EventTracker
www.eventtracker.com

# EventTracker DFIR capabilities

Fraud, intrusion, insider threats, phishing, and other cyber-crimes are now a fact of life. You are working under the assumption of a breach, and your mission is to identify suspicious artifacts to verify potential intrusions. Modern attackers:

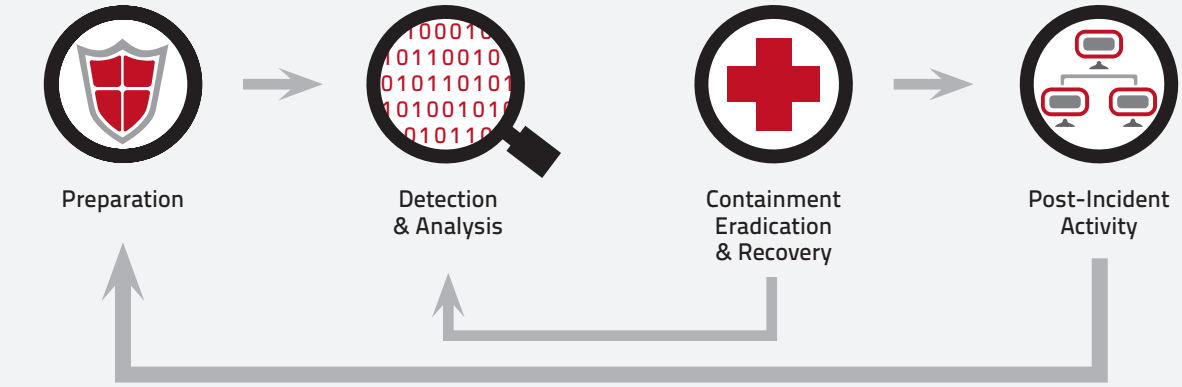
- Attempt to hide in plain sight
- Run in the background without user interaction
- Connect to external sites of low reputation
- Are hard to detect by observing only network traffic

Proper handling of a forensics investigation is critical to fighting back against computer crimes. Success at digital forensics is the ability to spot the difference between abnormal and normal. Artifacts include: Rogue processes, unknown services, suspicious network activity, evidence of persistence and unusual OS artifacts.

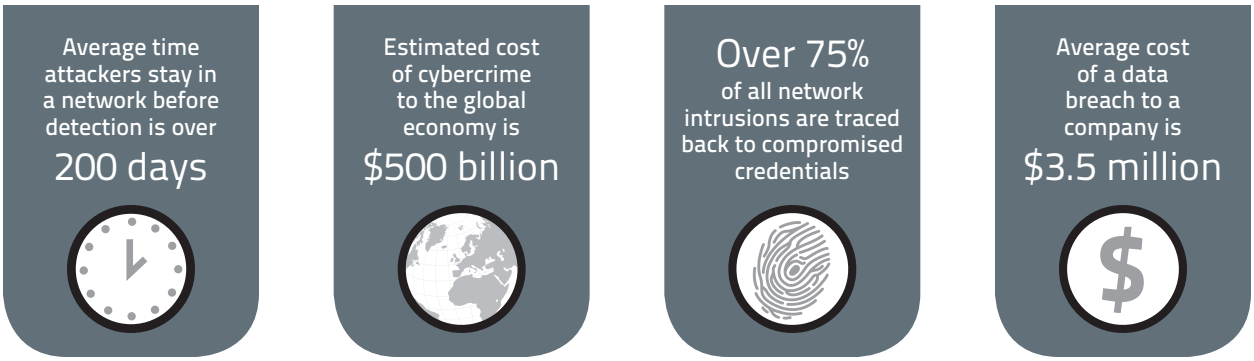
**Forensic Process**


Incident Response are the ***"actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to prevent the incident from happening again."***

**Incident Response Life Cycle**



EventTracker
www.eventtracker.com




EventTracker 8 includes various capabilities to assist both Digital Forensics and Incident Response ("DFIR") via the new Advanced Security Analytics package.

The steps are:

- Get data
- Monitor for anomalies
- Look for abnormal behavior
- Examine key applications and suspicious network traffic.

To quote the SANS Institute: ***Know Abnormal, Fight Evil.***

EventTracker 8 greatly simplifies and automates many of these difficult tasks, thereby empowering even junior analysts to participate actively in cyber defense.

**Rogue process detection:** Attackers like to hide in plain sight. They try to blend in by having apparently legitimate names (e.g., svhost.exe) or by hollowing out legitimate processes. EventTracker 8 compares full path names against a whitelist to detect rogue processes; EventTracker 8 also examines the parent process for legitimacy (e.g., lsass.exe should never spawn a child process).

Adversaries hijack legitimate apps to maintain persistence or pivot. To defend against this, when a process is launched on a monitored Windows machines, EventTracker 8 computes a hash (MD5 or SHA256) for comparison with known virus signatures (virusshare.com, a collection of 20M samples) and/or online scanners such as virustotal.com (a Google service for the identification of viruses, worms, trojans and other kinds of malicious content). This allows a defender to quickly pinpoint rogue processes and observe their progress around the entire network.

**Unexpected application usage:** Attackers pivot from the initial beachhead to other systems. To detect such attempts, EventTracker 8 monitors for unexpected (but legitimate) applications. For example, a typical end user never invokes cmd.exe or powershell.exe or psexec.exe; the use of such applications is suspicious.

**Suspicious network activity:** Attackers exfiltrate data by using legitimate ports and trying to hide in high traffic times. To detect such attempts, EventTracker 8 identifies processes communicating over ports 80/443/8080 that are not a browser; browsers communicating over non-standard ports; connections to unexplained external IP; web requests directly to an IP address

**Abnormal user behavior:** More than 76% of data breaches involve compromised credentials. In such cases, the stolen credentials are used at unusual places in the network. EventTracker employs machine learning to detect common username and workstation associations. For example if user "susan" normally logs in to wks5, then a login by "susan" at server6 will be highlighted.

**Attackers & Targets dashboard:** Public IP addresses that are present in any log entry are compared to IP reputation services such as ipvoid.com, reputationauthority.com etc. Based on the reputation score, a map is drawn showing the most prolific attackers, their reputation score and the targets they are attacking. Such a visual display empowers junior analysts to actively participate in cyber defense.