



VERISIGN™

DATA SHEET

VERISIGN® IDEFENSE® GLOBAL THREAT INTELLIGENCE SERVICES

CYBER ATTACKS AND HIGH-PROFILE DATA BREACHES REGULARLY DOMINATE TODAY'S HEADLINES, PROVING THAT THE VOLUME, SEVERITY, AND SOPHISTICATION OF CYBER ATTACKS IS EXPLOSIVE AND EXPANSIVE AND THAT THE IMPACT IS OFTEN DEVASTATING. INTERNAL SECURITY TEAMS STRUGGLE TO KEEP UP WITH THE SOARING VOLUME AND SOPHISTICATION OF THREATS.

To add to this challenge, understanding regional threat implications is a difficult yet important requirement in overall enterprise risk management as organizations extend business and operations around the world. A lack of visibility and analysis across cyber and geopolitical threats, late detection, poor clarity around which threats are most severe, and the difficulty of redirecting resources to implement mitigation strategies can place an entire business or mission on the line. Attacks come from everywhere, and most teams, which are already over loaded, cannot stay ahead of threats and vulnerabilities. Not knowing which threats are most important costs millions and puts security teams on the defensive constantly. The reality is that a single data breach can destroy a business, exposing an organization to

devastating losses in revenue, market share, reputation, and customer trust.

Vulnerability and malicious code feeds exist; however, there is a lack of context to effectively prioritize, make mitigation recommendations, and understand the entire threat and what it means to those who are vulnerable. Additionally, most intelligence feeds do not take into account the intersection point of both cyber threat and geopolitical threat implications. The result is that organizations are either exposed in areas they did not even know were vulnerable or such organizations overspend time, money, and resources in attempts to keep up with everything, as internal teams do not have the time or expertise to analyze the severity of threats.

Enterprise security teams need a reliable, accurate view of serious

threats based on geographical and contextual needs to know what is relevant and critical. It is not practical to hire a security subject-matter expert for all the points of presence in one enterprise.

Verisign® iDefense® Global Threat Intelligence Services puts enterprise security teams in control with proactive, accurate intelligence and informed recommendations for threat mitigation across global and regional threat landscapes. Basic "threat feeds" do not even come close to what Verisign iDefense can provide.

Verisign iDefense intelligence includes in-depth country and regional intelligence reports, a real-time threat feed, and access to subject-matter experts across vulnerability, malicious code, and global cyber security teams to equip security teams to:



VERISIGN™

- Understand the global implications of any emerging or existing threat as it evolves
- Proactively protect their organizations from the threats that matter most
- Prioritize threat mitigation strategies and to help focus internal resources
- Make more accurate and efficient decisions to support successful incident response and fraud response strategies and actions
- Move from security management to risk management and take the lead in communicating this strategy to the executive team

**ABOUT VERISIGN®
IDEFENSE® SECURITY
INTELLIGENCE SERVICES**

Verisign 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. Verisign iDefense in-depth analysis, insight, and response recommendations help keep businesses and government organizations ahead of new and evolving threats and vulnerabilities.

LEARN MORE

For more information about Verisign iDefense Security Intelligence Services, please e-mail learnmore@verisign.com or visit us at www.verisigninc.com/idefense.

KEY BENEFITS

Global Perspective - The Verisign iDefense global intelligence network includes more than 600 vulnerability researchers in more than 46 countries. A dedicated cyber intelligence team conducts threat research in more than 20 spoken languages and ongoing field operations in suspect regions of the world, all providing insight to the cyber underground, undiscovered vulnerabilities, and geopolitical threats.

Threats in Context - Instead of a reactive and often expensive response to vulnerabilities or suspicious activity, Verisign iDefense can assess and advise on a prudent course of action based on the unique geographical and contextual needs of a client's business across both cyber and geopolitical threat landscapes.

Threat Monitoring and Risk Management - The Verisign iDefense Vulnerability Aggregation Team (VAT) monitors security events 24 hours a day, 7 days a week. The team captures, analyzes, and correlates these events, providing primary and secondary analysis of new vulnerability exploits. The team proactively identifies suspicious and malicious events, therefore helping to mitigate an organization's potential for security risks.

VerisignInc.com