LAYER 3 communications

BUILDING NEXT GENERATION NETWORKS
ONE LAYER AT A TIME

INCIDENT RESPONSE

24x7x365 RESPONSE TEAM

Incident Response services are designed to assist in the remediation efforts following a cyberattack or security breach. Layer 3 Communications incident response team offers solutions to determine the cause, recover lost information and reduce future vulnerabilities. The goal is to handle the situation in a way that limits damage and reduces recovery time.

Layer 3 Communications uses our accurate and detailed view of how your network is constructed to optimize our response. Whether the incident is a large-scale malware outbreak or an advanced attacker, we use a systematic methodology that minimizes down time while ensuring an effective clean up.

6 STEPS FOR INCIDENT RESPONSE:

1.PREPARATION:	*The most important phase. Includes policy, communication, strategy, tools and training.*
2.DETECTION:	*Monitoring security events to detect, alert and report incidents.*
3.CONTAINMENT:	*Once an incident is detected, containing it is top priority.*
4.ERADICATION:	*Removing the threat and restoring the affected systems to their previous state.*
5.RECOVERY:	*Testing, monitoring and validating systems to get them back into production.*
6. POST INCIDENT ACTIVITY:	*A critical phase which includes reviewing lessons learned to educate and improve future incident response efforts.*

No matter how much we prepare, sometimes security incidents happen. Our responders are available 24x7x365 to begin working virtually when an incident occurs. If needed our response team can be onsite within hours to remedy the situation.

REALITY CHECK

– $6 TRILLION ANNUALLY–

THE WORLD COST OF CYBERCRIME DAMAGES BY 2021

– EVERY 39 SECONDS –

HOW OFTEN A HACKER ATTACK OCCURS

– 69 DAYS –

THE AVERAGE TIME NEEDED TO FULLY CONTAIN A DATA BREACH IN 2018

– OVER 6 MONTHS –

TYPICAL TIME IT TAKES COMPANIES TO REALIZE A DATA BREACH HAS OCCURRED