Pillr

PARTNER SALES ENABLEMENT

Services Quick Guide

Expert-driven services by Pillr, reliable outcomes to you and your customers

Not every network and infrastructure is built the same. Pillr services are led by expert teams capable of navigating and understanding the unique complexities of your customers' applications and networks, with attention to their compliance and security requirements.

Our services experience is designed to help you demonstrate your commitment to your customers, including co-branded communications, presentations, and reports.

Penetration testing

7-part assessment methodology is based on the Penetration Testing Execution Standard and follows industry best practices to produce consistent, timely outcomes.

All security components and vectors are documented and tested to identify areas of weakness.

Assessments are performed by dedicated white-hat hackers with backgrounds in IT, security operations, and software development and engineering.

Pillr penetration test reporting includes clear, prescriptive guidance to remediate identified threats, with the option of Pillr remediation support.

Pillr security assessment can go beyond the conventional technology stack, including testing services for:

Infrastructure	Applications	People
external + internal	code audit	social engineering +
cloud	internet of things	email
SCADA	mobile	SMS
wireless	web	voice

Incident response

The Pillr Incident Response Team (IRT) is available 24/7/365 to provide service for:

- Data breaches
- Email fraud and phishing
- Insider threat
- Network intrusion
- Malware infection
- Vulnerability exploitation

Full-service incident response (IR) can be activated by calling the Pillr 24/7/365 SOC line—most customers connect with the Pillr IRT in under three minutes.

A dedicated Pillr IRT Coordinator is assigned to cases to organize and oversee response efforts and report progress.

Collection, containment, eradication, and recovery protocols are defined and maintained according to incident type and customer needs—remediation processes are validated as the investigation evolves to eliminate threat.

Relevant data is collected and protected to support post-incident gap analysis, reporting, and review, and every Pillr IR case is supported by these deliverables:

1. **Pillr Incident Assessment:** Documents the pre-investigation state of the event, including definition of the incident type, proposed scope of impact, and recommendations on the remediation approach.
2. **Investigation Status Reports:** Daily or weekly investigation reporting—depending on the incident type and situational variables—with the option to schedule joint review with the Pillr IRT.
3. **Closing Incident Report:** Concluding case report, with options to collaborate in the review process to ensure alignment with customers' compliance and governance standards. Can be co-presented with the Pillr IRT.