Rapid Response Assurance

Know exactly what happened, respond quickly.

Challenges Addressed

Organizations often establish a “retainer” relationship with an incident response provider to prepare for the inevitable cyber incident. However, having a relationship doesn’t necessarily speed up the response or recovery process.

Actual time to resolution may depend on one or more factors:

- Contracted priority level
- Pending agreement negotiations
- Expert availability or time of day
- Knowledge of and experience with your environment

During an incident, a quick initial response is crucial.

Our Approach

PacketWatch Rapid Response Assurance (RRA) is a proactive readiness solution aimed at minimizing the impact of cyber incidents.

The solution includes a full packet capture network sensor, an expert cybersecurity analyst, and a limited version of the PacketWatch network threat hunting platform. The sensor collects and stores the last seven (7) days of network activity.

Once an incident is reported, PacketWatch incident responders get to work within minutes—utilizing the data collected by the PacketWatch sensors to investigate the tactics, techniques, and procedures used, systems affected, and data exfiltrated.

The pre-negotiated Incident Response Agreement enables PacketWatch to immediately begin containing the threat, restoring systems, recovering data, and coaching your teams on IR processes.

Benefits

- Daily sensor audits ensure network data is captured
- Monthly PacketWatch Cyber Threat Intelligence Reports
- Quarterly threat hunts and review calls

If an incident is reported,

- Incident responders can get started right away
- Expert analysts provide tribal knowledge to the IR team
- Captured network activity may be forensic evidence

Expose Hidden Threats

“The whole PacketWatch team is responsive and refreshingly approachable.”

Get Started

Contact sales@packetwatch.com for a demonstration, configuration, and pricing.

Features

- 24/7 Incident Response
- Full Packet Capture Sensor
- 7 Days of Stored Network Activity
- Expert Security Analyst
- Pre-negotiated IR Agreement
- Quarterly Threat Hunt and Review
- Monthly Cyber Threat Intel Report

RRA+

Critical network environments may need to “upgrade” the services provided with a standard RRA. Options may include monthly or more extensive threat hunts and increasing the number of days that the network activity is collected and stored. Ask us for the “plus” options.

Why Choose RRA?

We’ll get to work on your incident right away—no waiting for tools or people. Unlike a traditional retainer, the payment does not just prepay future IR services. The solution constantly collects network data and delivers quarterly services to improve your security posture proactively.