Our mission: Protect People, Defend Data

proofpoint. | Protect People.
Defend Data.

Risikofaktor Mensch

Wie aktuelle Bedrohungen den Mitarbeiter in das Zentrum Ihrer Sicherheitsstrategie rücken

Cybersecurity | Summit Masterclass | 12:00 Uhr

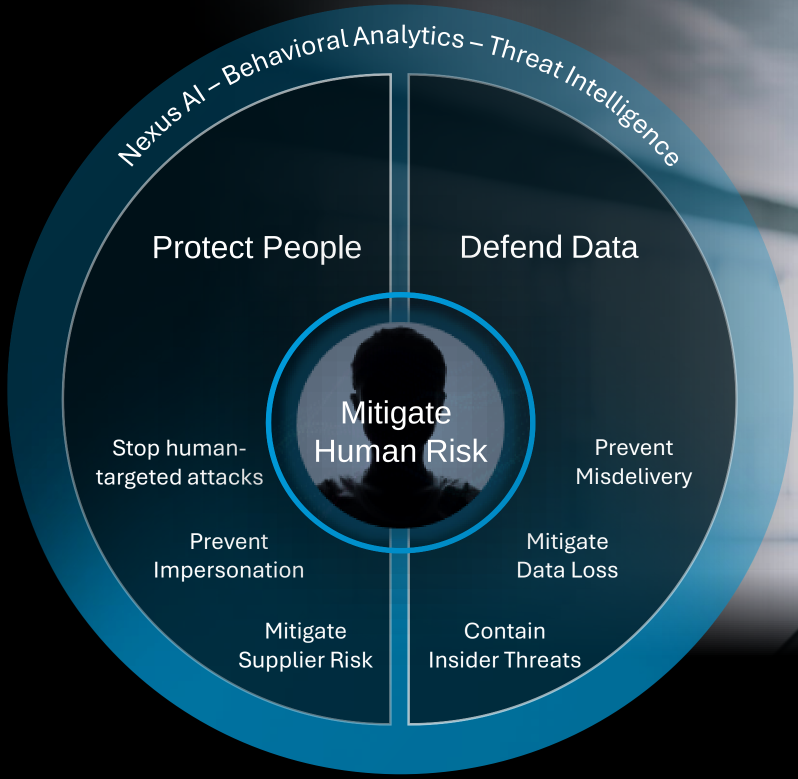
Hannes Schneider (Sr. Manager Sales Engineer)
Benjamin Renner (Sr. Named Account Manager)

HUMAN CENTRIC CYBER SECURITY

HUMAN CENTRIC CYBERSECURITY

Proofpoint

Protecting over half a million customers,
including 87 of the Fortune 100.



Nexus AI – Behavioral Analytics – Threat Intelligence

Protect People

Defend Data

Mitigate
Human Risk

Stop human-targeted attacks

Prevent Impersonation

Mitigate Supplier Risk

Prevent Misdelivery

Mitigate Data Loss

Contain Insider Threats

2024/2025 Business and Attack Trends

HUMAN CENTRIC CYBER SECURITY

Rise of AI

Improved phishing
Automated malware
Scaled attacks
Protecting data

Digital Transformation

Proliferation of attack and exfiltration surface

Social Engineering

Increased innovation and tools from threat actors targeting people

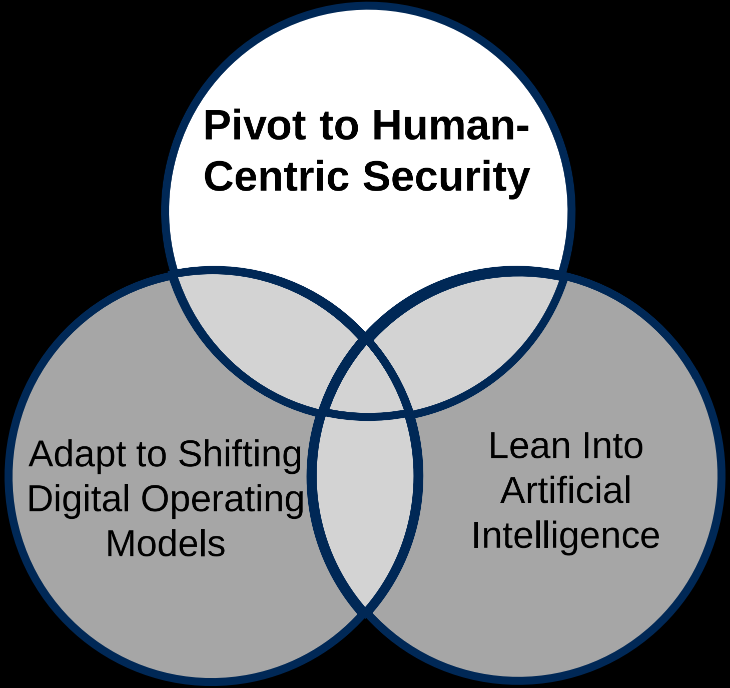
Increased Risk Across Attack Chain

- Recon
- Initial compromise
- Persistence
- Info gathering
- Priv Esc
- Lateral movement
- Staging
- Impact

© 2024 Proofpoint Inc.

Gartner 2024/2025 CISO Strategic Imperatives

HUMAN CENTRIC CYBER SECURITY



Pivot to Human-Centric Security

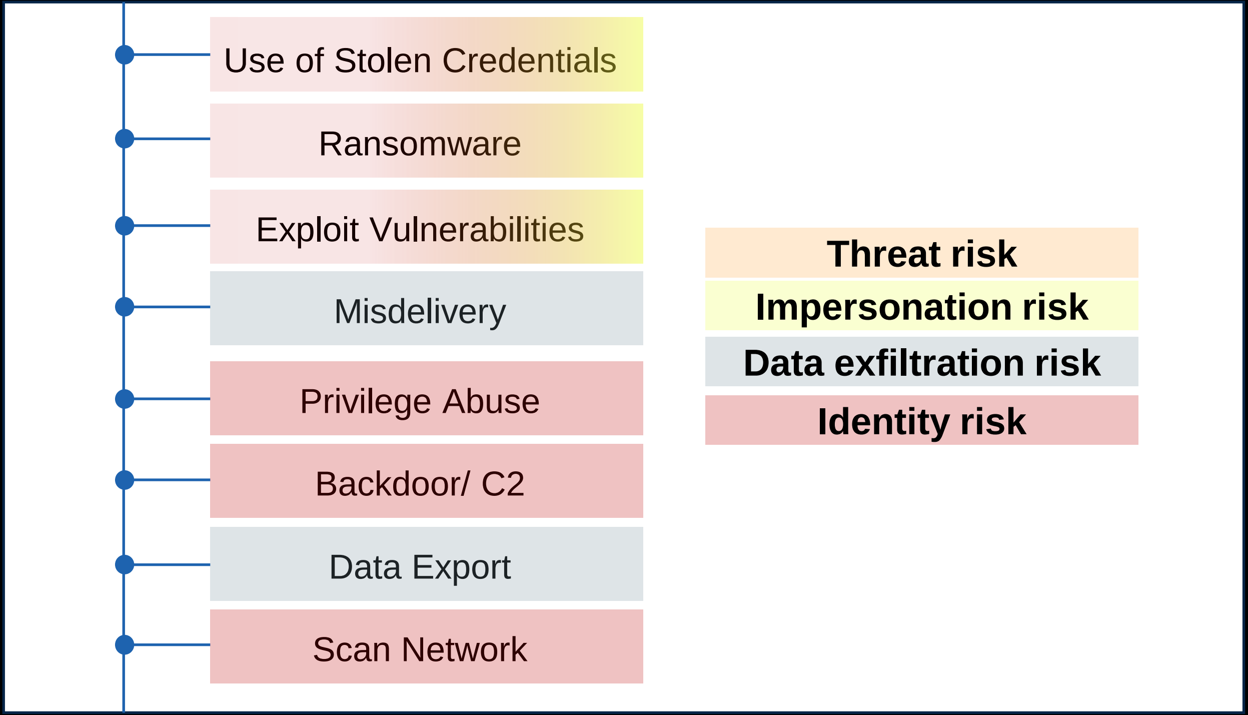
Adapt to Shifting Digital Operating Models

Lean Into Artificial Intelligence

Gartner, *Leadership Vision for 2024: Security and Risk Management* | Tom Scholtz, Lisa Neubauer | January 2024

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner Calls Out Risks in Addition to Phishing



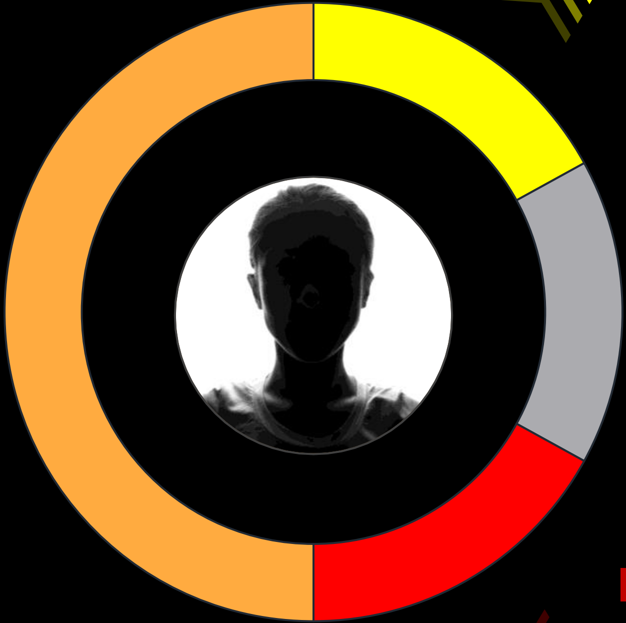
- Use of Stolen Credentials
- Ransomware
- Exploit Vulnerabilities
- Misdelivery
- Privilege Abuse
- Backdoor/ C2
- Data Export
- Scan Network

Threat risk
Impersonation risk
Data exfiltration risk
Identity risk

proofpoint.

© 2024 Proofpoint Inc.

The Four Dimensions of Human Risk



Impersonation Risk

- Internal targeting
- 3rd parties/customers
- Compromised/spoofed suppliers

Threat Risk

- BEC
- Malware
- Social Engineering
- Credential Phishing

Data Loss Risk

- Careless user
- Compromised user
- Malicious user

Identity Risk

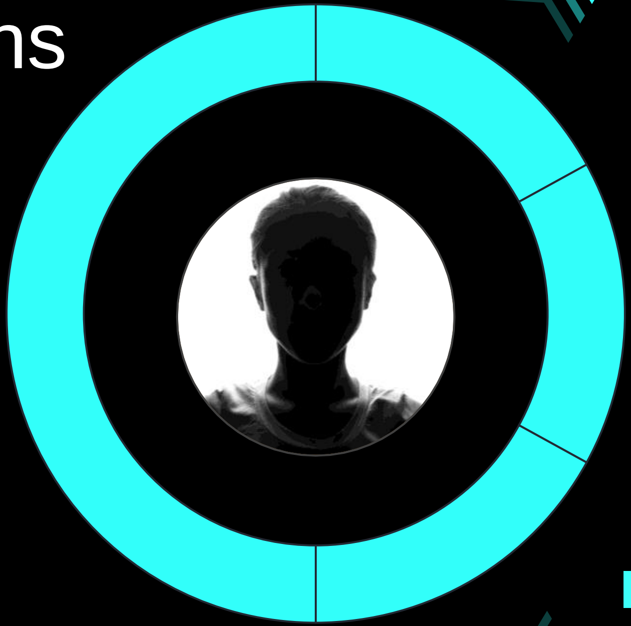
- M365 ATO
- Active Directory PrivEsc and lateral movement

proofpoint.

© 2024 Proofpoint Inc.

Protecting People with Human-centric Security Solutions

HUMAN CENTRIC CYBER SECURITY



Threat Protection

99.9%+
inbound threats

Impersonation Protection

100% direct spoofing risk reduction with authenticated email

Misdelivery Protection

65% data loss risk reduction

Identity Protection

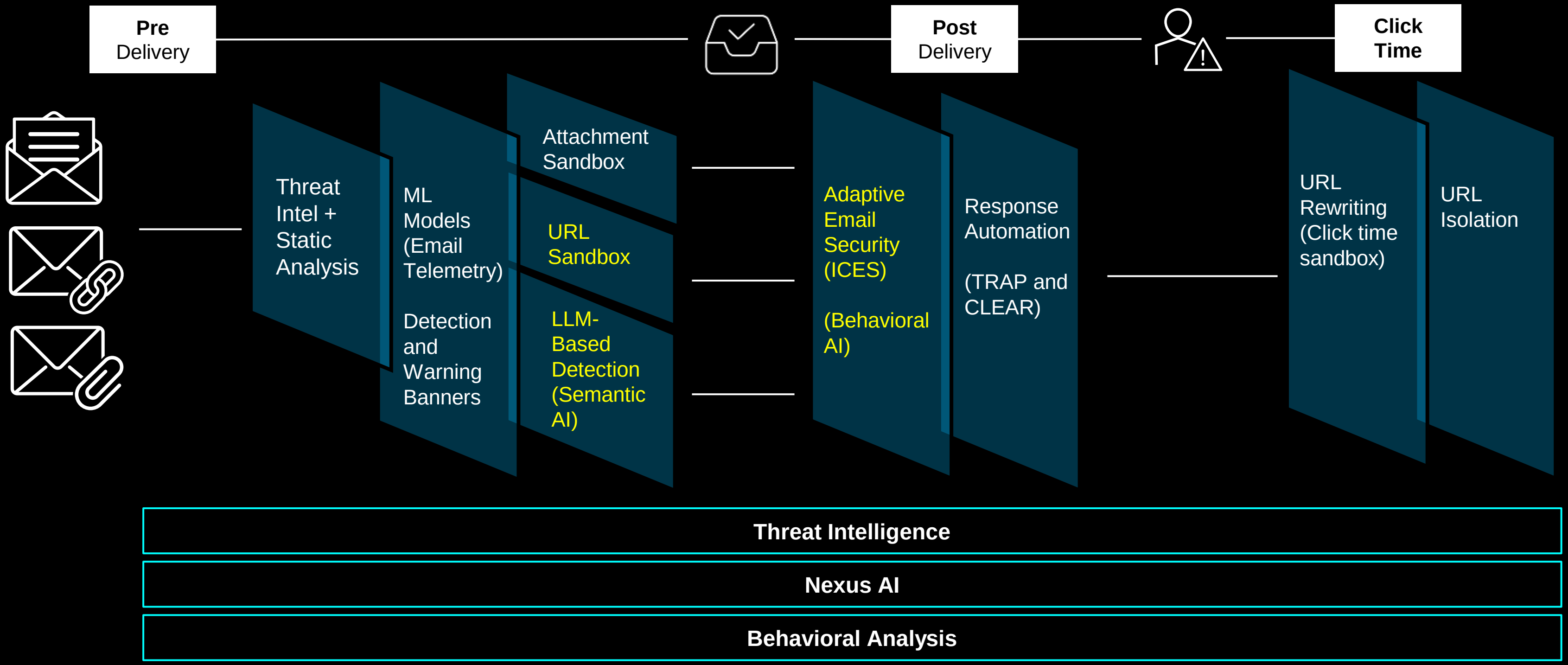
80% AD, M365, and identity risk reduction

© 2024 Proofpoint Inc.

