



# Reduce Vulnerabilities Using AIOps



## AI Ops for Cybersecurity – ZIF™



In business, an end user normally uses the same applications and communicates with the same set of devices everyday, transmitting a standard set of data routinely – called ‘Steady State’ (SS).

In a typical SS scenario, if anything in an endpoint changes from it's original state (for instance, installation of a new app or new communication between the endpoint and other devices), it is referred to as ‘Change of State’ (CoS).

Zero Incident Framework™ (ZIF™) is a comprehensive AI Ops platform that proactively detects and remediates Cybersecurity threats, thereby enabling Security Operations to transcend to a proactive approach.

### Risks Overlooked in CoS

#### *Probable endpoint intrusions indicated by CoS:*

- A new application within the endpoint could mean malware that could degrade the performance, corrupt or delete files/data
- A new application communicating with another device, or a new device may mean proliferation of performance degradation, data going out, or deletion of files
- Change in response time could indicate either a network choke or more data transmission
- Change in quantum of data transfer may indicate confidential and important data being sent out

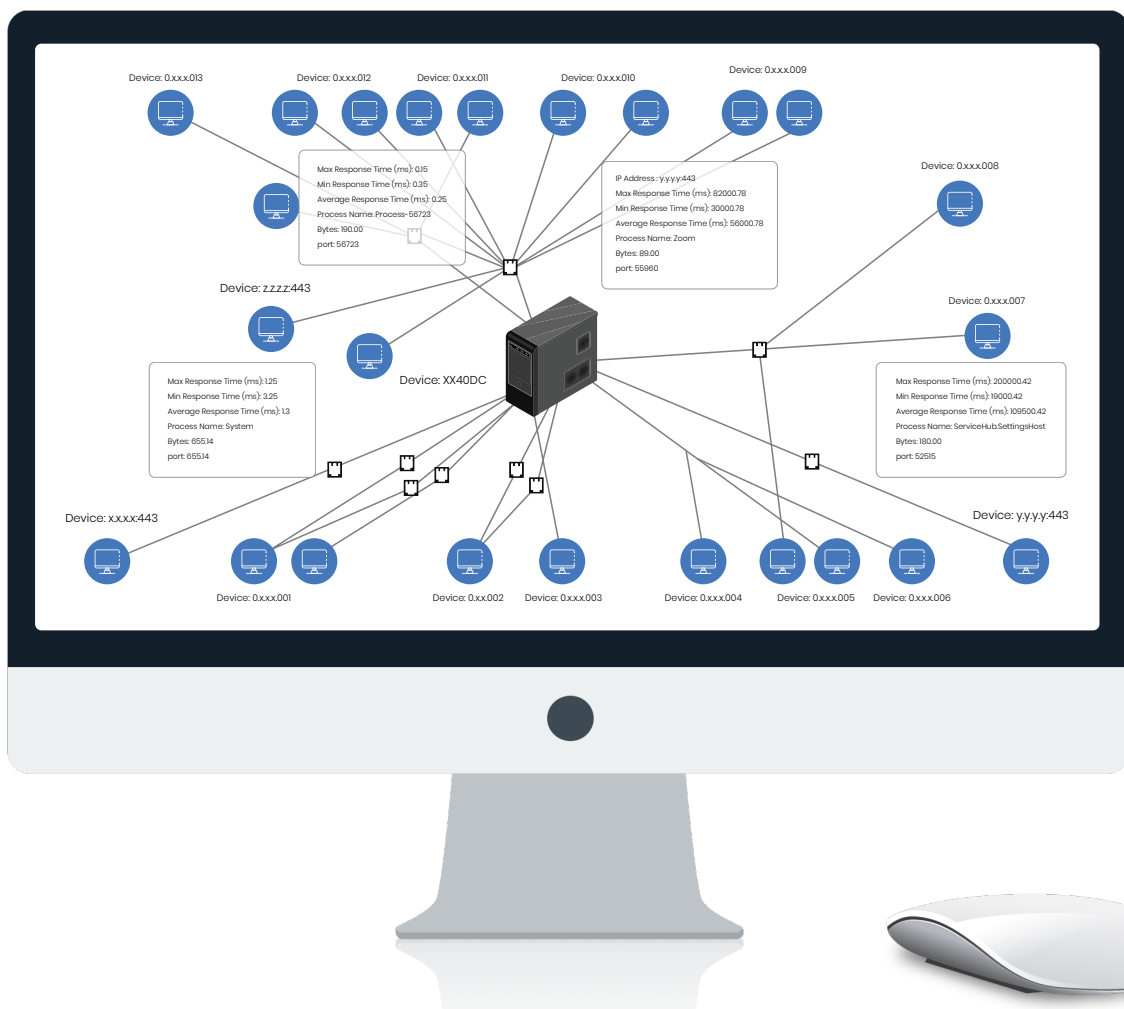
#### Generally, CoS is caused by one or more of the following:

