Accenture Security

iDefense® SECURITY INTELLIGENCE SERVICES

Business disruption and damaged reputation may cost an organization billions of dollars. Cyber attacks and high-profile data breaches dominate today's headlines. Security teams are struggling to keep up with the volume of threat intelligence and the sophistication of attacks. iDefense Security Intelligence Services provides timely, relevant and actionable security intelligence through the next generation IntelGraph platform that provides context, powerful visualizations, advanced searching, alerting and a robust RESTful API.

Threat actors are constantly evolving their tools and techniques, while launching powerful targeted campaigns against organizations. Traditional tools deployed against these actors are proving insufficient to detect and prevent attacks. Reliable threat intelligence is needed to understand the security risk before it hits. Threat Intelligence is not just important for protecting an organization's assets and preventing threats, but it is an essential component in all stages of the security life-cycle including mitigation, detection and recovery.

Accenture Security Security Intelligence Services, delivered by iDefense, provides 24/7 access to intelligence covering vulnerabilities of 1,000+ technology vendors, malware tools and techniques, indicators of compromise, target organizations and verticals, threat actors and their motivations, phishing campaigns, and more.

EXPERT HUMAN INTELLIGENCE

iDefense boasts nearly two decades in the security intelligence business, with a staff of more than 40 full-time, dedicated security intelligence analysts proficient in 20+ languages and cultures. These analysts are subject-matter experts in malware reverse engineering, vulnerability analysis, threat actor reconnaissance and geopolitical threats. In addition, iDefense offers customers access to an extended (external) network of more than 100 security research contributors worldwide, who provide customers with zero-day vulnerability information and intelligence on emerging regional security threats.

iDEFENSE INTELGRAPH

IntelGraph is built with graph database technology at its core. Graph databases utilize graph theory and allow nodes that contain relational information concerning malware, vulnerabilities, malicious tools, indicators, threat actors, campaigns, targets, phishing emails, and other threat elements. This structure enables faster access to relevant data and provides the ability to start at any data point and navigate, through use of the relational information.

Highlights of IntelGraph feature set:

- Advanced search features, including elastic search and graph traversal
- Visualization of relationships between actors; known infrastructure; tactics, techniques and procedures (TTPs), and other discrete threat elements
- Data-driven reporting
- Ad-hoc research flows, allowing security analysts and incident responders to "pivot" from a known data point and further explore the relationships inherent in the threat intelligence data
- Customized content and email alerting
- Threat type-specific dashboards, timeline graphs on threat activity

INTELGRAPH RESTful API

IntelGraph RESTful API is a powerful tool that supports various security use cases. iDefense provides a Vulnerability feed, a Threat Indicator feed and a Full API that gives access to the entire IntelGraph database—allowing the user to slice and dice the data as needed.

To streamline use of timely intelligence, iDefense data feeds can be integrated into security management tools and platforms. The feeds support automated threat prioritization based on severity, business criticality and relevance to the organization. iDefense feeds can be integrated into several SIEMS, TIPs not just limited to RSA Archer™, HP ArcSight™, Agiliance®, Skybox® and QualysGuard® VM.

CUSTOMIZED THREAT INTELLIGENCE OPTIONS

iDefense offers focused intelligence reports when an organization needs in-depth coverage on a threat of interest. Whether intelligence is sought on an attacker trend, or analysis is required on a threat campaign or threats targeting an industry, this product can be tailored to a client's needs.

ANALYST SERVICE

iDefense provides decision support that addresses both the strategic and tactical needs of a security organization:

- Global threat awareness is fundamental to critical decision-making. A client can learn who is targeting a vertical, what tools they are using, their motivation, and their infrastructure—enabling the client to be aware and proactive in its security posture.
- Enhanced vulnerability management and reverse engineering capabilities provide timely, actionable and in-depth research that reduces the amount of time and energy that a security team might use to track emerging threats. Ease of integration with IntelGraph helps automate day-to-day workflow to identify and respond to actionable intelligence.

SAMPLE QUESTIONS iDEFENSE INTELGRAPH CAN ANSWER

Cyber Espionage

- What are the verticals and countries the threat targets?
- What emails, blogs, URLs, handles or IPs are associated with an actor?
- What additional infrastructure is associated with this espionage campaign?
- What is the functionality of the malware?
- What specific defensive methods can be employed to detect this activity?

Cyber Crime

- What are the most popular banking Trojans in use today?
- What banks does the Trojan target?
- What are the C&C servers for an attack?
- What are the most popular forums for cyber criminals?
- What actor is associated with this operation?

Hacktivism

- What was the impact or severity of an attack?
- What is the name of the actor or organization that communicated a threat?
- What types of other initiatives or interests does an actor have?
- What is the attack's purpose or motivation?
- What is the timeline of the operation or its current duration?

Vulnerabilities

- What is iDefense's modified CVSS scoring for a vulnerability?
- What technologies does the vulnerability affect?
- What files exploit a vulnerability?
- What detection signatures identify an exploit?
- What IP addresses or URLs are associated with delivering exploits for a vulnerability?

BENEFITS OF INTELLIGENCE-DRIVEN SECURITY

Know which threats matter, and which don't

- Context provided by iDefense IntelGraph helps determine the relevance of a threat to an organization. Prioritization based on relevance and severity can help decision makers respond in the most efficient manner, allowing security teams to avoid unnecessary emergencies and costly "fire drills."

Stay 100+ days ahead of threats

- iDefense regularly provides deep analysis of software vulnerabilities more than 100 days before public disclosure. Staying ahead of vulnerabilities means staying ahead of threats.

Strengthen your security team

- With iDefense services, internal security teams have one of the world's most experienced multinational cyber intelligence networks at their fingertips—providing supplemental data to help better mitigate against costly threats.