Probable UX Audit — Hoxhunt Respond

Based on public product research and the Senior Product Designer role brief

Intake → Ingest & normalize signals

Triage → Prioritize & route to analyst

Investigation → Analyze, enrich & correlate

Remediation → Respond, contain & notify

Integration Event → Close loop & learn across systems

What the public research suggests

- Multi-product platform covering Awareness, Phishing, and Incident Response.
- Operator console for triage, investigation, remediation, and reporting.
- AI-assisted classification, clustering, and auto-resolution of low-risk items.
- Strong employee-feedback loop to improve detections and reduce risk.

Likely UX friction points

Table overload

Dense tables, many columns and badges create cognitive overload and scanning fatigue.

Weak prioritization hierarchy

Risk signals aren't surfaced consistently; important items get buried.

Legacy pattern inconsistency

Mixed patterns and terminology increase learning cost and slow down analysts.

Manual-filter burden

Heavy reliance on filters and custom views to find the right work.

Low AI explainability

AI decisions lack clear rationale, reducing trust and adoption.

Fragmented feedback loop

User and remediation feedback flows are siloed across surfaces.

Highest-value redesign opportunities

Decision-first queue

Outcome-oriented queue with clear next best action and confidence indicators.

Smarter default views

Context-aware defaults, saved views, and presets tailored to analyst roles.

Reusable workbench components

Consistent patterns, side panels, and activity timelines for faster investigation.

Evidence-first AI summaries

Show why it matters: key evidence, correlations, and confidence upfront.

Unified cross-channel incident model

One incident model across email, chat, endpoints, and integrations with shared context.

Clearer analyst-to-user communication state

Visible status, templates, and channels for updates and feedback.

Design principles

Clarity over density

Surface what matters; reduce cognitive load.

Progressive disclosure

Reveal detail at the right moment, not all at once.

Confidence with control

Make AI trustworthy and analyst-in-command.

