GOTHAM SECURITY

AN ABACUS GROUP COMPANY

Threat Management

Threat Intelligence: Plan and Prevent

Gotham Security's threat intelligence services accelerate the transformation of information system data into actionable threat intelligence by combining external and internal data sources for context and prioritization. Our threat intelligence services deliver comprehensive, actionable intelligence that allows you to understand attackers' intent and quickly prioritize threats.

Objectives:

- Reconnoiter data in real-time and detect external indicators of compromise (IOCs) pertinent to your organization including its employees, stakeholders, partners and clients from various clearnet (public records, company site content, social media sites, etc.), deepweb (data archives, metasearch engines, etc.) and darkweb (hacking forums, data breach lists, etc.) data sources.
- Evaluate IOC metadata for its potential impact on your organization's security posture including potential attack vectors, compromised credentials/systems and exposed sensitive corporate documents.
- Provide full due diligence information to your organization of all ongoing, past and predictive threat activity, analyzed organization data, risk mitigation recommendations, threat intelligence data sources and supporting evidence.

Incident Response and Threat Hunting: Respond and Recover

We focus on core areas of the network, endpoints, and server infrastructure to identify and understand the how, who, when, where and why of a security incident or systems breach.

Identify Security Breach:

- Analyze configurations, log history and file system data of various server and network information systems to identify indicators of compromise (IOCs).
- Analyze network traffic, user agent strings and DNS queries for indicators of compromise (IOCs).
- Detect malicious command and control (C2) network traffic and software across information systems.

Respond to Security Breach:

- Identify if exfiltration of sensitive data is occurring from the organization's information systems.
- Contain and quarantine malicious actor activities including isolating and blocking malicious command and control (C2) network traffic.
- Identify the root cause, attack vectors and intrusion points utilized by malicious actors.

- Discover the situation fallout and if there are any subsequent breaches from the security incident.
- Assist in organization breach notification strategy and incident response coordination activities.
- Provide a full due diligence report including a thorough list of all the examined information systems including:
  - Data points
  - Security findings from each set of data points
  - Correlations between all security findings
  - Incident root cause evidence
  - Subsequently affected users/systems/localities
  - Timeline of events
  - Incident retrospective and steps taken to prevent future incidents.