CYBER TRIAGE
SIMPLIFIED INCIDENT RESPONSE

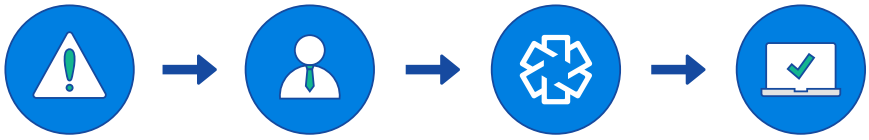
Rapid, Powerful Endpoint Investigation

Cyber Triage™ is an automated incident response software any company can use to investigate their alerts.

- **AGENTLESS:** Easier to deploy than EDR
- **AUTOMATED:** Easier to use than command lines
- **THOROUGH:** More complete than antivirus
- **PRACTICAL:** Designed for non-forensics experts

Investigate Your Endpoints

When your SIEM or detection system generates an alert, you need to investigate endpoints to determine severity and scope. Cyber Triage integrates with your SIEM, orchestration, or ticketing system to give your cyber first responders the endpoint visibility they need to make decisions and remediate.



An alert is generated from a SIEM or detection system

An analyst is assigned in a ticketing system

Cyber Triage is deployed to the endpoint

Severity is determined and the incident is remediated

Why Cyber Triage?

Every organization needs a cyber first response that is more thorough than a single antivirus scan, which can miss new malware and doesn't detect compromise user accounts.

FASTER THAN AD-HOC APPROACHES

Command line tools are time consuming and error prone. Cyber Triage's automated techniques and backend database allow you to more quickly collect, analyze and interpret results.

EASIER TO DEPLOY THAN AGENT-BASED SYSTEMS

Deploying agents can be expensive and time consuming. Cyber Triage's agentless approach means fewer approvals and works when the security team does not have administrator privileges.

SIMPLER THAN FORENSIC TOOLS

Forensic tools are hard to use for the average security team and have features that won't be used. Cyber Triage's focus on the triage step means a simpler interface and a lower price.

INTEGRATIONS

Integrate with other leading cyber security tools to respond as quickly and effectively as possible:

- Yara
- Volatility
- Splunk
- Phantom
- Polyswarm
- OPSWAT
- The Sleuth Kit

FREE VERSION AVAILABLE

Cyber Triage can be used without the automation and malware scanning for free. The Lite version allows you to collect data from live systems and view the results so that you can manually identify and report on suspicious activity.

How Does Cyber Triage Work?

Cyber Triage investigates the endpoint by pushing the collection tool over the network, collecting relevant data, and analyzing it for malware and suspicious activity.

A new session is created in Cyber Triage

The collection tool is sent to the endpoint over network or USB

Volatile, registry, and file data are collected

The automated analysis finds malware and known indicators

Suspicious data is flagged to help the analyst make decisions

Used by Companies Like Yours

Fortune 500 Companies

Medium Enterprises

Financial Institutions

State & Federal Government

Built by Forensics Experts

Cyber Triage was built by forensics experts so that you don't have to be one. Cyber Triage will automatically collect artifacts about malware persistence, user activity, and volatile data from memory. It extracts data from the registry and event log using forensic techniques that leave minimal traces and avoid rootkits.

You can more quickly find the indicators of compromise because Cyber Triage will flag items that an experienced responder would look for, such as DLL hijacking and suspicious startup items.

Built for Any Cyber First Responder

Cyber Triage was built for the incident response needs of any organization:

- **Internal Teams** investigate alerts from SIEMs
- **MSSPs** investigate client endpoints based on network traffic
- **Consultants** allow clients to do their own basic response
- **Law Enforcement** ensures consistent analysis from all agents

EMAIL info@basistech.com **WEBSITE** www.cybertriage.com **PHONE** +617-386-2090

CYBER TRIAGE
SIMPLIFIED INCIDENT RESPONSE

Cyber Triage performs an automated, forensic triage on your endpoints so that your incident responders can quickly determine if a host is compromised. Its agentless approach and ability to integrate with your infrastructure makes your team more efficient than using ad-hoc techniques.

BASIS
TECHNOLOGY

Basis Technology provides solutions for extracting meaningful intelligence from unstructured text. We help government organizations improve the accuracy of search, text mining, link analysis, and other applications through advanced linguistics. Our digital forensics team pioneers faster and cheaper techniques to extract forensic evidence, leveraging the Autopsy open source platform.