Proofpoint People Protection

Redefining Email Security: End-to-end, Complete and Continuous

HUMAN CENTRIC CYBER SECURITY



Pre Delivery

Post Delivery

Click Time

Threat Intel + Static Analysis

ML Models (Email Telemetry)

Detection and Warning Banners

Attachment Sandbox

URL Sandbox

LLM-Based Detection (Semantic AI)

Adaptive Email Security (ICES)

(Behavioral AI)

Response Automation

(TRAP and CLEAR)

URL Rewriting (Click time sandbox)

URL Isolation

Threat Intelligence

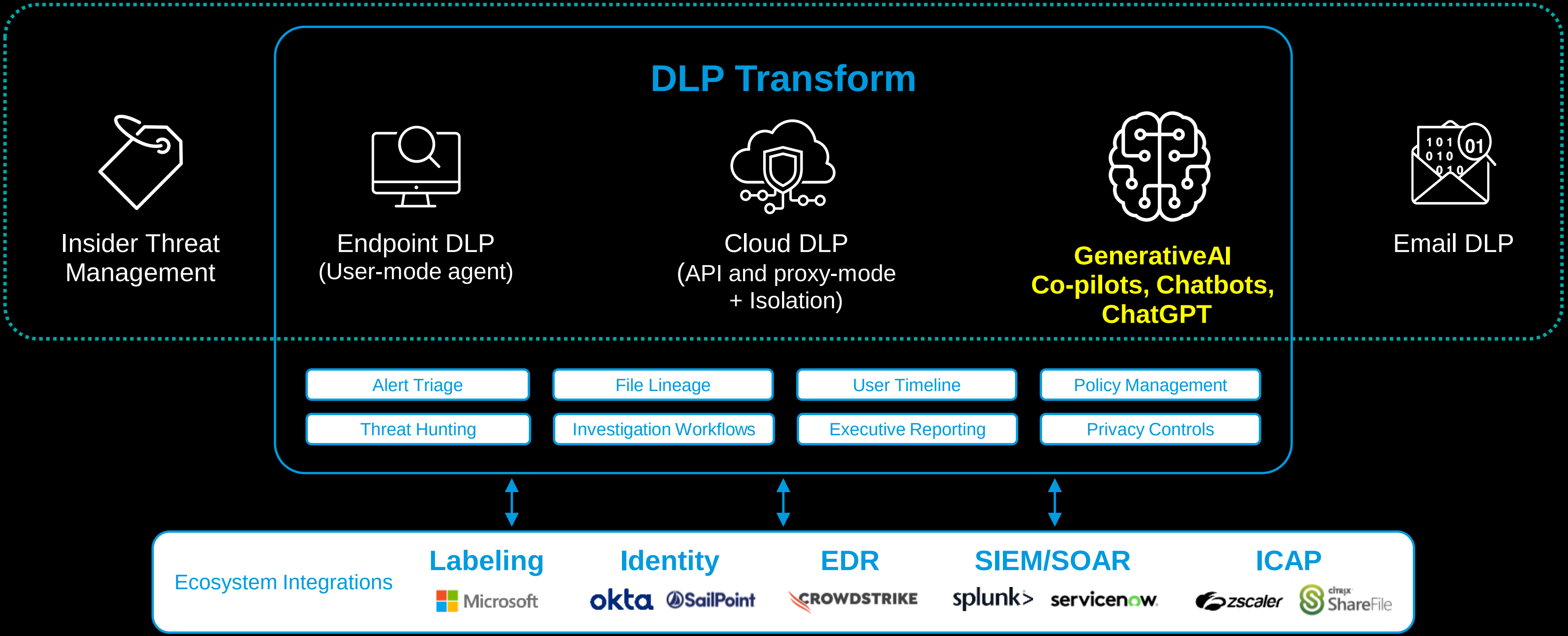
Nexus AI

Behavioral Analysis

© 2024 Proofpoint Inc.

Proofpoint Information Protection

Defend Data Across All Channels including Co-pilots and Chat GPT



DLP Transform

Insider Threat Management

Endpoint DLP
(User-mode agent)

Cloud DLP
(API and proxy-mode
+ Isolation)

**GenerativeAI
Co-pilots, Chatbots,
ChatGPT**

Email DLP

- Alert Triage
- File Lineage
- User Timeline
- Policy Management
- Threat Hunting
- Investigation Workflows
- Executive Reporting
- Privacy Controls

Ecosystem Integrations

Labeling: Microsoft

Identity: okta, SailPoint

EDR: CROWDSTRIKE

SIEM/SOAR: splunk>, servicenow

ICAP: zscaler, citrix ShareFile

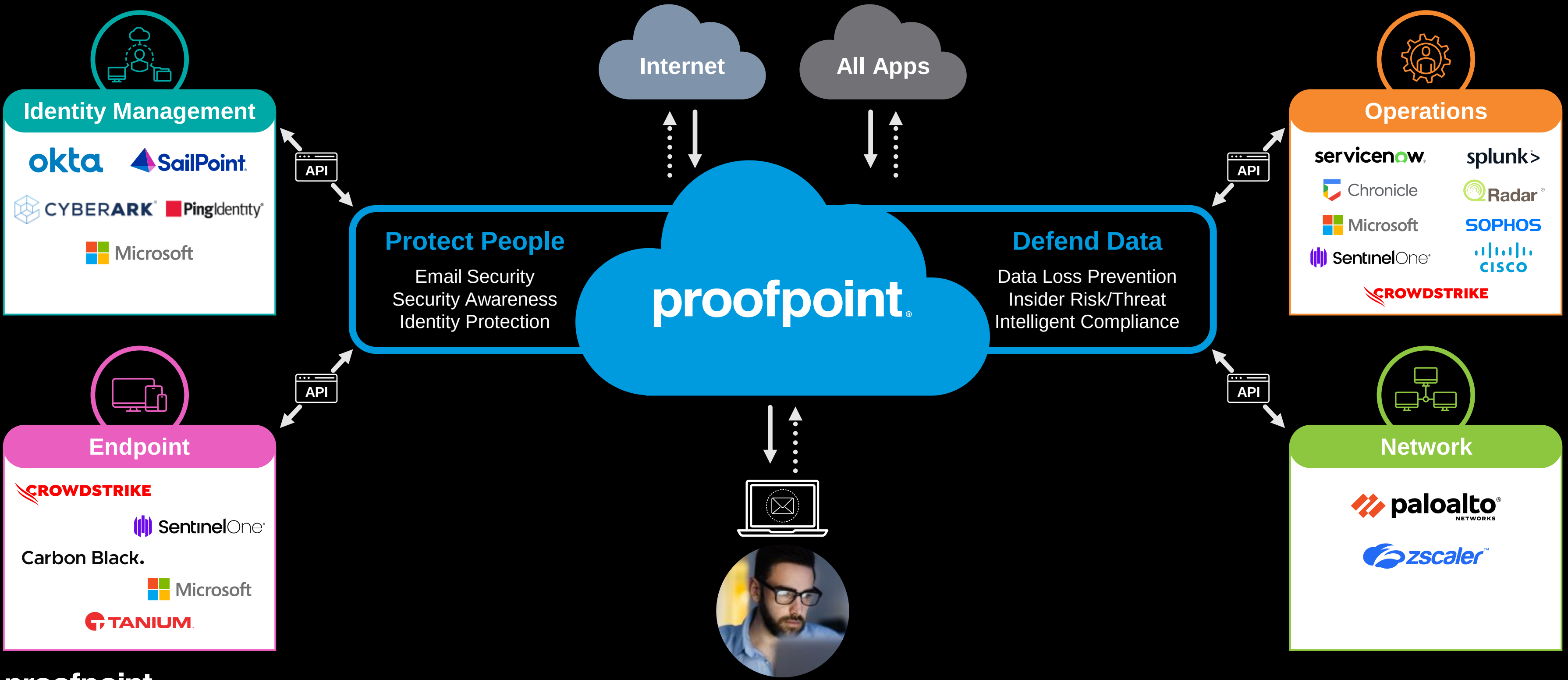
proofpoint.

© 2024 Proofpoint Inc.

Partnering to Deliver Human-Centric Security

Best-in-class Technology Partner Ecosystem

HUMAN CENTRIC CYBER SECURITY



Identity Management

okta
SailPoint
CYBERARK
PingIdentity
Microsoft

Endpoint

CROWDSTRIKE
SentinelOne
Carbon Black.
Microsoft
TANIUM

Operations

servicenow
splunk>
Chronicle
QRadar
Microsoft
SOPHOS
SentinelOne
cisco
CROWDSTRIKE

Network

paloalto NETWORKS
zscaler

Protect People

Email Security
Security Awareness
Identity Protection

Defend Data

Data Loss Prevention
Insider Risk/Threat
Intelligent Compliance

© 2024 Proofpoint Inc.

HUMAN CENTRIC CYBER SECURITY

Usecases and Tools

© 2024 Proofpoint Inc.

proofpoint.

Human Centric Security

Protect People

- Stop human-targeted attacks
- Prevent impersonation
- Mitigate supplier risk

People Use Cases

Mitigate Human Risk

Human Risk Use Cases

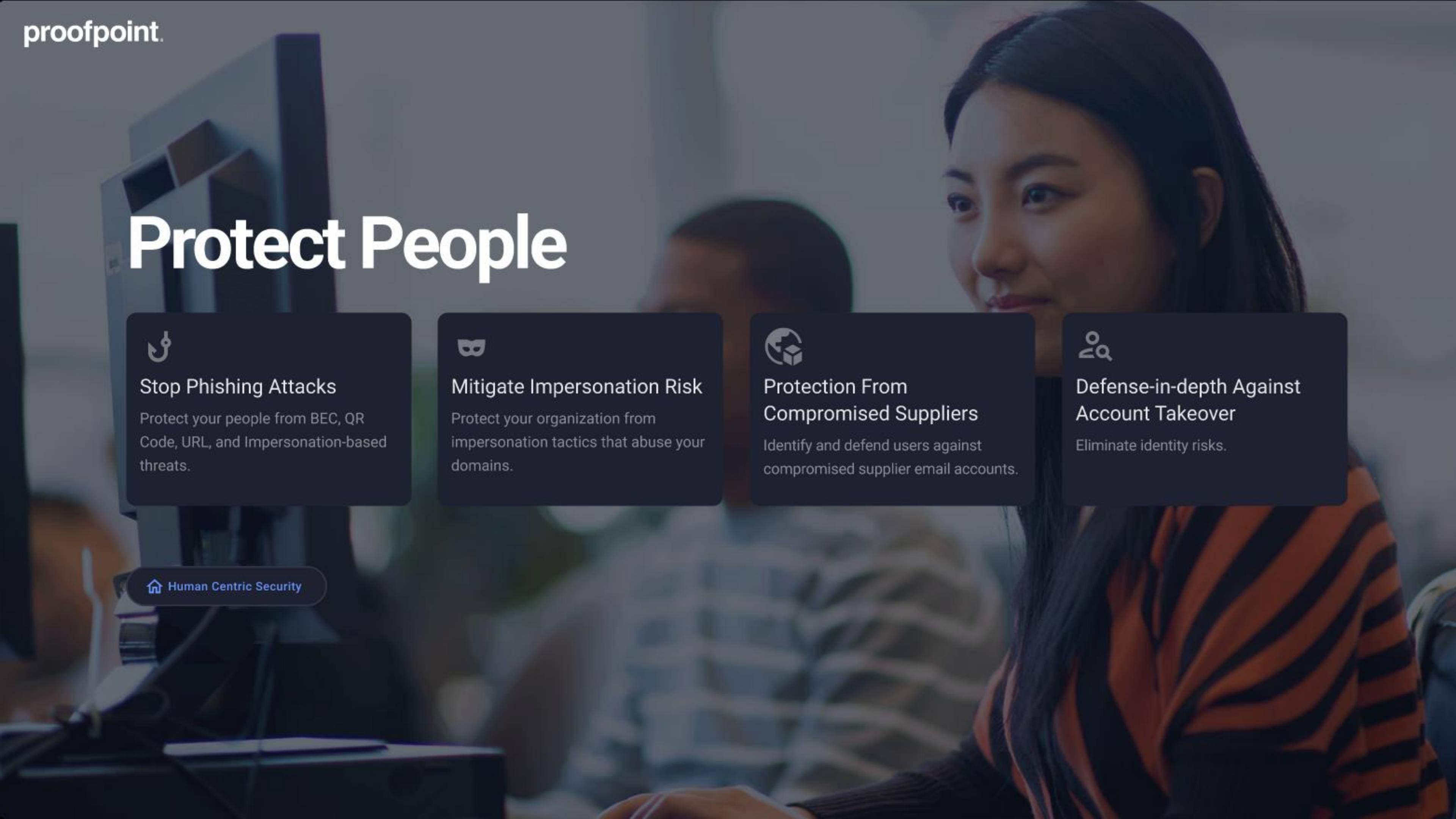
Defend Data

- Prevent misdelivery
- Mitigate data loss
- Contain insider threats

Data Use Cases

Complete Detection Ensemble

Nexus AI • Behavioral Analytics • Threat Intelligence



proofpoint.

Protect People

Stop Phishing Attacks

Protect your people from BEC, QR Code, URL, and Impersonation-based threats.

Mitigate Impersonation Risk

Protect your organization from impersonation tactics that abuse your domains.

Protection From Compromised Suppliers

Identify and defend users against compromised supplier email accounts.

Defense-in-depth Against Account Takeover

Eliminate identity risks.

Human Centric Security

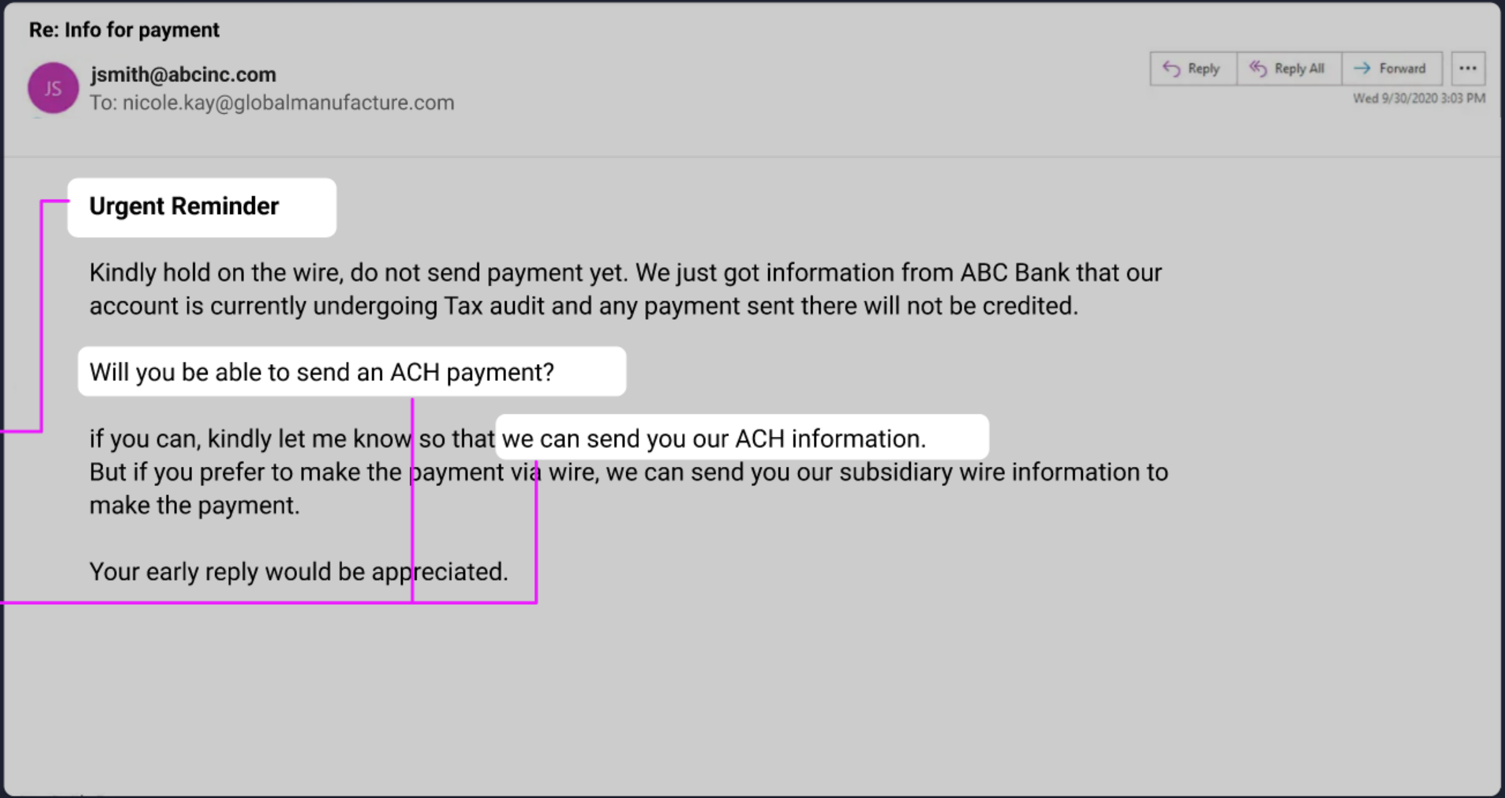
proofpoint. Stop Phishing Attacks: Pre-Delivery Detection

PROOFPOINT VIEW

Semantic Analysis

Proofpoint

- The Semantic Analysis LLM engine has detected suspicious intent insights within the email.
- Intent #1: Urgency. This is intended to get the recipient to react quickly without thinking.
- Intent #2, #3: Financial payment and new bank routing information. These are intended to get the recipient to send payment to the threat actor's bank account.



Re: Info for payment

JS **jsmith@abcinc.com**

To: nicole.kay@globalmanufacture.com

Wed 9/30/2020 3:03 PM

Urgent Reminder

Kindly hold on the wire, do not send payment yet. We just got information from ABC Bank that our account is currently undergoing Tax audit and any payment sent there will not be credited.

Will you be able to send an ACH payment?

if you can, kindly let me know so that we can send you our ACH information.
But if you prefer to make the payment via wire, we can send you our subsidiary wire information to make the payment.

