



April 30, 2020

# Managing Automated Phishing Response at Scale, In the Cloud

**Best Practices**

# 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



**Matt Petrosky**  
Vice President, Customer Experience  
GreatHorn



**Patrick McDonald**  
Solutions Engineer  
GreatHorn

# Agenda

1. Incident response in the cloud – what matters
2. Why cloud native controls are replacing legacy solutions
3. Customer case studies
  1. Technology company
  2. Global telecommunication
4. Recap: check list
5. To complete your email security – what else to consider
6. Demo

# Automated - Incident Response and Remediation





## What Matters:

- > Detecting and capturing threats automatically

### Relationship Analysis Factors

- From Address Reputation <sup>?</sup>  
No Reputation x ▾
- From Domain Reputation <sup>?</sup>  
Moderate Reputation x ▾
- From Recipient Relationship <sup>?</sup>  
Weak Relationship x ▾
- From Organization Relationship <sup>?</sup>  
Weak Relationship x ▾

### Risk Analysis Factors

- OWL Score <sup>?</sup>  
Higher than: 50 (High)  
0  100
- Sender Anomaly Score <sup>?</sup>  
Higher than: 50 (High)  
0  100
- Authentication Risk Score <sup>?</sup>  
Higher than: 50 (High)  
0  100
- Name Spoofing Score <sup>?</sup>  
Higher than: 50 (High)  
0  100
  - Domain Name
  - Display Name

### Policy Actions

- Move to Trash <sup>?</sup>
- Quarantine Message <sup>?</sup>  
Send Quarantine Admin Alert To:  
Please hit enter after each entry.  
 securityoperations@company.com
- End User will receive a notification email:
  - When an email is quarantined from their mailbox.
  - When an email is released from quarantine back to their mailbox.

# Manual - Incident Response and Remediation

## What Matters:

- > Time To Detection
- > Time To Remediation (speed of the remediation)
- > Integration with other security tools like SOAR using APIs
- > Giving your security exerts the tools they can use to respond quickly

The screenshot displays a 'Search Results' table with columns for 'Mailbox In', 'Return Path', 'Subject', and 'Policy Violated'. A context menu is open over the table, with 'Remove from user's mailbox...' highlighted. An orange box highlights the 'Apply Action to All Events' modal dialog, which contains the following text:

**Apply Action to All Events** ✕

Clicking apply will remove all 2418 searched events from the respective user's mailbox.

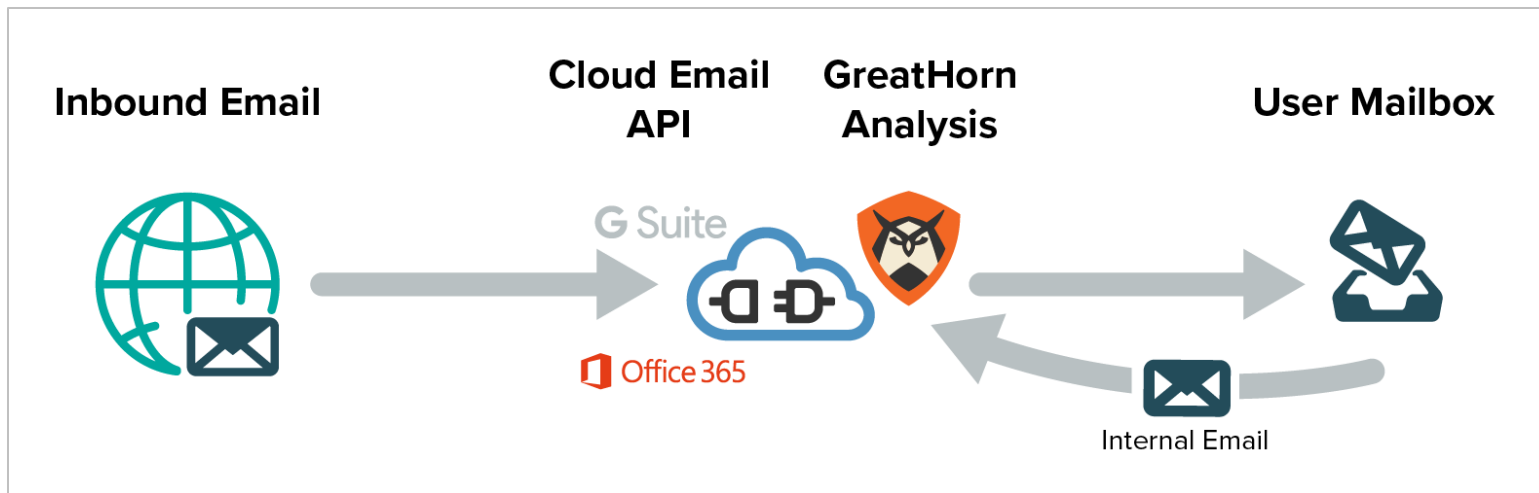
Are you sure?

