses traditional security products that are only looking for a malicious payload

A combination of social engineering tactics cons users and overrides their better judgment

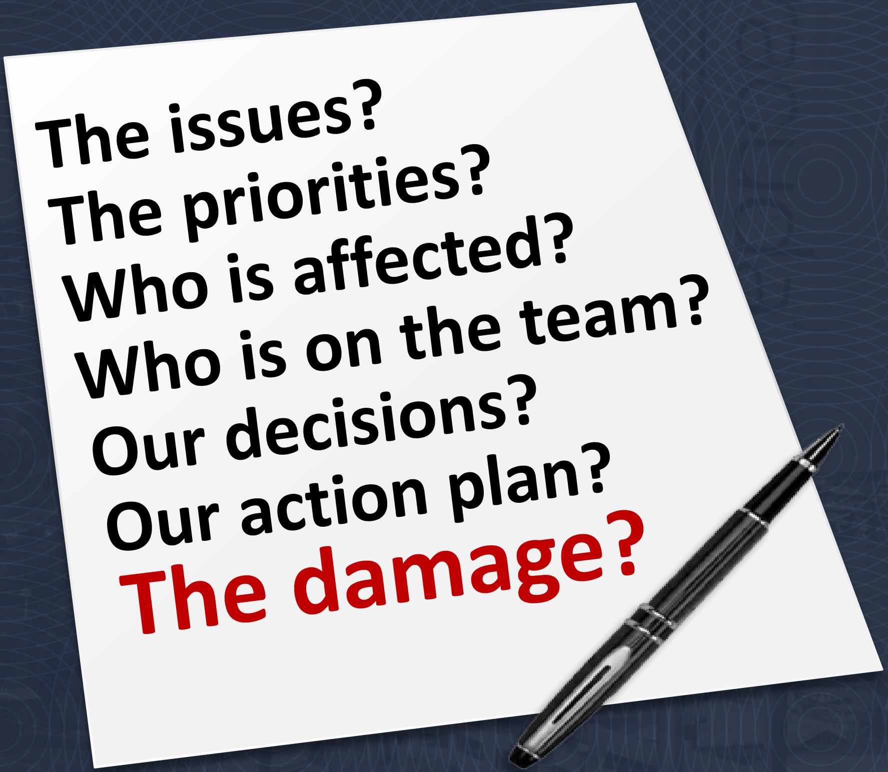
How to stop it:

Fix loopholes in business processes

Employ technology that can inspect message context by looking at the trustability and authenticity of the sender

Actively monitor your email systems and provide end users an easy path to report suspicious email communications

Day 1: Incident begins..



The issues?

The priorities?

Who is affected?

Who is on the team?

