Email Security Redefined: An Introduction to GreatHorn

Protection Before, During, and After an Attack

Logistics

- You will be on mute
- Submit questions in the Q&A box (probably on the right side of your screen) in the GoToWebinar control panel
- Webinar is being recorded and will be available for replay
- Slides will be made available after the webinar

EJ Whaley
Solutions Engineer
GreatHorn

Lorita Ba
Vice President, Marketing
GreatHorn

GreatHorn

GreatHorn Email Security is a threat detection and response platform for protecting organizations ***Before***, ***During***, and ***After*** an email attack.

> With GreatHorn, we get a multi-layered approach to email security – not just prevention of known threats and targeted phishing attacks, but also in-the-moment user awareness training and incredibly effective remediation tools.
>
> As a result, my security team spends less time on email threat management and more time on other critical security areas.

Jason Shane

VP of Technology, Hersha Hospitality Management

HHM

Businesses at Risk: A Flawed Approach

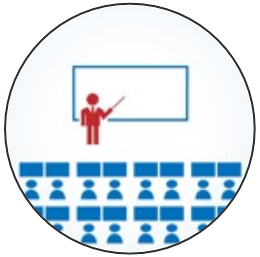
Despite
EMAIL SECURITY,
detection is failing

Email security tools fail to catch impersonations in

64%

of organizations

Despite
TRAINING,
users still engage with phish



50%

of professionals cannot differentiate advanced email threats from spam

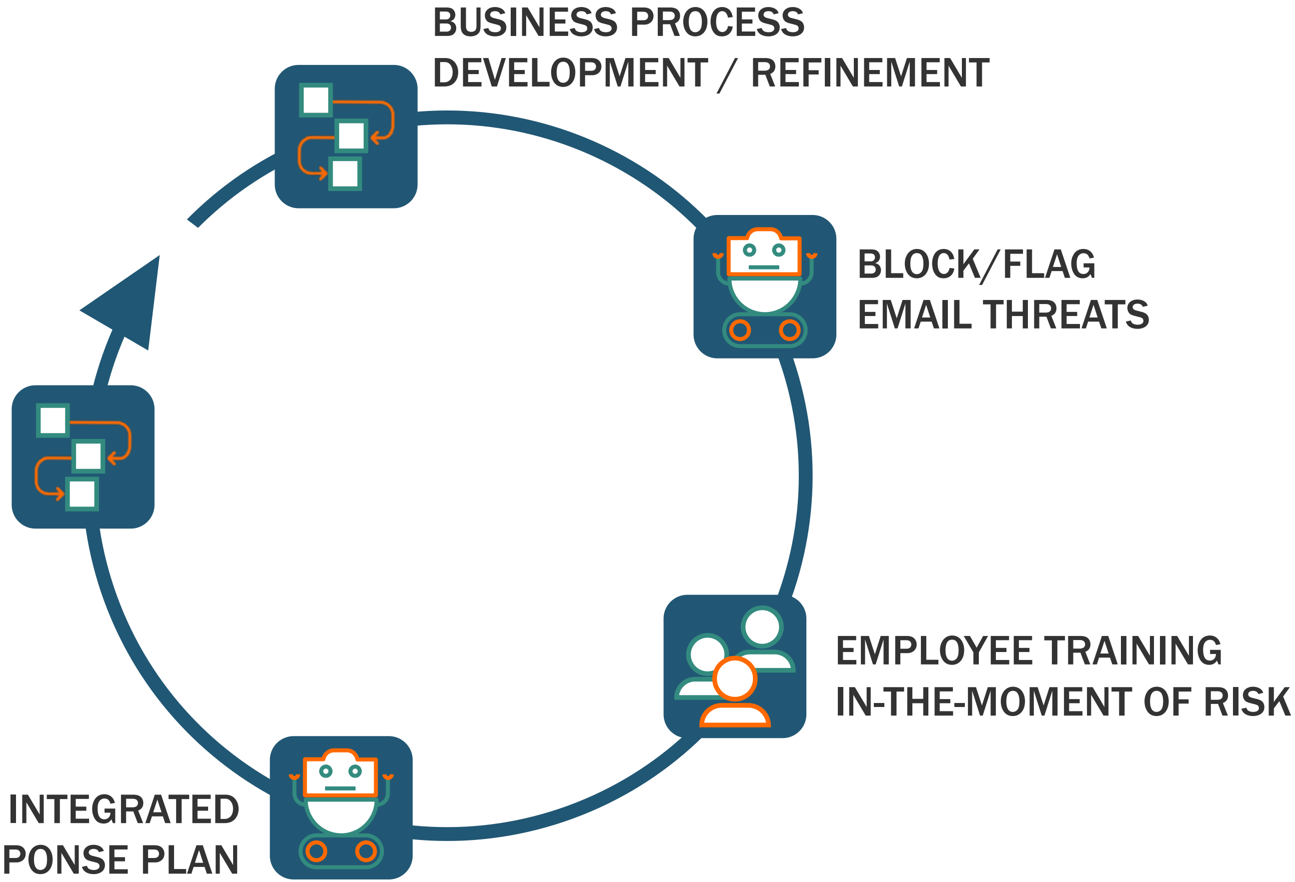
Despite
TOOLS & STAFFING,
IR is frequent / time-consuming

1 in **5**

security professionals have to take direct remediation action at least **weekly**

