servicenow

Disrupt phishing attacks. Leverage people and technology. Digitally transform your incident response.

Phishing presents a growing threat to organizations today. The volume and sophistication of phishing attacks leads to lengthy time syncs and backlogs for security analysts. Much of this is due to manual triage processes and outdated email security technologies which cannot keep up. This presents a need for tight integration and SOAR (security, orchestration, automation, and response) tools to outpace cybercriminals and prevent breaches.

57%

Reported to Cofense Phishing Defense Center (PDC) were credential theft phish[1]

80%

Reported security incidents identified as phishing[2]

73%

Percentage of employees who report real phish within 30-minutes[1]

Phishing gets tougher

95 unique malware families

Organizations with Cofense reported nearly 100 unique malware families in 2020. (Ryuk, Avaddon, Mass Logger, Cheetah Keylogger, Agent Tesla – to name a few).

300+ Command and Control infrastructure

Botnets communicating with command and control domains, URLs, or IP addresses to receive updates.

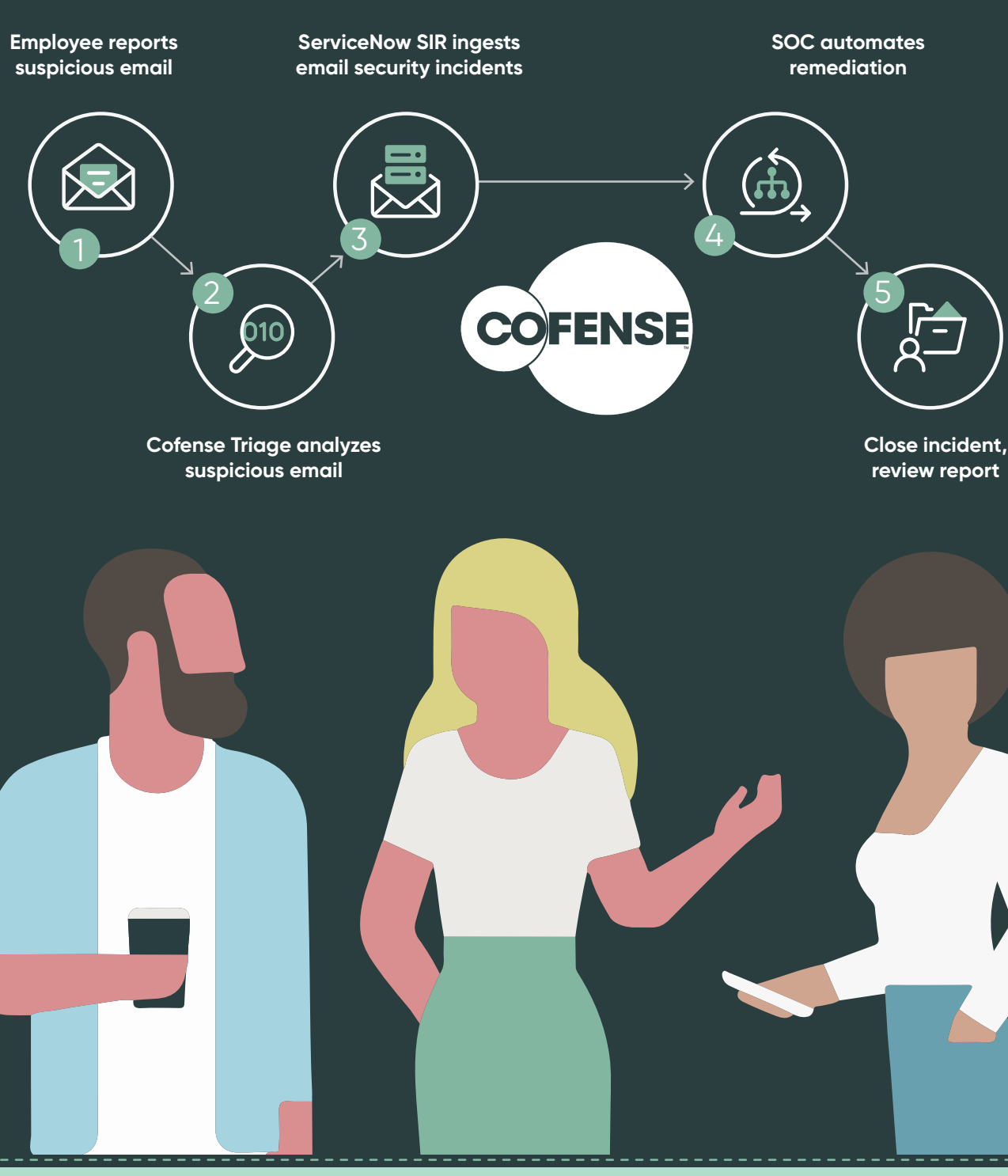
< 24 hours

The average lifespan of a phishing URL is less than 24 hours.

5 steps to creating a resilient, phishing defense culture

1. **Inform:** Educate and champion a security culture to create a network effect of human phishing sensors
2. **Detect:** Train employees to identify suspicious emails
3. **Report:** Make it easy for employees to alert to the security team when a suspicious email arrives in the inbox
4. **Analyze:** Enable security analysts with tools and expertise to uncover real phishing threats
5. **Respond:** Search and quarantine known phish from every inbox before employees interact

Identify and respond to phishing threats



Access Cofense Triage for Security Incident Response in the ServiceNow Store.

[1] Cofense's Annual State of Phishing Report 2020

[2] CSO Online, 2020 IDG Communications