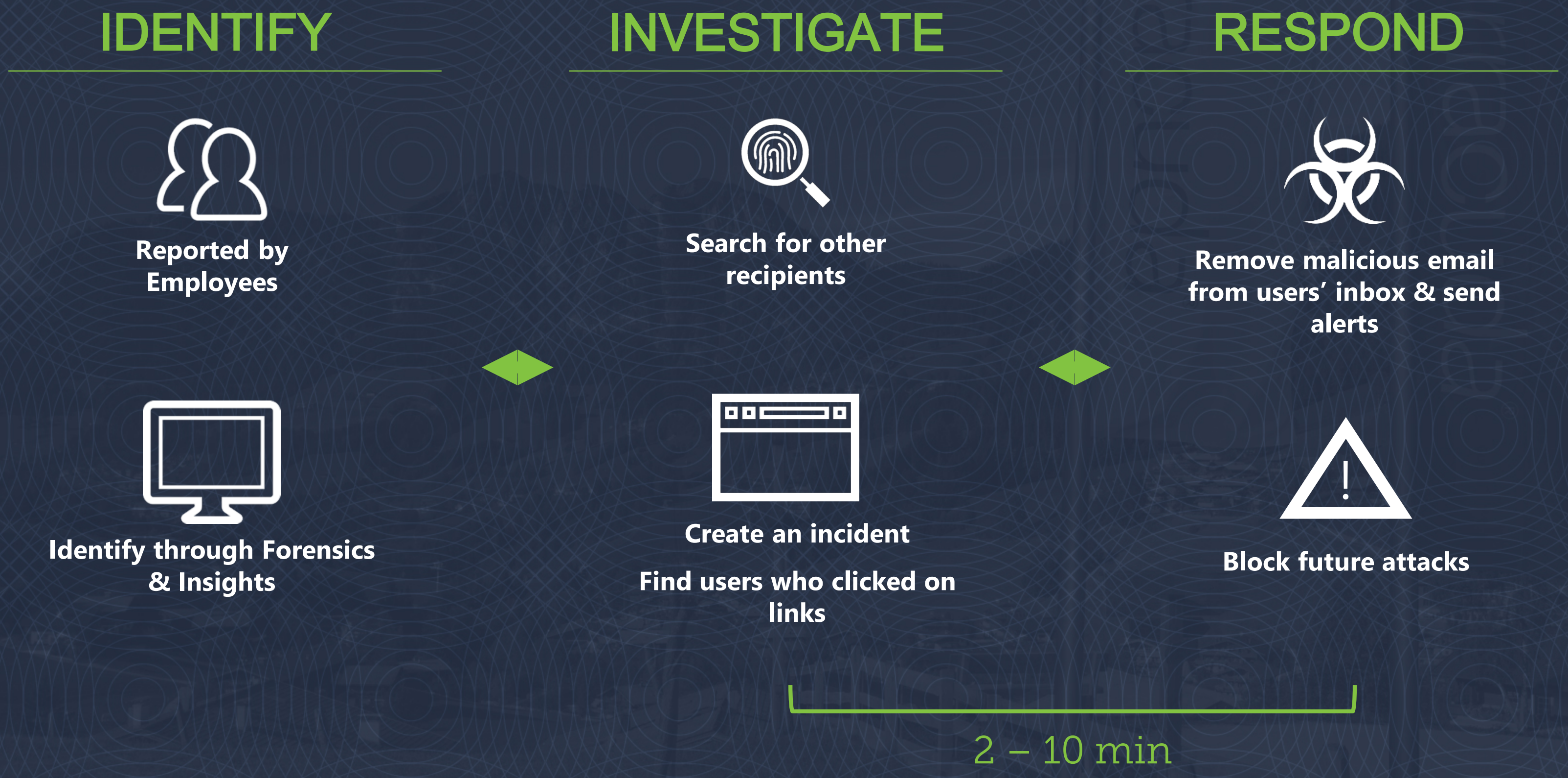
Our decisions?

Our action plan?

The damage?

Your incident response must be **fast**, **efficient**, and include both **reactive** and **proactive** measures

Automate incident response



IDENTIFY

Reported by Employees

Identify through Forensics & Insights

INVESTIGATE

Search for other recipients

Create an incident

Find users who clicked on links

RESPOND

Remove malicious email from users' inbox & send alerts

Block future attacks

2 – 10 min

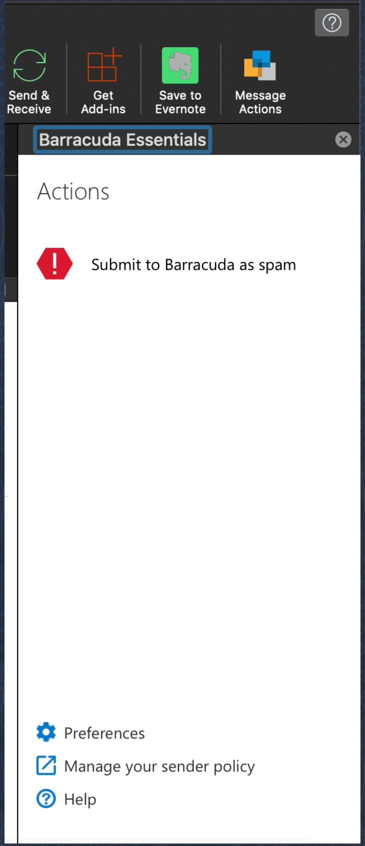
Enables best practice in incident response