Your early reply would be appreciated.

proofpoint.

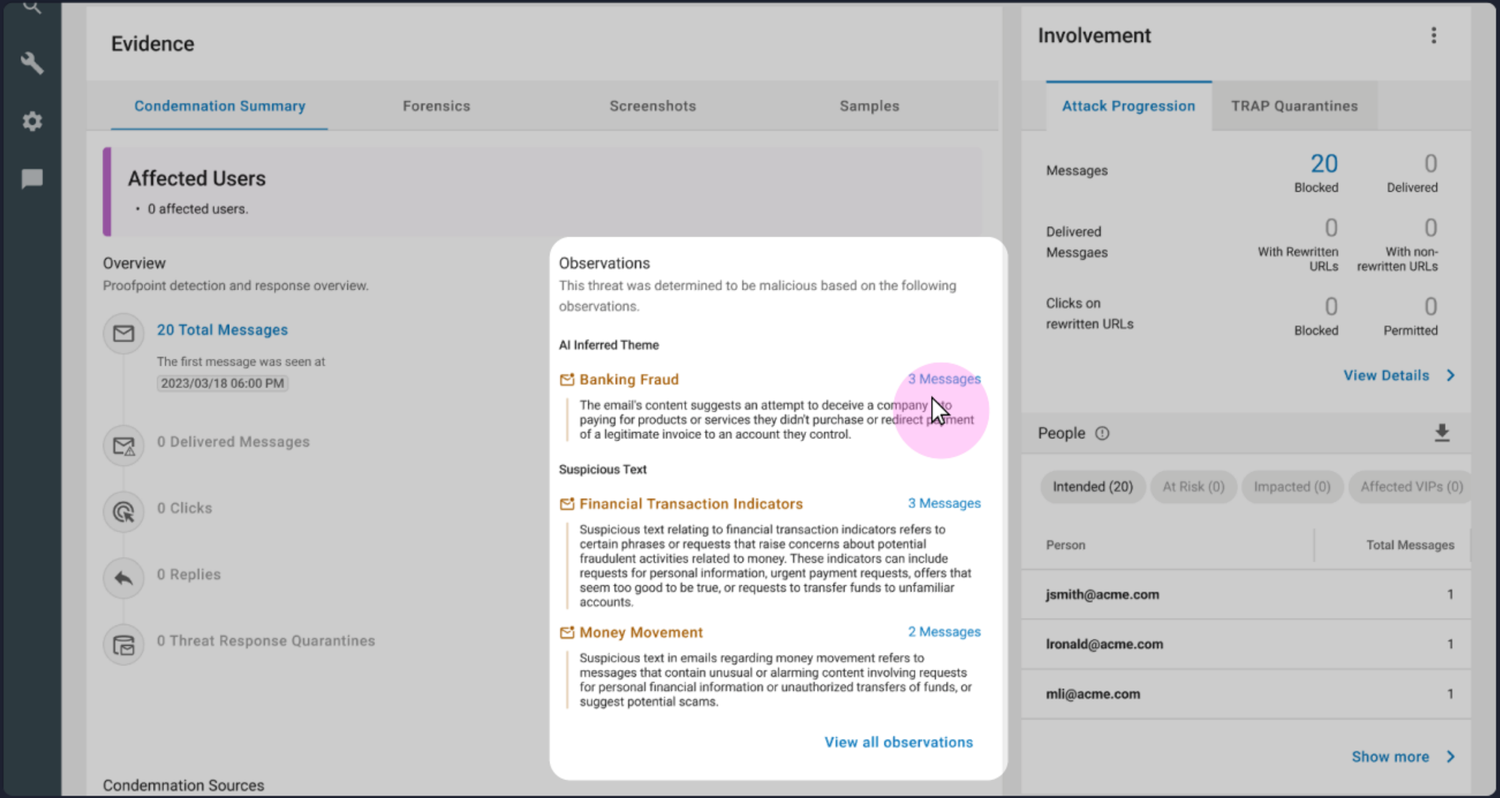
Stop Phishing Attacks: Pre-Delivery Detection

SOC ANALYST VIEW

John Shider
Security Analyst

- With easy-to-understand explainability, the SOC analyst can view the Semantic Analysis results and supporting intent evidence.

> The malicious email was classified as **Banking Fraud** and included intent evidence of **Financial Transaction** and **Money Movement** indicators.



Evidence

Affected Users

- 0 affected users.

Overview

Proofpoint detection and response overview.

20 Total Messages

The first message was seen at 2023/03/18 06:00 PM

0 Delivered Messages

0 Clicks

0 Replies

0 Threat Response Quarantines

Observations

This threat was determined to be malicious based on the following observations.

AI Inferred Theme

Banking Fraud — 3 Messages

The email's content suggests an attempt to deceive a company to paying for products or services they didn't purchase or redirect payment of a legitimate invoice to an account they control.

Suspicious Text

Financial Transaction Indicators — 3 Messages

Suspicious text relating to financial transaction indicators refers to certain phrases or requests that raise concerns about potential fraudulent activities related to money. These indicators can include requests for personal information, urgent payment requests, offers that seem too good to be true, or requests to transfer funds to unfamiliar accounts.

Money Movement — 2 Messages

Suspicious text in emails regarding money movement refers to messages that contain unusual or alarming content involving requests for personal financial information or unauthorized transfers of funds, or suggest potential scams.

View all observations

Condemnation Sources

Involvement

Messages	20 Blocked	0 Delivered
Delivered Messgaes	0 With Rewritten URLs	0 With non-rewritten URLs
Clicks on rewritten URLs	0 Blocked	0 Permitted

View Details >

People

Person	Total Messages
jsmith@acme.com	1
lronald@acme.com	1
mli@acme.com	1

Show more >

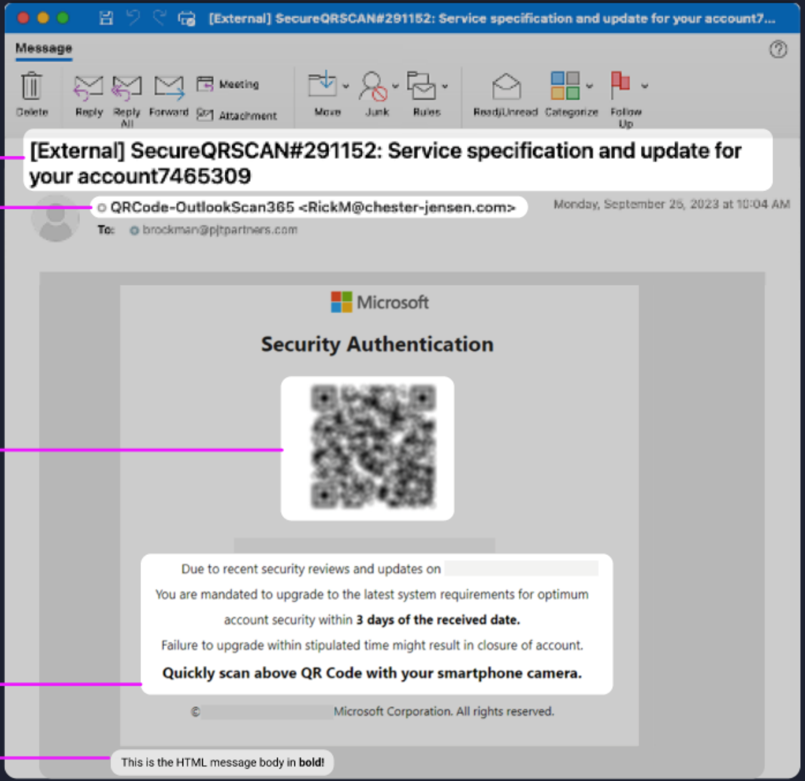
© 2024 Proofpoint Inc.

proofpoint. Stop Phishing Attacks: Pre-Delivery Detection

PROOFPOINT VIEW

Behavioral AI
Proofpoint

- Proofpoint's behavioral AI detection engine identifies key message attributes like, sender, receiver, images, URLs and many more that may indicate malicious messages.
- The following malicious message indicators were detected:
  - Suspicious Text and Theme
  - Uncommon Sender
  - QR Code Presence
  - Suspicious Text and Theme



[External] SecureQRSCAN#291152: Service specification and update for your account7465309

QRCode-OutlookScan365 <RickM@chester-jensen.com>

Monday, September 25, 2023 at 10:04 AM

To: brockman@pjtpartners.com

Microsoft

Security Authentication

Due to recent security reviews and updates on

You are mandated to upgrade to the latest system requirements for optimum account security within **3 days of the received date.**

Failure to upgrade within stipulated time might result in closure of account.

Quickly scan above QR Code with your smartphone camera.

© Microsoft Corporation. All rights reserved.

This is the HTML message body in **bold!**

← **Next →**

Human Centric Security

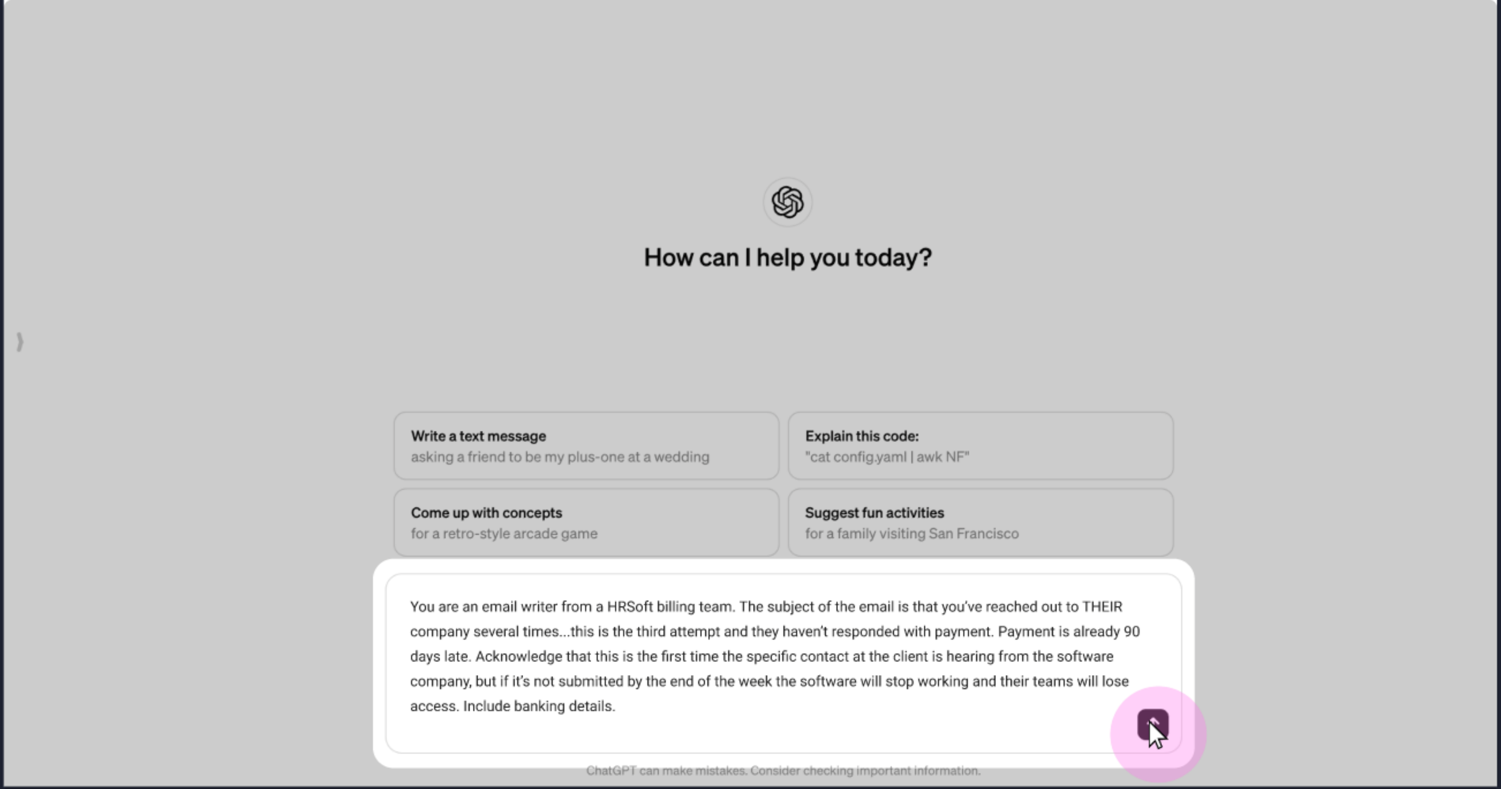
proofpoint. Stop Phishing Attacks: Post-Delivery Detection

THREAT ACTOR VIEW

Tempest
Threat Actor

Case 3:
Stop Advanced Email Threats With Behavioral AI

- Tempest uses a prompt that he's succeeded with in the past to socially engineer unwitting employees in accounts payable to send him funds meant for one of their trusted vendors.


How can I help you today?
Write a text message
asking a friend to be my plus-one at a wedding
Explain this code:
"cat config.yaml | awk NF"
Come up with concepts
for a retro-style arcade game
Suggest fun activities
for a family visiting San Francisco

You are an email writer from a HRSoft billing team. The subject of the email is that you've reached out to THEIR company several times...this is the third attempt and they haven't responded with payment. Payment is already 90 days late. Acknowledge that this is the first time the specific contact at the client is hearing from the software company, but if it's not submitted by the end of the week the software will stop working and their teams will lose access. Include banking details.

ChatGPT can make mistakes. Consider checking important information.

← Next →

Human Centric Security

© 2024 Proofpoint Inc.

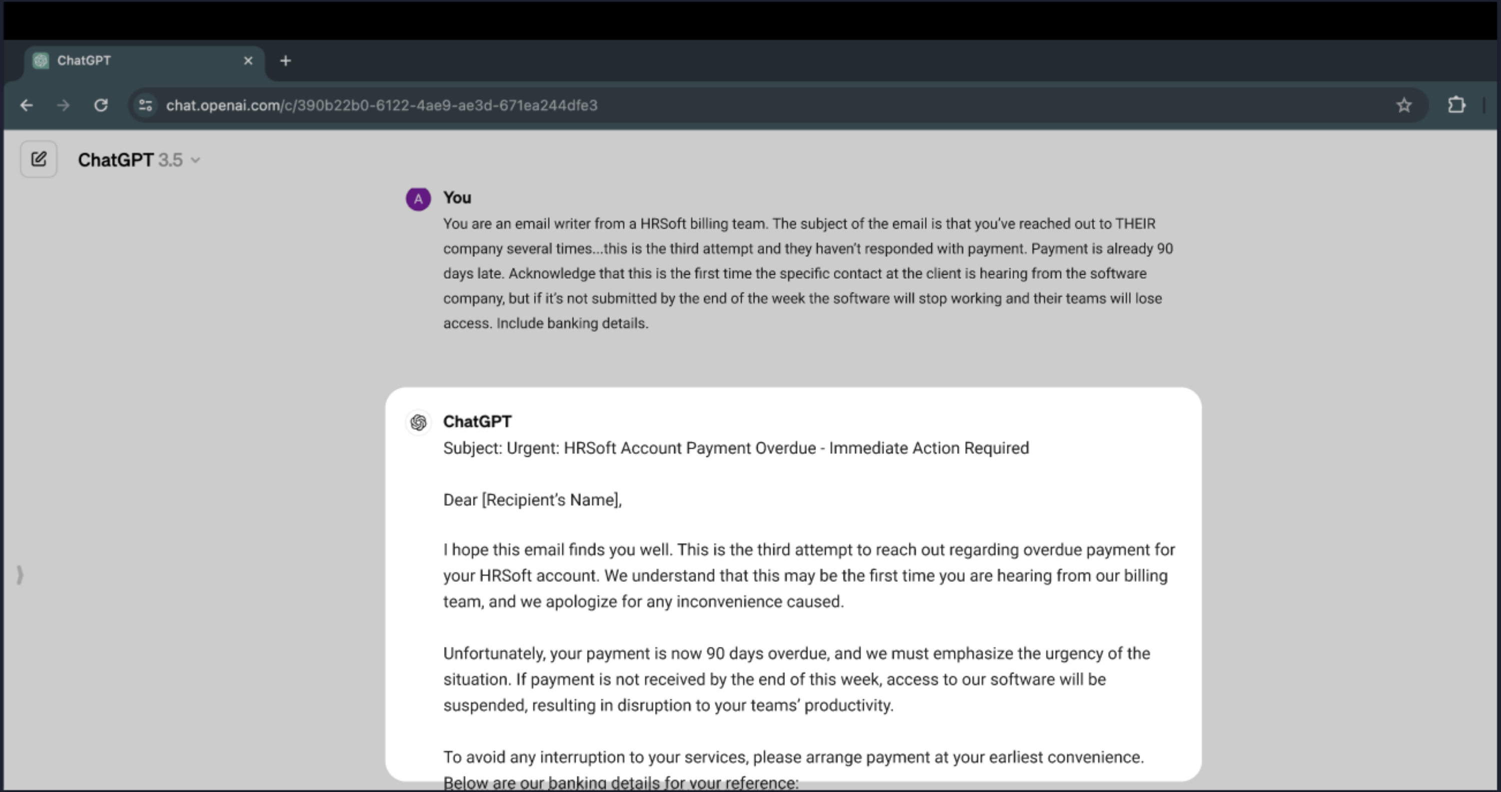
proofpoint.