GreatHorn

We Need a Holistic Approach



BUSINESS PROCESS DEVELOPMENT / REFINEMENT

BLOCK/FLAG EMAIL THREATS

EMPLOYEE TRAINING IN-THE-MOMENT OF RISK

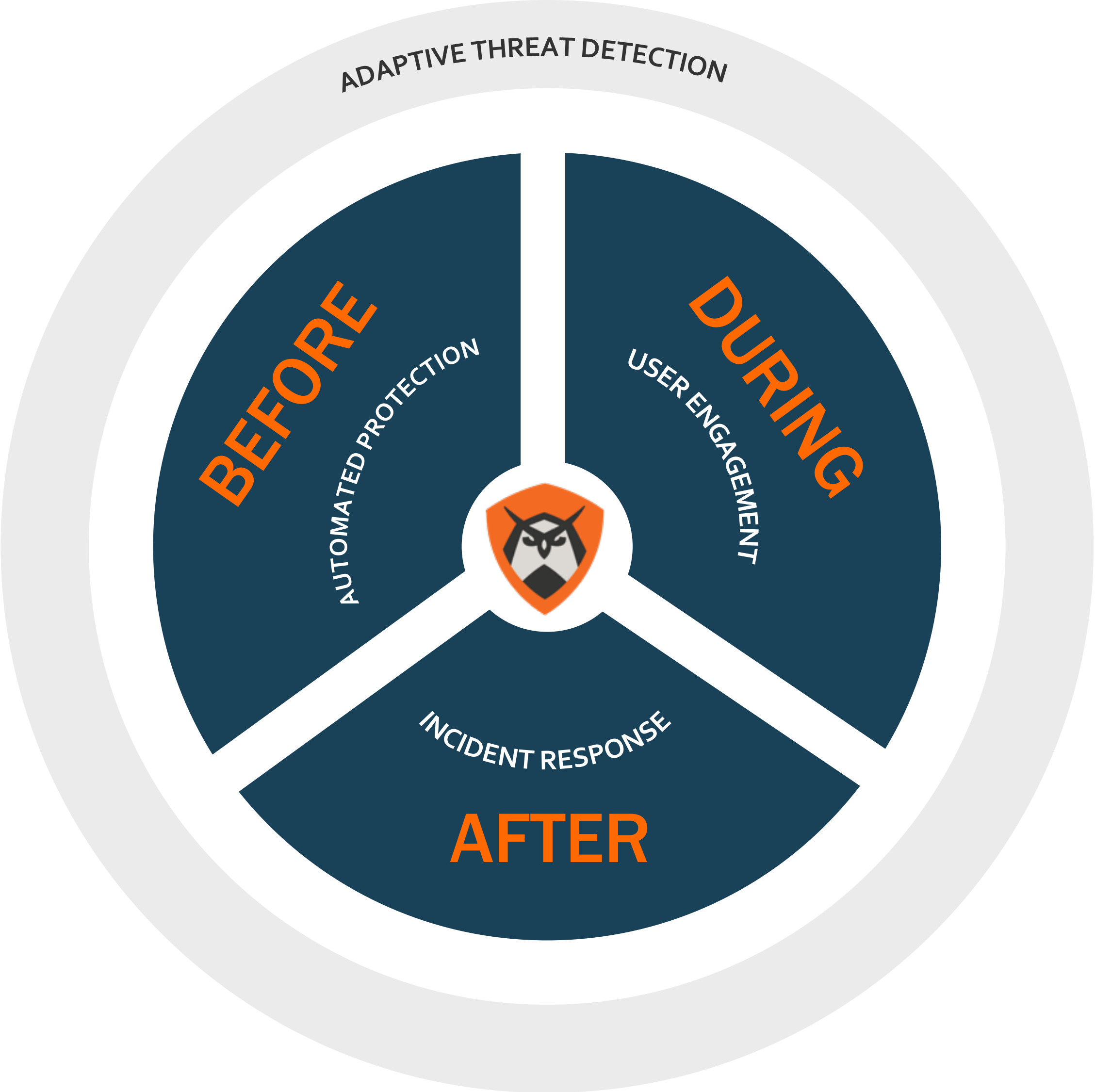
INTEGRATED RESPONSE PLAN

REVIEW, REVISE, REFINE

GreatHorn Platform

- Single unified model for comprehensive email security

- Complete Detection, Protection, and Response platform

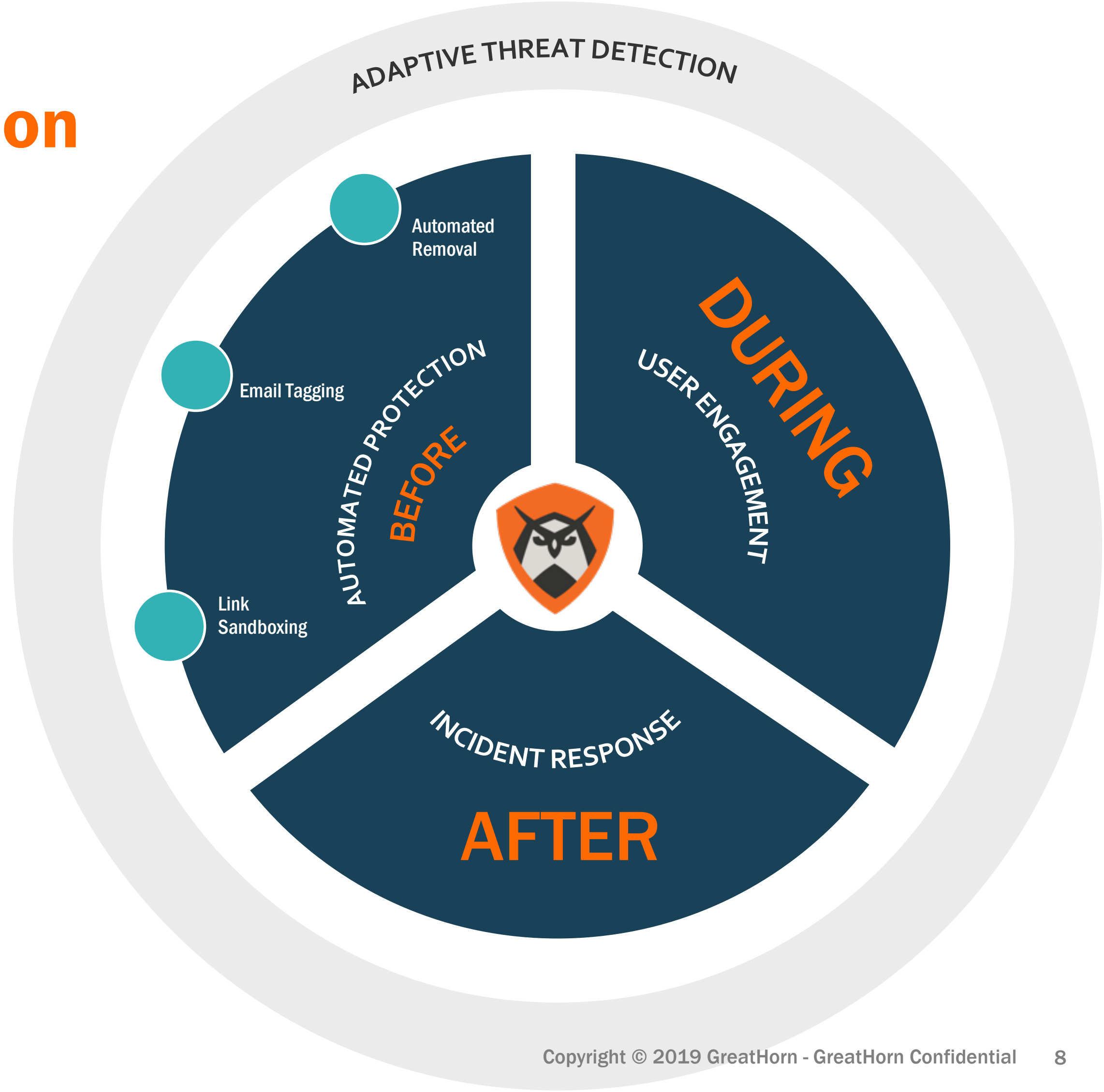


GreatHorn

BEFORE:
Automated Protection

> “We needed a robust solution that could protect us from zero-day attacks as well as phishing campaigns that were growing in frequency and sophistication. GreatHorn identifies more threats than other product.

SECURITY ANALYST
5,000 EMPLOYEE COMPANY



Threat Defense Analysis: Sample Customer

(Timeframe: 12 months, 20,000+ employees)

Email Security Environment:
Secure Email Gateway → Microsoft Advanced Threat Protection → GreatHorn

The following threats identified by GreatHorn were cleared by both the SEG and ATP.