Educate Users

Automate Incident Response

Block Future Attacks

Allow end-user to report phishing attacks

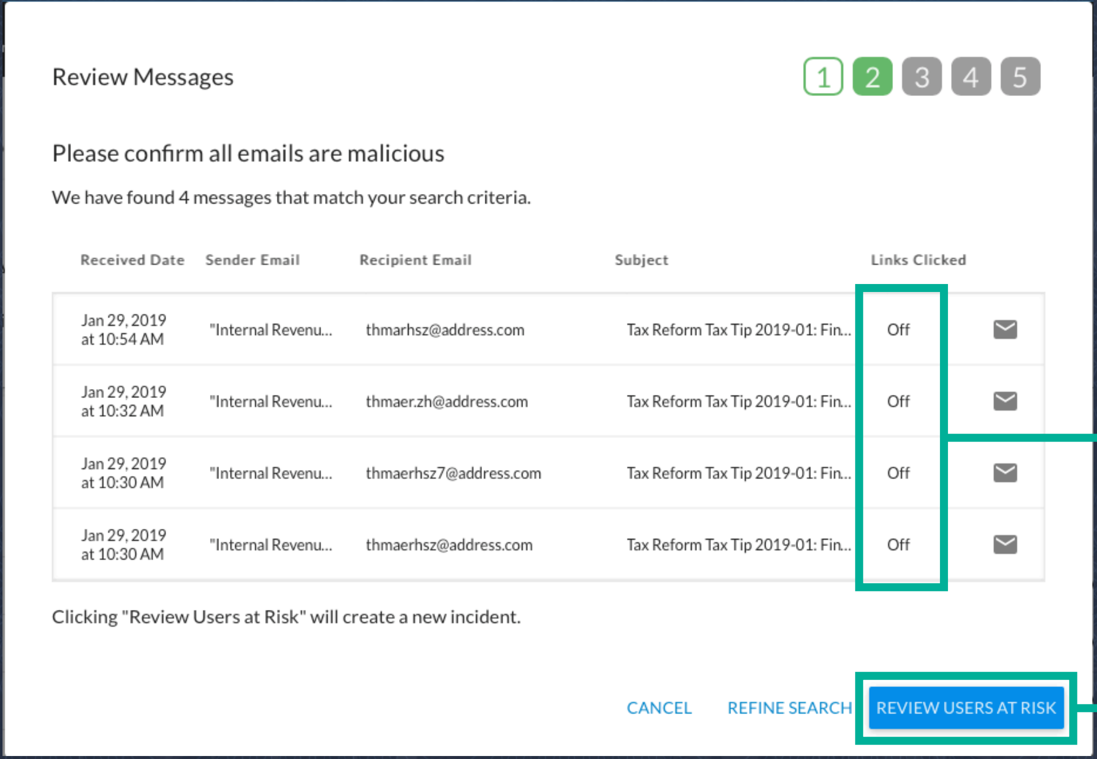


End-users’ reports of suspicious emails will show up in FIR UI

- As reported from Outlook add-in or Web UI

Admins will be able to start an incident from each report or dismiss them

Identify users in need of training



Review Messages

Please confirm all emails are malicious

We have found 4 messages that match your search criteria.

Received Date	Sender Email	Recipient Email	Subject	Links Clicked	
Jan 29, 2019 at 10:54 AM	"Internal Revenu...	thmarhsz@address.com	Tax Reform Tax Tip 2019-01: Fin...	Off	✉
Jan 29, 2019 at 10:32 AM	"Internal Revenu...	thmaer.zh@address.com	Tax Reform Tax Tip 2019-01: Fin...	Off	✉
Jan 29, 2019 at 10:30 AM	"Internal Revenu...	thmaerhsz7@address.com	Tax Reform Tax Tip 2019-01: Fin...	Off	✉
Jan 29, 2019 at 10:30 AM	"Internal Revenu...	thmaerhsz@address.com	Tax Reform Tax Tip 2019-01: Fin...	Off	✉

Clicking "Review Users at Risk" will create a new incident.