Stop Phishing Attacks: Post-Delivery Detection

THREAT ACTOR VIEW

Tempest
Threat Actor

- ChatGPT returns an email template which Tempest can use to send to a variety of organizations, with light personalization to increase authenticity and success rates.



You

You are an email writer from a HRSoft billing team. The subject of the email is that you've reached out to THEIR company several times...this is the third attempt and they haven't responded with payment. Payment is already 90 days late. Acknowledge that this is the first time the specific contact at the client is hearing from the software company, but if it's not submitted by the end of the week the software will stop working and their teams will lose access. Include banking details.

ChatGPT

Subject: Urgent: HRSoft Account Payment Overdue - Immediate Action Required

Dear [Recipient's Name],

I hope this email finds you well. This is the third attempt to reach out regarding overdue payment for your HRSoft account. We understand that this may be the first time you are hearing from our billing team, and we apologize for any inconvenience caused.

Unfortunately, your payment is now 90 days overdue, and we must emphasize the urgency of the situation. If payment is not received by the end of this week, access to our software will be suspended, resulting in disruption to your teams' productivity.

To avoid any interruption to your services, please arrange payment at your earliest convenience. Below are our banking details for your reference:

Stop Phishing Attacks: Post-Delivery Detection

THREAT ACTOR VIEW

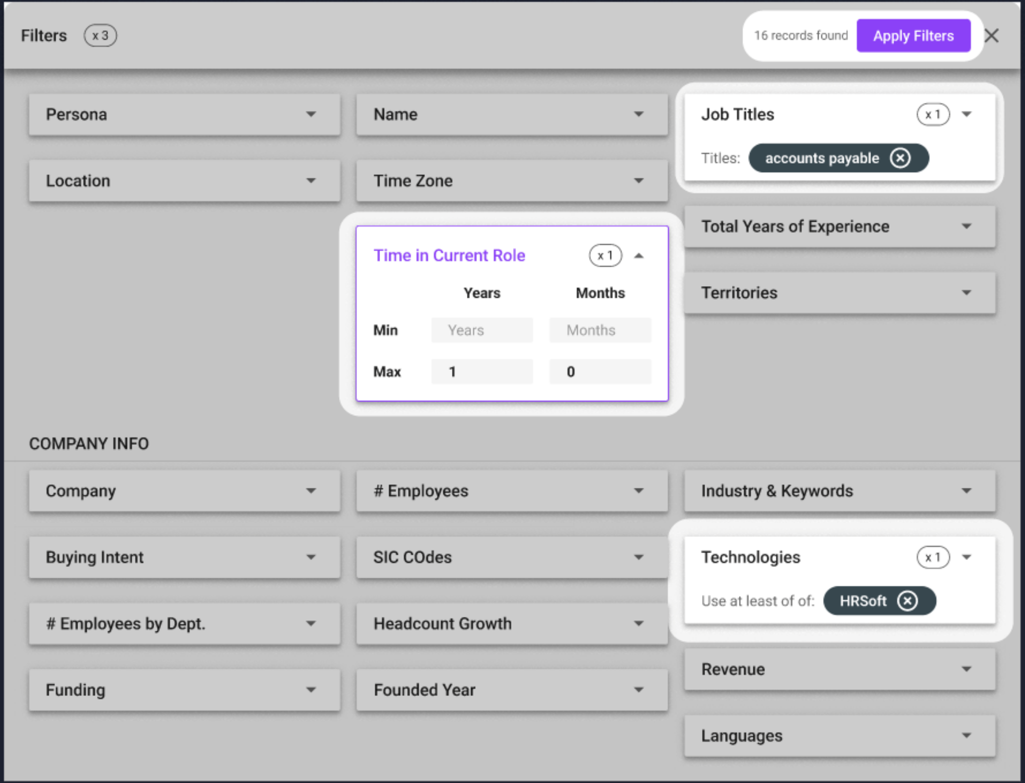
Tempest

Threat Actor

- Tempest then accesses a low-cost sales contact database. Conveniently, it not only allows him to filter for contacts by company, but also by the contact's tenure at the company and technology in use at the organization.
- Tempest filters for companies using HRSoft, and specifically for contacts in accounts payable who've been in their role for less than one month.

Next →

Human Centric Security



Filters x 3

16 records found

Job Titles x 1

Titles: accounts payable

Time in Current Role x 1

	Years	Months
Min	Years	Months
Max	1	0

Technologies x 1

Use at least of of: HRSoft

© 2024 Proofpoint Inc.

proofpoint. Stop Phishing Attacks: Post-Delivery Detection

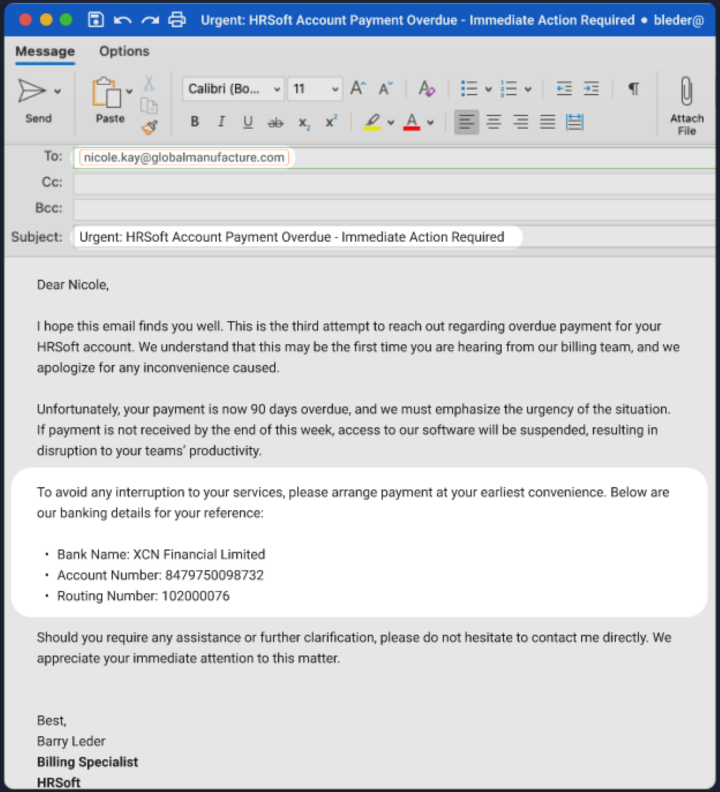
THREAT ACTOR VIEW

Tempest
Threat Actor

- With the best contacts in hand, Tempest crafts an email from a fake alias –**Barry Leder** (**bleder@hrs0ft.com**) to Nicole Kay, a new employee in accounts payable at a target company using HRSoft.

← **Next →**

Human Centric Security


Urgent: HRSoft Account Payment Overdue - Immediate Action Required • bleder@
Message
Options
Send
Paste
Calibri (Bo...
11
Attach File

To: nicole.kay@globalmanufacture.com
Cc:
Bcc:
Subject: Urgent: HRSoft Account Payment Overdue - Immediate Action Required

Dear Nicole,

I hope this email finds you well. This is the third attempt to reach out regarding overdue payment for your HRSoft account. We understand that this may be the first time you are hearing from our billing team, and we apologize for any inconvenience caused.

Unfortunately, your payment is now 90 days overdue, and we must emphasize the urgency of the situation. If payment is not received by the end of this week, access to our software will be suspended, resulting in disruption to your teams' productivity.

To avoid any interruption to your services, please arrange payment at your earliest convenience. Below are our banking details for your reference:

- Bank Name: XCN Financial Limited
- Account Number: 8479750098732
- Routing Number: 102000076

Should you require any assistance or further clarification, please do not hesitate to contact me directly. We appreciate your immediate attention to this matter.

Best,
Barry Leder
Billing Specialist
HRSoft

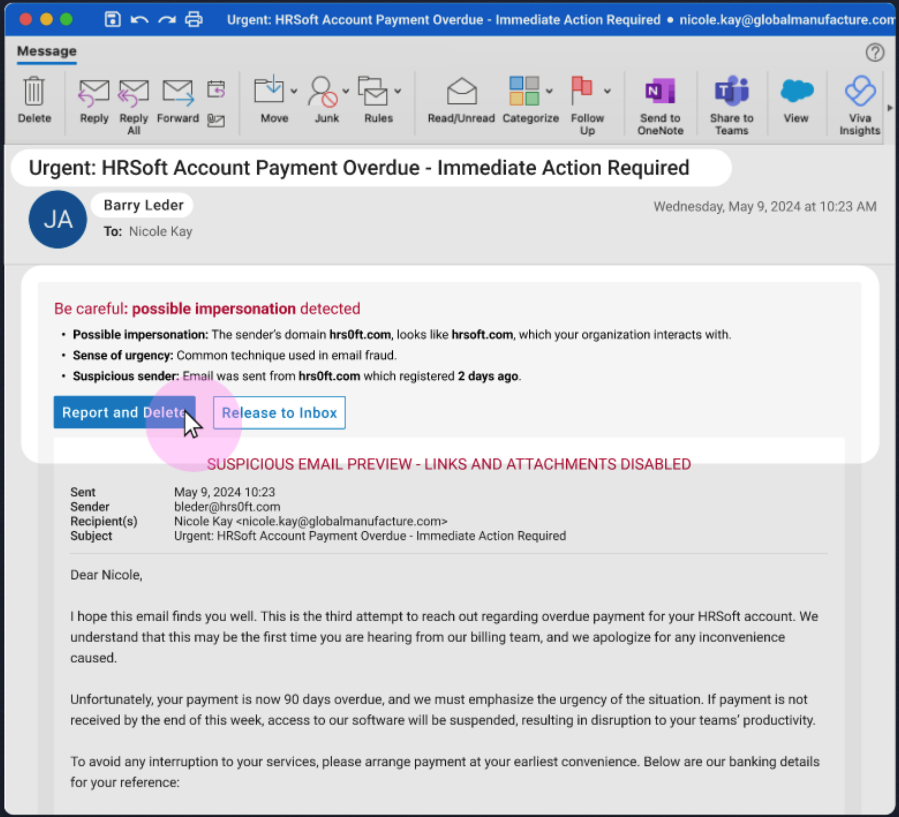
Stop Phishing Attacks: Post-Delivery Detection

END-USER VIEW

Nicole Kay
Account Payable

- Nicole receives the email with the contextual warning banner, and decides to report malicious and delete.

> Proofpoint flags the email as a **possible impersonation**, highlighting **urgency** in the email and a **newly registered domain**.



Urgent: HRSoft Account Payment Overdue - Immediate Action Required

Barry Leder
To: Nicole Kay
Wednesday, May 9, 2024 at 10:23 AM

Be careful: **possible impersonation** detected

- **Possible impersonation:** The sender's domain **hrs0ft.com**, looks like **hrsoft.com**, which your organization interacts with.
- **Sense of urgency:** Common technique used in email fraud.
- **Suspicious sender:** Email was sent from **hrs0ft.com** which registered **2 days ago**.

SUSPICIOUS EMAIL PREVIEW - LINKS AND ATTACHMENTS DISABLED

Sent May 9, 2024 10:23
Sender bleder@hrs0ft.com
Recipient(s) Nicole Kay <nicole.kay@globalmanufacture.com>
Subject Urgent: HRSoft Account Payment Overdue - Immediate Action Required

Dear Nicole,

I hope this email finds you well. This is the third attempt to reach out regarding overdue payment for your HRSoft account. We understand that this may be the first time you are hearing from our billing team, and we apologize for any inconvenience caused.

Unfortunately, your payment is now 90 days overdue, and we must emphasize the urgency of the situation. If payment is not received by the end of this week, access to our software will be suspended, resulting in disruption to your teams' productivity.

To avoid any interruption to your services, please arrange payment at your earliest convenience. Below are our banking details for your reference:

← Next →

Human Centric Security

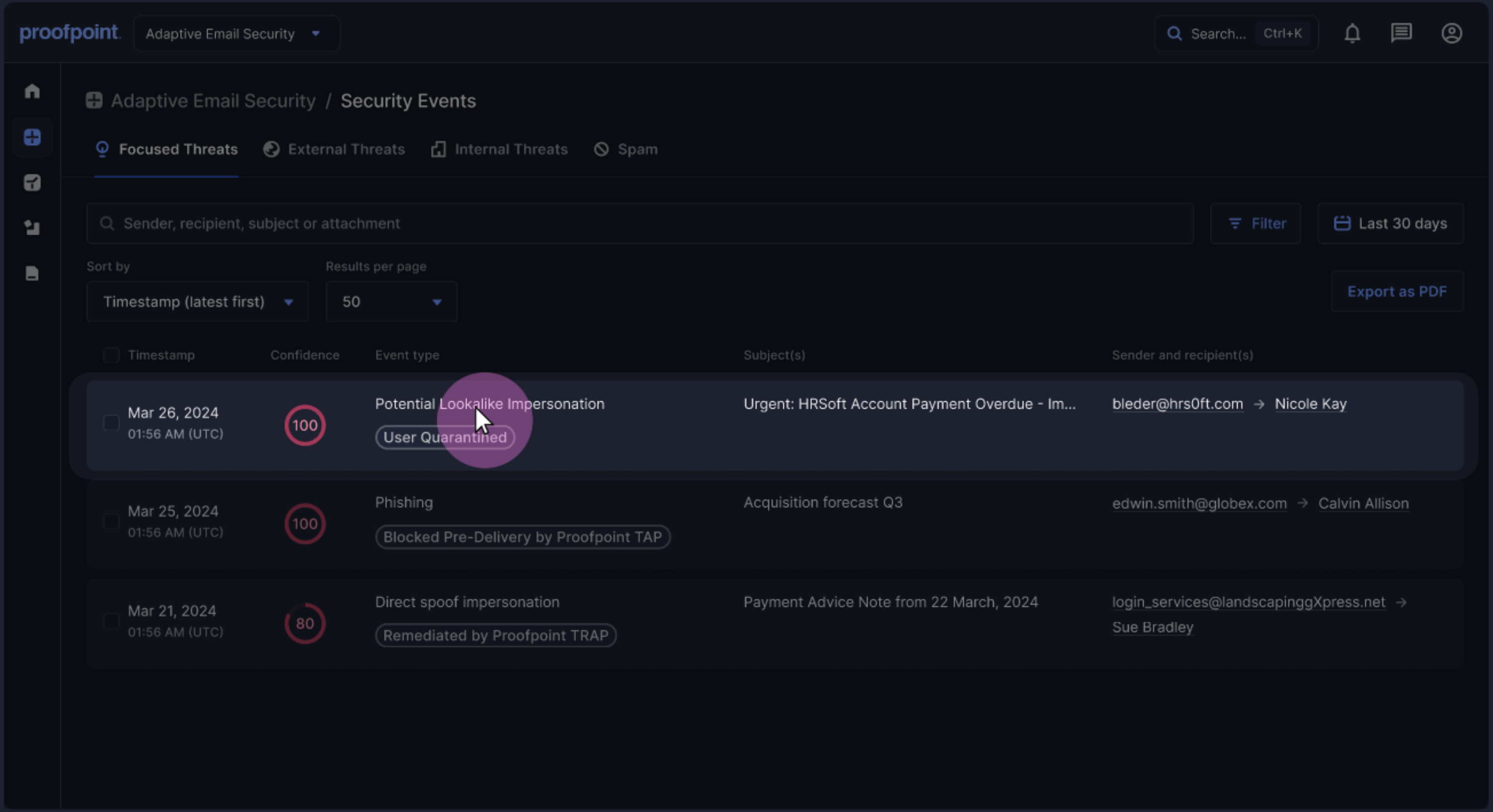
proofpoint.

Stop Phishing Attacks: Post-Delivery Detection

SOC ANALYST VIEW

John Shider
Security Analyst

- While investigating today's focused events, John sees a "**Potential Lookalike Impersonation**" of HRSoft, one of the trusted vendors to his company.



