Datasheet

CYBER EMERGENCY SERVICES

Avoiding a cyber crisis often comes down to properly managing a cyber incident before, during, and after it unfolds. ActiveBytes cyber emergency team is expert in Readiness, Response & Recovery. With 24/7 monitoring and expert resources we ensure Readiness and our rapid, coordinated responses to incidents limit loss of time, money, and customers, as well as damage to reputation or the costs of recovery. Our team quickly initiates Recovery to return to normal operations and limit damage to the organization and its stakeholders if an incident occurs. Post-event steps include assessments of the causes, forensics investigation to recover lost data, finding flaws and hardening the infrastructure.

With our support in emergency services your organization becomes

Secure

Through prioritization of digital assets, management can allocate resources on the basis of the value of the assets, and aim to obtain a level of security corresponding to their value.

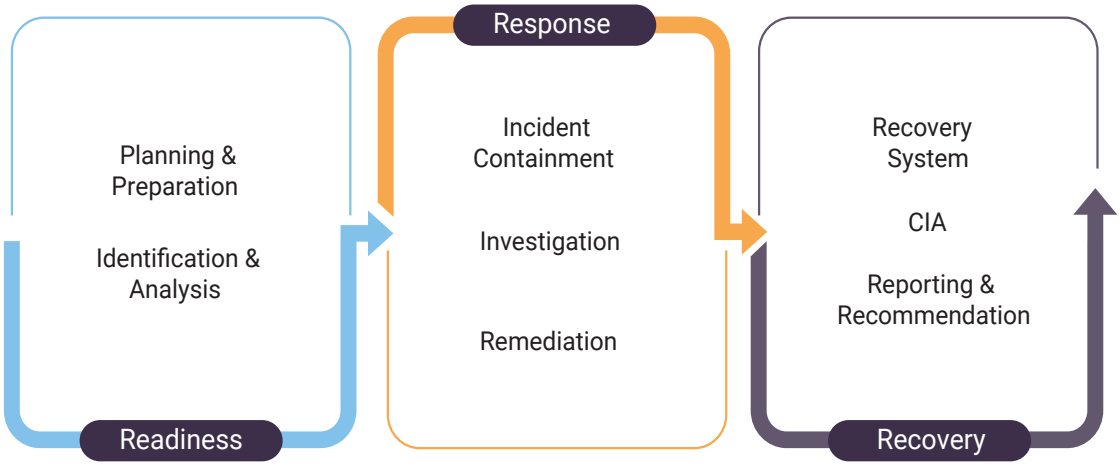
Vigilant

An enterprise is vigilant when everyone is aware of how they can expose the organization to cyber risk through their devices and online conduct.

Resilient

A resilient organization aims to minimize the impact of a security incident on its stakeholders and quickly restore operations, credibility, and security.

Our Approach



Planning & Preparation

Our team will be always ready to stop an attack by monitoring events, documenting, well defined IR team's roles and responsibilities and policy & Procedures. Along with the clear understanding or enterprise baseline we will assess relative value of all information, capacity of sufficient IT resources required to respond to an attack etc. Also, we will give awareness to employees regarding suspicious emails, maintain backups etc.

Identification & Analysis

Once we detect an anomaly in the enterprise events through an alert of any system, it will be reported and analyzed in depth and confirmed before escalation to incident response team. Then artifacts of the incident will be collected, forensic performed with manual and automated tools. We also find out the details of compromised data, what type of attack was performed etc.

Incident Containment

After learning which systems and data were compromised, the next focus will be, the containment of attack to stop it from affecting other networks and devices. This will involve actions like blocking unauthorized access, blocking malware sources, blocking certain ports and services etc. and more

Investigation

After an attack takes place, it's important to identify the root causes that led to it and each incident investigation shall help security teams to devise effective processes to prevent future attacks. Our team uses advanced tools to gather and analyze data and logs from networks and applications to identify the source of the incident, timelines the threat agent was operating within the target systems, attacker methodologies etc.

Remediation

Our team will provide post-incident repair for affected systems, coordinate communication and instruction to affected parties, and do analysis to confirm the threat has been contained. We will eradicate the risk to ensure that the attacker cannot regain access, perform additional vulnerability analysis to determine whether any other vulnerabilities exist

Recovery

After completing all critical emergency services, our team perform analysis of the incident for its procedural and policy implications, restore system to pre-incident state, ensure CIA, gather metrics, document to incorporate the knowledge gained into future response activities and training.

Benefits

- Improve enterprise security posture
- Continuous risk assessment & analysis to cover latest attack TTPs
- Security awareness training
- 24/7 monitoring
- Quick mitigation
- Organized approach in utilizing tools & resources
- Strengthen overall enterprise IT security
- Promote customer trust & Business reputation

Contact us

contact@active-bytes.com +971 50 513 3973

www.active-bytes.com