See users who clicked on malicious links

Review the list and send users to security awareness training

Enabling best practice in incident response

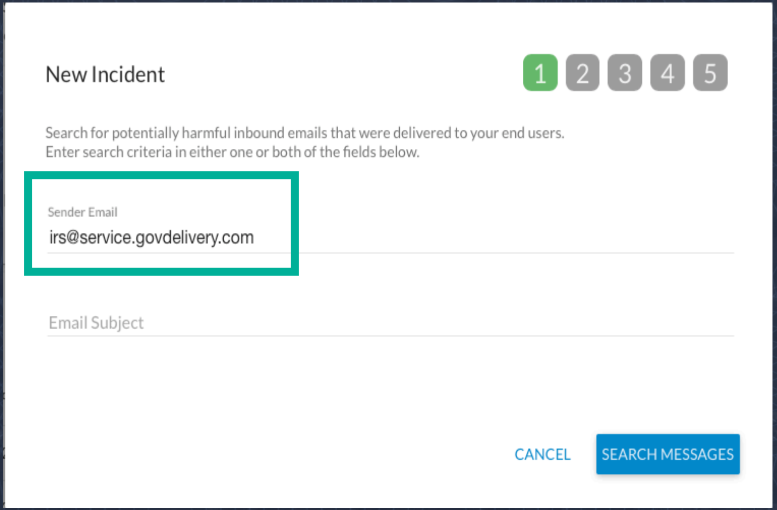
Educate Users

Automate Incident Response

Block Future Attacks

Automate remediation with few clicks

Fast search through all delivered mail



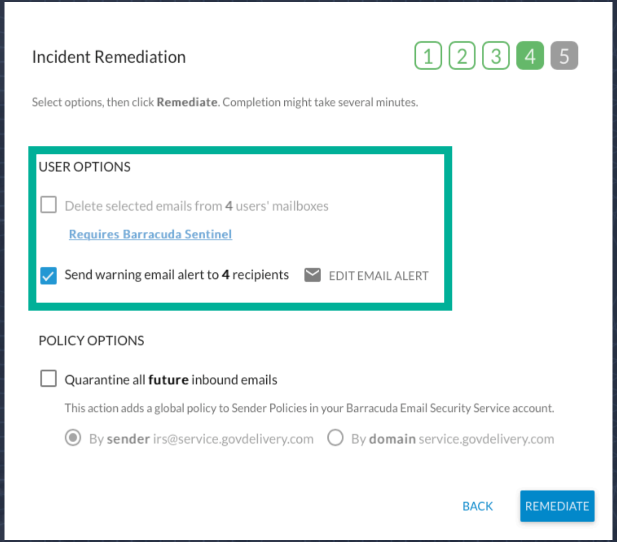
New Incident

Search for potentially harmful inbound emails that were delivered to your end users.
Enter search criteria in either one or both of the fields below.

Sender Email
irs@service.govdelivery.com

Email Subject

Delete emails from users inboxes with one click



Incident Remediation

Select options, then click **Remediate**. Completion might take several minutes.

USER OPTIONS

□ Delete selected emails from **4** users' mailboxes

Requires Barracuda Sentinel

☑ Send warning email alert to **4** recipients ✉ EDIT EMAIL ALERT

POLICY OPTIONS

□ Quarantine all **future** inbound emails

This action adds a global policy to Sender Policies in your Barracuda Email Security Service account.