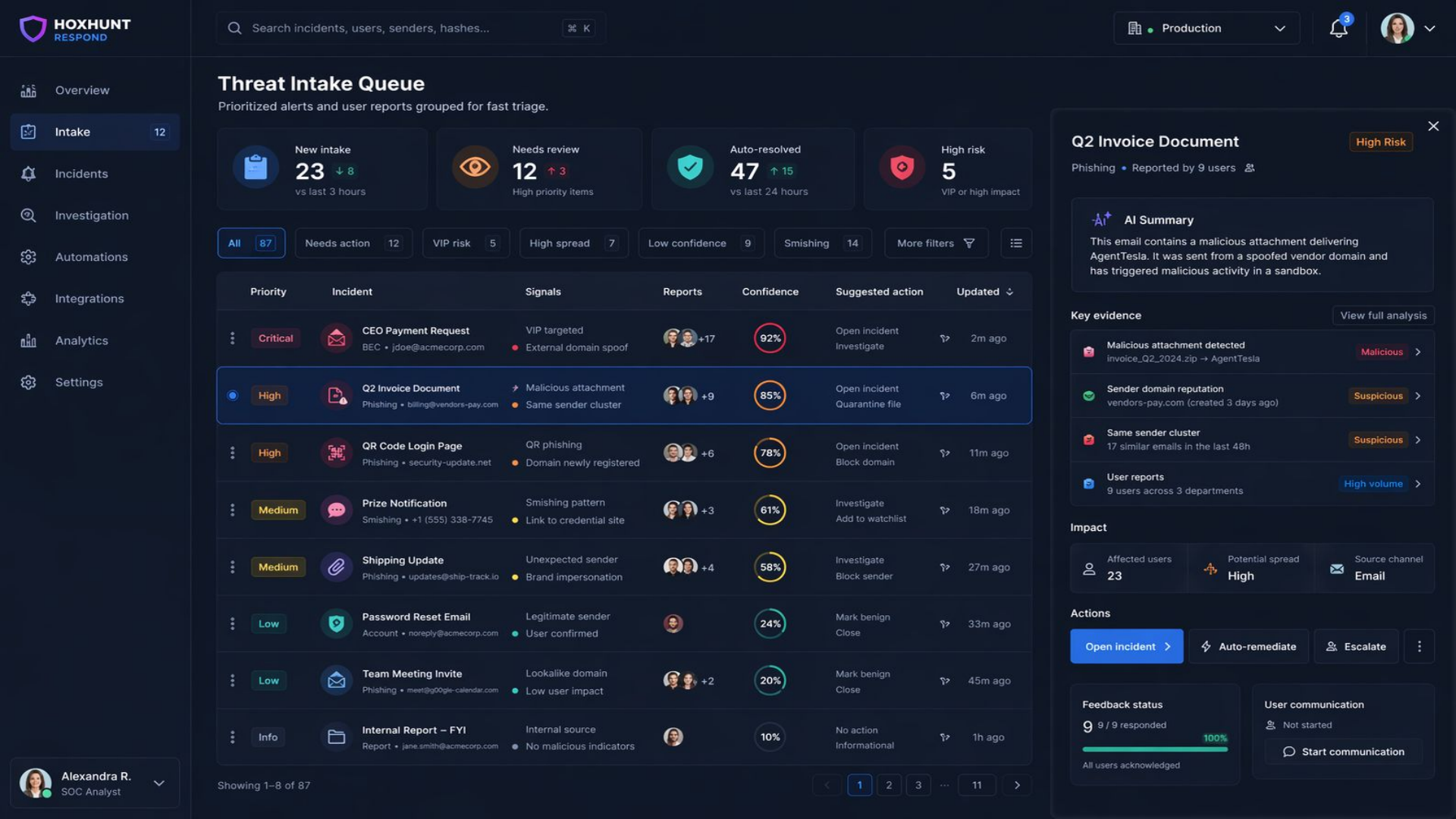
Reusable systems