792
internal email threats

16,140
credential theft attempts

2,173
malicious URLs

21,281
business email compromise attacks

50,000 threats missed by legacy email security

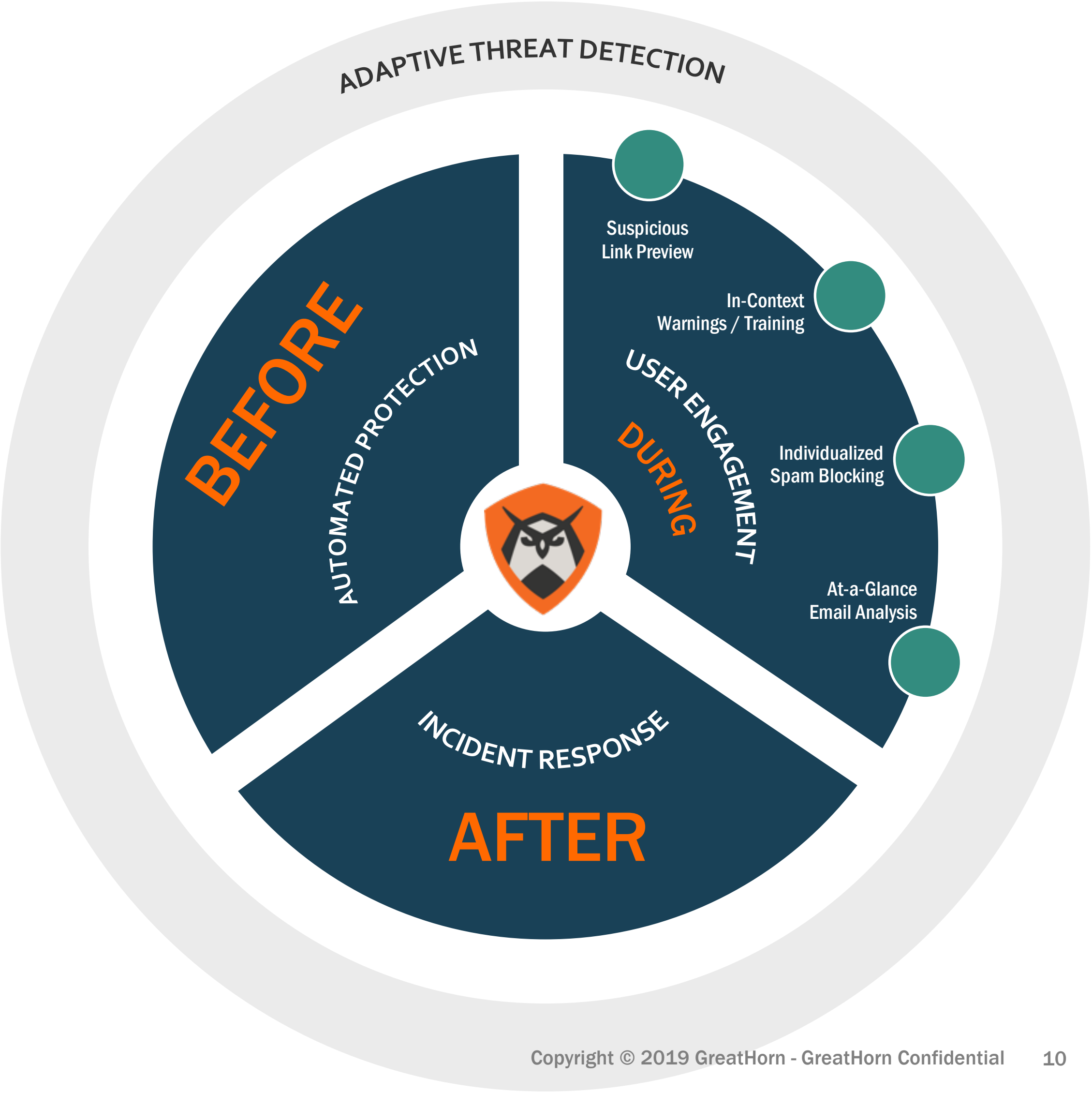
GreatHorn

DURING: User Engagement

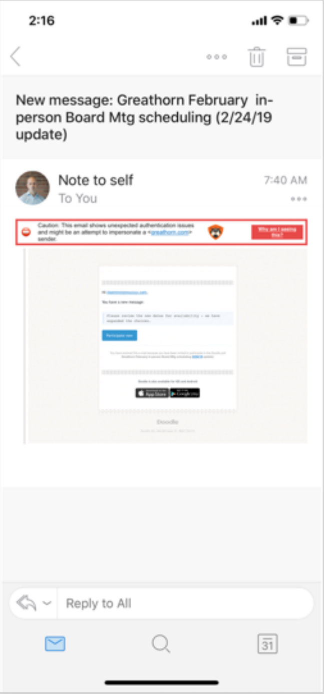
> Not only does GreatHorn have a unique ability to detect our more advanced attacks, but we can explain, in simple terms and at the exact moment when an employee could engage with a threat, that this might be a real attack.

HashiCorp

JEFF KOHRMAN
HEAD OF GLOBAL SECURITY


ADAPTIVE THREAT DETECTION
BEFORE
AUTOMATED PROTECTION
USER ENGAGEMENT
DURING
Suspicious Link Preview
In-Context Warnings / Training
Individualized Spam Blocking
At-a-Glance Email Analysis
INCIDENT RESPONSE