● By **sender** irs@service.govdelivery.com ○ By **domain** service.govdelivery.com

Enables best practice in incident response

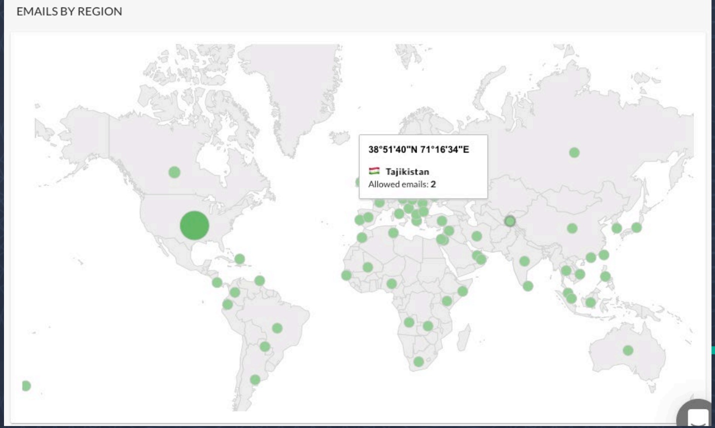
Educate Users

Automate Incident Response

Block Future Attacks

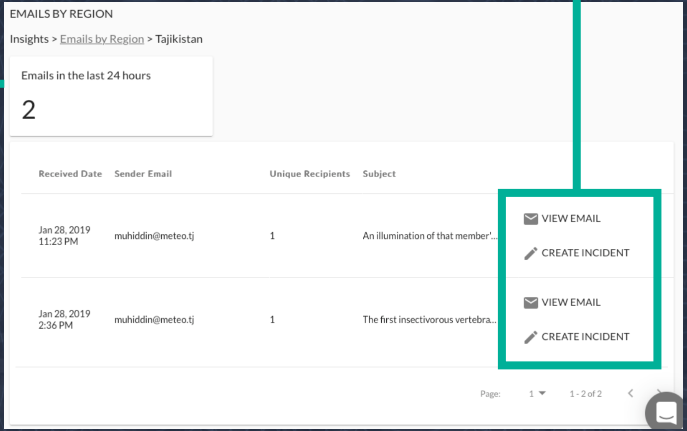
Proactively uncover malicious emails

Access Insights



Identify malicious mail based on geo-reporting

Block any future emails from the region through ESS



EMAILS BY REGION

Insights > Emails by Region > Tajikistan

Emails in the last 24 hours

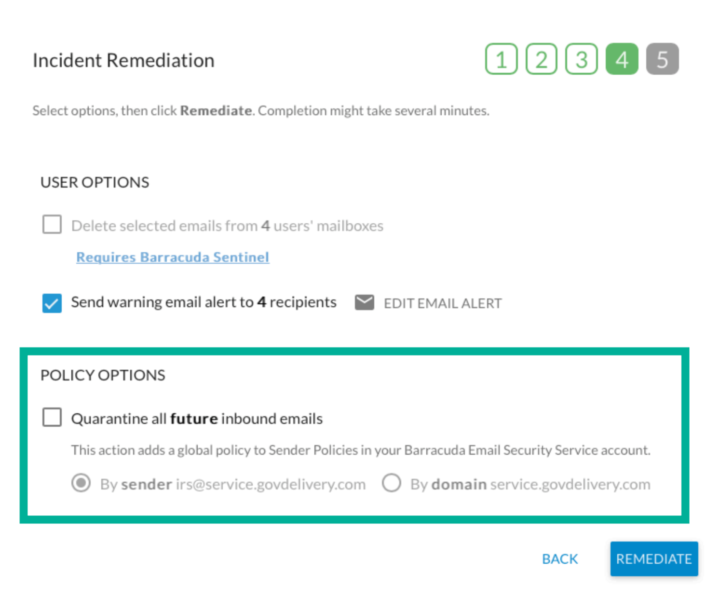
2

Received Date	Sender Email	Unique Recipients	Subject	
Jan 28, 2019 11:23 PM	muhiddin@meteo.tj	1	An illumination of that member'...	✉ VIEW EMAIL ✎ CREATE INCIDENT
Jan 28, 2019 2:36 PM	muhiddin@meteo.tj	1	The first insectivorous vertebra...	✉ VIEW EMAIL ✎ CREATE INCIDENT

Page: 1 ▾ 1 - 2 of 2

Thwart future attacks

Quarantine all future inbound email



Incident Remediation

Select options, then click **Remediate**. Completion might take several minutes.