Sort by: Timestamp (latest first)

Results per page: 50

Timestamp	Confidence	Event type	Subject(s)	Sender and recipient(s)
Mar 26, 2024 01:56 AM (UTC)	100	Potential Lookalike Impersonation User Quarantined	Urgent: HRSoft Account Payment Overdue - Im...	bleder@hrs0ft.com → Nicole Kay
Mar 25, 2024 01:56 AM (UTC)	100	Phishing Blocked Pre-Delivery by Proofpoint TAP	Acquisition forecast Q3	edwin.smith@globex.com → Calvin Allison
Mar 21, 2024 01:56 AM (UTC)	80	Direct spoof impersonation Remediated by Proofpoint TRAP	Payment Advice Note from 22 March, 2024	login_services@landscapinggXpress.net → Sue Bradley

← Next →

Human Centric Security

© 2024 Proofpoint Inc.

Stop Phishing Attacks: Post-Delivery Detection

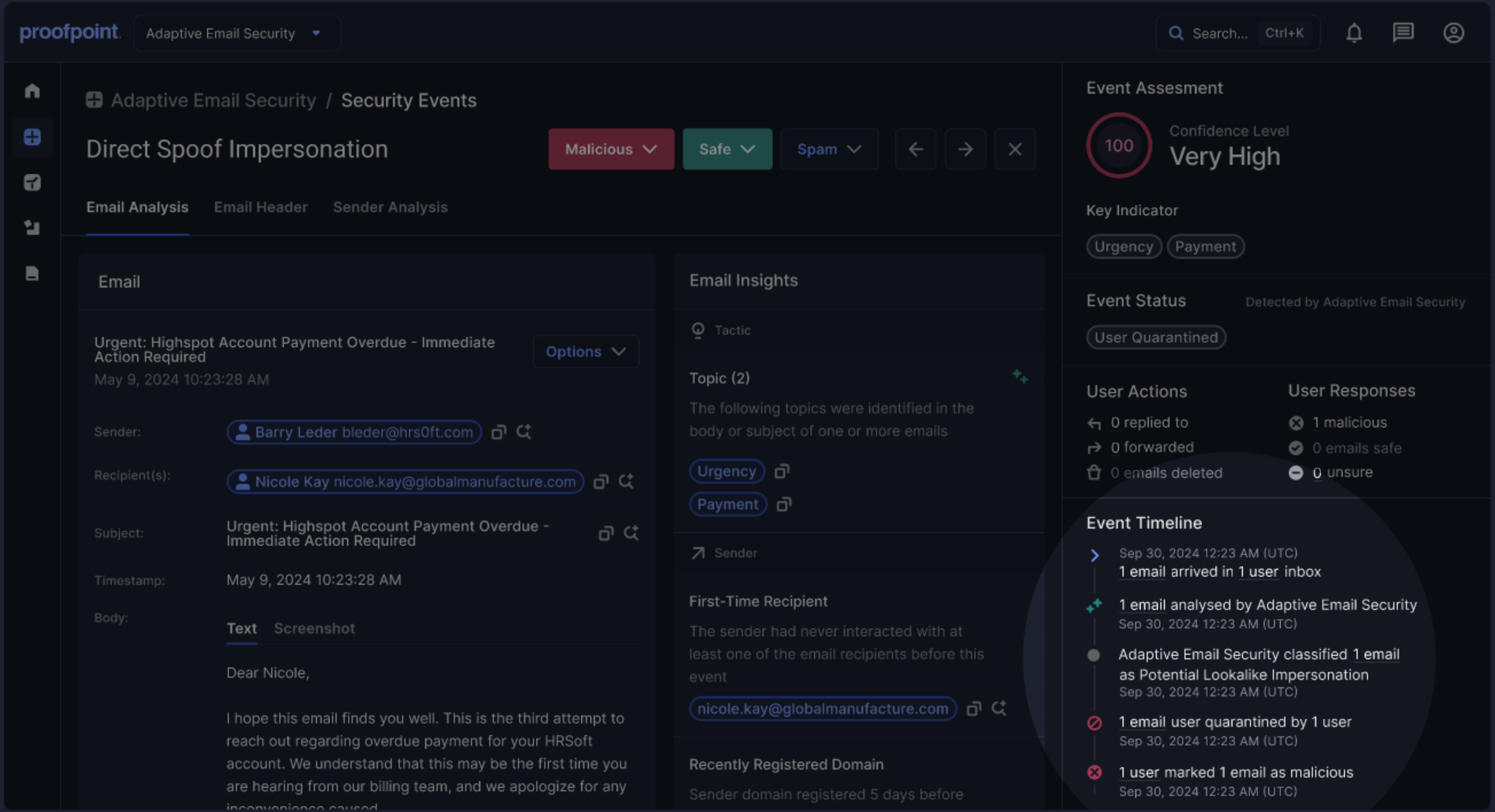
SOC ANALYST VIEW

John Shider
Security Analyst

- With Adaptive Email Security, John can see the email was quarantined by its recipient Nicole Kay, then automatically deleted from her inbox.

Next →

Human Centric Security



Adaptive Email Security / Security Events

Direct Spoof Impersonation

Email Analysis | Email Header | Sender Analysis

Email

Urgent: Highspot Account Payment Overdue - Immediate Action Required
May 9, 2024 10:23:28 AM

Sender: Barry Leder bleder@hrs0ft.com

Recipient(s): Nicole Kay nicole.kay@globalmanufacture.com

Subject: Urgent: Highspot Account Payment Overdue - Immediate Action Required

Timestamp: May 9, 2024 10:23:28 AM

Body: Text | Screenshot

Dear Nicole,

I hope this email finds you well. This is the third attempt to reach out regarding overdue payment for your HRSoft account. We understand that this may be the first time you are hearing from our billing team, and we apologize for any inconvenience caused.

Email Insights

Tactic

Topic (2)

The following topics were identified in the body or subject of one or more emails

Urgency
Payment

Sender

First-Time Recipient

The sender had never interacted with at least one of the email recipients before this event

nicole.kay@globalmanufacture.com

Recently Registered Domain

Sender domain registered 5 days before

Event Assesment

100 Confidence Level: Very High

Key Indicator: Urgency, Payment

Event Status Detected by Adaptive Email Security

User Quarantined

User Actions

- 0 replied to
- 0 forwarded
- 0 emails deleted

User Responses

- 1 malicious
- 0 emails safe
- 0 unsure

Event Timeline

- Sep 30, 2024 12:23 AM (UTC) — 1 email arrived in 1 user inbox
- 1 email analysed by Adaptive Email Security — Sep 30, 2024 12:23 AM (UTC)
- Adaptive Email Security classified 1 email as Potential Lookalike Impersonation — Sep 30, 2024 12:23 AM (UTC)
- 1 email user quarantined by 1 user — Sep 30, 2024 12:23 AM (UTC)
- 1 user marked 1 email as malicious — Sep 30, 2024 12:23 AM (UTC)

proofpoint.

Stop Phishing Attacks: Post-Delivery Detection

SOC ANALYST VIEW

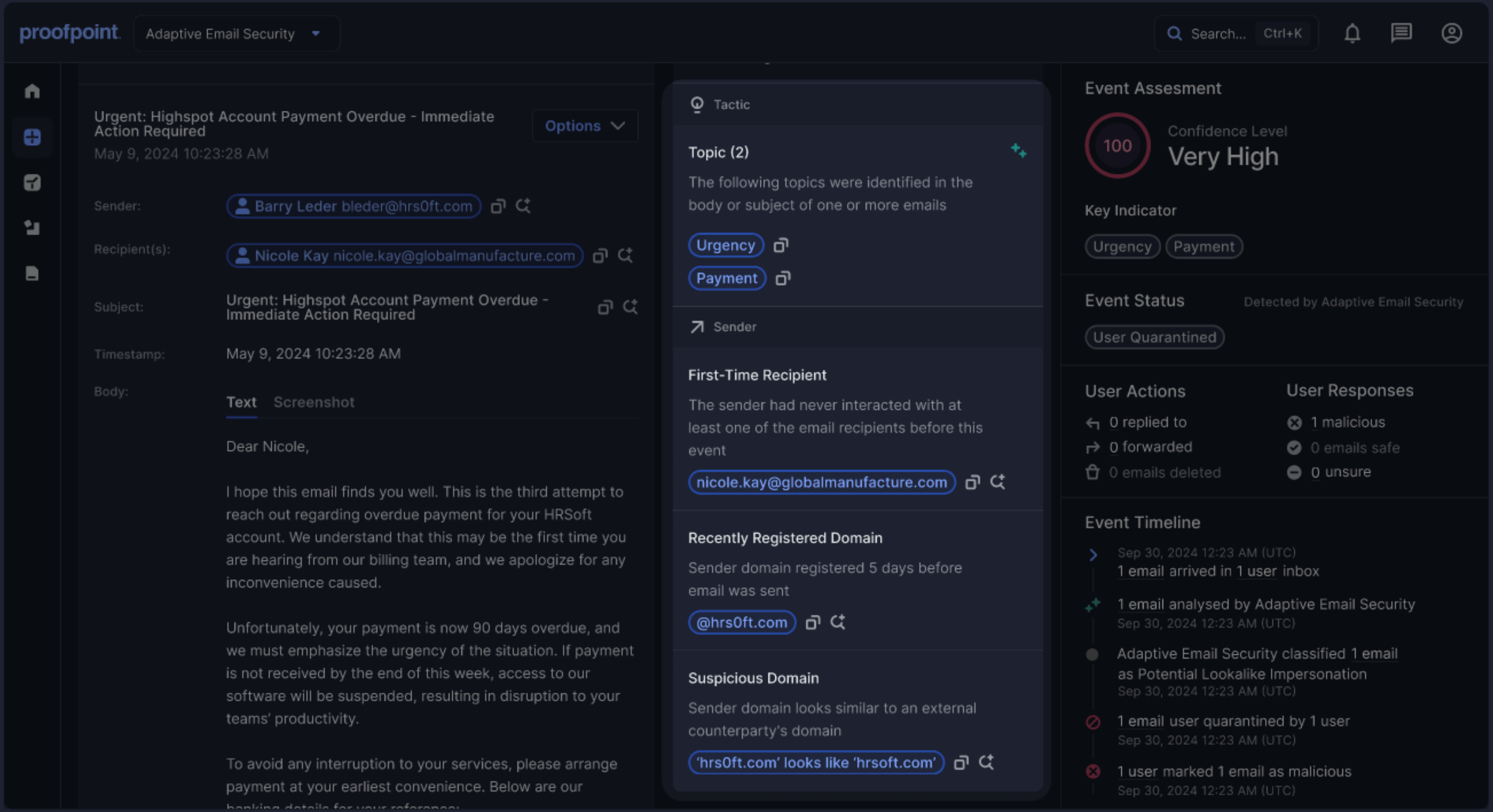
John Shider
Security Analyst

- John can see the domain was recently registered, that Nicole was a first-time recipient, and that urgency and payment topics were found, increasing confidence in labeling the email as potential lookalike impersonation.

> **Adaptive Email Security** reveals that the email was sent from **hrs0ft.com**, a domain similar to their trusted partner **hrsoft.com**.

← **Back to Main Menu →**

Human Centric Security



Urgent: Highspot Account Payment Overdue - Immediate Action Required
May 9, 2024 10:23:28 AM

Sender: Barry Leder bleder@hrs0ft.com

Recipient(s): Nicole Kay nicole.kay@globalmanufacture.com

Subject: Urgent: Highspot Account Payment Overdue - Immediate Action Required

Timestamp: May 9, 2024 10:23:28 AM

Body: Text Screenshot

Dear Nicole,

I hope this email finds you well. This is the third attempt to reach out regarding overdue payment for your HRSoft account. We understand that this may be the first time you are hearing from our billing team, and we apologize for any inconvenience caused.

Unfortunately, your payment is now 90 days overdue, and we must emphasize the urgency of the situation. If payment is not received by the end of this week, access to our software will be suspended, resulting in disruption to your teams' productivity.

To avoid any interruption to your services, please arrange payment at your earliest convenience. Below are our banking details for your reference:

Tactic

Topic (2)

The following topics were identified in the body or subject of one or more emails

Urgency

Payment

Sender

First-Time Recipient

The sender had never interacted with at least one of the email recipients before this event

nicole.kay@globalmanufacture.com

Recently Registered Domain

Sender domain registered 5 days before email was sent

@hrs0ft.com

Suspicious Domain

Sender domain looks similar to an external counterparty's domain

'hrs0ft.com' looks like 'hrsoft.com'

Event Assesment

100 Confidence Level Very High

Key Indicator: Urgency Payment

Event Status: User Quarantined (Detected by Adaptive Email Security)

User Actions	User Responses
0 replied to	1 malicious
0 forwarded	0 emails safe
0 emails deleted	0 unsure

Event Timeline

- Sep 30, 2024 12:23 AM (UTC) 1 email arrived in 1 user inbox
- 1 email analysed by Adaptive Email Security Sep 30, 2024 12:23 AM (UTC)
- Adaptive Email Security classified 1 email as Potential Lookalike Impersonation Sep 30, 2024 12:23 AM (UTC)
- 1 email user quarantined by 1 user Sep 30, 2024 12:23 AM (UTC)
- 1 user marked 1 email as malicious Sep 30, 2024 12:23 AM (UTC)

Human Centric Security

Protect People

- Stop human-targeted attacks
- Prevent impersonation
- Mitigate supplier risk

People Use Cases

Mitigate Human Risk

Human Risk Use Cases

Defend Data

- Prevent misdelivery
- Mitigate data loss
- Contain insider threats

Data Use Cases

Complete Detection Ensemble

Nexus AI • Behavioral Analytics • Threat Intelligence

proofpoint.

Mitigate Human Risk

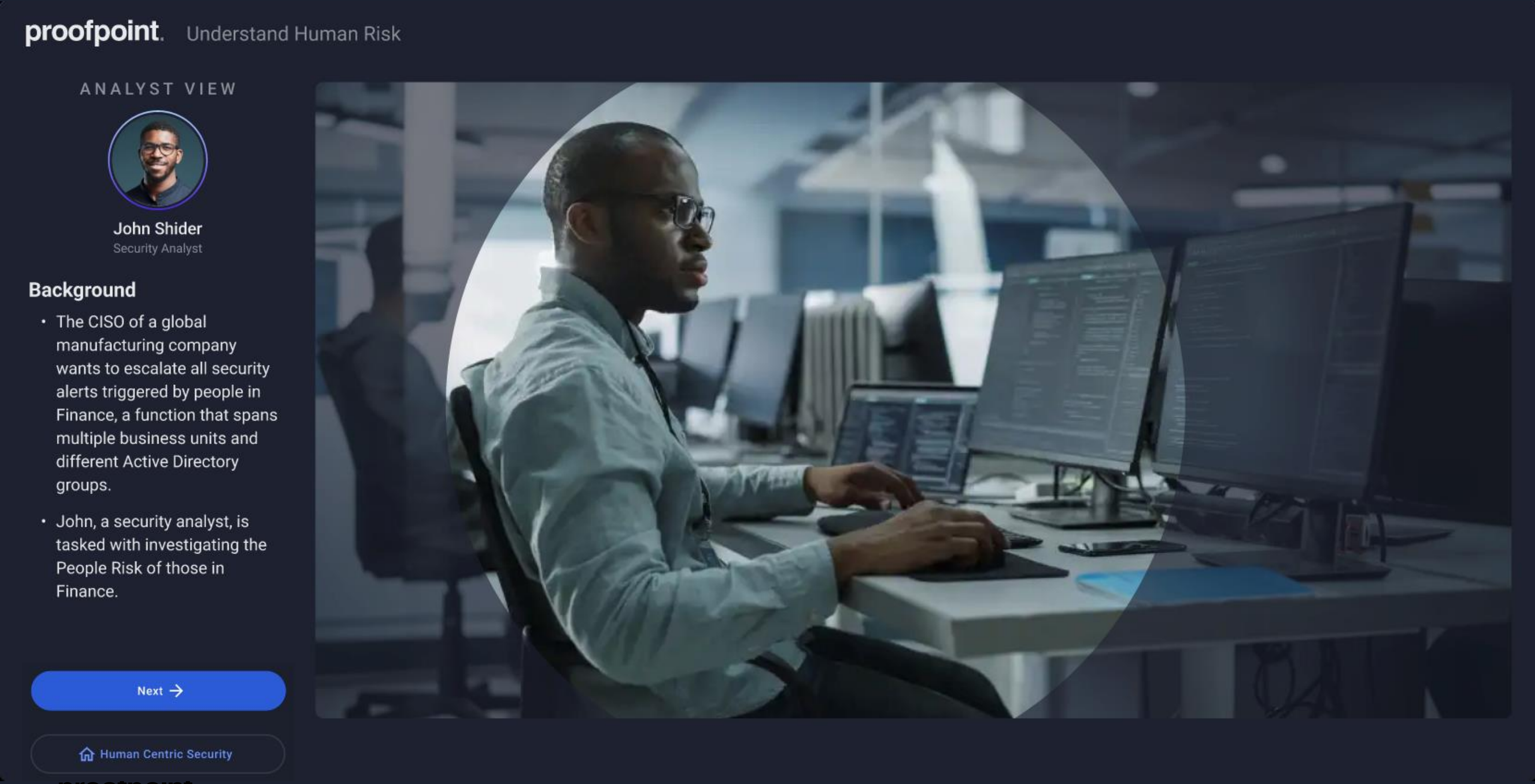
Understand Human Risk

Correlate your security awareness program with real-world human risk

Threat-Guided Education

Change User Behavior

Human Centric Security



ANALYST VIEW

John Shider
Security Analyst

Background

- The CISO of a global manufacturing company wants to escalate all security alerts triggered by people in Finance, a function that spans multiple business units and different Active Directory groups.
- John, a security analyst, is tasked with investigating the People Risk of those in Finance.

