LookingGlass Cyveillance Machine Readable Threat Intelligence (MRTI)

Overview

There is an across the board increase in the number of threat feeds, the number of entries in each feed and, more importantly, uniqueness of threat intel. It means that analysts are expected to glean intelligence from a broad variety of threat intel sources. The LookingGlass Cyveillance Machine Readable Threat Intelligence (MRTI) provides high quality threat intel on the latest phishing attacks, malicious URLs, botnet infections and compromised account credentials in an easily consumable data format. MRTI is aggregated, analyzed and curated via algorithms as well as human analysis and made available via secure and standard delivery mechanisms for immediate ingestion. The high quality of the intelligence ensures that your analysts are prioritizing their time and energy on the most important security events.

High Quality Multifaceted Threat Coverage

- The LookingGlass Cyveillance MRTI raw intelligence is gathered from a wide network of deployed internet sensors, surface & deep web and darknet sources, Botnet Sinkholes, underground channels, human analysis and LookingGlass proprietary crawling algorithms.
- The MRTI feeds offer comprehensive protection against dynamic threats (APTs, Command and Control servers), static attack vectors (eg. phishing urls and malicious urls) and compromised account credentials, which can be used to launch a directed attack.
- Cut through the noise and quickly look at the highly relevant security items.

Flexible Consumption Model

High-quality threat intelligence that can be easily consumed and integrated with your own workflows and security platforms. Specifically:

- Security Information and Event Management (SIEM).
- Threat Intelligence Management and Platform products.
- Security appliances (e.g Application Level Gateways).

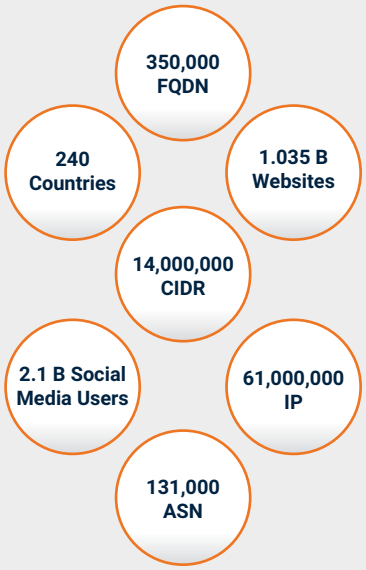
Ease of Integration

- With easy to understand documentation, downloadable code samples and 24x7 developer support, MRTI feeds can be ingested and consumed in a matter of minutes.
- Application programming interface (API)-based integration (e.g., JSON/OpenTPX, XML, CSV).
- Helper libraries to speed up the integration process (e.g., SDKs, bundled scripts, etc.).

KEY FEATURES

- Continuously refined threat intelligence vetted by expert security analysts and machine learning algorithms.
- Real-time updates with full context around a specific intel.
- 99.9% historical accuracy with over 2 billion infection records
- Broadest coverage of global Advanced Persistent Threats in the industry.
- Maximize the value of security tools and processes already deployed.
- LookingGlass Threat Intelligence Platforms comes prepackaged with MRTI along with hundreds of 3rd party threat intel feeds.

THREAT INTEL STATISTICS: 24-HOUR DATA CONTEXT



LOOKINGGLASS

LOOKINGGLASS CYVEILLANCE MRTI: THREAT INTEL SWISS ARMY KNIFE			
Name	**Frequency**	**Delivery**	**Format**
Infection Records	Real-Time	API	OpenTPX, CSV
Malicious C2 Domains	Real-Time	API	OpenTPX, CSV
Phishing URLs	Real-Time	API	XML
Malicious URLs	Real-Time	API, FTP	XML
New Domain Registrations	Daily	FTP	CSV
Compromised Information Monitoring	Daily	API, FTP	XML

LOOKINGGLASS CYVEILLANCE MRTI: LICENSING		
Name	**Description**	**SKU**
Infection Records: Global	List of newly identified and historical global infections collected by our VirusTracker botnet monitoring technology	DATA-VT-INFECTION-ALL
Infection Records: Country Specific	List of newly identified and historical global infections collected by our VirusTracker botnet monitoring technology	DATA-VT-INFECTION-COUNTRY
Malicious C2 Domains	Daily updated blacklist of 100% known C2 command and control botnet servers	DATA-VT-MAL-FQDN
Phishing URLs	Real-time feed of global phishing URLs	DATA-CYV-MAL-PHISHING
Malicious URLs	Real-time feed of global malicious URLs	DATA-CYV-MAL-URL
New Domain Registrations	Aggregated list of TLDs (.com, .net, .info, etc) registered globally in the last 24h	DATA-CYV-NRD
Compromised Information Monitoring	Early warning of compromised Account Credentials (CACs), compromised Credit Card Numbers (CCNs), and/or compromised Social Security Numbers (SSNs) discovered in the wild	DATA-CAC-TIER-[1-5]
Cyveillance Malware Total Lifecycle Protection	Bundle includes: • Cyveillance Malicious URLs • Cyveillance Malicious C2 Domains • Cyveillance Phishing URLs	DATA-MAL-TLP-BUNDLE

LookingGlass is the only threat-centric security company in the industry with the portfolio to holistically operationalize cyber threat intelligence.

LOOKINGGLASS