USER OPTIONS

□ Delete selected emails from **4** users' mailboxes

Requires Barracuda Sentinel

☑ Send warning email alert to **4** recipients ✉ EDIT EMAIL ALERT

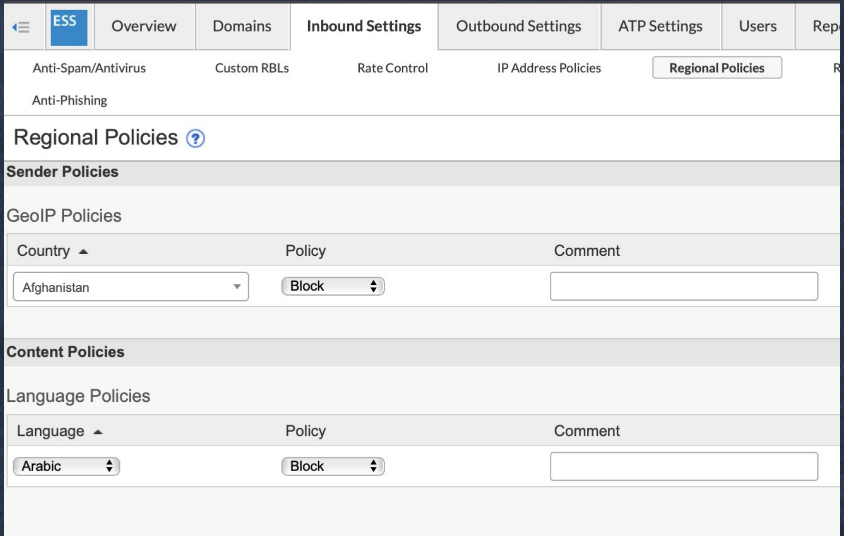
POLICY OPTIONS

□ Quarantine all **future** inbound emails

This action adds a global policy to Sender Policies in your Barracuda Email Security Service account.

● By **sender** irs@service.govdelivery.com ○ By **domain** service.govdelivery.com

Use Essentials to block all mail from a specific country



Regional Policies

Sender Policies

GeoIP Policies

Country ▲	Policy	Comment
Afghanistan	Block	

Content Policies

Language Policies

Language ▲	Policy	Comment
Arabic	Block	

Benefits of Forensics & Incident Response

- Significant IT time savings
- Expedited response to advanced threats
- Reduced impact of malicious email
- Focus on security education efforts
- Proactive threat hunting

Time savings is significant ROI

"When a suspicious email is reported we can remediate the environment in just a couple minutes … Before it could take hours to run down all these details. Barracuda Forensics is a big win for us."

Rick Cahoon, Director Enterprise Security & Support

WILBUR-ELLIS

Wilbur Ellis before Forensics

While users reported a few of these attacks every day, IT found it hard to act quickly in response to an incident.

IT had to search through tens of thousands of emails on their servers to see if any other of their 4,000 users received same message.

All affected users had to be contacted and warned to make sure not to open and remove malicious messages from their inboxes.

Lack of information and tools resulted in a manual, inefficient, and time-consuming process that could lead to further spread of attack.

Discovery on Incident Response

How do you deal with threats that get through?

Do you have process for users to report phishing emails?

How do you respond to reported phishing emails?

How long does it take you to respond and remediate against phishing attacks?

Do you carry out independent investigations?

What is the process for removing malicious emails delivered to users' inboxes?

How do you know which users need security awareness training?

Thank you

Barracuda

TECHSUMMIT19

BARRACUDA TECHNICAL SUMMIT