AFTER

Training in-the-Moment of Risk

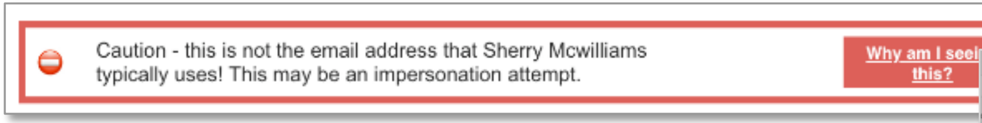


2:16

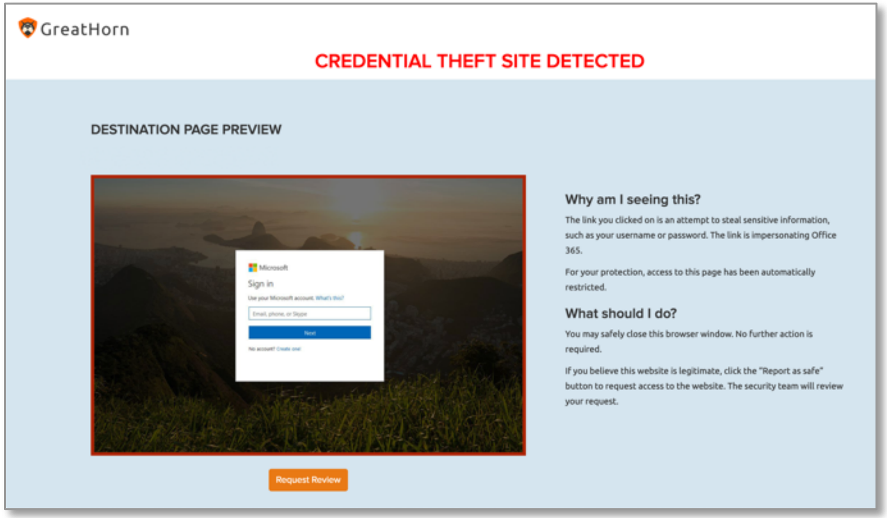
New message: Greathorn February in-person Board Mtg scheduling (2/24/19 update)

Note to self
To You
7:40 AM

Caution: This email shows unexpected authentication issues and might be an attempt to impersonate a <greathorn.com> sender.



Caution - this is not the email address that Sherry Mcwilliams typically uses! This may be an impersonation attempt.



GreatHorn

CREDENTIAL THEFT SITE DETECTED

DESTINATION PAGE PREVIEW

Why am I seeing this?

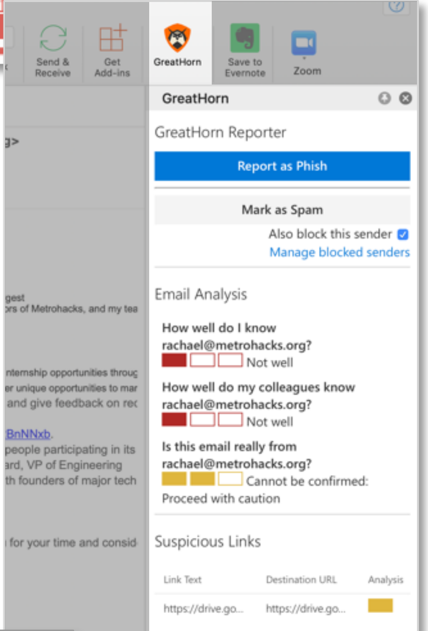
The link you clicked on is an attempt to steal sensitive information, such as your username or password. The link is impersonating Office 365.