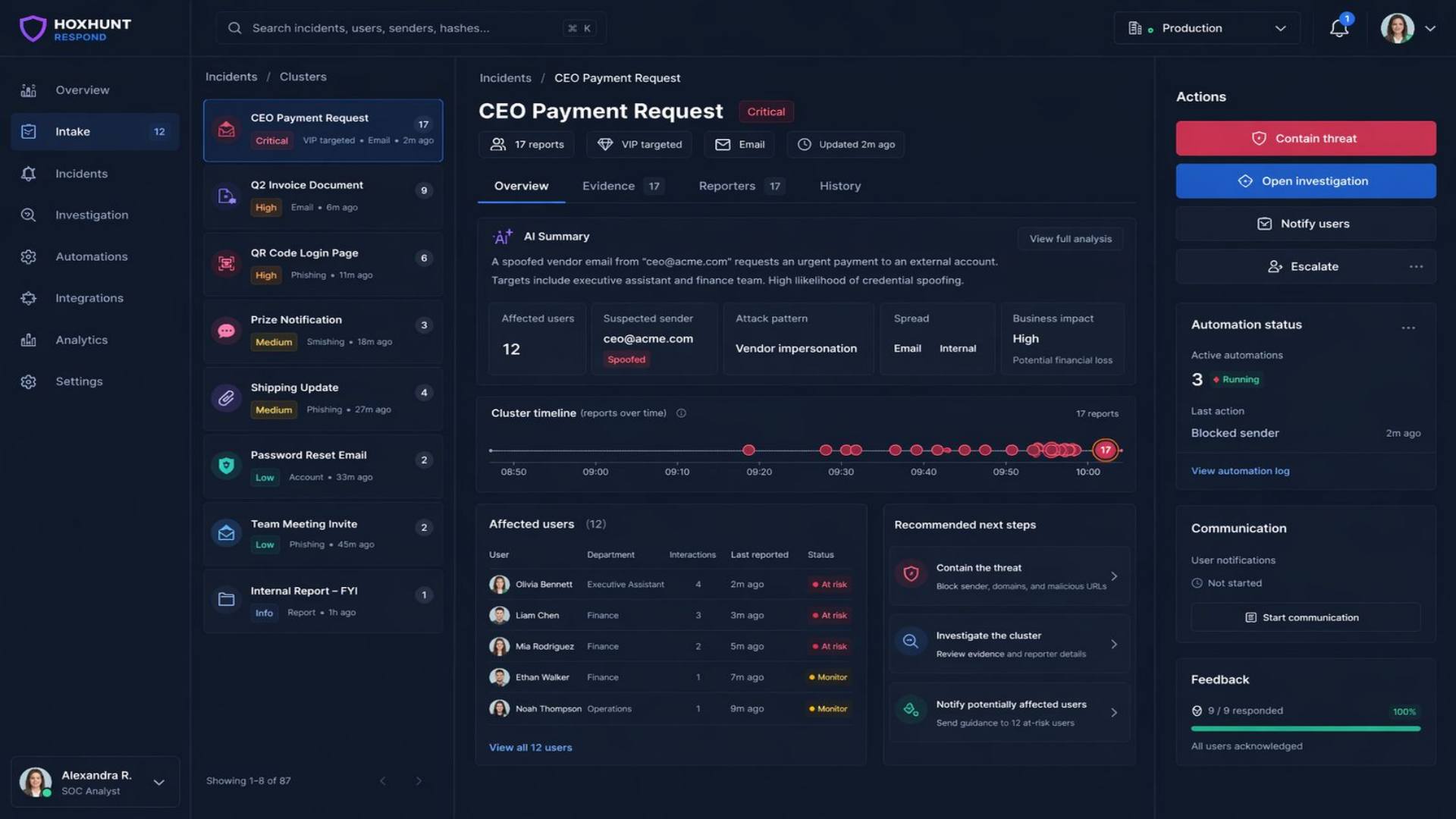
Consistent components speed up work and scale.

