# Cy:Twist

**Detect, Visualize, Terminate Sophisticated Cyber Attacks**

## Current SOC and Incident Response Challenges

**Despite yearly spending exceeding $12 billion (according to Gartner) on network, endpoint detection, SOC & SIEM, over three quarters of enterprises still expect a critical infrastructure breach in the near future.**

### Sophisticated Attacks

Current Solutions generate many alerts, making it very hard to find the relevant ones, or completely miss sophisticated attacks

### Team Discontent

Teams grow larger than they really should be while handling routine boring work. This costs both directly, and in turnover.

### Alert Desensitization

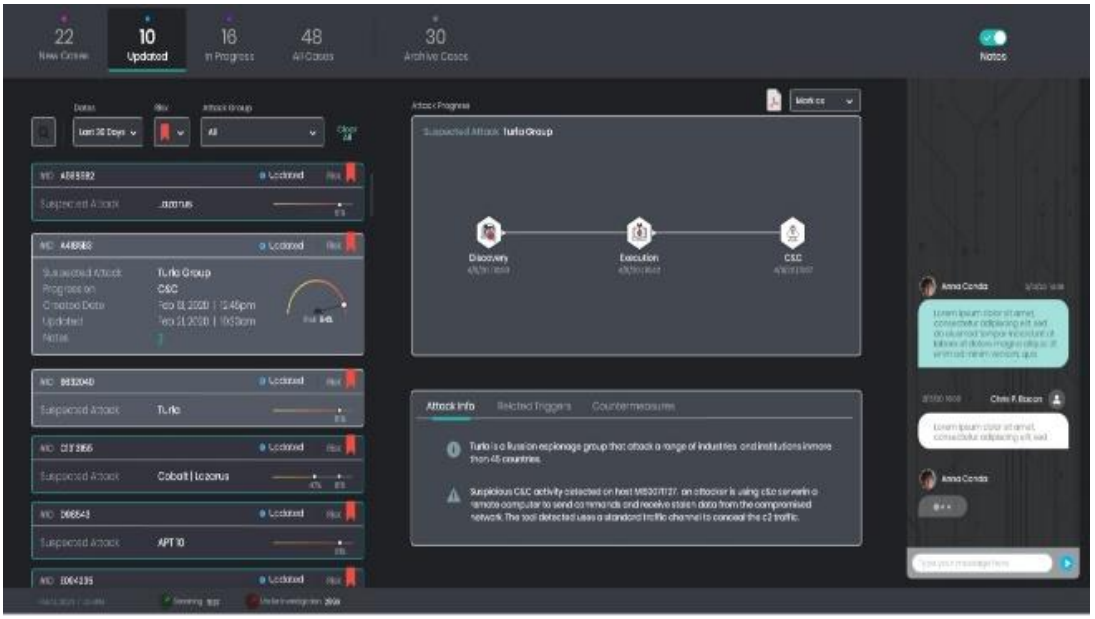
Over 30% of security alerts are ignored due to fatigue while even true positives lack context.

### Delayed Response

Because alerts can't be properly prioritized, incident response timeliness and relevance suffers.

## Holistic Detection & Response

**Cytwist delivers an automatic Holistic attack detection solution That is mapped to an augmented Version of the MITRE ATT&CK Matrix, based on existing data**



# Benefits

### Team Empowerment

Automatically tracks and stops modern cybersecurity attacks.

### Cost Reduction

Eliminates SecOps productivity loss due to manual triaging.

### Spend Leverage

Enhances the value of existing security investments without complex deployments

## PLATFORM CAPABILITIES

- Generate comprehensive multi-stage Attack Graph and Report
- Only highlight Confirmed Attack alerts as high priority
- Save time handling false positives
- Save significant time fine tuning individual alert thresholds for both SOC analysts and Data Scientists
- Pinpoint areas for Incident Response and predict next steps for attacker

"As an infrastructure provider in Israel, we are attacked daily. We always introduce the most forward-thinking solutions to detect those attacks, but it was not enough. Cytwist detected attacks that would have required weeks of manual hunting and freed up our SOC analysts to further improve our detection policy."

**Kobi** *CISO, Cellular Operator*

"As a global company, we are always looking to improve our operational effectiveness and the value of our services to our customers. Cytwist allowed us to onboard them faster because we did not need to invest our best team in reconfiguring detection rules"

**Y, MSSP practice head**

**Data Types Supported:**

- SIEM (CIF, ELK)
- Cloud logging
- EDR
- NDR
- XDR
- UEBA
- Data Lakes

**Request a Demo**

info@cytwist.com
www.cytwist.com

Cy:Twist