For your protection, access to this page has been automatically restricted.

What should I do?

You may safely close this browser window. No further action is required.

If you believe this website is legitimate, click the "Report as safe" button to request access to the website. The security team will review your request.



GreatHorn

GreatHorn Reporter

Also block this sender ☑
Manage blocked senders

Email Analysis

How well do I know rachael@metrohacks.org?
🟥□□ Not well

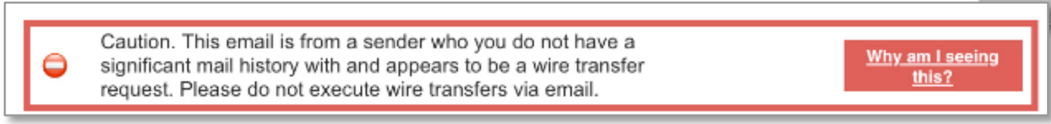
How well do my colleagues know rachael@metrohacks.org?
🟥□□ Not well

Is this email really from rachael@metrohacks.org?
🟨🟨□ Cannot be confirmed: Proceed with caution

Suspicious Links

Link Text	Destination URL	Analysis
https://drive.go...	https://drive.go...	🟨

gest
ors of Metrohacks, and my tea
nternship opportunities throug
er unique opportunities to mar
and give feedback on rec
BnNNxb.
people participating in its
ard, VP of Engineering
th founders of major tech
for your time and consid

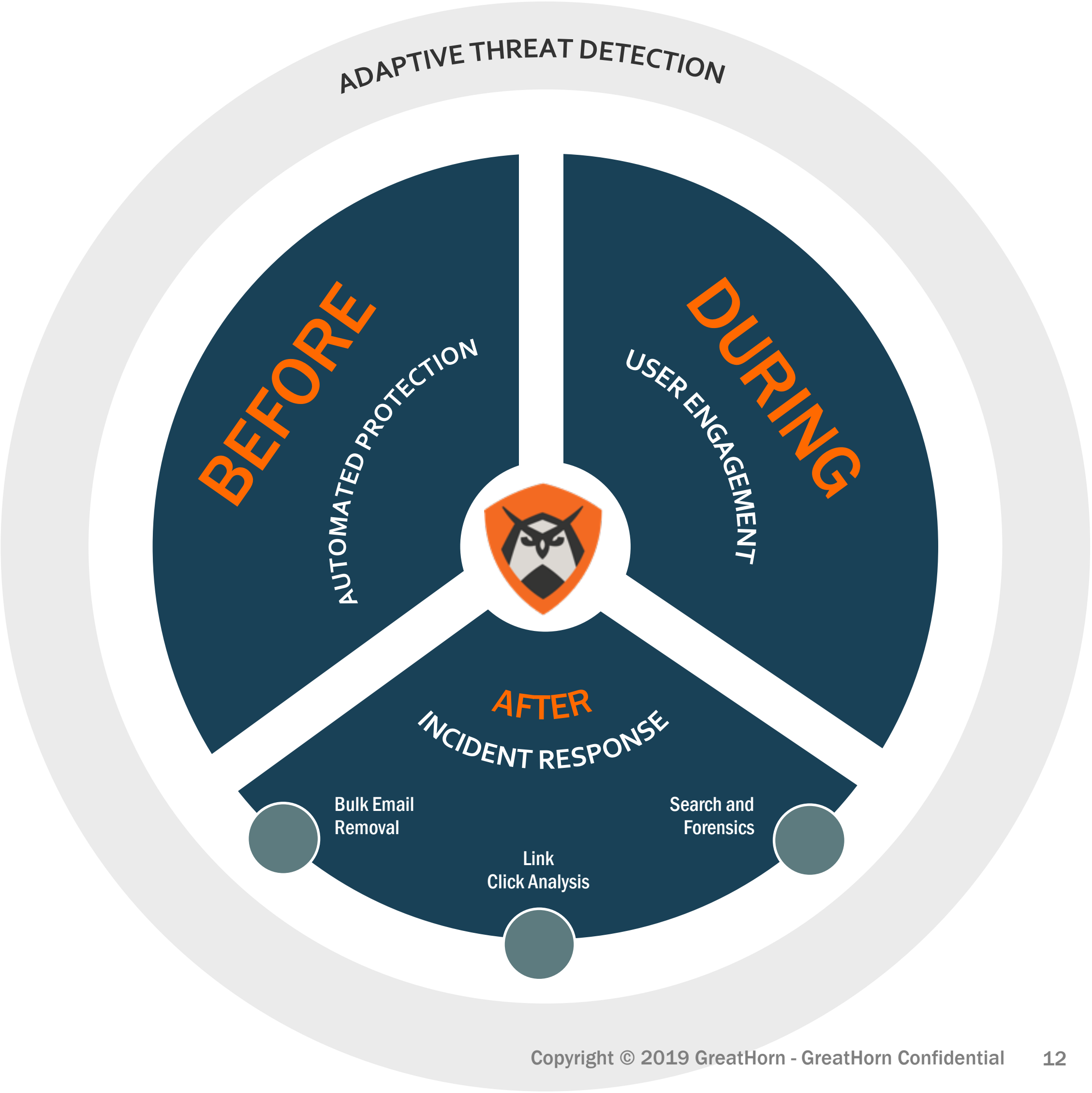


Caution. This email is from a sender who you do not have a significant mail history with and appears to be a wire transfer request. Please do not execute wire transfers via email.

