

ActiveResponse

INCIDENT RESPONSE AND COMPROMISE ASSESSMENT



An attacker can hide on your network for days, months, or years before being discovered, and it often takes a third party to make that discovery. The damage inflicted in that time can result in devastating costs and long-term harm.

Whether you want to minimize the cost and damages that result from an incident, or you're concerned that you've been breached and don't know it, Delta Risk's incident responders and threat hunters are ready to help. Our proven, methodical, and evidence-driven approach will keep you in control of whatever chaos an incident may bring.

Our dedicated consultants work quickly to detect an attacker's activities, determine root causes and impact, and enable swift containment, eradication, and recovery.

Solutions and What to Expect

If you've had an incident: Incident Response

- ▶ An initial call to understand your situation
- ▶ Identification of key questions and data sources
- ▶ The tools and expertise to get started right away
- ▶ Daily status updates and recommended actions
- ▶ 24x7 support while the incident is ongoing
- ▶ A final report of all findings and response efforts

If you don't trust your network: Compromise Assessment

- ▶ An initial call to understand your environment
- ▶ A solution suitable for your network.
- ▶ An on-site team to analyze your network
- ▶ 45-days of in-depth endpoint monitoring
- ▶ An identification of malicious activity and artifacts
- ▶ A final report of all findings and recommendations

TECHNOLOGIES & SKILLS



Incident
Management



Cloud Analytics



Endpoint
Threat Hunting



Log & Data Analytics



System Forensics



Malware Analysis



CASE STUDY 1:

Payment System Compromised

An ActiveResponse Compromise Assessment uncovered an advanced network intrusion that targeted a customer's payment systems. The resulting investigation determined the attacker had been hiding and active for the two months prior. Delta Risk determined the scope of the compromise, the risk to financial data, and advised on necessary response actions.



CASE STUDY 2:

Ransomware Outbreak

A private equity firm fell victim to a ransomware outbreak. Their first attempt to recover was thwarted after a week when the attacker began re-infecting systems. Within three days, Delta Risk identified the intrusion vector, secured the environment, and provided the customer with expertise in restoring critical and revenue-generating services.

Pre-Incident

- ▶ Our incident response retainers enable a rapid response at a fixed rate. Unused time may be used toward other services.
- ▶ A proactive compromise assessment will uncover the attackers that may have bypassed your first line defenses.

Post-Incident

- ▶ Our on-demand incident response team is ready to learn about your situation and can get started as soon as possible.
- ▶ A reactive compromise assessment after an incident gives you the visibility you need to regain trust in your network.

About Delta Risk LLC

Delta Risk LLC provides tailored, high-impact cyber security and risk management services to government and private sector clients worldwide. Formed in 2007, Delta Risk consists of trusted professionals with expert knowledge around technical security, policy and governance, and infrastructure protection to help clients improve their cyber security operational capability and protect business operations. Delta Risk is a Chertoff Group company.

 @deltarisk  /delta-risk-llc  /deltariskcyber

106 S. St. Mary's St.
Suite 601
San Antonio, TX 78205

1010 N. Glebe Rd.
Suite 750
Arlington, VA 22201

901 E. 8th Ave.
Suite 111
King of Prussia, PA 19406

www.deltarisk.com
info@deltarisk.com
888-76-DELTA (888-763-3582)

