CYSIV

DATA SCIENCE & THE SOC

A snapshot of the current situation and how organizations can deploy data science to their advantage.

Automating, Accelerating & Improving Threat Detection

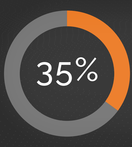
Cybersecurity teams can be bombarded with hundreds or thousands of new security incidents every week, each one often taking days to fully investigate. The massive volume is unmanageable, and opens the door for threats to slip through.

Cybersecurity has a big data problem.

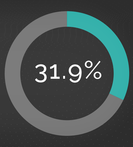
Cybersecurity teams deploy dozens of security products across their networks, endpoints, data centers, and cloud workloads. The problem isn't simply that there's too much data. There are other big concerns:

- Incomplete Data
- Insufficient Data
- Normalization of Data
- Correlation of Data
- False Positives
- Storage & Retention

SOC analysts are feeling the strain.



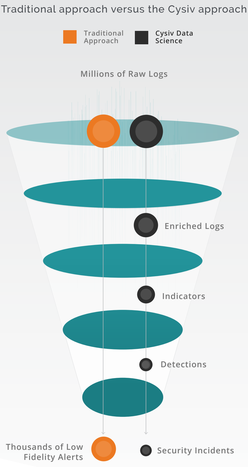
of security teams say **gathering data** related to an alert is their most time-consuming task.[1]



IT security professionals report that they **ignore alerts** because so many are false positives.[2]

Filtering down to the threats that matter.

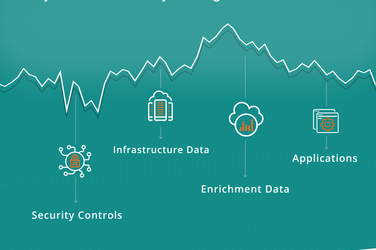
At Cysiv, data science is used to more efficiently and effectively convert raw logs and data from other relevant sources. The end result is actionable, high-quality, high-confidence detections and security incidents that warrant deeper human investigation.



Data is the problem. It's also the *solution.*

The more data we have, the better Cysiv's solution is able to make important correlations, reduce false positives, and improve confidence in the detections to be investigated.

Cysiv SOC Telemetry leverages data from:



Detect with confidence.

Cysiv's data science-driven approach automates, simplifies and accelerates the critical tasks of threat detection, threat investigation and threat hunting, to reduce the probability of a successful attack, breach, theft or disruption.

- Reduce the Mean-Time-To-Detect
- Reduct Alert Fatigue
- Avoid Costs + Damages
- Improve Agility

Let's discuss how Cysiv data science can improve the effectiveness of your security.

1.833.229.9800 | info@cysiv.com

CONTACT US

1. The Enterprise Strategy Group, 2017
2. Alert Fatigue: 31.9% of IT Security Professionals Ignore Alerts

CYSIV