© 2024 Proofpoint Inc.

Understand Human Risk

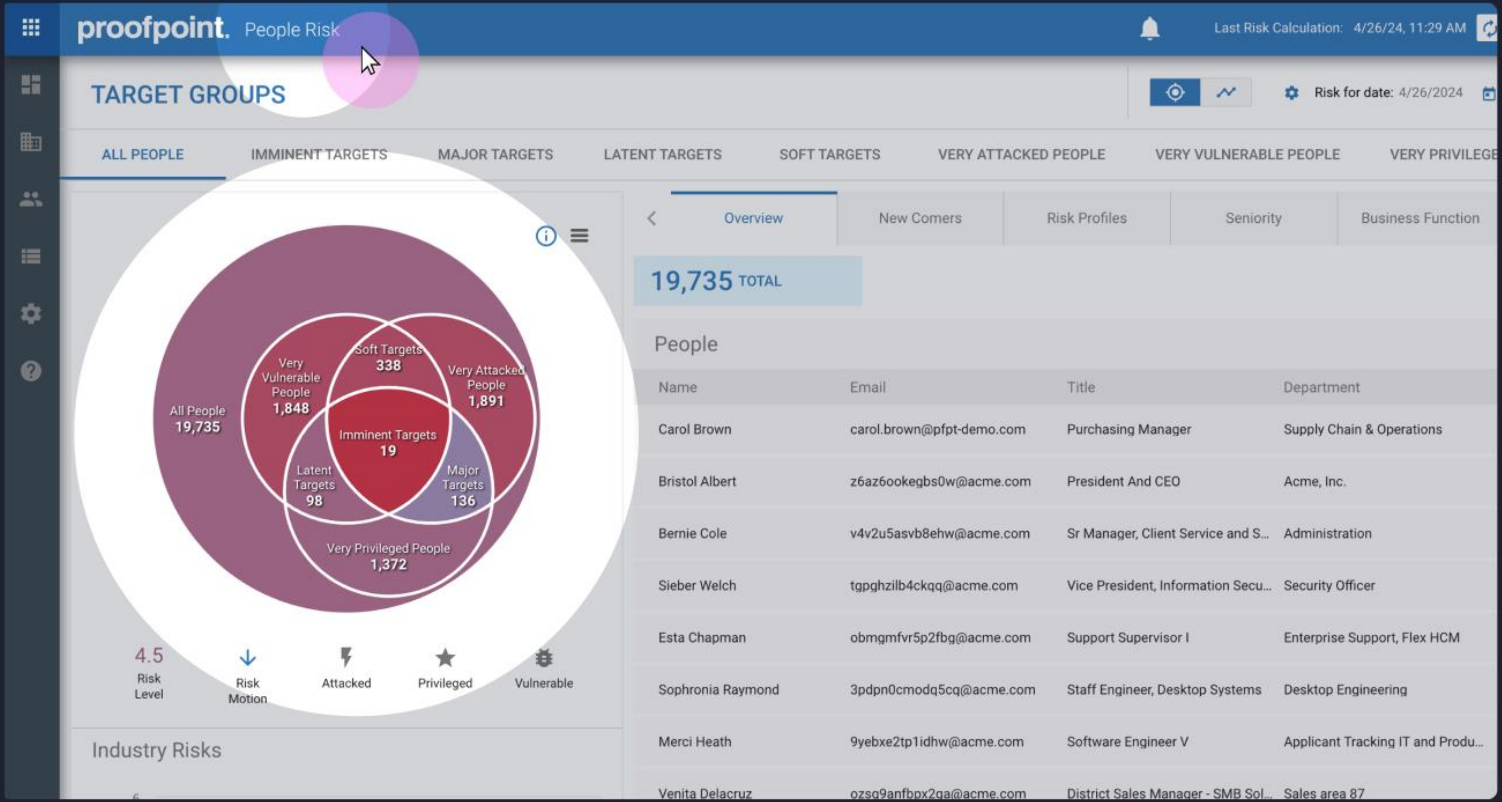
ANALYST VIEW

John Shider
Security Analyst

- John's main questions are:
  - Which people are putting the organization at risk?
  - How are risky people handling data?
  - What is the right level and type of training to mitigate human risk?
- John uses **Nexus People Risk Explorer** (NPRE) to answer all these questions with integrated views of risk across your Proofpoint products.

← Next →

Human Centric Security



Name	Email	Title	Department
Carol Brown	carol.brown@pfpt-demo.com	Purchasing Manager	Supply Chain & Operations
Bristol Albert	z6az6ookegbs0w@acme.com	President And CEO	Acme, Inc.
Bernie Cole	v4v2u5asvb8ehw@acme.com	Sr Manager, Client Service and S...	Administration
Sieber Welch	tgpghzilb4ckqq@acme.com	Vice President, Information Secu...	Security Officer
Esta Chapman	obmgmfvr5p2fbg@acme.com	Support Supervisor I	Enterprise Support, Flex HCM
Sophronia Raymond	3pdpn0cmodq5cq@acme.com	Staff Engineer, Desktop Systems	Desktop Engineering
Merci Heath	9yebxe2tp1idhw@acme.com	Software Engineer V	Applicant Tracking IT and Produ...
Venita Delacruz	ozsg9anfbpx2ga@acme.com	District Sales Manager - SMB Sol...	Sales area 87

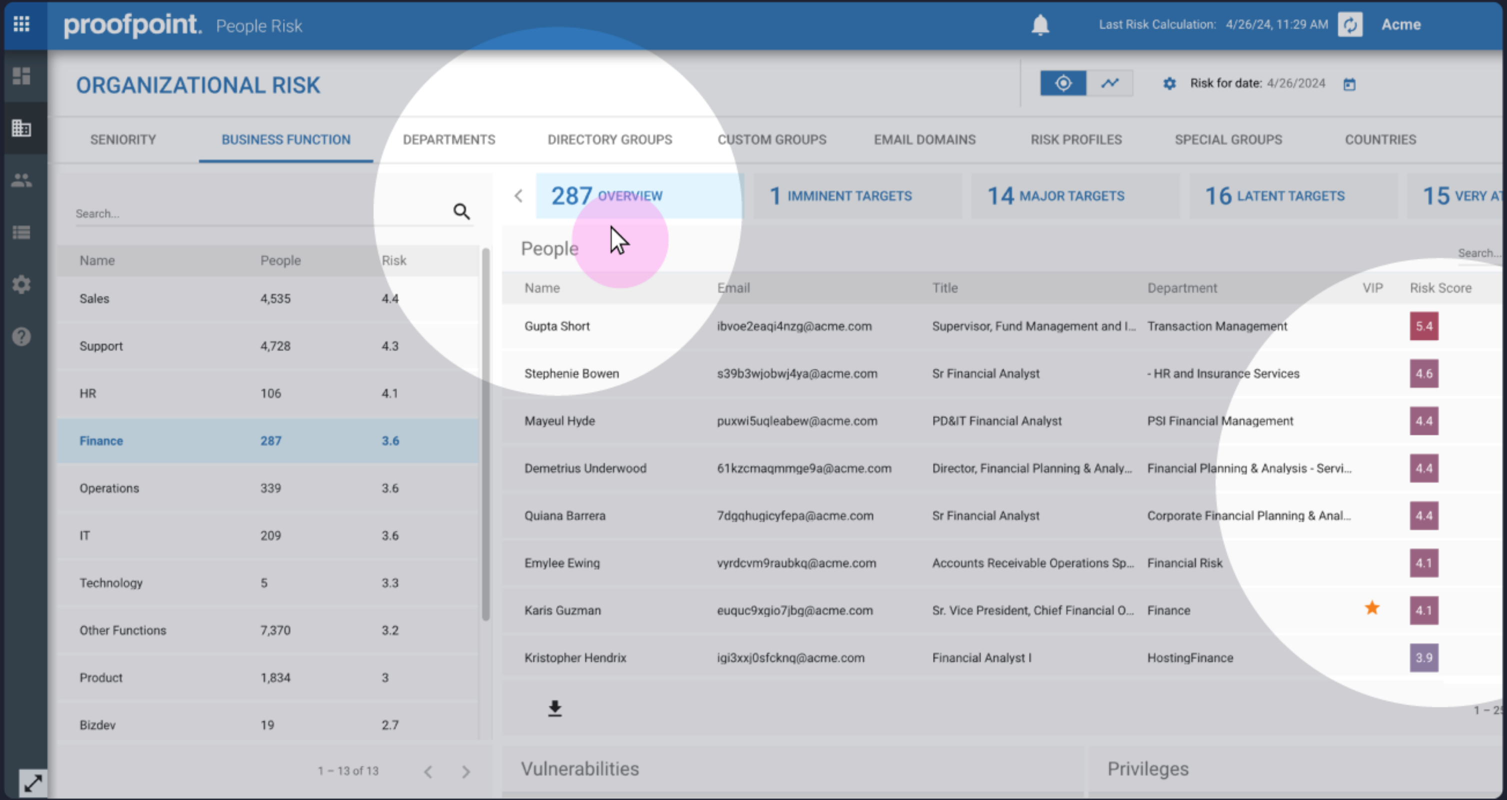
© 2024 Proofpoint Inc.

proofpoint. Understand Human Risk

ANALYST VIEW

John Shider
Security Analyst

- John navigates to look at Organizational Risk by Business Function and can see the exact list of **287** people in Finance and their risk scores.



ORGANIZATIONAL RISK

Name	People	Risk
Sales	4,535	4.4
Support	4,728	4.3
HR	106	4.1
Finance	287	3.6
Operations	339	3.6
IT	209	3.6
Technology	5	3.3
Other Functions	7,370	3.2
Product	1,834	3
Bizdev	19	2.7

1 – 13 of 13

People

Name	Email	Title	Department	VIP	Risk Score
Gupta Short	ibvoe2eaqi4nzg@acme.com	Supervisor, Fund Management and I...	Transaction Management		5.4
Stephenie Bowen	s39b3wjobwj4ya@acme.com	Sr Financial Analyst	- HR and Insurance Services		4.6
Mayeul Hyde	puxwi5uqleabew@acme.com	PD&IT Financial Analyst	PSI Financial Management		4.4
Demetrius Underwood	61kzcmaqmmge9a@acme.com	Director, Financial Planning & Analy...	Financial Planning & Analysis - Servi...		4.4
Quiana Barrera	7dgqhugicyfepa@acme.com	Sr Financial Analyst	Corporate Financial Planning & Anal...		4.4
Emylee Ewing	vyrdcvm9raubkq@acme.com	Accounts Receivable Operations Sp...	Financial Risk		4.1
Karis Guzman	euquc9xgio7jbg@acme.com	Sr. Vice President, Chief Financial O...	Finance	★	4.1
Kristopher Hendrix	igi3xxj0sfcknq@acme.com	Financial Analyst I	HostingFinance		3.9

proofpoint.

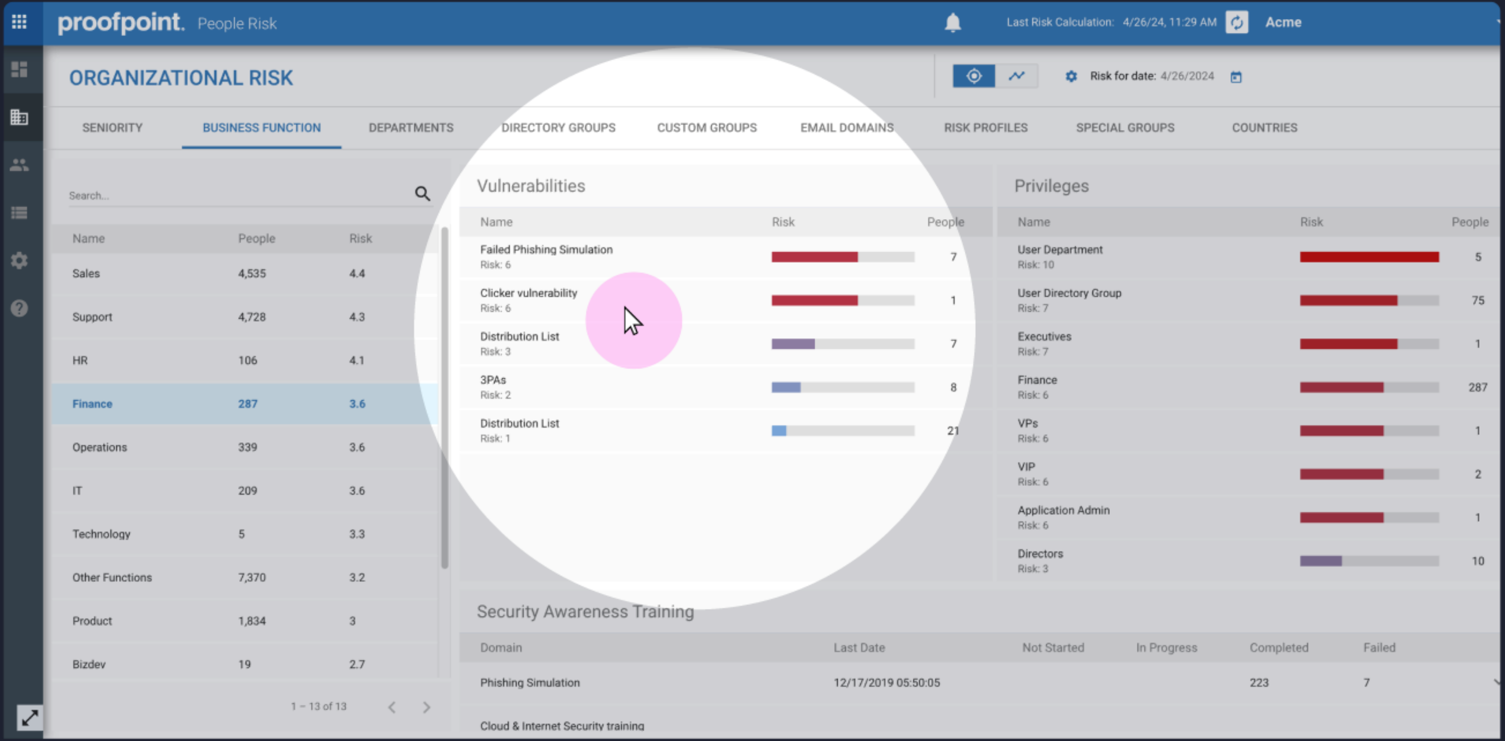
© 2024 Proofpoint Inc.

proofpoint. Understand Human Risk

ANALYST VIEW

John Shider
Security Analyst

- John scrolls to Vulnerabilities to see that within Finance:
  - 7 people failed phishing simulation within the last training period
  - 1 person clicked on a malicious link at least once in the last 30 days
- Clicker vulnerability is concerning, so John wants to see who clicked on a malicious link.



proofpoint. People Risk

Last Risk Calculation: 4/26/24, 11:29 AM Acme

ORGANIZATIONAL RISK

Risk for date: 4/26/2024

Name	People	Risk
Sales	4,535	4.4
Support	4,728	4.3
HR	106	4.1
Finance	287	3.6
Operations	339	3.6
IT	209	3.6
Technology	5	3.3
Other Functions	7,370	3.2
Product	1,834	3
Bizdev	19	2.7

1 – 13 of 13

Vulnerabilities

Name	Risk	People
Failed Phishing Simulation Risk: 6		7
Clicker vulnerability Risk: 6		1
Distribution List Risk: 3		7
3PAs Risk: 2		8
Distribution List Risk: 1		21

Privileges

Name	Risk	People
User Department Risk: 10		5
User Directory Group Risk: 7		75
Executives Risk: 7		1
Finance Risk: 6		287
VPs Risk: 6		1
VIP Risk: 6		2
Application Admin Risk: 6		1
Directors Risk: 3		10

Security Awareness Training

Domain	Last Date	Not Started	In Progress	Completed	Failed
Phishing Simulation	12/17/2019 05:50:05			223	7
Cloud & Internet Security training					

proofpoint.