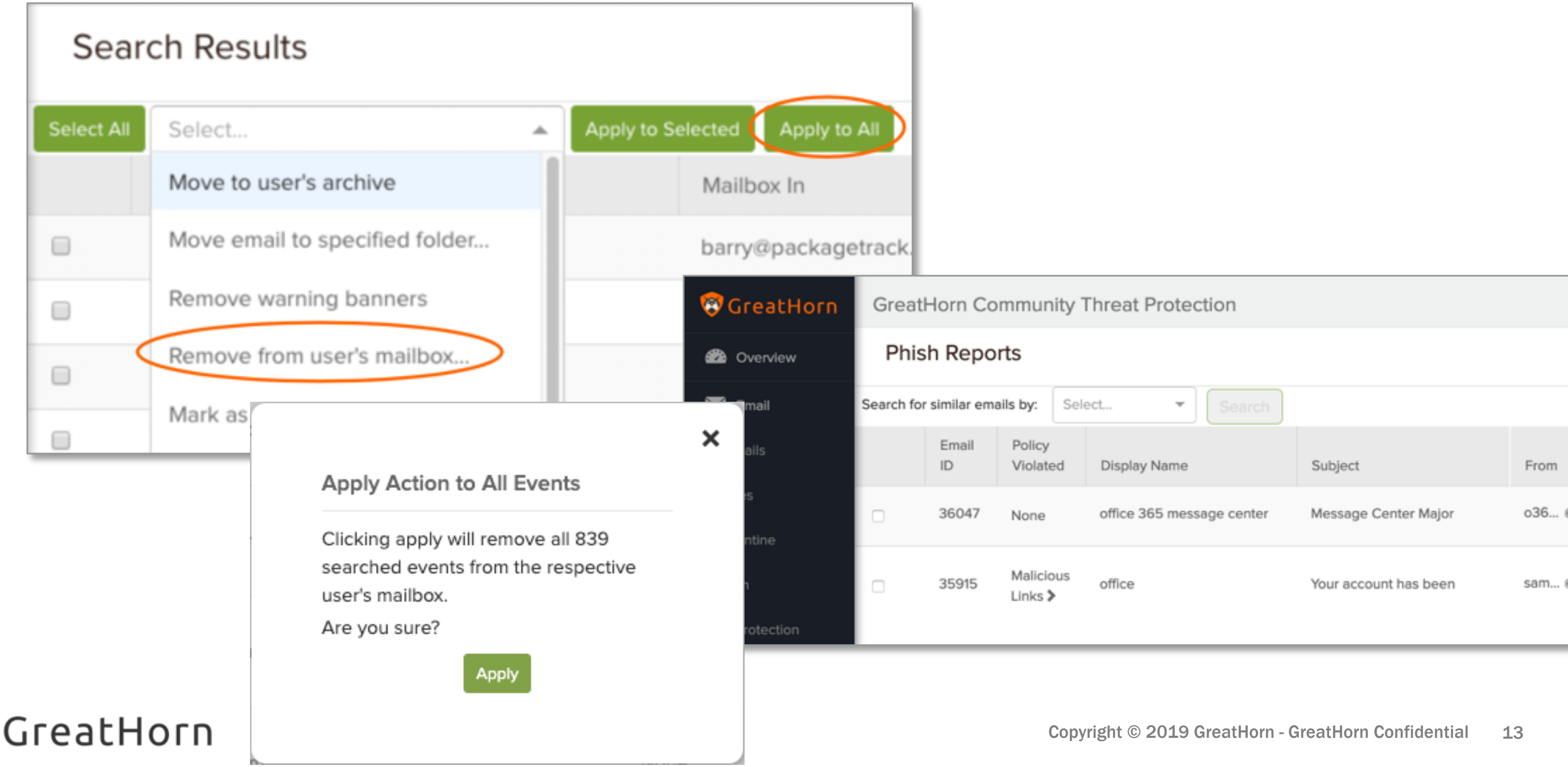
AFTER:
Incident Response

> Our incident response turnaround went from around 48 hours to less than five minutes due to GreatHorn.

CISO
HIGH-PROFILE TECHNOLOGY COMPANY



Simplify Threat Removal and Reduce Risk Exposure



Search Results

GreatHorn Community Threat Protection

Phish Reports

	Email ID	Policy Violated	Display Name	Subject	From
□	36047	None	office 365 message center	Message Center Major	o36...
□	35915	Malicious Links >	office	Your account has been	sam...

