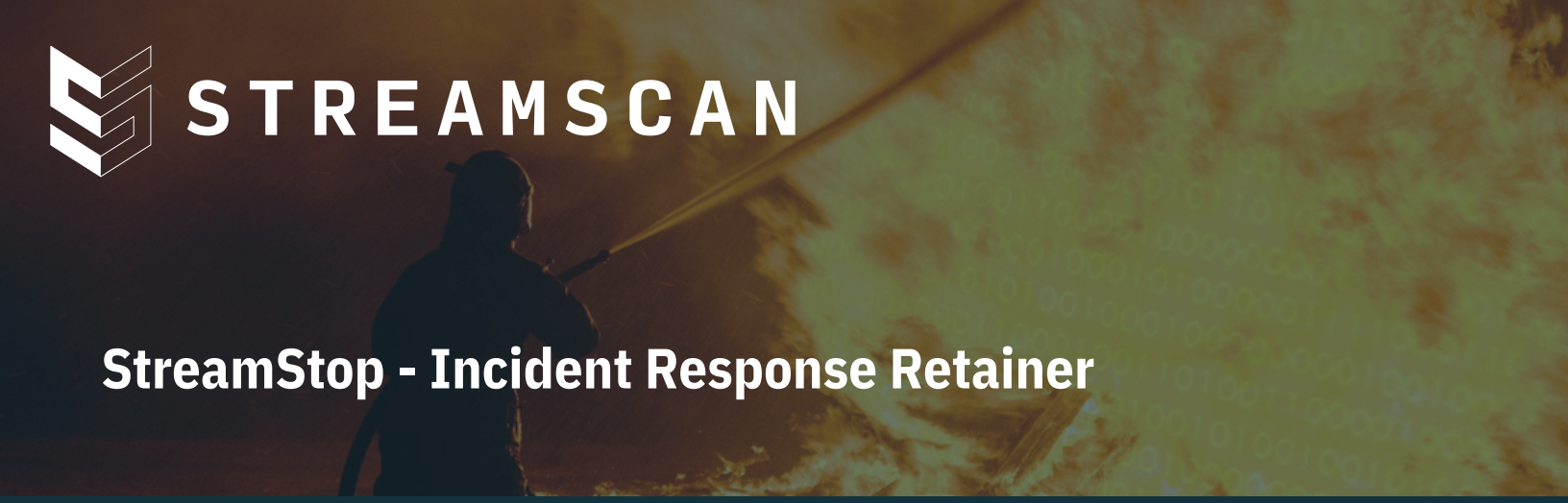


STREAMSCAN

StreamStop - Incident Response Retainer

Stop the threat. Regain control. Forward to stronger.

StreamStop is an incident response retainer that gives your business 24/7 priority access to our incident response expert team, giving your peace of mind while minimizing downtime, limiting the impact of an incident, and getting your business back on track.

What is an Incident Response Retainer

An incident response (IR) retainer is a proactive agreement with a trusted cybersecurity partner that ensures rapid, expert support when a security breach or other cyber incident occurs.

With a retainer in place, organizations can count on faster mobilization of the IR team, predictable processes, and priority access to specialized expertise.

Why get an Incident Response Retainer

With cyberattacks continuing to rise in frequency and complexity, an IR retainer is no longer just a safeguard, it is a critical component of a proactive resilient cybersecurity strategy.

StreamScan's IR retainers combine rapid response with deep technical expertise, giving organizations the confidence to contain threats quickly and recover with minimal disruption.

StreamStop. When every minute counts.

Benefits of an IR Retainer

- 24/7 access to incident response experts.
- Faster incident analysis, containment, and recovery by experts familiar with your environment.
- Better cost management with pre-agreed engagement terms and rates.
- Risk mitigation by following cybersecurity best practices.
- Can improve your insurability and reduce your insurance premiums.
- Assistance with regulatory compliance requirements relevant to your industry.

Incident Response Process

Initial Diagnosis and Confinement

When an incident occurs, the priority is to rapidly assess the situation to understand its scope, nature, and potential business impact. An accurate assessment enables faster recovery and minimizes damage.

