Software vulnerabilities in critical assets increase an organization’s threat exposure. They also open the door to malicious actors. Proactively mitigating security risk to your organization requires staying ahead of these vulnerabilities. iDefense vulnerability intelligence covers 1,000+ vendors and 71,000+ product versions—and the service continues to grow with our customers and the technologies they utilize. iDefense understands the complexity of patch prioritization and vulnerability management. iDefense security analysts fully research and analyze each vulnerability and provide crucial details regarding its severity, exploitability, and proof of concept—thereby helping organizations proactively prioritize IT security operations and decisions.

WHY iDEFENSE VULNERABILITY INTELLIGENCE?

Vulnerabilities are discovered every day in nearly every organization’s technologies. Vulnerability management should therefore be a critical component of an enterprise’s security policies and procedures.

iDefense Vulnerability Intelligence provides around-the-clock access to relevant and actionable cyber intelligence to support vulnerability management decision makers. iDefense Vulnerability Intelligence analysts cover both public and zero-day vulnerabilities, tracking them across their entire lifecycle, from discovery, to proof of concept, to exploits in the wild—all the way until the vendor issues a patch.

STAY AN AVERAGE OF 100+ DAYS AHEAD OF ZERO-DAY THREATS

The only way to guard against new cyber-attacks and malware infection is to identify potential threats before they become active threats. iDefense provides deep analysis of software vulnerabilities more than 100 days, and in some cases, more than 200 days, before public disclosure. Staying ahead of vulnerabilities means staying ahead of threats.

STRENGTHEN YOUR SECURITY TEAMS

With iDefense, internal security teams have 24/7 access to some of the world’s most experienced multinational cyber intelligence analysts. The iDefense team works as an extension of its customers’ internal security teams through the iDefense Analyst Service. Please refer to the Analyst Service Datasheet for more information.

INTEGRATION-READY FEEDS

iDefense IntelGraph offers a powerful RESTful API that allows customers to easily integrate with many industry standard vulnerability management tools, SIEMs and TIPs.

EXPERT HUMAN INTELLIGENCE

The iDefense team includes 40+ full-time, dedicated cyber intelligence analysts who are experts in vulnerability discovery, analysis and alerting. In addition, iDefense offers customers access to an extended network of security research contributors worldwide, who provide iDefense customers with zero-day vulnerability information and current intelligence on emerging regional security threats.
RELEVANCE THROUGH CONTEXT WITH iDEFENSE INTELGRAPH

iDefense gives customers vulnerability security intelligence in context with IntelGraph, a proprietary, next-generation security intelligence platform (and API) that allows users to search, manipulate, visualize and contextualize relationships between elements within the 18+ year iDefense security intelligence knowledge base.

iDefense IntelGraph can add additional context and further perspective into threats because it is built with graph database technology at its core. Unlike traditional relational databases that rely on index lookups, graph databases are based on graph theory and allow nodes that contain information on threat actors, malware, vulnerabilities, campaigns, targets, domains, phishing emails, etc. and how they are related to one another. This data structure enables faster access to relevant data and the ability to visualize relationships among disparate vulnerability data. The context achieved through iDefense IntelGraph can provide organizations with vulnerability countermeasure options, through both indicators of compromise (IOCs) and signatures, even if patching is not feasible.

Vulnerability intelligence in context helps decision makers effectively prioritize and efficiently respond to threats, allowing security teams to focus on relevant threats and avoid unnecessary emergencies and costly “fire-drills.”

ABOUT iDEFENSE SECURITY INTELLIGENCE SERVICES

iDefense Security Intelligence Services gives information security executives access to accurate and actionable cyber intelligence related to vulnerabilities, malicious code and global threats 24 hours a day, 7 days a week. iDefense’s in-depth analysis, insight and response recommendations help keep businesses and government organizations ahead of new and evolving threats and vulnerabilities.