EventTracker
Secure. Comply. Succeed.

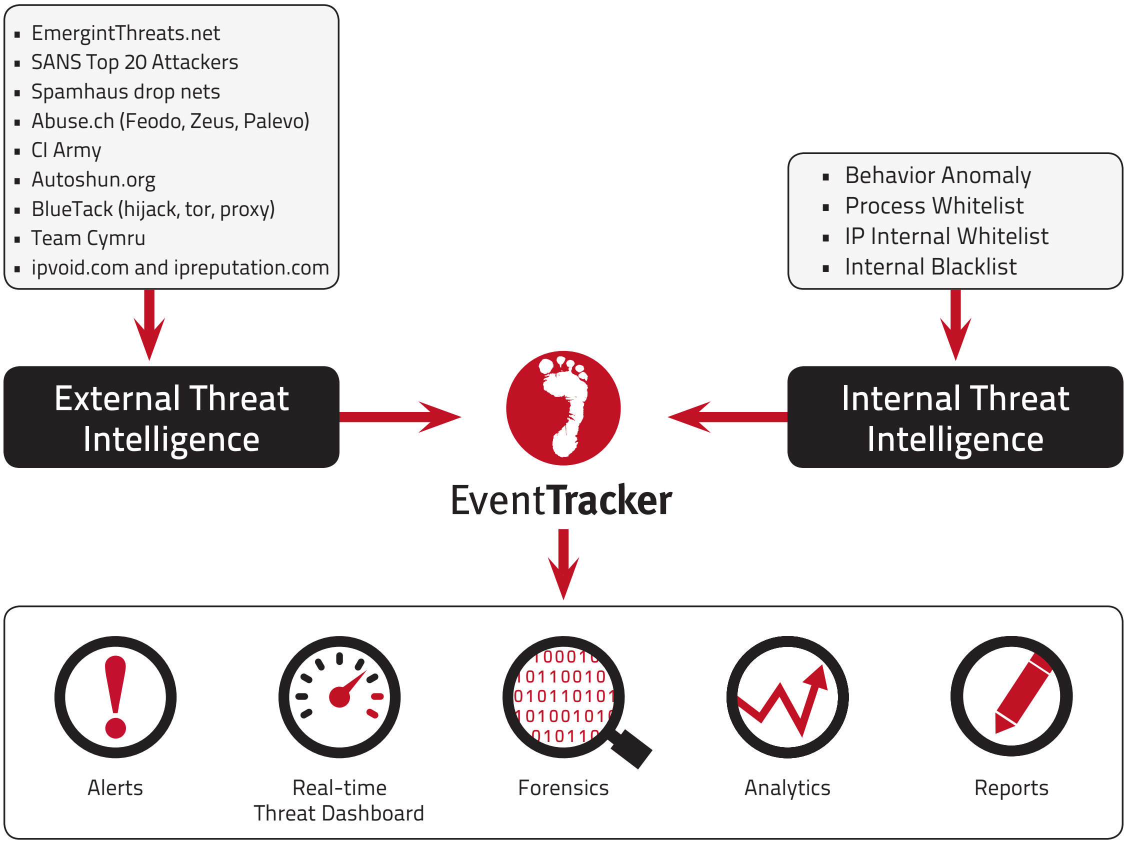
EventTracker Threat Intelligence Integration

Safeguarding the IT environment is an increasingly difficult challenge as cyber attackers become more sophisticated and prolonged in their efforts to steal valuable information. Traditional intrusion detection (IDS) is excellent at monitoring systems and networks for malicious activities or policy violations, but many of today's successful breaches exploit users through social engineering attacks by stealing their credentials. Then, operating as a "trusted" user, they access assets on a network to ex-filtrate sensitive or valuable data. IDS is rendered less effective during the initial exploit because of a lack of context.

Threat Intelligence is evidence-based information which has been acquired and analyzed to assess a malicious actor's possible capabilities and opportunities. The information is collected and disseminated by global sources, allowing organizations to determine if the threat poses a danger to their local assets. Threat intelligence can be used to inform decisions regarding the possible responses to a potential threat.

With **EventTracker Threat Intelligence Integration,** organizations can:

- Improve alerting by elevating the priority of rules that reference "bad" IPs or URLs as determined by current threat intelligence
- Be notified automatically if an external IP with a poor reputation communicates with assets behind your firewall
- Detect compromised systems that "phone home" from inside the network
- Review history of IPs and incidents based on collected threat intelligence data to provide context for previous events and alerts related to particular IPs
- Enable automatic or remedial actions with better information available from threat intelligence feeds



- EmergintThreats.net
- SANS Top 20 Attackers
- Spamhaus drop nets
- Abuse.ch (Feodo, Zeus, Palevo)
- CI Army
- Autoshun.org
- BlueTack (hijack, tor, proxy)
- Team Cymru
- ipvoid.com and ipreputation.com

- Behavior Anomaly
- Process Whitelist
- IP Internal Whitelist
- Internal Blacklist

External Threat Intelligence

Internal Threat Intelligence

EventTracker

EventTracker will automatically import open-source and paid threat intelligence/information. Feeds are available from industry groups, volunteers, vendors that specialize in threat intelligence, U.S. government agencies, and other sources. EventTracker supported external threat intelligence sources include EmergingThreats.net, Spamhaus and IPReputation.com, IPvoid.com, abuse.ch, and SANS Dshield among many others.

Internal sources of relevant intelligence are easier to maintain, and provide another valuable layer of threat intelligence integration and monitoring. Also known as white listing, internal intelligence includes a catalog of what is known and acceptable to the enterprise, and is readily available and easy to include in your EventTracker Threat Intelligence Integration. EventTracker will automatically generate, aggregate, and manage your internal and external intelligence feeds.

Tactical Threat Intelligence

EventTracker Threat Intelligence Integration provides information about organized cyber-security risks such as those posed by state-sponsored attacks, or hacking collectives, whose preferred breaching methods include APTs, and a more methodic and less visible backdoor attack, or by internal threats who use their access to your network to cause damage. Our Process Whitelist provides protection against .exe files that fall outside the accepted list of "safe" or "whitelisted" .exe programs. When a bad actor attempts to launch an .exe file that doesn't match the processes identified in this bounded, finite list, the process is terminated and an alert is sent.

Global Resources, Local Action

EventTracker Threat Intelligence Integration collates up-to-date information about top attackers, spammers, poisoned URLs, and malware domains are available through open source lists such as SANS DShield, U.S. government maintained lists such as InfraGuard, and through paid services. These lists include:

- Known command and control hosts
- Attack response rules – data that systems on your network are likely to send back to a host after they have been compromised
- Compromised hosts
- Systems of known spammers
- Exploit rules for detecting things like Windows exploits, SQL injection, etc.
- User-Agent strings for known malware
- Web server attack detection rules

The intelligence is analyzed and provides a detailed, global resource of useful data that can be enacted locally. When a known bad actor, or a malware is reported globally, EventTracker Threat Intelligence Integration can give you the data in real-time, enabling you to address the risk and perform necessary patch and software updates.

With EventTracker Threat Intelligence Integration, you have a relevant, ongoing feed for vulnerability, emerging threats, malware and other cyber security issues, allowing you to focus on operations and neutralize potential malicious activity as soon as it becomes visible.