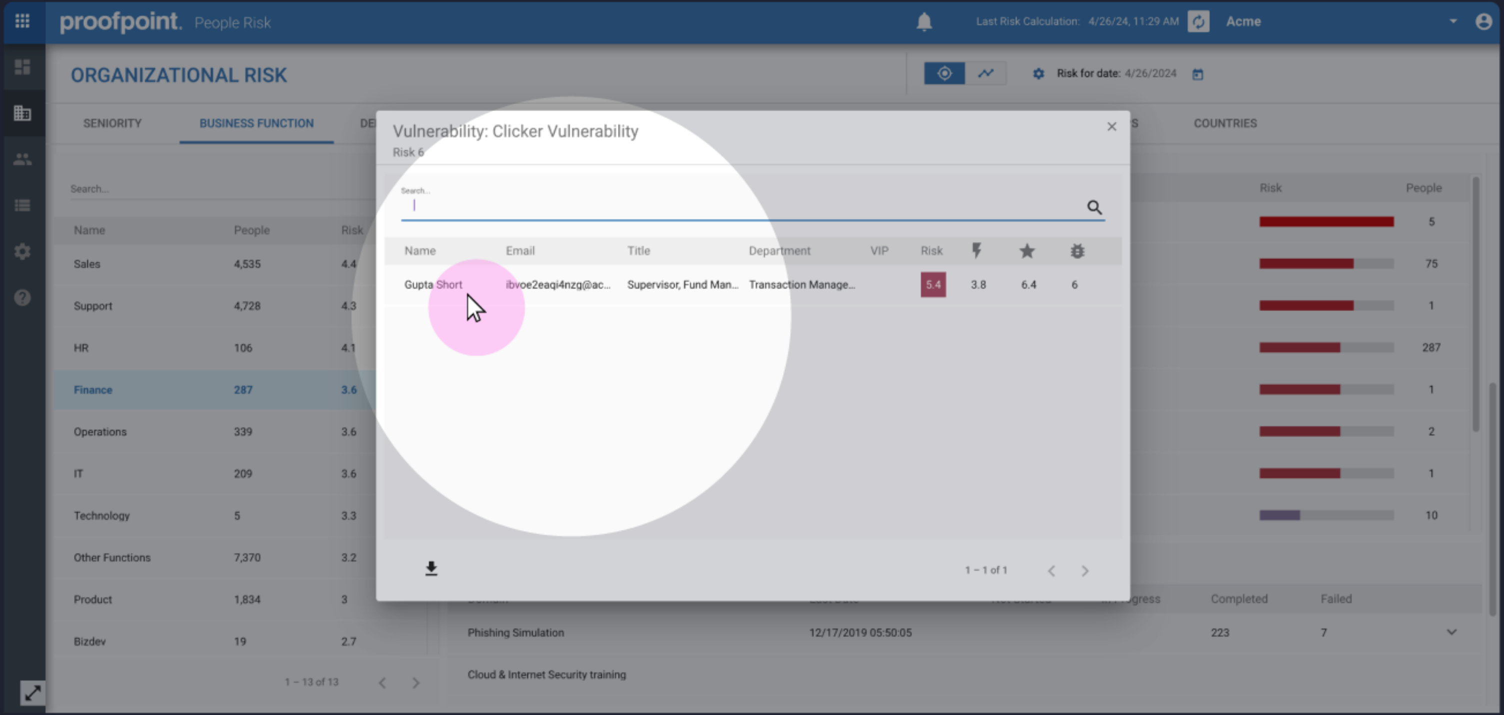
© 2024 Proofpoint Inc.

proofpoint. Understand Human Risk

ANALYST VIEW

John Shider
Security Analyst

- John finds that the person in Finance who clicked on a malicious link is Gupta Short, who is part of the Transaction Management Department
- He then clicks into Gupta's risk profile to collect more information.



Name	People	Risk
Sales	4,535	4.4
Support	4,728	4.3
HR	106	4.1
Finance	287	3.6
Operations	339	3.6
IT	209	3.6
Technology	5	3.3
Other Functions	7,370	3.2
Product	1,834	3
Bizdev	19	2.7

Vulnerability: Clicker Vulnerability
Risk 6

Name	Email	Title	Department	VIP	Risk	⚡	★	⚙
Gupta Short	ibvoe2eaqi4nzg@ac...	Supervisor, Fund Man...	Transaction Manage...		5.4	3.8	6.4	6

1 – 1 of 1

Domain	Last Date	Not Started	In Progress	Completed	Failed
Phishing Simulation	12/17/2019 05:50:05			223	7
Cloud & Internet Security training					

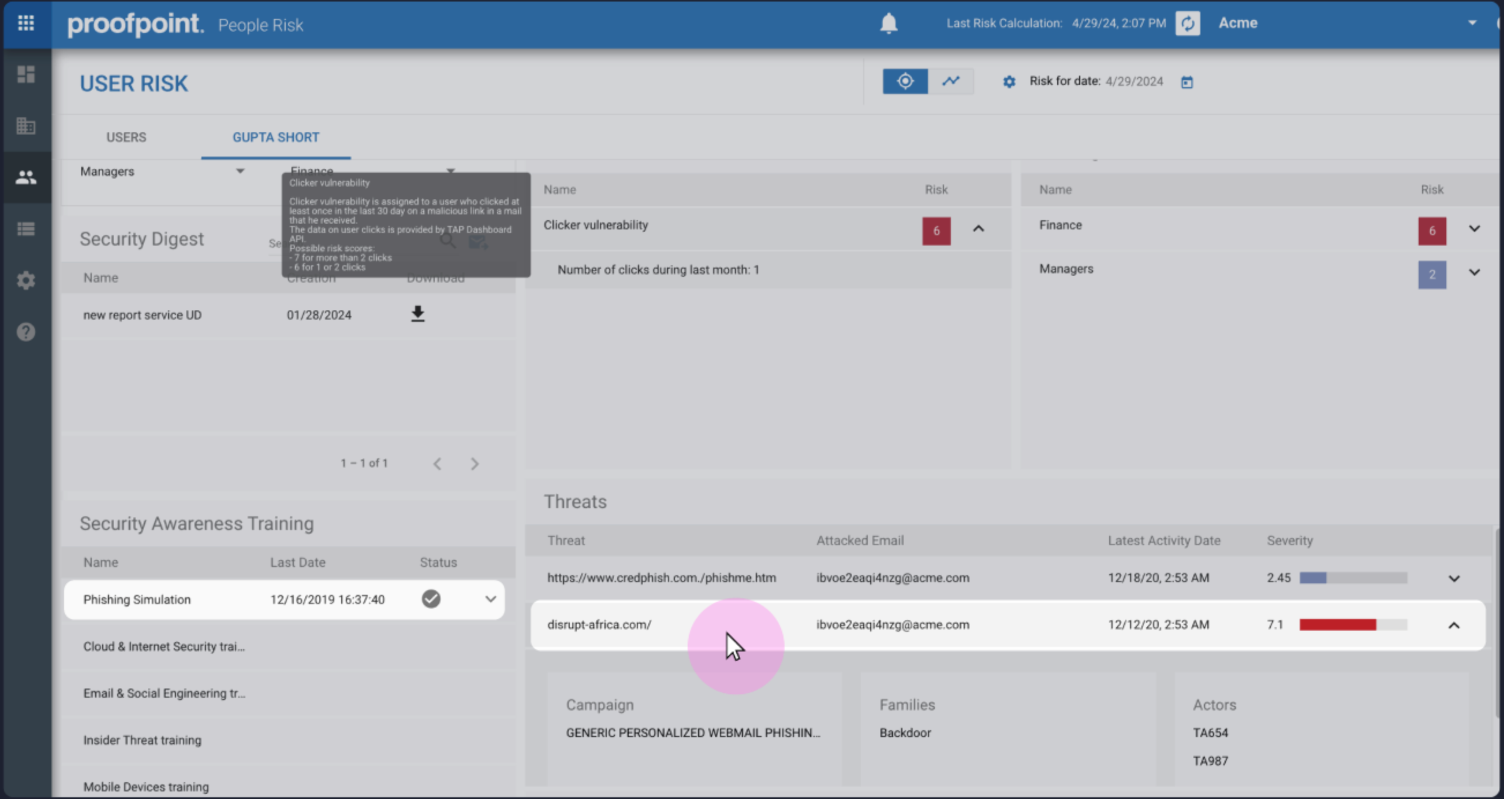
Understand Human Risk

ANALYST VIEW

John Shider
Security Analyst

- John finds out that Gupta was attacked by a credential phishing campaign using disrupt-africa.com.
- He also sees Gupta passed a phishing simulation exercise years ago, so perhaps it's time for another one!

> John can put Gupta on an Adaptive Learning Track for clickers and use a phishing simulation template from the same credential phishing campaign.



Clicker vulnerability

Clicker vulnerability is assigned to a user who clicked at least once in the last 30 day on a malicious link in a mail that he received.
The data on user clicks is provided by TAP Dashboard API.
Possible risk scores:
- 7 for more than 2 clicks
- 6 for 1 or 2 clicks

Security Digest

Name	Creation	Download
new report service UD	01/28/2024	⬇

1 – 1 of 1

Name	Risk
Clicker vulnerability	6

Number of clicks during last month: 1

Name	Risk
Finance	6
Managers	2

Security Awareness Training

Name	Last Date	Status
Phishing Simulation	12/16/2019 16:37:40	✓
Cloud & Internet Security trai...		
Email & Social Engineering tr...		
Insider Threat training		
Mobile Devices training		

Threats

Threat	Attacked Email	Latest Activity Date	Severity
https://www.credphish.com./phishme.htm	ibvoe2eaqi4nzg@acme.com	12/18/20, 2:53 AM	2.45
disrupt-africa.com/	ibvoe2eaqi4nzg@acme.com	12/12/20, 2:53 AM	7.1

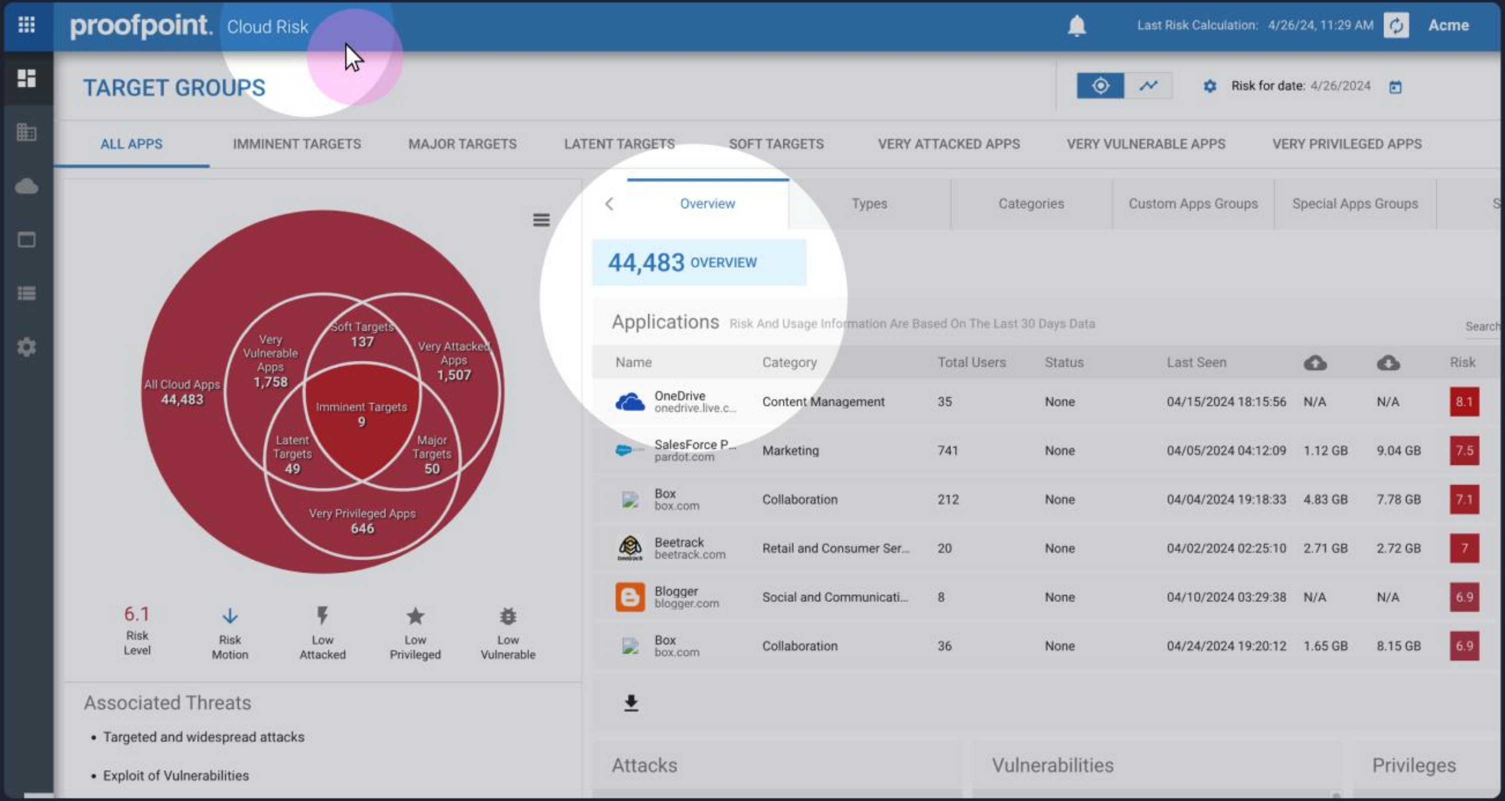
Campaign	Families	Actors
GENERIC PERSONALIZED WEBMAIL PHISHIN...	Backdoor	TA654 TA987

ANALYST VIEW

John Shider

Security Analyst

- For further investigation, John decides to look at the **Cloud Risk** view, to understand potentially risky cloud applications being used by Finance.
- Rather than parsing the 44,483 different applications, he decides to segment only by Finance.



Last Risk Calculation: 4/26/24, 11:29 AM

Risk for date: 4/26/2024

44,483 OVERVIEW

Applications Risk And Usage Information Are Based On The Last 30 Days Data

Name	Category	Total Users	Status	Last Seen	↑	↓	Risk
OneDrive onedrive.live.c...	Content Management	35	None	04/15/2024 18:15:56	N/A	N/A	8.1
SalesForce P... pardot.com	Marketing	741	None	04/05/2024 04:12:09	1.12 GB	9.04 GB	7.5
Box box.com	Collaboration	212	None	04/04/2024 19:18:33	4.83 GB	7.78 GB	7.1
Beetrack beetrack.com	Retail and Consumer Ser...	20	None	04/02/2024 02:25:10	2.71 GB	2.72 GB	7
Blogger blogger.com	Social and Communicati...	8	None	04/10/2024 03:29:38	N/A	N/A	6.9
Box box.com	Collaboration	36	None	04/24/2024 19:20:12	1.65 GB	8.15 GB	6.9

Associated Threats

- Targeted and widespread attacks
- Exploit of Vulnerabilities

← **Next →**

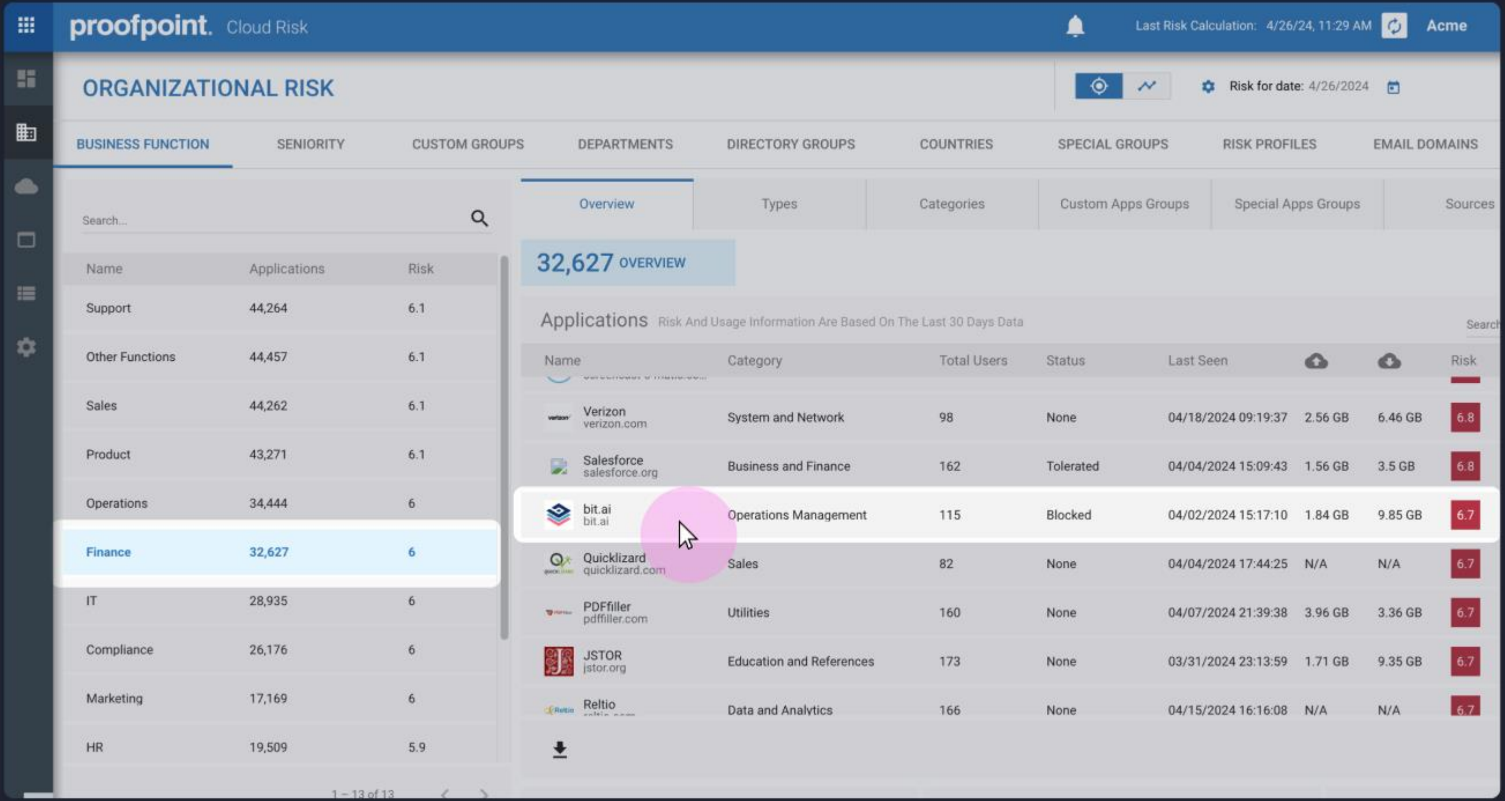
Human Centric Security

proofpoint. Understand Human Risk

ANALYST VIEW

John Shider
Security Analyst

- John sees that 32,627 risky applications are being used by Finance, most of these seem to be permitted or tolerated.
- Further scrolling shows that 115 users are using the web application **Bit.ai**, which has been blocked. John wants to learn more about **Bit.ai**.