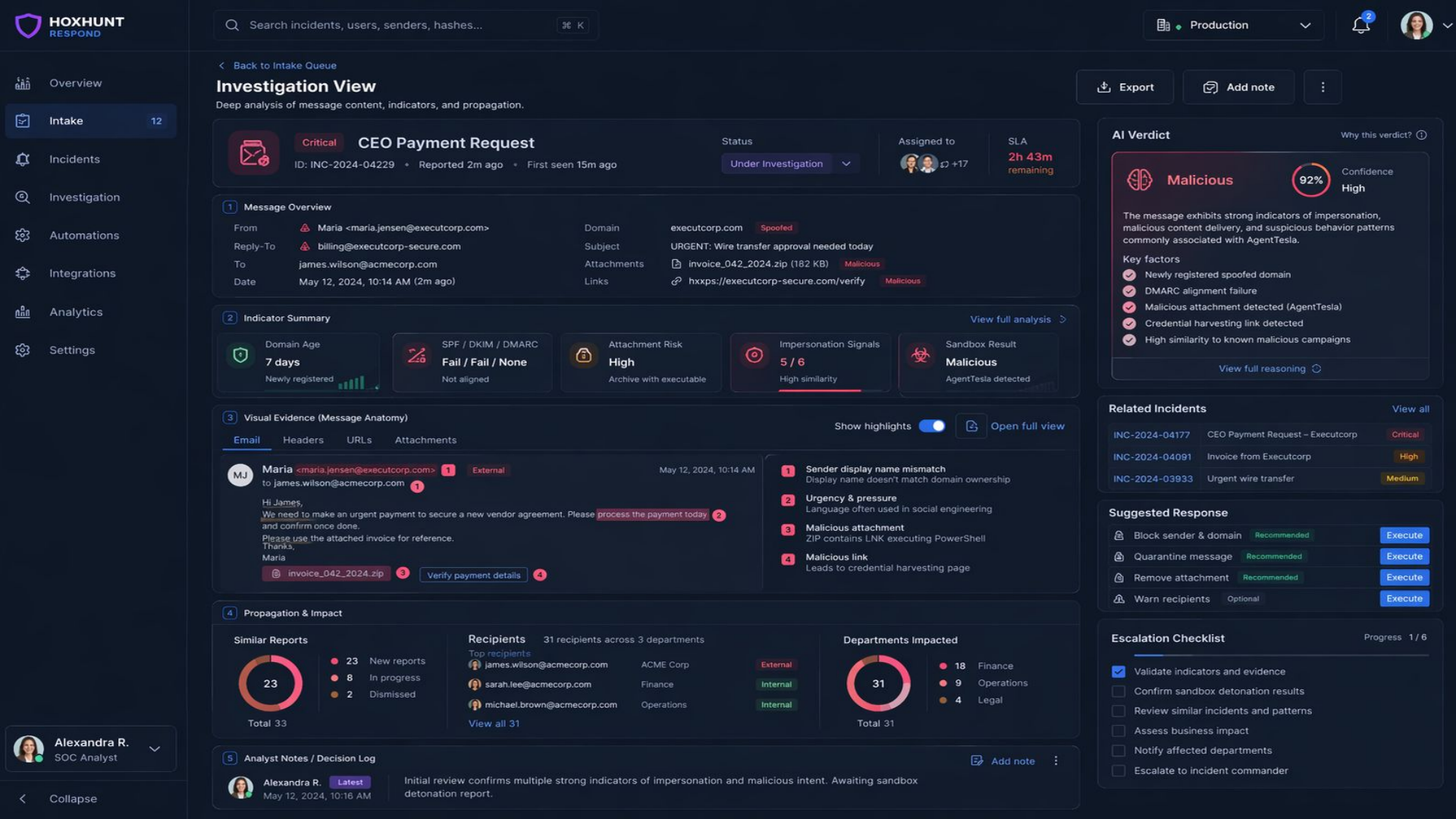
First screens to prototype

1. Threat Intake Queue
2. Incident Workspace
3. Investigation View
4. Remediation Plan
5. Integration Event

Hypothesis-led concept, not an official Hoxhunt design.


HOXHUNT
RESPOND
Search incidents, users, senders, hashes... ⌘ K
Production
3
Overview
Intake 12
Incidents
Investigation
Automations
Integrations
Analytics
Settings
Alexandra R.
SOC Analyst
Threat Intake Queue
Prioritized alerts and user reports grouped for fast triage.
New intake 23 ↓ 8 vs last 3 hours
Needs review 12 ↑ 3 High priority items
Auto-resolved 47 ↑ 15 vs last 24 hours
High risk 5 VIP or high impact
All 87
Needs action 12
VIP risk 5
High spread 7
Low confidence 9
Smishing 14
More filters
Priority
Incident
Signals
Reports
Confidence
Suggested action
Updated
Critical
CEO Payment Request
BEC • jdoe@acmecorp.com
VIP targeted
External domain spoof
+17
92%
Open incident
Investigate
2m ago
High
Q2 Invoice Document
Phishing • billing@vendors-pay.com
Malicious attachment
Same sender cluster
+9
85%
Open incident
Quarantine file
6m ago
High
QR Code Login Page
Phishing • security-update.net
QR phishing
Domain newly registered
+6
78%
Open incident
Block domain
11m ago
Medium
Prize Notification
Smishing • +1 (555) 338-7745
Smishing pattern
Link to credential site
+3
61%
Investigate
Add to watchlist
18m ago
Medium
Shipping Update
Phishing • updates@ship-track.io
Unexpected sender
Brand impersonation
+4
58%
Investigate
Block sender
27m ago
Low
Password Reset Email
Account • noreply@acmecorp.com
Legitimate sender
User confirmed
24%
Mark benign
Close
33m ago
Low
Team Meeting Invite
Phishing • meet@g00gle-calendar.com
Lookalike domain
Low user impact
+2
20%
Mark benign
Close
45m ago
Info
Internal Report – FYI
Report • jane.smith@acmecorp.com
Internal source
No malicious indicators
10%
No action
Informational
1h ago
Showing 1–8 of 87
1 2 3 ... 11
Q2 Invoice Document
High Risk
Phishing • Reported by 9 users
AI Summary
This email contains a malicious attachment delivering AgentTesla. It was sent from a spoofed vendor domain and has triggered malicious activity in a sandbox.
Key evidence
View full analysis
Malicious attachment detected
invoice_Q2_2024.zip → AgentTesla
Malicious
Sender domain reputation
vendors-pay.com (created 3 days ago)
Suspicious
Same sender cluster
17 similar emails in the last 48h
Suspicious
User reports
9 users across 3 departments
High volume
Impact
Affected users 23
Potential spread High
Source channel Email
Actions
Open incident
Auto-remediate
Escalate
Feedback status
9 / 9 responded
100%
All users acknowledged
User communication
Not started
Start communication


