Volta

voltainc.com | 888.479.9672 | hello@voltainc.com

Incident Response

Get Back to Business Faster

The reality of cyber threats demands constant attention from organizations regardless of their size, industry and maturity level. In order to minimize the damage after an attack, you must implement a holistic strategy which combines threat intelligence with incident response experience. The securest level of IR planning challenges organizations to find and maintain a defense team they can count on to respond to advanced threats at the earliest stages of an attack. Trust Volta's Security Team to rapidly investigate, triage and remediate a cyber incident as soon as it's detected, so your organization can get back to business.

TYPES OF INCIDENTS VOLTA RESPONDS TO:

+ Financial violations
+ Stolen Personally Identifiable Information (PII)
+ Insider threats
+ Intellectual property theft
+ Destructive malware

THREE SETS OF ACTIONS: **CONTAIN** | **ANALYZE** | **RECOMMEND**

Volta's Response Process

Our team executes three sets of actions to quickly and efficiently resolve a cyber security incident:

1. IDENTIFY, INVESTIGATE, CONTAIN

Volta will assess the incident, identify root cause where possible, and contain the damage. Our response team will triage based on the most critical assets in your environment in order to minimize the effects of the breach. During the investigation Volta will identify:

+ Impacted networks, facilities, systems, applications, accounts
+ Data compromised or stolen
+ Malware and manipulated vulnerabilities

2. ADVANCED ANALYSIS + MONITORING

Although the worst anxieties created by a breach are somewhat alleviated after it is contained, recovery work is just as important. To catch every vulnerability that led up to an incident, Volta will perform an in-depth investigation, and continue to monitor affected systems. Analysis vectors include:

+ Live alert analysis
+ Network traffic analysis
+ Forensic analysis
+ Malware analysis

3. RECOMMENDATIONS + PROACTIVE CHANGES

By utilizing the in-depth analysis of the event, your organization can be better prepared for the next attack. Volta will guide whatever necessary actions are discovered in order to remediate issues on endpoints. These services might include adjustments to configurations or infrastructure.

What sets us apart?

We have thorough knowledge of historic and rising threat actors, and are very familiar with the quick evolution of their tactics, techniques and methodologies. Volta experts possess the real-world experience of actually responding to malicious attacks. The foundational experience of responding to security incidents is necessary. During IR engagements, the Volta team works alongside yours to optimize procedures and decrease the likelihood of similar events occurring again.

DEDICATED RESPONSE TEAM

During an Incident Response engagement, Volta provides your organization with a dedicated team of experts who will support you from start to finish. We have software development talent among our experts, with the necessary experience responding to incidents.

CUSTOM CONTAINMENT

We develop a custom containment and remediation strategy based on the actions of the attacker and tailored to the needs of your business. The strategy will eliminate the attacker's access and improve the security posture of the environment to prevent or limit the damage from future attacks.

RANSOMWARE RESISTANT RECOVERY

If needed, Volta is able to assist with the recovery phase once the response has been completed. In this phase, the IR team restores the systems affected by the incident to normal operation.

LEADING TECHNOLOGY

Depending on your level of maturity and the type of incident, Volta can deploy best-of-breed security controls to supplement your technology stack as we respond to and remediate the incident. These tools scrub all traces of compromise and act as a preventative measure against future attacks.

IN-DEPTH ANALYSIS AND DELIVERABLES

Attack attribution is difficult and mostly unimportant when vital applications are down. Volta will determine the scope of the incident and get your business back up and running. After analyzing the attack, we will deliver an overview that attempts to pinpoint After our analysis of the attack we will deliver an overview that breaks down:

- The initial attack vector
- The timeline of activity
- Malware used in the killchain

Volta will provide recommendations to prevent future incidents and consultation on near-term, mid-range and long-term goals in order to close cybersecurity gaps.

PEACE OF MIND

Our primary goal is to achieve restoration as quickly as possible and reduce business impact. We strive to leave our clients with peace-of-mind and confidence in the integrity of their critical business systems.