Once the diagnosis is complete, an action plan is developed, and containment measures are implemented to prevent the incident from spreading further. Common containment measures include:

- Disconnecting compromised devices
- Adding rules to firewalls
- Deactivating certain user accounts
- Changing passwords

Investigation and Reconstruction

During an incident, it is essential to regain control of the network and confirm that no other attacks are underway. StreamScan's XDR can be deployed to provide full network visibility, allowing experts to analyze suspicious activity in real time.

Working closely with your IT team, our team restores control and removes any active threats from the environment.

In complex cases such as ransomware or advanced intrusions, a deeper investigation is carried out to determine exactly what occurred. This may include reverse-engineering malicious tools to understand their purpose, methods of propagation, and points of entry.

Following the investigation, the IR team can:

- Reconstruct the full attack scenario
- Determine how the incident occurred and pinpoint vulnerabilities
- Identify "patient zero," the first infected system
- Define and prioritize response measures

Eradication, Recovery, and Analysis

After containment and investigation, the eradication phase focuses on eliminating the root cause of the incident and removing any remaining traces of the threat. In the recovery phase, the team works with the client to restore systems to production. Typical actions include:

- Reinstalling affected systems
- Hardening configurations to improve security
- Restoring data from backups
- Gradually bringing systems back online

If required, a forensic analysis is conducted to collect and preserve evidence for potential legal action. This may involve acquiring and preserving evidence, gathering network logs, recovering hidden files, and producing a forensic report.

Once the incident is resolved, a final review is carried out to understand the event and prevent future incidents. A comprehensive incident report is delivered, covering:

- The attacker's methods and exploited vulnerabilities
- The scope and impact of the incident
- The response measures taken
- Findings from any reverse engineering
- Strengths and weaknesses of the response
- Recommendations to prevent future recurrence

Ransomware Negotiation Expertise

When ransomware strikes, StreamScan acts decisively to protect operations and limit damage. If negotiation is required, it is conducted strategically to gather intelligence, buy critical time, and protect your interests, all while ensuring compliance with legal requirements.
With StreamScan, clients have a proven partner capable of navigating high-pressure situations with precision and control.

Getting StreamStop Ready

StreamStop is designed to be ready when you need it, with a streamlined onboarding process that establishes the access, communication channels, and information our team needs to respond quickly to an incident..

- **Kick-off Session:** The team meets with key stakeholders to confirm objectives, clarify roles, and collect essential information such as network diagrams, a list of critical assets, current security tools, and any existing incident response plans.
- **Establish Communication Channels:** Clear lines of communication are established, including escalation contacts and agreed-upon protocols for incident handling. This step also includes configuring StreamScan's intrusion detection tool for full network visibility.
- **Access Validation:** Tests are performed to ensure the team can remotely install and manage security tools, with support from an internal IT contact.
- **On-Call Readiness:** With access confirmed and preparations complete, the StreamStop team is on standby, fully equipped to respond at the first sign of an incident.

Plans

Standard - $5,000/year

Ideal for businesses looking for priority access and savings on incident response services.

- 4-hour response SLA
- Full onboarding process
- 20% discount on standard IR fees

Most Popular

Pro - $9,000/year

For teams looking for greater coverage, faster response, and additional savings.

- Everything included in the Standard plan, plus:
- 30% discount on standard IR fees
- Up to 15 hours of IR services included
- $2 000 credited toward other services if no incident occurs

Premium - $30,000/year

For organizations seeking maximum coverage, response capacity, and flexibility.

- Everything included in the Pro plan, plus:
- 40% discount on standard IR fees
- Up to 100 hours of IR services included
- $7 500 credited toward other services if no incident occurs
- Optional: Integration of our NDR into your network*

* On a virtual server within the client's infrastructure. Installation and configuration fees of $5,000 per site.

Additional Benefits on All Plans:

- 15% discount on vulnerability scanning services
- 15% discount on incident response plan review or development support
- 15% discount on tabletop exercises

STREAMSCAN
Your cybersecurity partner