HOXHUNT
RESPOND
Search incidents, users, senders, hashes...
⌘ K
Production
Overview
Intake 12
Incidents
Investigation
Automations
Integrations
Analytics
Settings
Incidents / Clusters
CEO Payment Request 17
Critical VIP targeted • Email • 2m ago
Q2 Invoice Document 9
High Email • 6m ago
QR Code Login Page 6
High Phishing • 11m ago
Prize Notification 3
Medium Smishing • 18m ago
Shipping Update 4
Medium Phishing • 27m ago
Password Reset Email 2
Low Account • 33m ago
Team Meeting Invite 2
Low Phishing • 45m ago
Internal Report – FYI 1
Info Report • 1h ago
Showing 1-8 of 87
Alexandra R.
SOC Analyst
Incidents / CEO Payment Request
CEO Payment Request
Critical
17 reports
VIP targeted
Email
Updated 2m ago
Overview
Evidence 17
Reporters 17
History
AI Summary
View full analysis
A spoofed vendor email from "ceo@acme.com" requests an urgent payment to an external account.
Targets include executive assistant and finance team. High liikelihood of credential spoofing.
Affected users
12
Suspected sender
ceo@acme.com
Spoofed
Attack pattern
Vendor impersonation
Spread
Email
Internal
Business impact
High
Potential financial loss
Cluster timeline (reports over time)
17 reports
08:50
09:00
09:10
09:20
09:30
09:40
09:50
10:00
17
Affected users (12)
User
Department
Interactions
Last reported
Status
Olivia Bennett
Executive Assistant
4
2m ago
At risk
Liam Chen
Finance
3
3m ago
At risk
Mia Rodriguez
Finance
2
5m ago
At risk
Ethan Walker
Finance
1
7m ago
Monitor
Noah Thompson
Operations
1
9m ago
Monitor
View all 12 users
Recommended next steps
Contain the threat
Block sender, domains, and malicious URLs
Investigate the cluster
Review evidence and reporter details
Notify potentially affected users
Send guidance to 12 at-risk users
Actions
Contain threat
Open investigation
Notify users
Escalate
Automation status
Active automations
3
Running
Last action
Blocked sender
2m ago
View automation log
Communication
User notifications
Not started
Start communication
Feedback
9 / 9 responded
100%
All users acknowledged