Last Risk Calculation: 4/26/24, 11:29 AM

Risk for date: 4/26/2024

Name	Applications	Risk
Support	44,264	6.1
Other Functions	44,457	6.1
Sales	44,262	6.1
Product	43,271	6.1
Operations	34,444	6
Finance	32,627	6
IT	28,935	6
Compliance	26,176	6
Marketing	17,169	6
HR	19,509	5.9

32,627 OVERVIEW

Applications Risk And Usage Information Are Based On The Last 30 Days Data

Name	Category	Total Users	Status	Last Seen	☁↑	☁↓	Risk
Verizon verizon.com	System and Network	98	None	04/18/2024 09:19:37	2.56 GB	6.46 GB	6.8
Salesforce salesforce.org	Business and Finance	162	Tolerated	04/04/2024 15:09:43	1.56 GB	3.5 GB	6.8
bit.ai bit.ai	Operations Management	115	Blocked	04/02/2024 15:17:10	1.84 GB	9.85 GB	6.7
Quicklizard quicklizard.com	Sales	82	None	04/04/2024 17:44:25	N/A	N/A	6.7
PDFfiller pdffiller.com	Utilities	160	None	04/07/2024 21:39:38	3.96 GB	3.36 GB	6.7
JSTOR jstor.org	Education and References	173	None	03/31/2024 23:13:59	1.71 GB	9.35 GB	6.7
Reltio	Data and Analytics	166	None	04/15/2024 16:16:08	N/A	N/A	6.7

© 2024 Proofpoint Inc.

proofpoint. Understand Human Risk

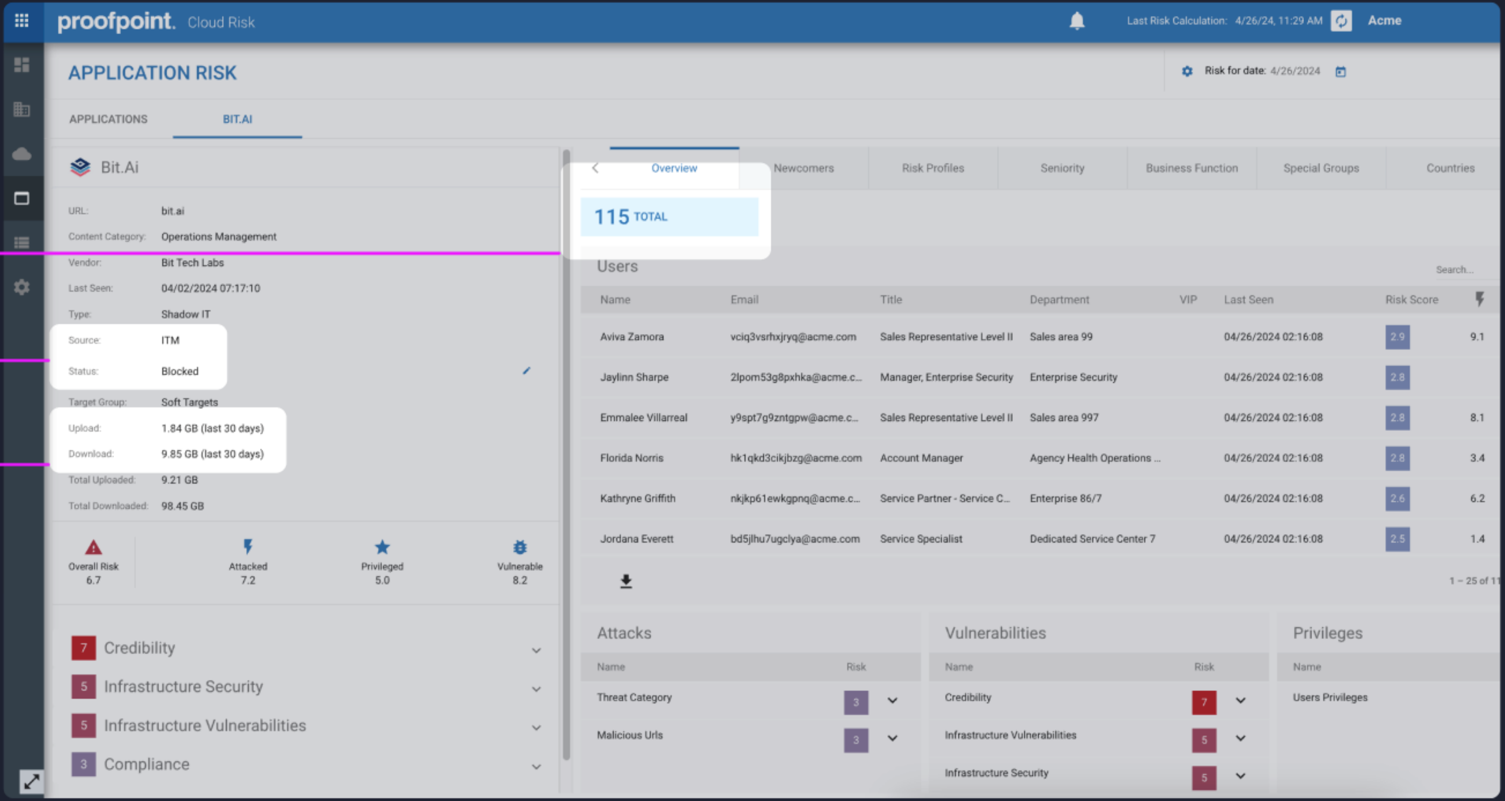
ANALYST VIEW

John Shider
Security Analyst

- John sees a exact list of 115 users of the cloud app
- The app was blocked by ITM (Insider Threat Management) and considered a Soft Target (vulnerable and attacked).
- 1.84 GB was uploaded and 9.85 GB was downloaded in the past 30 days.

Next →

Human Centric Security



proofpoint. Cloud Risk

Last Risk Calculation: 4/26/24, 11:29 AM

Acme

APPLICATION RISK

Risk for date: 4/26/2024

Bit.Ai

URL:	bit.ai
Content Category:	Operations Management
Vendor:	Bit Tech Labs
Last Seen:	04/02/2024 07:17:10
Type:	Shadow IT
Source:	ITM
Status:	Blocked
Target Group:	Soft Targets
Upload:	1.84 GB (last 30 days)
Download:	9.85 GB (last 30 days)
Total Uploaded:	9.21 GB
Total Downloaded:	98.45 GB

Overall Risk	Attacked	Privileged	Vulnerable
6.7	7.2	5.0	8.2

- 7 Credibility
- 5 Infrastructure Security
- 5 Infrastructure Vulnerabilities
- 3 Compliance

115 TOTAL

Users

Name	Email	Title	Department	VIP	Last Seen	Risk Score	⚡
Aviva Zamora	vciq3vsrhxjryq@acme.com	Sales Representative Level II	Sales area 99		04/26/2024 02:16:08	2.9	9.1
Jaylinn Sharpe	2lpom53g8pxhka@acme.c...	Manager, Enterprise Security	Enterprise Security		04/26/2024 02:16:08	2.8	
Emmalee Villarreal	y9spt7g9zntgpw@acme.c...	Sales Representative Level II	Sales area 997		04/26/2024 02:16:08	2.8	8.1
Florida Norris	hk1qkd3cikjbzg@acme.com	Account Manager	Agency Health Operations ...		04/26/2024 02:16:08	2.8	3.4
Kathryne Griffith	nkjkp61ewkgpnq@acme.c...	Service Partner - Service C...	Enterprise 86/7		04/26/2024 02:16:08	2.6	6.2
Jordana Everett	bd5jlhu7ugclya@acme.com	Service Specialist	Dedicated Service Center 7		04/26/2024 02:16:08	2.5	1.4

1 – 25 of 11

Attacks

Name	Risk
Threat Category	3
Malicious Urls	3

Vulnerabilities

Name	Risk
Credibility	7
Infrastructure Vulnerabilities	5
Infrastructure Security	5

Privileges

Name
Users Privileges

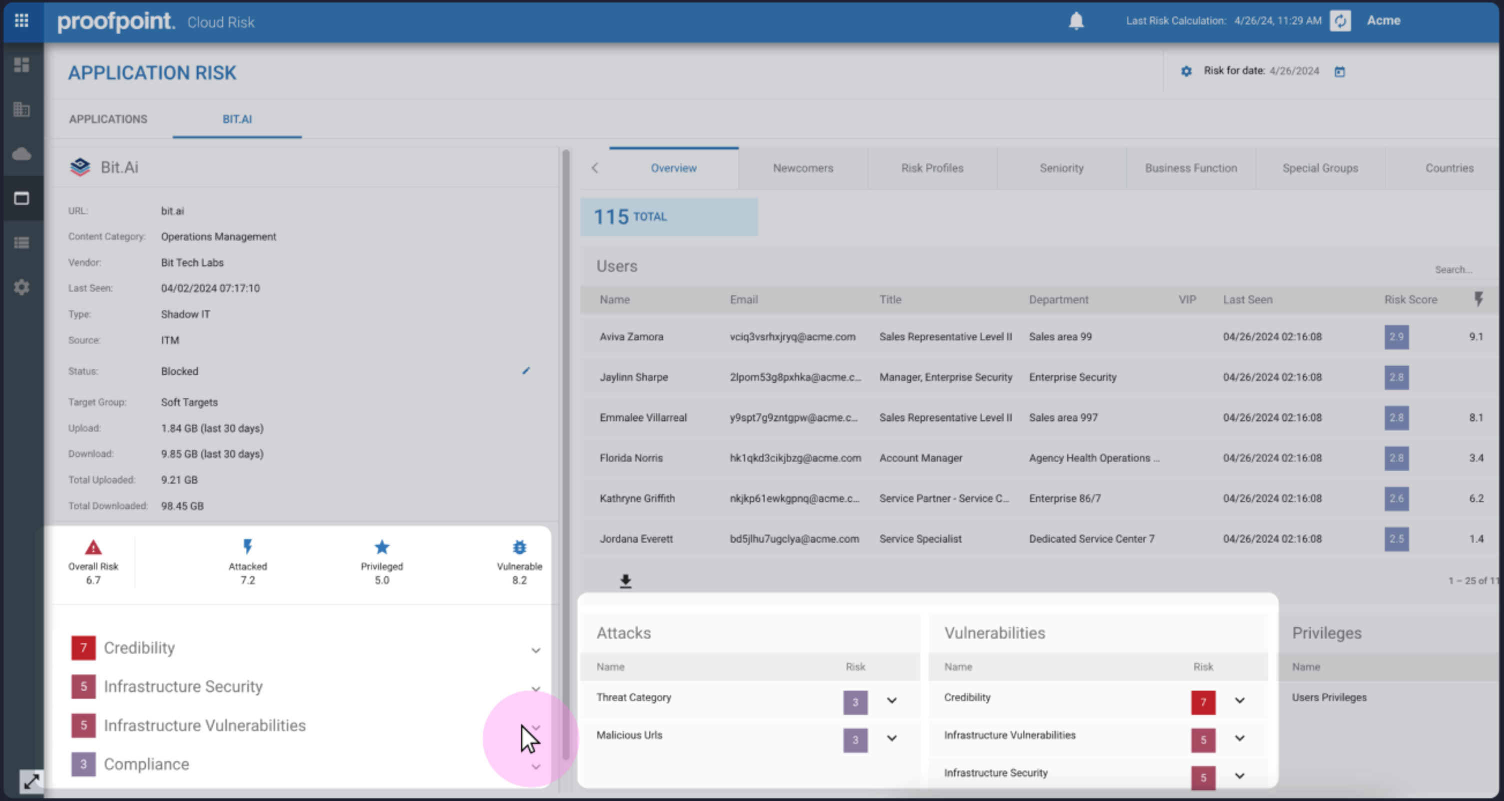
© 2024 Proofpoint Inc.

proofpoint. Understand Human Risk

ANALYST VIEW

John Shider
Security Analyst

- John can look at the overall Application Risk profile and from there:
  - Discuss with the business users, whether the app should be unblocked.
  - Discuss with the security team, whether they can manage those vulnerabilities and risks.



proofpoint. Cloud Risk

Last Risk Calculation: 4/26/24, 11:29 AM Acme

APPLICATION RISK

Risk for date: 4/26/2024

APPLICATIONS BIT.AI

Bit.Ai

URL: bit.ai
Content Category: Operations Management
Vendor: Bit Tech Labs
Last Seen: 04/02/2024 07:17:10
Type: Shadow IT
Source: ITM
Status: Blocked
Target Group: Soft Targets
Upload: 1.84 GB (last 30 days)
Download: 9.85 GB (last 30 days)
Total Uploaded: 9.21 GB
Total Downloaded: 98.45 GB

Overall Risk	Attacked	Privileged	Vulnerable
6.7	7.2	5.0	8.2

7	Credibility
5	Infrastructure Security
5	Infrastructure Vulnerabilities
3	Compliance

Overview | Newcomers | Risk Profiles | Seniority | Business Function | Special Groups | Countries

115 TOTAL

Users

Name	Email	Title	Department	VIP	Last Seen	Risk Score	⚡
Aviva Zamora	vciq3vsrhxjryq@acme.com	Sales Representative Level II	Sales area 99		04/26/2024 02:16:08	2.9	9.1
Jaylinn Sharpe	2lpom53g8pxhka@acme.c...	Manager, Enterprise Security	Enterprise Security		04/26/2024 02:16:08	2.8	
Emmalee Villarreal	y9spt7g9zntgpw@acme.c...	Sales Representative Level II	Sales area 997		04/26/2024 02:16:08	2.8	8.1
Florida Norris	hk1qkd3cikjbzg@acme.com	Account Manager	Agency Health Operations ...		04/26/2024 02:16:08	2.8	3.4
Kathryne Griffith	nkjkp61ewkgpnq@acme.c...	Service Partner - Service C...	Enterprise 86/7		04/26/2024 02:16:08	2.6	6.2
Jordana Everett	bd5jlhu7ugclya@acme.com	Service Specialist	Dedicated Service Center 7		04/26/2024 02:16:08	2.5	1.4

Attacks

Name	Risk
Threat Category	3
Malicious Urls	3

Vulnerabilities

Name	Risk
Credibility	7
Infrastructure Vulnerabilities	5
Infrastructure Security	5

Privileges

Name
Users Privileges

Back to Main Menu →

Human Centric Security

proofpoint®

Protect People.
Defend Data.