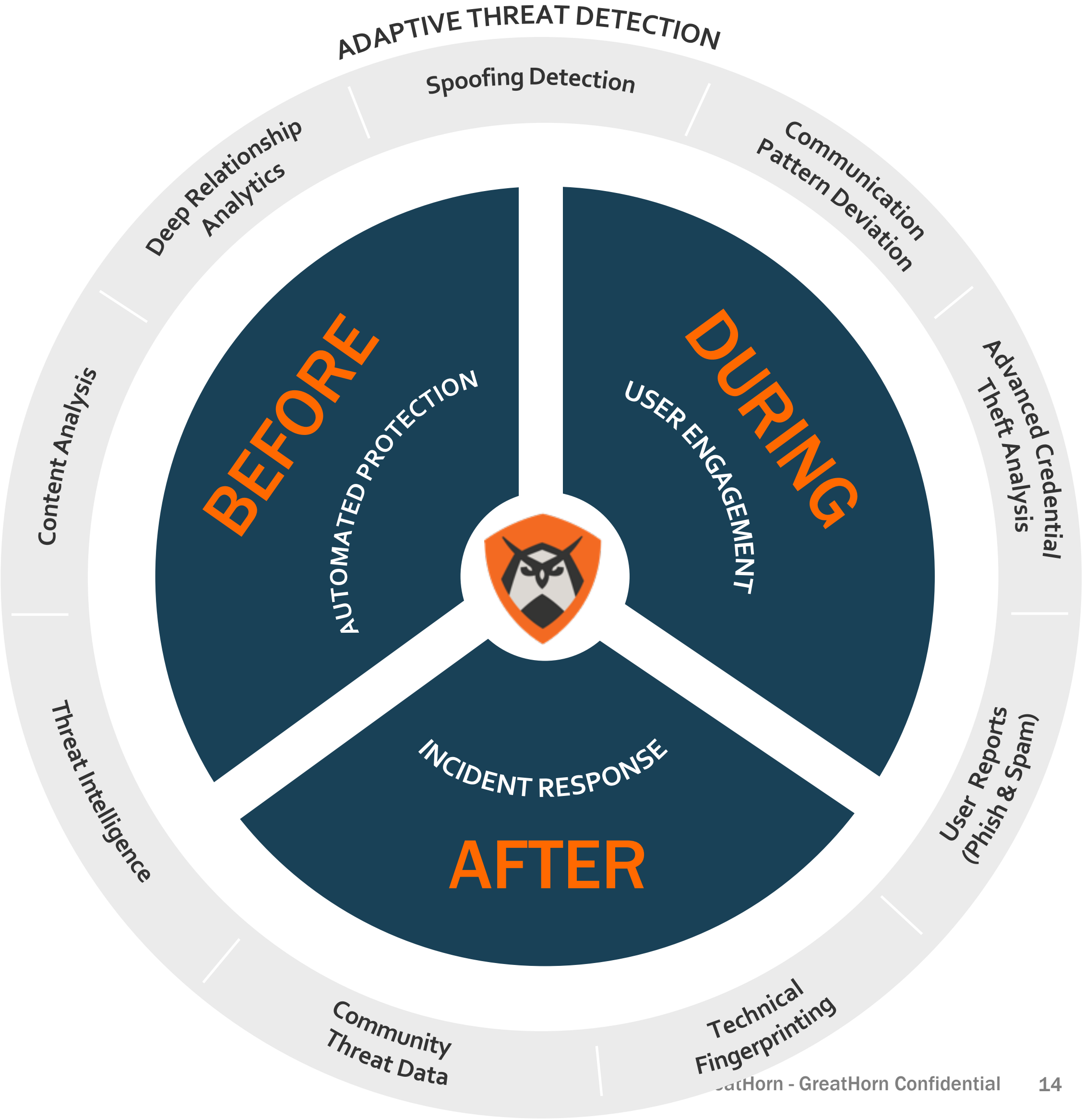
Apply Action to All Events

Clicking apply will remove all 839 searched events from the respective user's mailbox.

Are you sure?

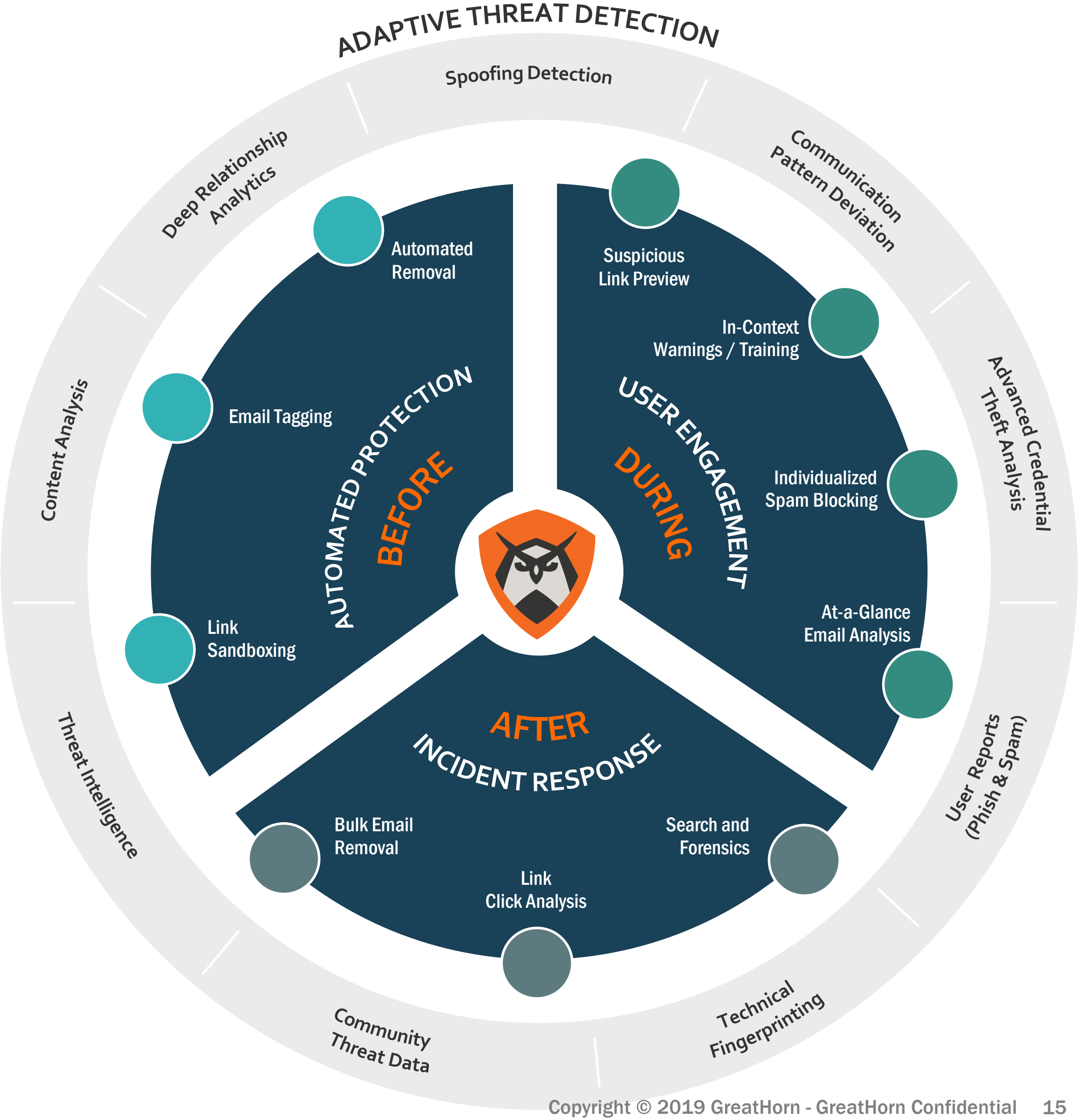
Adaptive Threat Detection

- Adapts over time as communication patterns and relationships change
- Baseline capabilities identify advanced threats more accurately than purely reactive methods
- Can be adjusted if organization has unique risk profile / tolerances