**Apply**

		Mailbox In	Return Path	Subject	Policy Violated	
✕		Move to user's archive				
☑	3	Move email to specified folder...	toby@flyingdeliveries.com	gmail.com	"Invoice - Payment Due"	Name Spoofs
☑	2	Remove warning banners	lawrence@flyingdeliveries.com	gmail.com	"Invoice - Payment Due"	Name Spoofs
☑		Remove from user's mailbox...	emily@flyingdeliveries.com	gmail.com	"Invoice - Payment Due"	Name Spoofs
☑		Mark as Reviewed	aaron@flyingdeliveries.com	gmail.com	"Invoice - Payment Due"	Name Spoofs
☑	3	Mark as Unread				
☑	36583	smw189038@gmail.com	morgan@flyingdeliveries.com	gmail.com	"Invoice - Payment Due"	Name Spoofs
☑	36571	smw189038@gmail.com	morgan@flyingdeliveries.com	gmail.com	"Invoice - Payment Due"	Name Spoofs
☑	36570	smw189038@gmail.com	emily@flyingdeliveries.com	gmail.com	"Invoice - Payment Due"	Name Spoofs
☑	36574	smw189038@gmail.com	toby@flyingdeliveries.com	gmail.com	"Invoice - Payment Due"	Name Spoofs
☑	36577	smw189038@gmail.com	lawrence@flyingdeliveries.com	gmail.com	"Invoice - Payment Due"	Name Spoofs
☑	36582	smw189038@gmail.com	aaron@flyingdeli			
☑	36563	smw189038@gmail.com	emily@flyingdeli			
☑	36568	smw189038@gmail.com	lawrence@flying			
☑	36566	smw189038@gmail.com	aaron@flyingdeli			
☑	36564	smw189038@gmail.com	toby@flyingdeliv			
☑	36567	smw189038@gmail.com	morgan@flyingd			
☑	36555	smw189038@gmail.com	morgan@flyingd			
☑	36559	smw189038@gmail.com	emily@flyingdeli			
☑	36553	smw189038@gmail.com	emily@flyingdeli	gmail.com	"Invoice - Payment Due"	Name Spoofs

# Incident Response and Remediation

Why cloud native controls are replacing legacy email gateways



# Why Cloud Native Controls Are Replacing Legacy Solutions

## Secure Email Gateways



GreatHorn

EFFECTIVENESS



Automated remediation is based on threat intel and can take 15-20 min to identify / remove threats



Email removal built into both policy results and search screens to make remediation easy and fast

SIMPLICITY



Lacking post-delivery modification or remediation



Robust and simple-to-use search capabilities

TIME



Limited manual remediation capabilities with reliance on PowerShell (O365)



Find and remediate incidents via APIs in seconds



**JEFF KOHRMAN**  
Global Security Leader

# We Mitigated a BEC Attack Within Five Minutes

## > Before

- + “We had to use our email provider’s API to manually drudge email attacks or build custom scripts to intercept messages”

## > With GreatHorn:

- + “We’ve gone from detecting and responding to business email compromise within 48 hours at best, to having instant alerts, able to catch these events in real time”
- + **“We couldn’t have done that without GreatHorn”**



# Global Telecommunications Company

- Over 20,000 employees
- Located worldwide
- Many global locations

## From Days To Minutes

- > Before:
  - + the Help Desk team addressed malicious emails by writing a custom script that went through the company's entire O365 tenant (and its hundreds of domains) to look for matching emails.
  - + The process took days, leaving the team to identify alternative ways to reduce risk such as blocking links.
- > **With GreatHorn:**
  - + **Pushing a button to easily see, match, and delete email threats across the global organization**

