Description:
Threat Intelligence

1. Overview

Threat Intelligence is an Application Programming Interface ("**API**") feed which includes cyber threat intelligence data curated by eSentire (the "**Feed**"). The Feed is sold on an annual basis and may be downloaded with Feed data imported by Client into Client's firewall, TIP, e-mail server, EDR, or other systems. The Feed contains multiple Indicators of Compromise and is available in different standardized data formats.

2. Definitions

Any capitalized terms contained in this Description are as defined in the Order Form, below, or otherwise herein:

"**API feed**" means a data stream accessible via an API, distributing threat intelligence in standard formats.

"**Indicator of Compromise**" or "**IOC**" means distinctive elements of data used to detect potential security breaches or malicious actions.

"**Structured Threat Information Expression**" or "**STIX**" is an open standard language and framework used for structured and standardized representation and sharing of cybersecurity threat information, including IOCs, threat actors, malware, and more. It facilitates consistent and contextual threat data exchange between different cybersecurity tools, organizations, and platforms, enhancing the interoperability and effectiveness of cybersecurity efforts.

"**Threat Intelligence Platform**" or "**TIP**" is a technology solution that collects aggregates and organizes threat intel data from multiple sources and formats. A TIP provides security teams with information on known malware and other threats powering efficient and accurate threat identification investigation and response.

"**Endpoint Detection and Response**" or "**EDR**" is a cybersecurity technology that monitors and investigates endpoint devices for potential threats and provides a rapid response to security incidents.

"**Email Server**" is a computer system or software application responsible for sending, receiving, and storing email messages on a network, facilitating email communication.

"**Firewall**" is a network security device or software that acts as a barrier to control and filter incoming and outgoing network traffic, helping to protect against unauthorized access and threats.

3. Description

The Feed includes data developed by eSentire, that Client may ingest into Client's security tools such as a TIP, firewall, email server, or EDR, to enhance such tools with high value and up-to-date IOCs. eSentire offers IOC data, available via the Feed, in multiple formats which includes new line delimited for singular IOCs and STIX format for multiple, correlated IOCs. Client will receive access to the eSentire portal (the "**Insight Portal**"), where they will be able to access the API and any documentation related to Feed access or various IOC types. Client has the ability to access the Feed via API endpoint, and depending on the subscriptions ordered, the following IOC's will be included (as applicable):

- "IP address" - A unique numerical label assigned to each device connected to a computer network (note: only IOC included in the IPWatch subscription).
- "Domain name" - A human-readable web address used to access websites on the internet and used to identify one or more IP addresses.
- "URL" - A reference or address used to access resources on the internet, consisting of a protocol (like

HTTP or HTTPS), a domain name, and optionally a path and other components.

- "Email address" - A unique identifier for an email box to which messages can be sent. It is typically composed of a local part and a domain part, separated by the "@" symbol.
- "JA3 fingerprint" - Digital fingerprints of SSL/TLS client applications, based on specific parameters in the SSL/TLS handshake process.
- "File hash" - A unique alphanumeric code generated from the binary content of a malicious file using a hash function like MD5 or SHA-256.

4. Subscription Tiers

There are two standard subscription tiers available:

- Threat Intelligence - IPWatch – which provides Client access to a single IOC feed which includes only IP addresses; and
- Threat Intelligence - Advanced – which provides Client access to all IOCs in STIX format.

Both subscriptions are offered for the exclusive use of Client and may not be shared or redistributed. This is inclusive of the authorization token and the content contained within the Feed accessed using the token. eSentire proactively monitors the Feed for token expiration and automatically e-mails Client 90 Days prior to token expiration by way of Client's Insight Portal dashboard, and by email. Abuse of the Feed is monitored. eSentire employs rigorous security protocols to shield the Feed, inclusive of providing API tokens. The unique security credentials used are to authenticate and authorize access to the Feed. Tokens are set to expire 30 days following expiry of Client's Feed Term.

5. Deployment, Configuration and Tuning

Client is responsible for downloading, integrating, and configuring the Feed into its security tools and other systems not managed by eSentire. This includes scripting or middleware development for automation purposes or manual efforts to consume the threat intelligence data. Client is also responsible for ensuring its integration with the Feed is resilient to interruptions by implementing error handling, retry mechanisms, and backups, as necessary.

6. Feed Availability

Technical support for the Feed is available 8am-6pm EST, Monday-Friday excluding Canadian statutory holidays. After-hours support for high severity issues is available by contacting eSentire's SOC. eSentire does not guarantee uninterrupted or error-free access. eSentire is not liable for any damages due to Feed interruptions. The Feed may be occasionally offline for maintenance.