



SECURE IT

CYBER INCIDENT RESPONSE



RAPIDLY RESPOND TO ACTIVE THREATS

PRODUCT OVERVIEW

Organizations must respond quickly to active threats to ensure threat actors are not able to achieve their objectives. With our Cyber Incident Response service, we provide rapid assistance with our global security team of remote incident responders and threat analysts. Triage starts within hours, with most customers starting the recovery phase in 48-hours or less. Our Cyber Incident Response is available for both new and existing customers.



IMMEDIATE SUPPORT

We will rapidly discover, isolate and contain active threats.



THREAT EJECTION

Remove threats and threat actors from your estate to prevent further harm.



DETAILED FORENSICS

Forensic report providing investigation results and mitigation activities.



POST INCIDENT MONITORING

Always-on EDR/XDR monitoring and incident response for 30 days.



3 HOURS

Average time to respond and begin preparation



48 HOURS

Majority of customers begin the recovery phase



30 DAYS

Subscription to our managed EDR/XDR platform



24/7 COVERAGE

Threat hunting, detection, and incident response

HOW IT WORKS

Our Cyber Incident Response Team starts by establishing a communication schedule, cadence, prioritized requirements and recommended actions. For identification and containment, we apply remedial actions from a defined and proven playbook, and secure vital artifacts to prevent further damage to your estate. To ensure eradication and full recovery, we safely restore critical systems back into production by patching, hardening and applying real-time EDR/XDR response services. Lastly, we review forensics evidence to strengthen your security posture, and use it for post incident analysis and service enablement.





PREPARATION & GROUND RULES



IDENTIFICATION & CONTAINMENT



ERADICATION & RECOVERY



FORENSICS REVIEW

CYBER THREAT NEUTRALIZATION

Our Cyber Incident Response Team is part of global, world class, 24/7 threat hunting, detection, and response Security Operations Center (SOC) that proactively hunts, identifies, investigates, and responds to threats on behalf of our customers as part of our award-winning Secure IT portfolio of Managed Services.

DEFEND AGAINST THREATS WITH 24/7 DETECTION AND RESPONSE

Once the incident is resolved and the threat to your organization is neutralized, we will transition you to our global, best in class EDR/XDR platform, providing real-time proactive threat detection, and response. Should threat actors re-emerge or new threats present themselves, we will be prepared to respond. We will continue to defend your assets for a full 30 days as part of our incident response service.

DETAILED FORENSICS REPORTING

We will provide a detailed forensics summary report of our investigation including discoveries made, actions we took and a strategic roadmap of how to mitigate the recurrence of similar threats in the future.

RAPIDLY SECURE YOUR ENVIRONMENT

Our cloud-based security platform has been purpose-built to offer rapid deployment to all of your assets by our team of cybersecurity response engineers. This ensures that whether your environment is small or large, we can rapidly secure yourestate giving you the confidence that your environment is prepared to defend against further threats.

	SECURE IT CYBER INCIDENT RESPONSE
Rapid on-boarding and engagement with our global team of security response engineers	•
Enablement of our world class 24/7 threat monitoring, hunting, and response services	•
Dedicated Incident Manager during the entirety of the engagement	•
Detailed analysis of data from third-party technologies and event systems	•
Immediate account activation with predictable, fixed cost pricing	•
Detailed post-incident report detailing forensic findings and recommendations	•
Seamless transition into our industry leading EDR/XDR platform	•

To learn more about Secure IT - CIR, contact us at: Sales@AcronymSolutions.com

1.866.345.6820

Join our mailing list

[SIGN UP ▶](#)