# Remediation In The Cloud – Checklist:

- > Automated and manual remediation
- > Bulk remediation, remediation at scale
- > Search and forensics capabilities - Robust and simple-to-use
- > Post delivery capabilities
- > SPEED!!! remediate incidents even across:
  - + thousands or tens of thousands of users
  - + multiple domains at once
- > Integration with other security tools
- > Select a vendor that you can trust

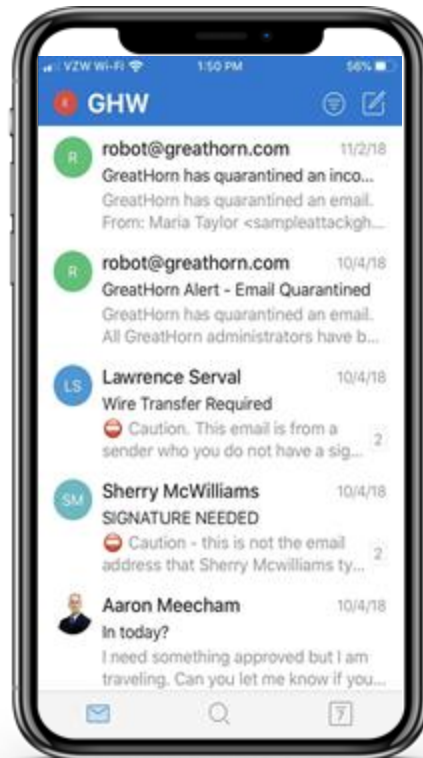


# Demonstration

---

# Comprehensive Protection

- > Do more than just train users
- > Pull them into the loop
- > Show them real-time alerts that are useful



CAUTION: CFO Sherry McWilliams does not typically email from smw189038@gmail.com. Do not engage with, download attachments or click links from unknown senders



'Why am I seeing this?'

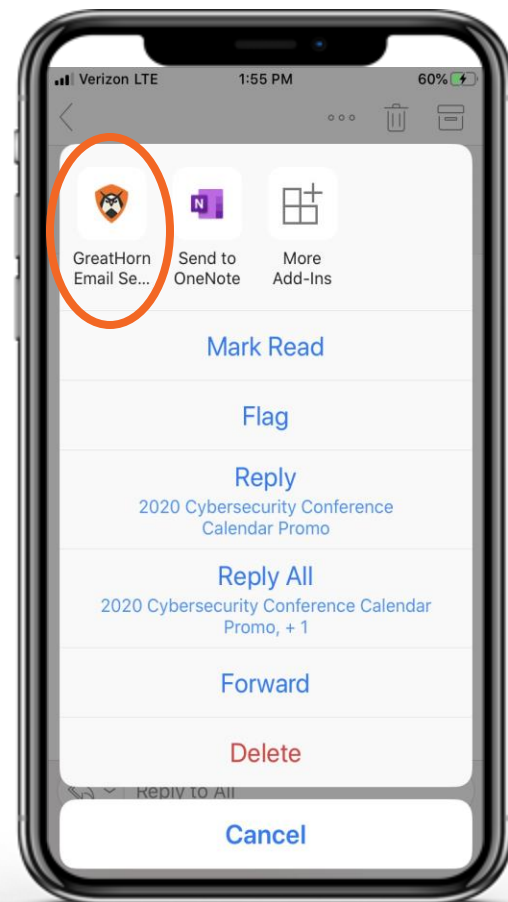
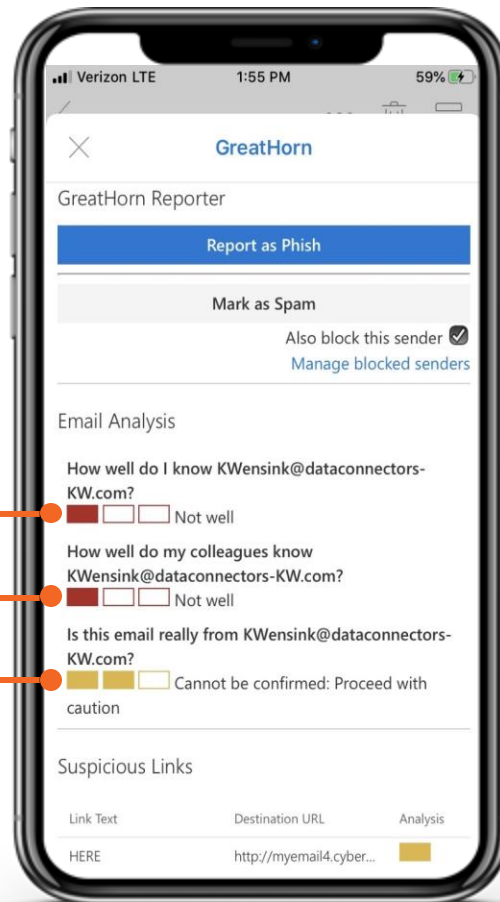
# Empower Your Users

