eventus

eventustechsol.com

INCIDENT RESPONSE SERVICE

Rapid Response to Cybersecurity Incidents with speed and accuracy

EVENTUS INCIDENT RESPONSE SERVICE

Eventus aims to deliver excellence in next generation cyber security services and custom-tailored solutions for enterprises by defining proof of value and measuring it continuously to achieve customer success.

We have successfully dealt with some of the most complex cyberattacks and our approach is based on real-world security incident experience. We have crafted a reliable and comprehensive 'Incident Readiness and Response' service covering all aspects of incident response – detection, investigation, containment, remediation, recovery, and reporting. Our team of experts works collaboratively to address any security incidents, leveraging our extensive experience and knowledge, combining manual and tool-based techniques.

BENEFITS

- Detect, contain, investigate and recover from cybersecurity incidents with speed and accuracy.
- Rapid response SLAs and guaranteed response time.
- 24/7/365 support (email/call).
- Industry-leading expertise and technology stack.
- Access to the Incident Response Preparedness Service during the entire engagement cycle.
- Access to Enriched Incident Response Playbooks during the entire engagement
- Retainer based engagement model for emergency support and faster response
- Meet regulatory compliance and industry standard requirements.

HOW EVENTUS IS ENABLING ORGANIZATIONS TO STAY AHEAD OF THE CURVE?

PROACTIVE ENGAGEMENT MODEL:

Shift your incident response strategy from reactive to proactive. We can help you in crafting a well-defined incident response plan that includes robust 24x7x365 security monitoring and alerting features. Our plan equips you with the appropriate resources, tools, and procedures to quickly and efficiently detect, investigate, and address security incidents. With our resilient model, you can count on enriched quality, with extended services that go beyond pre-configured alerts to include proactive measures:

- Threat Hunting
- IOC Sweeping
- MITRE ATT&CK
- Threat profiles
- Attack Simulations
- Compromise Assessment

We help enhance your current cyber defence posture by:

- Creating Incident Playbooks
- Determine techniques which are missed, detected and prevented by current security solutions
- Preparing Incident Readiness Report and Security Control Validation Report

KEY INCIDENTS TYPES COVERED

- Ransomware
- Advanced Persistent Threat (APT)
- Cloud Breach Response
- Malware Analysis
- Phishing Attack Analysis
- Web App Compromise
- Digital Investigation
- Insider Threat
- Data Breach & Exfiltration (loss of PII and other sensitive information)

INCIDENT RESPONSE:

Every second counts when your systems are compromised. Eventus partners with your team to create a tailored response and remediation plan that is optimized for your operational needs, harnessing your current investments and resources to expedite onboarding. We handle the entire incident lifecycle from triage to containment and remediation with detailed documentation and reports. Our team of highly-trained threat hunters and incident responders leverages experience of handling hundreds of incidents to quickly identify and respond to any type of attack, including ransomware or advanced persistent threats (APT).

Leverage the Incident Response Service by Eventus:

We quickly setup a virtual control room and our experts take the charge to perform the following services:

1. Identify the incident

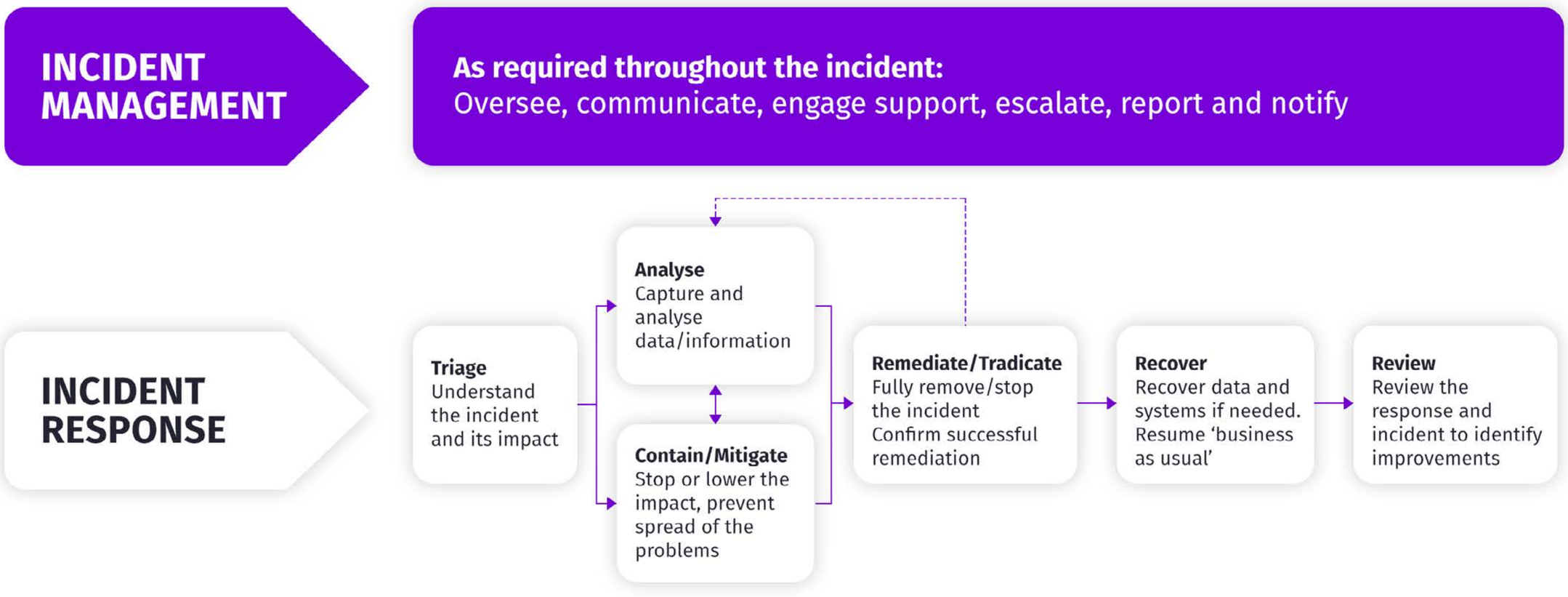
This involves incident analysis, determining what type of incident has occurred followed by prioritizing, and categorizing the incident so that more critical issues are addressed first.

2. Contain the incident

Once the incident is identified, the next step is to isolating the affected systems and data to prevent further damage.

3. Response plan and execution

The response plan includes steps to remediate the incident and implementing additional security controls.



4. Deep Forensics

- Root Cause Analysis and detailed impact analysis (business impact, reputation impact, technical impact)
- Forensic Investigation and lateral movement analysis
- Evidence Collection (optional) for legal and Insurance claim purposes

5. Reporting

A detailed report of the incident post remediation and reports covering up to 16 operations performed by our team for better senior management visibility.

6. Post Remediation Plan

- Vulnerability assessment and penetration testing Breach Attack Simulation (one time)
- Hardening assessment (impacted assets)
- Regular Tabletop exercise and continuous security validation

CHOOSE YOUR PACKAGE:

INCIDENT RESPONSE

- Threat containment
- Threat hunting
- Digital forensics
- Root Cause Analysis (RCA)
- Malware analysis
- Remediation & Recovery guidance
- Reports tailored to your organization

INCIDENT READINESS

- Tabletop exercise
- Maturity Assessment
- Ransomware Simulation Assessment
- IR Plans and Playbooks
- 24/7/365 Assistance

Eventus incident response experts are available 24/7 to help you quickly investigate critical security incidents and eradicate threats, so you can recover and get back to business fast.

Contact us at

sales@eventustechsol.com

www.eventustechsol.com