Pillr

Pillr Services | Incident Response

A trusted resource for containment and recovery.

When threats arise, you want to be supported by a team capable of quickly, reliably securing at-risk data and systems. The Pillr Incident Response Team (IRT) is available to provide immediate service when a data breach, security incident, or systemic threat occurs.

Take back control with Pillr

For Pillr customers, full-service incident response can be activated by calling our security operations center line—a resource that's staffed 24/7/365 to ensure every incoming issue is addressed in real time. The IRT is committed to responding to all incoming requests within a 3-hour span for retainer customers.

Once an incident is confirmed and logged, the IRT assesses its severity and begins to resolve the issue working in accordance with the customer's Service Level Agreement. An issue report is created, then escalated to a dedicated IRT Coordinator for immediate action.

What is a security incident?

Any observed or suspected event that may jeopardize the availability, confidentiality, or integrity of information or information systems can be declared an incident. Confirmed incidents generally fall into one of these 6 categories:

- Data breaches (e.g., accidental leakage of sensitive information; criminal exfiltration)
- Email fraud and phishing incidents
- Insider threat (e.g., rogue employee behavior)
- Network intrusion (e.g., abuse of exposed services; compromised credentials)
- Malware infection
- Vulnerability exploitation

A reliable process—regaining security

When an incident is confirmed and escalated with the Pillr IRT, the following steps take place:

- We assign a Pillr IRT Coordinator to organize and oversee response efforts
- Establish on-site and/or remote coordination and communication channels
- Begin investigation of the open incident, including identifying severity and nature of the incident, resource needs, and other requirements
- Manage artifact collection and documentation in accordance with evidence management best practices
- Facilitate assessment, data analysis, and incident containment processes
- Develop and validate remediation processes to eliminate threat as the investigation evolves, revising processes as needed
- Provide oversight and guidance to client personnel in execution of remediation activities
- Collect relevant data points in support of post-incident gap analysis, reporting, and review
- Define containment, eradication, and recovery protocols according to specific incident type and customer needs
- Prepare and deliver final Pillr Incident Report and evidence to the customer

Comprehensive documentation and reporting

Every incident response case with the Pillr IRT is supported by these deliverables:

- Pillr Incident Assessment: Initial documentation developed by the Pillr IRT capturing the pre-investigation state of the event, including definition of the incident type, proposed scope of impact, and early recommendations on the remediation approach.
- Investigation Status Reports: Routine investigation reporting provided by the Pillr IRT; materials are composed and delivered at a defined cadence—daily or weekly depending upon the incident type and situational variables—with the option to schedule joint review with the Pillr IRT.
- Closing Incident Report: Customers have the option to play an active role in the report review process; the Pillr IRT will deliver the drafted Closing Incident Report and collaborate with the customer to compose the final documents to ensure they align to organizational compliance and information governance requirements.