PreVeil for Incident Response in the A&D Industry

When an IT Incident Response team at an Aerospace & Defense company is faced with a security breach or potential data loss, the communication service employed is a critical factor in the team's ability to diagnose, analyze and contain the situation effectively. The Defense Federal Acquisition Regulation Supplement (DFARS) regulations require an Incident Response (IR) plan that relies on highly available communication tools in scenarios where the company's standard communication assets may be compromised or out of service.

A&D companies, when selecting a communication service for an Incident Response team, should seek the following attributes:

1. **Strong Data Security** – During an incident, the company may already be dealing with a security violation and, in some cases, cyber attackers may be freely operating within the digital infrastructure of the organization. This is no time for the IR team to be compromised as well.

All data in PreVeil's Email and Cloud Storage service is end to end encrypted with private keys available only at the device level. There is virtually no attack on the cloud, on an individual user or on an admin that can compromise the IR team's communications.

2. **Out of Band Communication** – The IR team should not count on using the standard corporate email or messaging options in situations where these could already be compromised. The communication service should run in parallel and not be dependent on standard operating systems.

PreVeil is seamlessly integrated at the client level but the back end operates separately from normal corporate email and document storage solutions. The PreVeil service is cloud-based and the encrypted application data can be flexibly stored in the AWS public cloud, AWS GovCloud or on-premise based on the needs of the company.

3. **Available 7x24** – IR crisis situations typically don't follow an 8-5 schedule. IR team members need to be able to quickly access important information and communicate with others via laptops, tablets and mobile phones from anywhere in the world.

Only an internet connection and an authorized user device is necessary to access PreVeil. Accounts can be easily shared across a user's devices including tablets and mobile phones but can also be easily managed by Admins. In the office, on the road or at home, secure interaction with the IR team is always available.

PreVeil for Incident Response in the A&D Industry

4. **Restricted Access** – Information sharing must be controlled during a crisis situation. Unanticipated data exfiltration during an incident, even accidental, can be damaging to the organization. The communication channel should be restricted to only IR team members.

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 and the list can be updated at any time by Admins. Any other email traffic or document sharing requests inbound or outbound are restricted.

5. **Easy to Use** – An IR communication service may not be used for months at a time, but when it is needed, there isn't time for users to pull out a manual or try to recall a password. The service should be intuitive and not require any special credentials.

PreVeil uses secret keys on authorized devices and doesn't rely on passwords so there is never an issue with a user not being able to access IR email or file sharing immediately on any of their devices. On desktop or mobile, PreVeil's interface is intuitive in either browser mode or when integrated seamlessly into Outlook and File Explorer.

6. **Event Logging and Archiving** – Maintaining a record of IR team communications that can be reviewed after the fact is essential for event reconstruction and improving incident response performance over time.

PreVeil creates a complete set of encrypted and tamperproof logs in real time that can be reviewed by Admins or management after an incident. PreVeil email and files cannot be permanently deleted. They are archived and can be reviewed at any time with Admin approval.