CYSIV

USING A BLEND OF TECHNIQUES FOR ADVANCED THREAT DETECTION & RESPONSE.

How Cysiv automates, accelerates, and improves the process of finding and prioritizing threats.

of cybersecurity professionals say threat detection and response is more difficult than it was two years ago.[1]

But an advanced threat detection engine

enables CISOs and security leaders to more quickly and confidently detect threats that warrant deeper human investigation.

Implementing the right blend of techniques.

Cysiv relies on five complementary and essential techniques that it combines based on the use case to improve the speed and accuracy of the threat detection and response process.

Cyber Intelligence

is the act of comparing known activities in an environment — for example, firewall logs or new files being generated on a computer — to known sources of bad activity.

1

Signature-based

detection techniques match all or some attributes of an object to a known bad object and is most commonly associated with finding malware and ransomware.

2

Behavior-based

detection techniques match some type of digital pattern, footprint, human activity, or network behavior to known bad behavior. Behavioral techniques are linked to detecting insider threats.

3

Statistics-based

detection techniques use clustering, grouping, stack counting, baseline and variation, outlier detection, logistic regression, and other methods to detect anomalous activity. This is often used to detect brute force attempts.

4

Algorithm-based

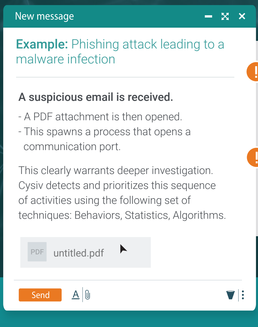
detection uses machine learning techniques, such as supervised or unsupervised learning or deep learning, to detect malicious or anomalous activity and predict attacks.

5

> *these techniques are combined to improve the speed & accuracy of threat detection, investigation and response.*

Detection and response in action.

The key is to combine the above techniques in a flexible way, based on use case, to improve the quality and confidence of detections.



User and entity behavior analytics (UEBA) is used to look at patterns of human behavior

Algorithms and statistical analysis are used to detect meaningful anomalies from those patterns

Can your team **quickly detect** targeted attacks, ransomware, zero-day exploits, malware, and other attacker behavior with confidence?

Cysiv SOC-as-a-Service provides comprehensive 24/7 threat detection and response, supported by:

- **Vital sources** of telemetry & important contextual data
- Cloud-native, co-managed, next-gen **SIEM platform**
- Data Science that uses a **blend of threat detection techniques**
- Comprehensive actionable **cyber intel**
- Security, threat, data and IR **experts**

CYSIV

Let's discuss how Cysiv can improve your security and resilience.

1.833.229.9800 | info@cysiv.com

CONTACT US

1. The Enterprise Strategy Group, 2019