pennAware

Incident Responder

Incident Responder

When you have been breached, time is critical. PennAware Incident Responder automates response processes and works at the inbox level to quickly close down and contain active threats.

SAVE TIME, RESPOND QUICKER

SAVE MONEY, FREE INTEGRATIONS

REDUCE TECHNICAL DEPENDENCY

Over 90% of successful data breaches are initiated by an email-based attack costing businesses $3 trillion per year and driving considerable technological investments, such as firewalls and anti-spam, to provide protection.

Technology solutions will never detect and block 100% of email-based attacks, leaving you reliant on the response of your users. How do your users report a suspicious email? How do you respond to these events?

INCIDENT RESPONDER WORKFLOW

Incidents of email-based attack are reported by end-users (using our Outlook plugin), SOC team members and 3rd party IOC feeds to the PennAware Incident Response Platform (IRP).

Once received, the IRP analyses the header, body and attachments using our proprietary technology in addition to a number of integrated, best-in-class services for Anti-Spam, URL Reputation, Anti-Virus, Malware Sandboxing etc.

PennAware will also integrate and automate other threat analysis services you may have, such as Fireeye, Bluecoat or Palo Alto, saving you time and reducing your technical dependency. It is a simple process to create custom rules, playbooks and workflow to ensure PennAware IRP responds to threats in ways that suit your specific policies.

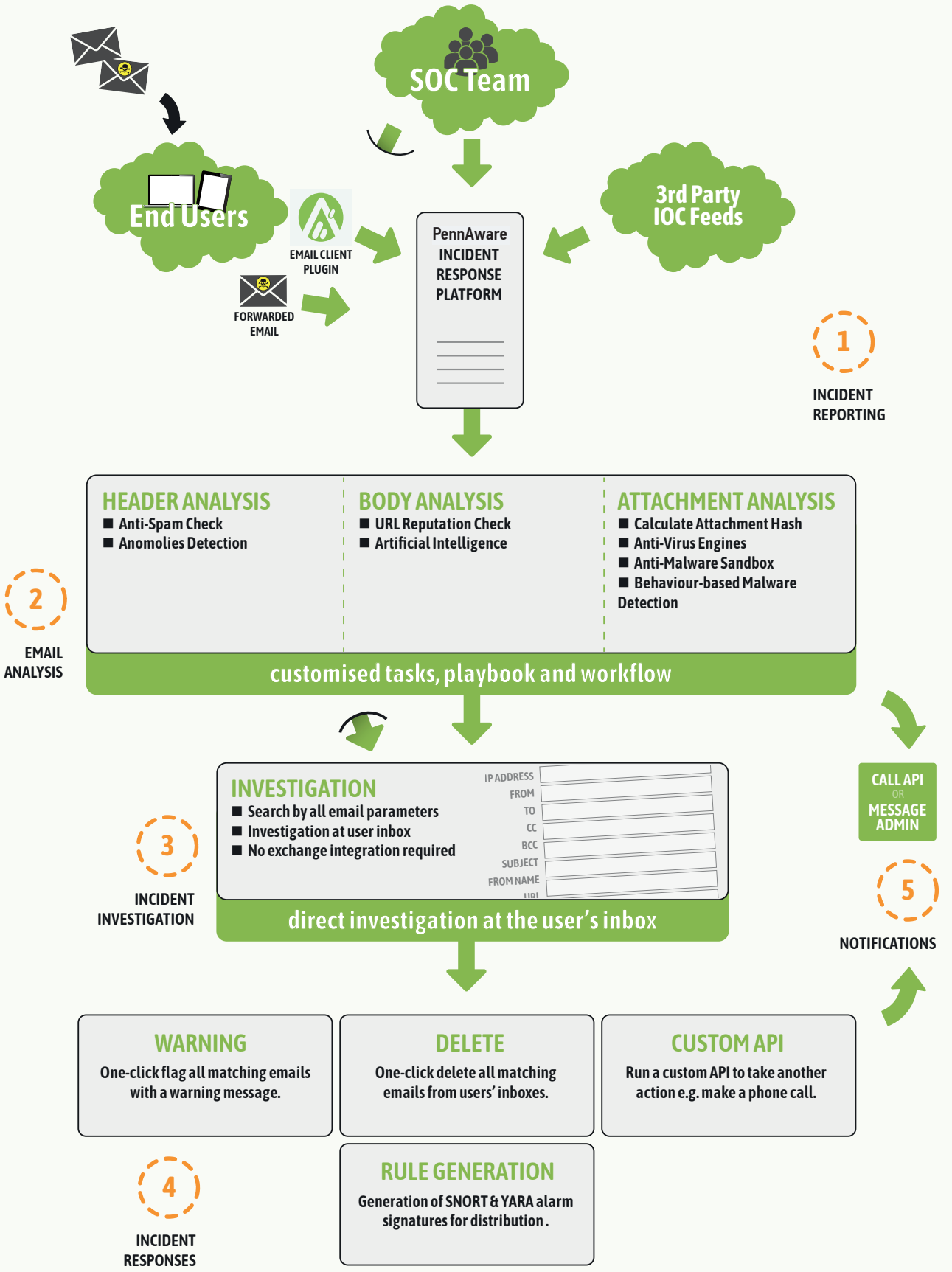
On completion of the analysis, PennAware IRP delivers detailed results, with industry-leading certainty, to the SOC team for further investigation and response.

