ITSolutions™
Powered By DEEP seas

Threat Severity Scale

DeepSeas' Cyber Defense Team identifies potential security threats in Customer environments using a combination of alert enrichment and review, open and closed source cyber threat intelligence, enterprise data search, and targeted cyber threat hunting. When DeepSeas identifies and validates a potential security threat in a monitored Customer environment, a Threat Notification report is documented and delivered to the Customer in alignment with a scaled threat severity model. Threat Notification reports are created in the form of a case event in the DeepSeas customer portal. Depending on the threat severity, direct contact is made in accordance with the Customer-provided notification escalation order, per the Customer MDR Runbook and as described below:

THREAT SEVERITY	THREAT DESCRIPTION	DEEPSEAS NOTIFICATION
Level 1 Critical	• Could result in severe business impact or service disruption to critical services or system(s) • Risk potential includes financial, reputational, regulatory, legal, etc. • Targeted attack/hack attempts by internal or external parties • Repeated attempts to obtain or export unauthorized information or access • Could have significant public impact	Within 30 minutes of detecting a critical validated threat, a DeepSeas cyber defense analyst will make direct contact with the Customer and create a case record in the customer portal. In the event a critical threat is detected and validated, the cyber defense analyst will deliver comprehensive updates to the Customer until the incident is contained using any mode of communication necessary or as preferred by the Customer.
Level 2 High	• Could result in a major impact to multiple critical services or systems • Risk potential includes major impact to sensitive data • Typically includes malware infections within the network on five or more hosts • Could have impact on the public	Within 60 minutes of threat declaration by a DeepSeas cyber defense analyst, the analyst will notify customer point of contact by phone and email, create a case in the customer portal. In the event a high threat is detected and validated, the analyst will deliver comprehensive updates to the Customer until the incident is contained using any mode of communication necessary or as preferred by the Customer.
Level 3 Moderate	• Defined as an infection beyond a potentially unwanted program/adware • Typically includes malware infections within the network on 1-4 hosts • Presents a potential for service disruption • Based primarily upon network traffic anomalies • Repeated violations of Customer's information Security Policies	Within 4 hours of threat declaration by a DeepSeas cyber defense analyst, the analyst will create a case in the customer portal and notify customer point of contact by email.
Level 4 Low	• Potential impact is on a single system or service • Impact detected is on a non-critical enterprise system or service • Potentially unwanted or unintentional activity by internal or external parties • Activity violates Customer's Information Security Policies • Threat Notification reports will be delivered to the Customer based upon potential Customer and public impact	Within 4 hours of threat declaration by a DeepSeas cyber defense analyst, the analyst will create a case in the customer portal and notify customer point of contact by email.