INCIDENT READINESS AND RESPONSE SERVICES

Ebryx Incident Readiness and Response service contributes to your current state of incident detection, management, and response capabilities. In addition to the Incident Response Retainer bucket that can be readily consumed during a breach without wasting time negotiating a contract right in the middle of the breach, we assist in developing custom IR playbooks and conduct readiness assessment and breach response drills. We recommend on how you can improve the security posture and develop capabilities to detect the modern day cutting-edge attack campaigns by focused adversaries that easily bypass the conventional security controls.

The service helps an organization answer the following questions:

- Does your organization have appropriate threat detection and response capability?
- Does your staff possess training required to properly handle the incident so no forensic evidence is lost?
- Does your staff have clearly defined roles and responsibility in case of an attack?
- Does your organization have the capability to respond to the security incidents right in the initial phase before they turn into a hazard?

Incident Readiness and Response Service

Incident Readiness Assessment

Assessment of current security posture against industry best practices in alignment with the NIST standards covering the following areas:

- Existing Detection and Response tooling and technologies
- Incident response processes & procedures in place
- Ability to sweep IOCs across all endpoints from a single point
- Ability to contain and isolate assets in case of an infection
- Ability to correlate current events with the past data
- Ability to eradicate injections from the endpoints in surgical manner instead of reimaging
- Ability to attain enhanced endpoint and network visibility from forensic evidence collection and investigation perspective

IR Plan, Procedures & Playbooks

Development the bespoke Incident Management Plan procedures coving:

- Incident identification and definition as per the nature of the business
- Incident types and lifecycle
- Incident escalation scenarios and handling process
- Roles and responsibilities of the stakeholders
- Escalation matrix and response SLAs
- Response playbooks for the SOC and IT team to handle various type of security incidents
- Incident management lifecycle integrated with Security Operations & SIEM/SOAR

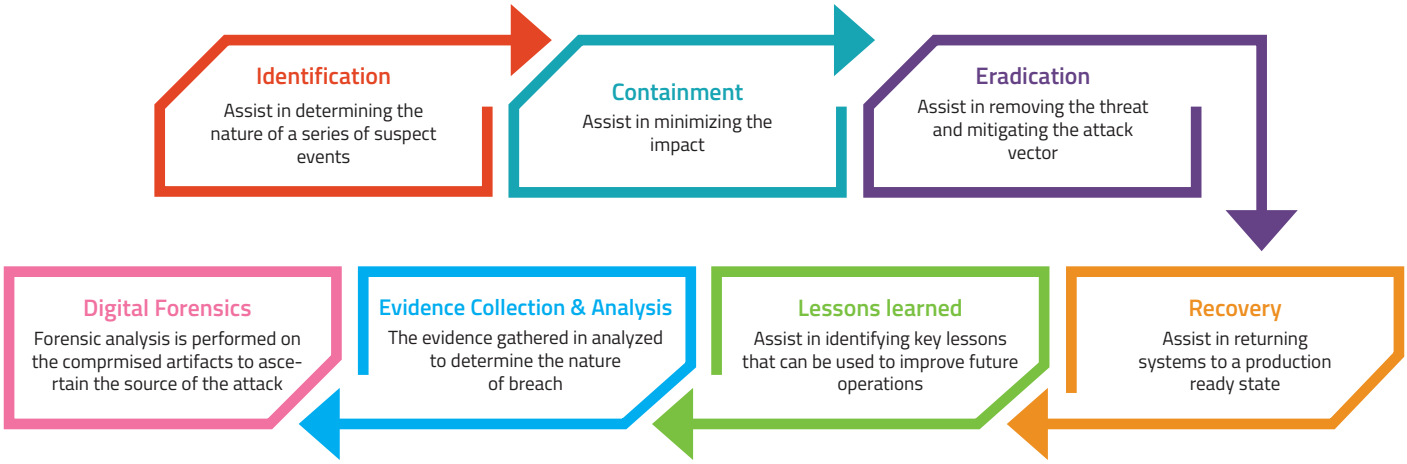
Breach Response Drills

Breach response drills every 6 months with assumed compromise in order to:

- Execute the breach response playbooks as per the IR plan
- Evaluate the efficacy of the breach response tools deployed in the infrastructure
- Gauge the preparedness of the internal team to respond to a breach
- Lessons learned for IR process improvement

Incident Response & Digital Forensics

Security Incidents that show signs of a breach are handled by Ebryx's qualified Incident Response and Forensics Services team either remotely or on-site as per the nature of the incident. The incident response and digital forensic services comprise the following stages:



Compromise Assessment Service

The threat landscape continues to evolve, and the sophistication of attacker tactics and techniques continues to advance. With Ebryx Compromise Assessment we can evaluate your enterprise to confirm a suspected incident or provide a health check to determine if attackers have evaded your security measures.

Why you should choose Ebryx for compromise assessment?

We apply our extensive knowledge of advanced attackers' tactics, tools and techniques gained from our experience responding to some of the largest security incidents

- Non-intrusive forensic assessment of the critical production services without causing a down time
- Complete 360 degree forensic evidence collection and analysis coverage including but not limited to Network, Operating System, Databases,
- Cloud Services and Mobile devices
- Hunting for the indications of compromise of the specialized, evasive malware used by motivated adversaries focused on your environment and technology stack
- Advanced reversing and analysis team to dissect malware having APT capabilities
- Timely identification and reporting of both malicious and anomalous activity

Compromise Assessment Methodology

Our proven compromise assessment methodology is aligned with MITRE ATT&CK framework and validates whether or not attackers have infiltrated your environment, installed any backdoors, established any covert C2 (command and control) channels and provides actionable steps you can take to keep them out.

OS specific malware presistence mechanisms	Process injection methods	Attacker lateral movement
Common attacker tools	Indicators derived from investigations	Environment-specific considerations