packet
watch

# PacketWatch IR

## Incident Response

## Daily Threats

Companies experience cybersecurity threats every day. They may or may not know it. Sadly, it often takes a security incident to realize that they could have done more to secure their environment.

## Falling Victim

Regardless of their IT team's size or experience, responding to a security incident is likely unfamiliar and scary. Most organizations will request assistance from a trusted and experienced partner to reduce the pressure, anxiety, and liability placed on their internal resources.

## Responsive Expertise

PacketWatch helps organizations respond to security incidents caused by all forms of attack, such as malware, ransomware, or business email compromise. Our team consists of threat hunters, investigators, threat intelligence analysts, forensic analysts, and cybersecurity experts with experience in federal law enforcement, military, national security, local law enforcement, and large enterprises.

Our team engages quickly and gets right to work—triaging, investigating, and remediating the incident. As a boutique consultancy, the experts we introduce at the beginning of the project remain involved and lead the entire engagement. Our clients can also leverage our extended team of forensic specialists, data scientists, cyber insurance professionals, intelligence experts, and cyber-focused legal experts.

**Clients look for 3 things:**

**Immediate Engagement**

**Battle-hardened Security Professionals**

**Proven Methodology and Tools**

## The Human Element

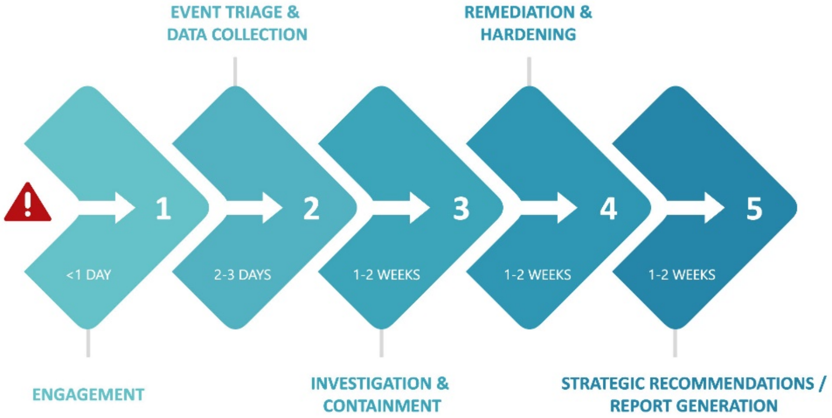
> "Your team gave us the direction and confidence we needed to regain composure."

A security incident is an unsettling time. Stakeholders want to know that everything is going to be okay. But that often involves several crucial steps, collaboration with experts, and time. We believe there is a human element to cybersecurity. So, we work with our clients shoulder-to-shoulder—leading them through the incident and teaching them how to strengthen their defenses. The result is an IT team and infrastructure that is better prepared for a future attack. Our security experts also help the client's executive team regain confidence in their systems, processes, policies, and people.

# PacketWatch Incident Response

## Our Approach

PacketWatch rapidly deploys world-class tools and technology to ensure threats can no longer operate unnoticed—the goal is more visibility than you've ever seen before. We actively partner with our clients to identify and eliminate any threats. Our collaborative incident response methodology shares the "hows" and "whys" along the way to develop the clients' cybersecurity skills and capabilities.


EVENT TRIAGE & DATA COLLECTION
REMEDIATION & HARDENING
1
<1 DAY
2
2-3 DAYS
3
1-2 WEEKS
4
1-2 WEEKS
5
1-2 WEEKS
ENGAGEMENT
INVESTIGATION & CONTAINMENT
STRATEGIC RECOMMENDATIONS / REPORT GENERATION

### Endpoint Protection

We leverage our expertise with Crowdstrike Falcon, trusted by many of the world's most discerning security organizations, to detect memory-resident, file-less, and polymorphic malware on the endpoints. We actively monitor file activity, processes, and communications on hosts to detect known and unknown threats.

### Network Monitoring

Our proprietary technology, PacketWatch, records all packet-level network activity to identify and analyze persistent anomalous events. This proven network monitoring, analysis, and threat hunting platform also enables us to monitor and investigate known and unknown network-connected devices.

## Additional Services

Protecting an environment from cyberattacks requires a combination of assessments, planning, policies, and daily security operations. If our clients do not have the internal resources necessary to perform these functions, PacketWatch offers:

### PacketWatch RR

Our rapid recovery service uses our enhanced visibility, global threat intelligence, and Crowdstrike Falcon Real Time Response technology to quickly identify and eradicate persistent threats with pinpoint accuracy and minimal disruption.

### PacketWatch MDR

Our monthly managed detection and response (MDR) service monitors your network using full packet capture and robust analysis tools to provide on-going network protection with daily threat hunting, global threat intelligence, and concierge support.

### PacketWatch ESA

Our enterprise security assessment (ESA) is a 30-day audit of your network using full packet capture and robust analysis tools to find persistent threats and associated risks. The overall security posture is evaluated using industry-standard frameworks.

### Advisory Services

Our security advisory services help organizations with assessments, strategic plans, compliance, policies, governance, education, and risk management. These services leverage our industry experience, enterprise methodology, and proven best practices.

## Next Steps

If your business operations have been negatively affected by a security incident, we are here to help any time of the day, 24x7. The PacketWatch incident response team of battle-hardened security professionals will engage immediately to deploy our proprietary tools and walk you through our proven methodology to get you back online.

**Call 480-444-7070 or visit www.packetwatch.com for more information.**

6263 N Scottsdale Rd, Suite 255, Scottsdale AZ 85250