John Snow LABS

INTEGRATED SECURITY
AND THREAT INTELLIGENCE

The cyber security team at **John Snow Labs** has developed an integrated solution for comprehensive security intelligence and threat management. The John Snow Labs Delivery Framework automatically integrates actionable intelligence from Threat Intelligence Platform with other machine data collected throughout the enterprise for comprehensive, real-time threat visibility and next generation security analytics. **See Figure 1**

Figure 1: Delivery Type

JOHN SNOW LABS INTEGRATION API ALLOWS CUSTOMERS TO:

- Dynamically sync threat data from John Snow Labs Threat Intelligence Delivery Framework into your choice Delivery Type for immediate recognition of internal resources communicating with identified bad actors. **See Figure 2**
- Automate the corroboration of network activity to or from threat indicators with other behavioral changes to hosts and users for more accurate prioritization of high risk events.
- Continually share and receive relevant threat data within the existing security infrastructure to optimize workflows and enable real-time countermeasures.
- Automate the remediation of attacks recognized from prioritized IOCs by blocking communication with compromised domains to prevent data theft, block malware and terminate **APT** communication with a command and control infrastructure.

Figure 2:
Threat Intelligence Delivery Methods

By leveraging **John Snow Labs Threat Intelligence Delivery Framework**, customers benefit from increased threat intelligence and accurate risk management. The combined solution delivers the ability to rapidly detect, validate, and streamline incident response time to cyber attacks.

See Figure 2: Threat Intelligence Delivery Methods

BRIDGING THE GAP BETWEEN YOUR STIX/TAXII REPOSITORY AND YOUR SECURITY INFRASTRUCTURE

The Cyber Security Team at John Snow Labs has developed an integrated solution for AN EASILY OPERATIONALIZED STIX/TAXII COMPLIANT THREAT INFORMATION ACROSS YOUR SECURITY INFRASTRUCTURE.

SOC operators, **CSIRT** teams, and security analysts and researchers are in a race against time. The good news is that an overwhelming amount of Threat Intelligence is available today. The bad news is that it takes a long time to consume and make operational this intelligence across your security infrastructure.

If your organization is part of an Information Sharing and Analysis Center or Organization – **an ISAC or an ISAO**– much of the threat intelligence you're consuming is probably based on the **STIX/TAXII** standards for describing and exchanging cyber threat information. Many ISACs, such as the **Financial Services ISAC** (FS-ISAC), rely on a STIX/TAXII repository to facilitate threat information sharing across the members of their trusted communities. This Threat Intelligence is still difficult to integrate with other security products essential to protecting an organization. The process is manual and error-prone.

JOHN SNOW LABS THREAT INTELLIGENCE FRAMEWORK, PROVIDES THE ESSENTIAL CONNECTION FROM **STIXX/TAXII** COMPLIANT SOURCES TO **SECURITY PRODUCTS AND SOLUTIONS THAT CAN OPERATIONALLY LEVERAGE THIS THREAT INTELLIGENCE.**

John Snow Labs Threat Intelligence Delivery Framework provides the essential connection that security and incident response teams need to translate raw STIX/TAXII data into usable intelligence. It integrates any STIX/TAXII repository with your security infrastructure.

John Snow Labs Threat Intelligence Delivery Framework can connect to any STIX/TAXII server in the cloud (for example, http://hailataxii.com or a server hosted by an ISAC), or on premise, and pull threat information from it into existing security solutions – including HP ArcSight ESM and Splunk – in a format appropriate for that solution.

An instance of **John Snow Labs Threat Intelligence Delivery Framework** can retrieve threat information from multiple sources and forward it to multiple destinations in an organization's infrastructure. The **John Snow Labs Threat Intelligence Delivery Framework** has easy-to-use, interactive dashboards enable threat intelligence visualization, deeper analysis, and advanced searches.

KEY FEATURES

Optimized to work with ISAC communities and raw IOC aggregators

- Translate raw STIX/TAXII data into formats that HP ArcSight ESM and Splunk can understand; many more integrations to come
- Easy-to-use interface to view threat information received through STIX/TAXII feeds
- Ability to run a keyword search to look for a specific indicator, search for an indicator type over a time range of your choice, and drill-down on specific indicator matches for details