- > Phish reporting with context
- > Relationship analysis
- > In-the-moment education

"I've never engaged with this user"

"No one at my organization has ever engaged with this user"

"Is this really who they say it is?"



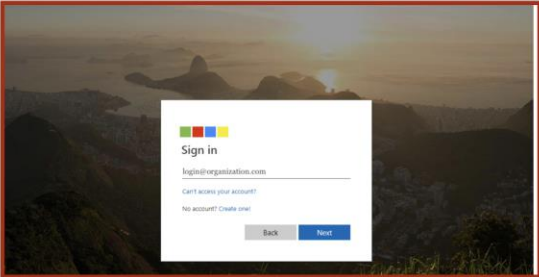
# Protecting Against Malicious Links

- > Link Protection
- > Educating the users real-time
- > Safeguard users from suspicious & malicious links

### Suspicious Link Detected

**DESTINATION PAGE PREVIEW**

Hosting Domain: <http://www.jerrysflowershop.com/user-login/emilypost-flying-deliveries>



**Why am I seeing this?**

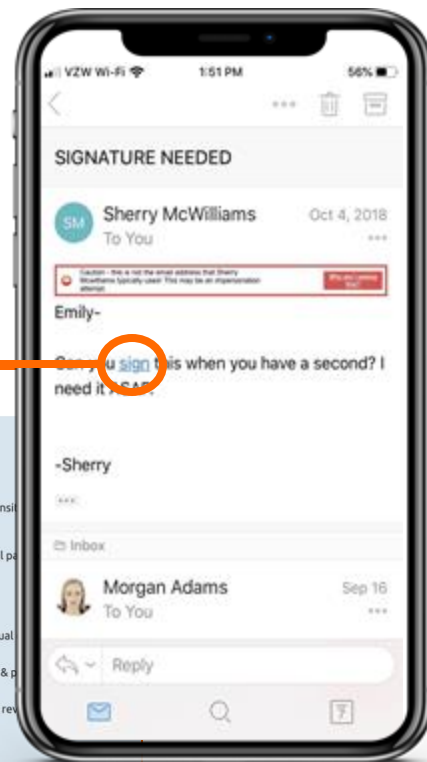
You have clicked on a link that may be an attempt to steal sensitive information such as your username or password.

Cybercriminals often create fake "phishing" websites to steal personal information and malware.

**What should I do?**

- 1 Carefully review both the website preview and the actual destination page.
- 2 Watch out for fake login screens requesting username & password.
- 3 "Take Me There" to visit the website anyway. "Request Review" to request a review of the link that the website is trustworthy.

[Credential Theft Check](#) [Request Review](#) [Take Me There](#)



# GreatHorn Email Security

- > **Detect** – How to build a new policy
  - + Situational and timely
- > **Protect** – How to give users better context
  - + Reinforce new or existing policies
  - + Deploy GreatHorn Reporter widely
- > **Respond** – How to search and remove identified threats
  - + Respond to phish reports
  - + Search for new threats





# Q&A

---



# Follow Up & Where to Learn More

Recording and Slides will be sent out following today's session



Blog: [Automated Phishing Response Tools: 4 Things to Consider](#)



Blog: [Email Threat Remediation: The Secret Weapon to Fighting Phishing](#)



Datasheet: [GreatHorn Email Security](#)



Contact Us: [info@greathorn.com](mailto:info@greathorn.com)



**Thank you.**

---