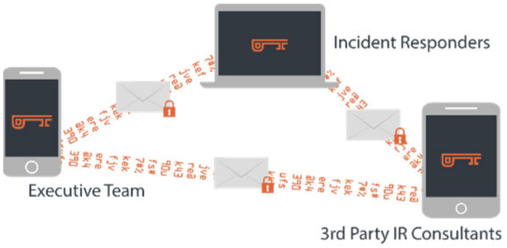
PREVEIL

Tips for evaluating out-of-band communication solutions for your Incident Response team

The Problem: You can’t fight fire with a burning fire truck. When IT Incident Response (“IR”) teams encounter a security incident, it is critical to have a dedicated out-of-band IR communication system already in place that enables your team to securely coordinate response activities.

Once attackers are in your network, assume they’re monitoring your response efforts

Encrypted out-of-band communication solutions ensure your IR efforts stay protected and private



Recommendations: Whether you’re an Incident Response consultant or a corporate IT/Security team, you should consider an IR communication solution with the following capabilities:

1. Out-of-Band Communication – IR teams should not rely on their standard corporate email and messaging systems when responding to incidents. In many cases the victim’s primary networks and communication systems have been infiltrated by attackers. To address this, you should have an out-of-band IR communication solution already in place that runs independently of primary systems.

PreVeil’s front-end integrates seamlessly with existing email and file interfaces, but the back-end runs completely independent from your existing infrastructure. PreVeil is a cloud-based service that can be deployed on-prem if necessary.

2. Exceptional Security – When responding to a potential cybersecurity breach, it’s highly likely that attackers are still hiding in your network. In order to ensure the confidentiality and integrity of response team communications, IR communication solutions must be purpose-built for security and offer far better protection than standard email systems.

All emails and files sent via PreVeil are encrypted end-to-end, and the decryption keys are only accessible on authorized devices. This ensures that IR communications stay protected and private even if servers are breached, passwords stolen, and IT admins compromised.

3. Restricted Access – Responder communications and data exchange should be tightly controlled and monitored throughout the crisis to avoid potential leaks or data exfiltration. Your out-of-band IR channel should only be accessible to response participants (exec team, legal, IR consultants, etc).

PreVeil’s Trusted Community feature permits Admins to specify and limit the domains or email addresses for users/devices that can access the IR team communications and documents. Trusted Community members can be internal or external to the company. Any other (inbound or outbound) email traffic or document sharing attempts are blocked.

Tips for evaluating out-of-band communication solutions for your Incident Response team

4. Event Logging and Archiving – Retaining an immutable record of all incident communications is essential for monitoring and improving your IR execution over time. These logs and archives may also be required for subsequent legal or regulatory discovery.

With PreVeil, your designated IR administrators can access encrypted and tamperproof logs in real time during or after the incident. PreVeil email and files cannot be permanently deleted except where required by your email retention policy. They can be archived and/or exported for eDiscovery at a later date.

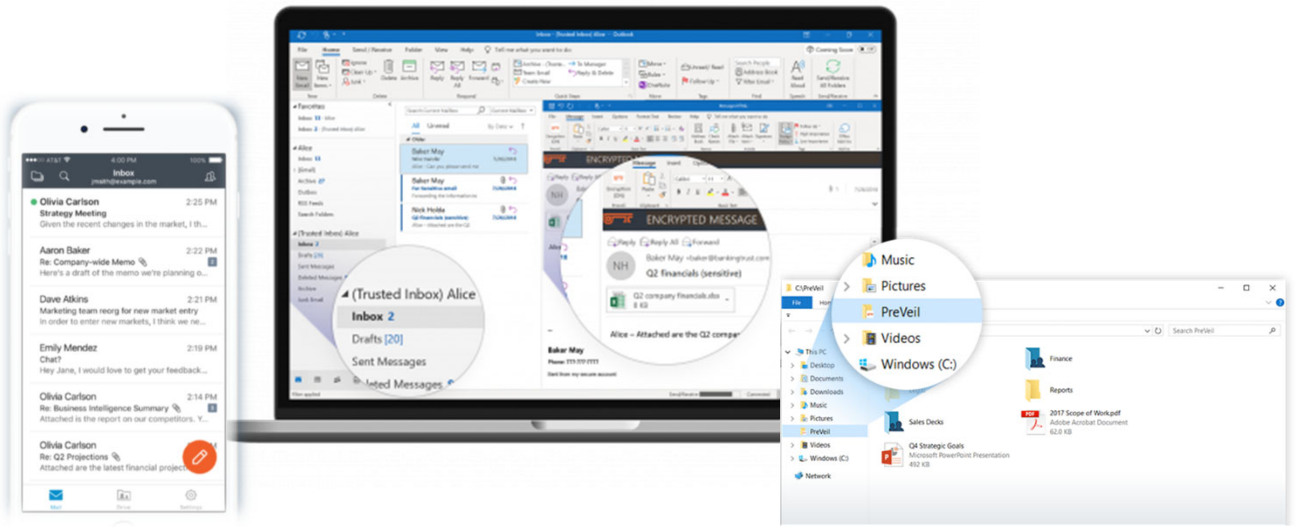
5. Accessible and available 24x7 – IR crisis situations don't follow a 9-5 schedule. It is critical that your entire response team can instantly access urgent IR communications and data via their laptops, tablets, and mobile phones.

Responders can securely access PreVeil 24x7 while in the office, on the road, or at home. Only an internet connection and a cryptographically authorized laptop, tablet, or mobile phone is required to exchange communications and files via PreVeil.

6. Ease-of-Use – Your IR communication solution should be highly intuitive to technical and non-technical users. Although it may not be used frequently, when it is needed every second counts. There isn't time for users to familiarize with new services or learn new email addresses / passwords.

PreVeil integrates seamlessly with your email and file sharing interfaces, and enables them to keep using existing email addresses. Unlike systems that rely on passwords, PreVeil uses cryptographic keys to transparently authenticate authorized user accounts and devices. Say farewell to password resets and clunky portals.

PreVeil integrates seamlessly with existing interfaces &
mobile platforms, enabling your users to be trained and running in minutes



Inbox
jmsith@example.com

Olivia Carlson 2:25 PM
Strategy Meeting
Given the recent changes in the market, I th...

Aaron Baker 2:22 PM
Re: Company-wide Memo
Here's a draft of the memo we're planning o...

Dave Atkins 2:21 PM
Marketing team reorg for new market entry
In order to enter new markets, I think we ne...

Emily Mendez 2:19 PM
Chat?
Hey Jane, I would love to get your feedback...

Olivia Carlson 2:14 PM
Re: Business Intelligence Summary
Attached is the report on our competitors. Y...

Olivia Carlson
Re: Q2 Projections
Attached are the latest financial project...

ENCRYPTED MESSAGE
Baker May
Q2 financials (sensitive)
Q2 company financials.xlsx
Alice – Attached are the Q2 compa...