GreatHorn Platform

- Single unified model for comprehensive email security
- Complete Detection, Protection, and Response platform
- Seamlessly operates at enterprise scale, reading hundreds of millions of messages every month
- Patented technology for deep analysis of relationships, impersonations, and modern attacks



GreatHorn

GreatHorn Email Security Addresses Critical Gaps

CURRENT PAIN POINT	GREATHORN VALUE
Initial threat detection is failing	Proactive analysis blocks advanced threats more accurately
Users continue to engage with phish and "report" too many false positives	In-context user tools and alerts help users make better decisions in the moment
Incident response requires manual scripting and remediation	Simplified threat removal minimizes exposure time
Lack of visibility results in unnecessarily broad response	Deep forensics ensure admins quickly understand full incident impact

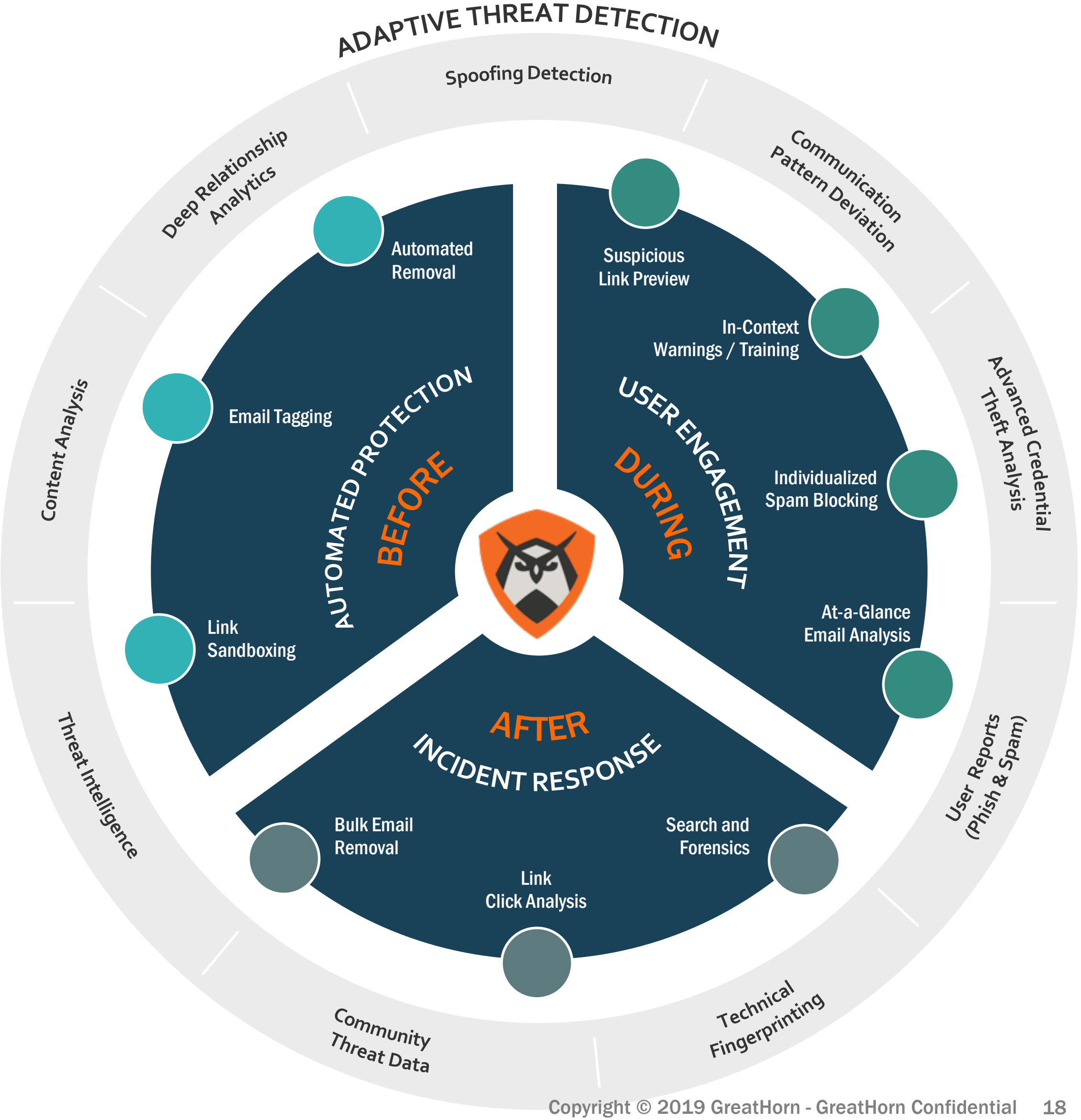
Multiple layers of defense returns trust to the inbox and time to the security team

GreatHorn

Demo

Questions

- Single unified model for comprehensive email security
- Complete Detection, Protection, and Response platform
- Seamlessly operates at enterprise scale, reading hundreds of millions of messages every month
- Patented technology for deep analysis of relationships, impersonations, and modern attacks



GreatHorn