EventTracker
Actionable Security Intelligence

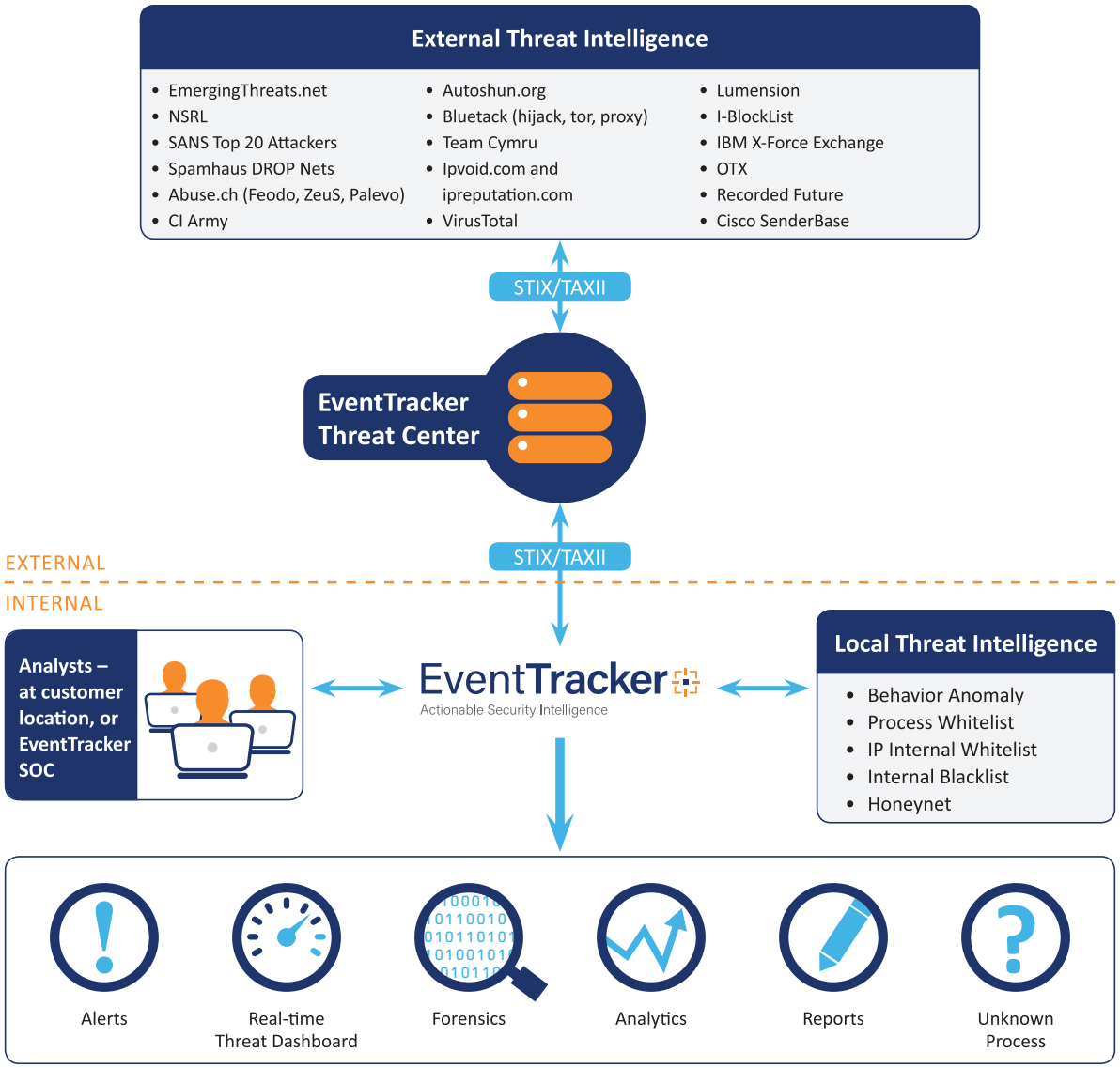
EventTracker Threat Center

A central repository of indicators of compromise

The EventTracker Threat Center is an integration platform for commercial and open source threat feeds. By integrating the valuable threat data provided by ecosystem partners and open source providers with the machine data collected from throughout the enterprise, EventTracker enables quick and accurate threat detection and response.

Threats are dynamic and attack vectors change constantly. Respond quickly and minimize damage by using the rich external context enabled by threat intelligence. Immediately know about dangerous IP addresses, files, processes, and other risks in your environment.

EventTracker easily incorporates threat intelligence from STIX/TAXII-compliant providers, commercial and open source feeds, and internal honeypots, all via an integrated threat intelligence ecosystem. This threat intelligence includes data, such as low-reputation IP addresses and URLs, nefarious email addresses, file names, processes and user agent strings. The platform uses this data to reduce false-positives, detect hidden threats and prioritize your most concerning alarms. Customers can easily select which feeds to integrate from within the EventTracker Console.



EventTracker | 8815 Centre Park Drive, Columbia MD 21045

www.eventtracker.com

EventTracker
Actionable Security Intelligence

Global threat feeds, while highly valuable, are often noisy and the information they provide may not be relevant to the network. Local or community information when overlaid across global feed data provides superior and targeted coverage. EventTracker's Threat Center, combines that data with data from internal sources. This includes data from the network and includes:

- Behavior anomalies
- Process whitelists
- IP Internal whitelists
- Internal blacklists
- Honeynets
- Contributions from our EventTracker analysts, as well as analysts at customer sites

With **EventTracker's Threat Intelligence,** organizations can:

- Improve alerting by elevating the priority of rules that reference "bad" IPs or URLs 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 a 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

How it Works

EventTracker will automatically import up-to-date information about top attackers, spammers, poisoned URLs and malware domains from open-source and paid threat intelligence/information. Feeds are available from industry groups, vendors that specialize in threat intelligence, U.S. government agencies, volunteers and other sources. EventTracker supports external threat intelligence from sources including EmergingThreats.net, Spamhaus, IPReputation.com, IPVoid.com, the NSRL and SANS, among many others. These lists of information can 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

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.

We exchange threat intelligence information via STIX/TAXII, which will also enable us to share with others outside of our community in the future.

About EventTracker EventTracker delivers business critical solutions that transform high-volume cryptic log data into actionable, prioritized intelligence that will fundamentally change your perception of the utility, value and organizational potential inherent in log files. Our leading solutions offer Security Information and Event Management (SIEM), real-time Log Management, and powerful Change and Configuration Management to optimize IT operations, detect and deter costly security breaches, and comply with multiple regulatory mandates.

EventTracker | 8815 Centre Park Drive, Columbia MD 21045
www.eventtracker.com