HOXHUNT
RESPOND
Search incidents, users, senders, hashes... ⌘ K
Production
Overview
Intake 12
Incidents
Investigation
Automations
Integrations
Analytics
Settings
Alexandra R.
SOC Analyst
Collapse
Back to Intake Queue
Investigation View
Deep analysis of message content, indicators, and propagation.
Export
Add note
Critical
CEO Payment Request
ID: INC-2024-04229 • Reported 2m ago • First seen 15m ago
Status
Under Investigation
Assigned to
+17
SLA
2h 43m
remaining
1 Message Overview
From Maria <maria.jensen@executcorp.com>
Reply-To billing@executcorp-secure.com
To james.wilson@acmecorp.com
Date May 12, 2024, 10:14 AM (2m ago)
Domain executcorp.com Spoofed
Subject URGENT: Wire transfer approval needed today
Attachments invoice_042_2024.zip (182 KB) Malicious
Links hxxps://executcorp-secure.com/verify Malicious
2 Indicator Summary
View full analysis
Domain Age
7 days
Newly registered
SPF / DKIM / DMARC
Fail / Fail / None
Not aligned
Attachment Risk
High
Archive with executable
Impersonation Signals
5 / 6
High similarity
Sandbox Result
Malicious
AgentTesla detected
3 Visual Evidence (Message Anatomy)
Show highlights
Open full view
Email
Headers
URLs
Attachments
MJ
Maria <maria.jensen@executcorp.com> 1 External
to james.wilson@acmecorp.com 1
May 12, 2024, 10:14 AM
Hi James,
We need to make an urgent payment to secure a new vendor agreement. Please process the payment today 2
and confirm once done.
Please use the attached invoice for reference.
Thanks,
Maria
invoice_042_2024.zip 3
Verify payment details 4
1 Sender display name mismatch
Display name doesn't match domain ownership
2 Urgency & pressure
Language often used in social engineering
3 Malicious attachment
ZIP contains LNK executing PowerShell
4 Malicious link
Leads to credential harvesting page
4 Propagation & Impact
Similar Reports
23
Total 33
23 New reports
8 In progress
2 Dismissed
Recipients
31 recipients across 3 departments
Top recipients
james.wilson@acmecorp.com ACME Corp External
sarah.lee@acmecorp.com Finance Internal
michael.brown@acmecorp.com Operations Internal
View all 31
Departments Impacted
31
Total 31
18 Finance
9 Operations
4 Legal
5 Analyst Notes / Decision Log
Add note
Alexandra R. Latest
May 12, 2024, 10:16 AM
Initial review confirms multiple strong indicators of impersonation and malicious intent. Awaiting sandbox detonation report.
AI Verdict
Why this verdict?
Malicious
92%
Confidence
High
The message exhibits strong indicators of impersonation, malicious content delivery, and suspicious behavior patterns commonly associated with AgentTesla.
Key factors
Newly registered spoofed domain
DMARC alignment failure
Malicious attachment detected (AgentTesla)
Credential harvesting link detected
High similarity to known malicious campaigns
View full reasoning
Related Incidents
View all
INC-2024-04177 CEO Payment Request – Executcorp Critical
INC-2024-04091 Invoice from Executcorp High
INC-2024-03933 Urgent wire transfer Medium
Suggested Response
Block sender & domain Recommended Execute
Quarantine message Recommended Execute
Remove attachment Recommended Execute
Warn recipients Optional Execute
Escalation Checklist
Progress 1 / 6
Validate indicators and evidence
Confirm sandbox detonation results
Review similar incidents and patterns
Assess business impact
Notify affected departments
Escalate to incident commander

Overview
Intake 12
Incidents
Investigation
Automations
Integrations
Analytics
Settings

Remediation Plan

Preview, validate, and execute response actions with confidence.

Incident
CEO Payment Request
INC-102_2024-02-24 • Reported 2h ago

Severity
Critical

1 Intake — 2 Investigation — 3 Remediation — 4 Post-Incident

Overall risk
92%
Critical

Scope
23
Affected users

Confidence
85%
High

Expected impact
High
Risk reduction

Est. completion time
18–22 min
With automation

Remediation action plan

Review each action before execution. Actions will run in sequence.

Reorder | Add action

#	Action	Status	Owner	Destination	Safeguards / Preview	
1	Quarantine messages Move detected messages to quarantine	Pending	Auto (Respond)	Microsoft 365	Will move 32 messages Older than 30 days excluded	☑
2	Block sender/domain Block malicious sender and related domain	Pending	Auto (Respond)	Microsoft 365	Block sender: agentTesla Block domain: spoofed-vendor.com	☑
3	Remove malicious URLs Revoke and remove URLs from messages	Pending	Auto (Respond)	Microsoft 365 Defender	5 URLs will be removed Safe links will be updated	☑
4	Notify affected users Send notification to impacted users	Pending	Alexandra R.	Email	Message preview available 23 recipients	☑
5	Open post-incident follow-up Create follow-up tasks and review	Pending	Auto (Respond)	Hoxhunt	Create incident summary Schedule follow-up in 48h	☑

☑ Analyst approval required
Require my approval before executing each action
Recommended

☑ Rollback enabled
Automatically rollback actions if issues are detected
Safe by default

☐ Exclude list
Manage exclusions
4 users • 1 domain • 2 URLs

☑ Dry-run preview
Simulate actions and show results before execution
Recommended

Run dry test
Simulate all actions

Execute remediation
Execute 5 actions in sequence

Actions are performed using automated playbooks with built-in safeguards.