INCIDENT INVESTIGATION & RESPONSE

A unique feature and major benefit of PennAware IRP is all investigation is done directly on the user's inbox instead of at the server exchange, giving you maximum agility and reducing response time.

After finding all instances of an attack PennAware IRP offers a suite of response options. Malicious messages can be flagged with a warning in the user's inbox, they can be deleted from the inbox or PennAware can call a custom API to perform another action e.g. call the user's phone.

Additionally, PennAware IRP will generate SNORT and YARA alarm signatures to update your other cyber-security technologies.


SOC Team
End Users
EMAIL CLIENT PLUGIN
FORWARDED EMAIL
PennAware INCIDENT RESPONSE PLATFORM
3rd Party IOC Feeds
1
INCIDENT REPORTING
HEADER ANALYSIS
Anti-Spam Check
Anomolies Detection
BODY ANALYSIS
URL Reputation Check
Artificial Intelligence
ATTACHMENT ANALYSIS
Calculate Attachment Hash
Anti-Virus Engines
Anti-Malware Sandbox
Behaviour-based Malware Detection
2
EMAIL ANALYSIS
customised tasks, playbook and workflow
CALL API OR MESSAGE ADMIN
INVESTIGATION
Search by all email parameters
Investigation at user inbox
No exchange integration required
IP ADDRESS
FROM
TO
CC
BCC
SUBJECT
FROM NAME
3
INCIDENT INVESTIGATION
direct investigation at the user's inbox
5
NOTIFICATIONS
WARNING
One-click flag all matching emails with a warning message.
DELETE
One-click delete all matching emails from users' inboxes.
CUSTOM API
Run a custom API to take another action e.g. make a phone call.
RULE GENERATION
Generation of SNORT & YARA alarm signatures for distribution.
4
INCIDENT RESPONSES

Key Benefits

- *Cost Effective* – with built-in integrated services, you do not need to invest in other anti-malware sandbox and anti-exploitation solutions.
- *Time Saving* – reduces the time and effort spent analysing malicious e-mails from hours to minutes.
- *Fast Response* – warn or delete directly in the user's inbox with one click. Close down active threats and limit damage quickly and easily.
- *Mobilise Employees* - users report suspicious emails with one click, turning them from a vulnerability to a strength, and strengthening the organisations security culture.

Arrange a free demo at *www.pennaware.com*

Powered by keepnet LABS

pennAware
www.pennaware.com