- Devices running a new application that is not part of SS, within the endpoint
- Devices running a new application that is not part of SS, and communicating with the others
- Devices communicating with a new device that is not part of SS
- Devices taking longer than usual to communicate with another device
- Devices sending or receiving more data than they usually do

## Addressing CoS with the Transaction Journey Mapper (TJM)

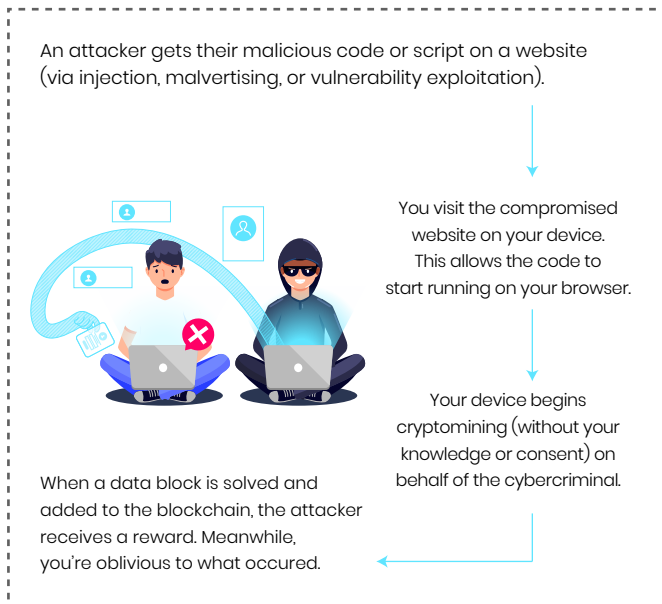
- I. Helps highlight endpoint behavior – for example, unusual communication with other nodes, unusual applications used, or any deviations from regular patterns
- II. Enables understanding and planning for network bandwidth required between a set of nodes
- III. Highlights any unusual communication, and thereby aids identification of anomalies between Server-to-Server, User-to-Server, etc.

- *Zoom with average latency of 5,600.78 msec - not a good sign if it is a continuing trend*
- *ServiceHub.SettingsHost with an average latency of 109,500.42 msec - not a good sign if it is a continuing trend*



## Cryptojacking






Cryptojacking aka malicious cryptomining, is a threat that embeds itself within a computer or mobile device and then uses its resources to mine cryptocurrency.



## Ransomware

Always takes advantage of human, system, network, and software vulnerabilities to infect the victim's device, which can be a computer, printer, smartphone, wearable, point-of-sale (POS) terminal, or any other endpoint.

### How Ransomware Works

- 01**  Malware received via spam email
- 02**  The malware downloads malicious files (code)
- 03**  The malicious code encrypts your files
- 04**  You will see a ransom notice with a deadline
- 05**  You will need to pay ransom to get your data back (we recommend not paying)

## Protecting your Business and IP from Cryptojacking and Ransomware with TJM

- ZIF Universal Connector has out-of-the-box capability to integrate with multiple Open Threat Exchange (OTX) platforms.
- ZIF TJM helps monitor all traffic, detects and identifies anomaly traffic from devices based on Indicators of Compromise (IoC).
- Enables identification of endpoints that have communicated with compromised systems and alerts about the established communication, thereby driving a proactive approach to identify and detect vulnerable systems that could potentially lead to enterprise disasters.



**ZIF™ (Zero Incident Framework™)**, is an award-winning AIOps platform for IT Operations. ZIF™ delivers business outcomes by leveraging unsupervised pattern-based machine learning algorithms. Infrastructure and application telemetry data are aggregated, correlated, and potential failures are predicted. To enable faster resolution and better user experience, ZIF™ deploys intelligent bots for proactive remediation. Developed by GAVS Technologies ([www.gavstech.com](http://www.gavstech.com)), ZIF™ is available as an on-premises and SaaS solution.

**Contact us now for personalized onboarding service!**

To find out more about ZIF™, please visit [www.zif.ai](http://www.zif.ai) or write to [inquiry@zif.ai](mailto:inquiry@zif.ai)