Impact & preview

Affected mailboxes — View list
23
Critical 5 High 12 Medium 6

Estimated completion time
18–22 min With automation • Business hours

Automation playbook
Phishing – Containment & Remediation v2.4 Verified
View playbook details

Audit trail
All actions will be logged with before/after state and user attribution.
Full audit log available after execution.

User communication preview

Email notification to affected users

```
Subject: Important: Potential phishing email contained

Hello,
We detected and removed a suspicious email that was sent to you. The message has been quarantined and any links have been disabled.

If you clicked on any links or shared any information, please contact the IT team immediately.

Thank you,
Security Team
```

Delivery via Microsoft 365 • 23 recipients

Overview
Intake 12
Incidents
Investigation
Automations
Integrations
Analytics
Settings

Integration Event

Incident data synchronized to downstream systems with traceable status.

CEO Payment Request — Incident
Remediated — Incident status
Synced — Integration state

Actions

← Back to incident

Event summary

Event ID	Source incident	Triggered by	Timestamp	Destination system
INT-2025-05-15-7F3A	INC-2025-05-15-00087	Alexandra R.	May 15, 2025 10:42:17 AM UTC	ServiceNow — ServiceNow ITSM

Payload preview

View full payload

- Title: CEO Payment Request
- Description: Phishing email requesting payment with spoofed domain and malicious attachment.
- Threat type: Business Email Compromise
- Severity: High
- Category: Phishing
- Detected by: Hoxhunt Phishing Defense
- Status: Remediated
- Assigned to: Alexandra R. (SOC Analyst)
- Tags: phishing, bec, attachment, +2
- Incident ID: INC-2025-05-15-00087

Status timeline

Synced

Queued	Sent	Acknowledged	Ticket created
10:42:17 AM	10:42:18 AM	10:42:19 AM	10:42:21 AM ServiceNow

Field mapping

Hoxhunt field	Mapped to (ServiceNow)	Status
Title	short_description	Mapped
Description	description	Mapped
Severity	u_risk_level	Mapped
Incident ID	u_hoxhunt_incident_id	Mapped
Status	state	Mapped

View all mappings

Retry / error handling

- Retry policy — 3 attempts with exponential backoff — Edit
- On failure — Alert SOC channel and mark as Failed — Edit
- Dead-letter queue — Failed events stored for 7 days — View DLQ
- Last retry —

Linked systems

Splunk Enterprise	SIEM	Synced 10:42:19 AM
Microsoft Sentinel	SIEM	Synced 10:42:20 AM
ServiceNow ITSM	Ticketing	Synced 10:42:21 AM
Slack #sec-ops	Notification	Delivered 10:42:22 AM

View all integrations

Audit trail

Export audit log

10:42:17 AM	Event created	Alexandra R.
10:42:18 AM	Event sent to ServiceNow	System
10:42:19 AM	Acknowledged by ServiceNow	ServiceNow Integration
10:42:21 AM	Ticket created	ServiceNow Integration

View full audit trail

Follow-up automation

View automation

ServiceNow Playbook: Phishing Incident — Started

Triggered 10:42:21 AM • Run ID: PLB-2025-05-15-42

Intake › Enrich › Notify › Contain › Retrive

Delivery metrics

Deliveries	Avg. latency	Failures	Retries
4 / 4 (100%)	1.2s Last 24h	0 Last 24h	0 Last 24h

Re-send event | Open ticket | View payload | More actions