

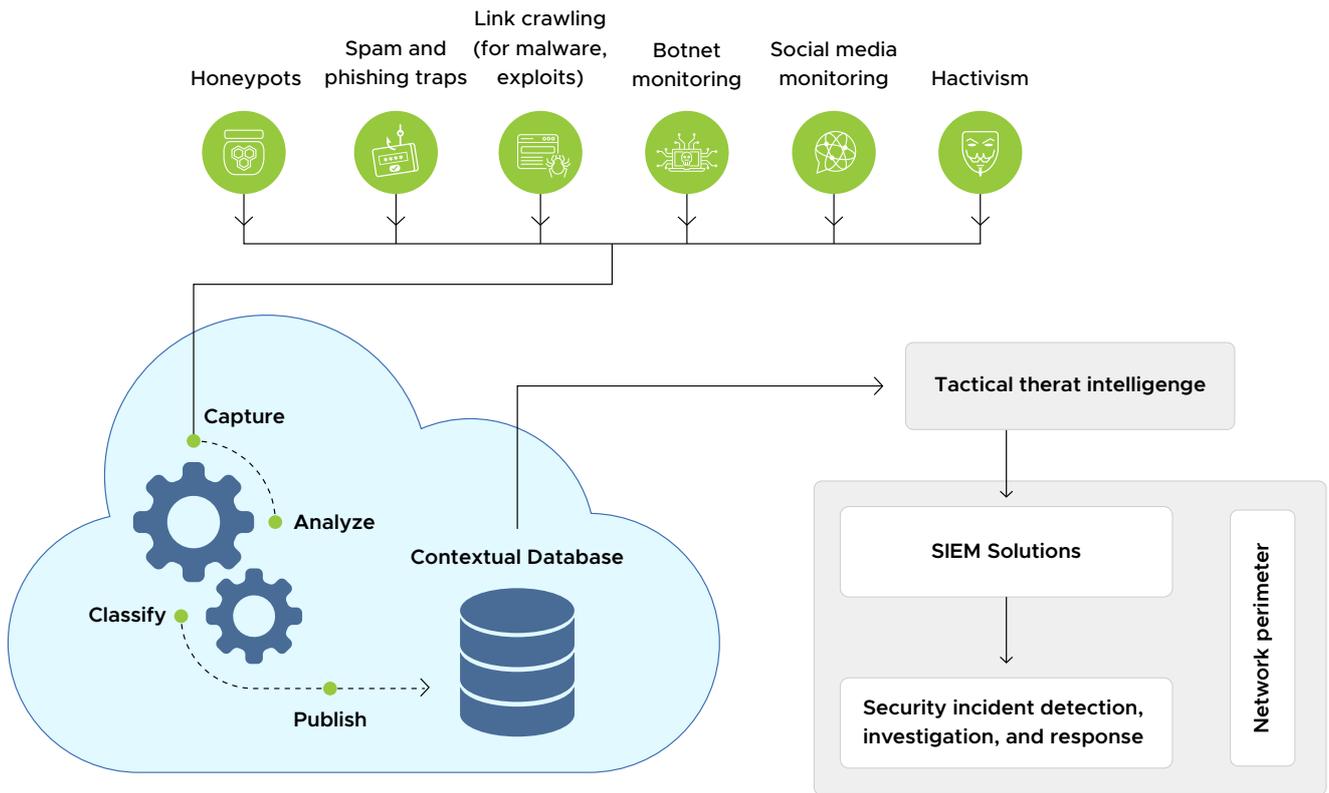
DATASHEET

Advanced threat analytics in ManageEngine Log360

How do you defend yourself against threats you don't know about? According to AV-TEST, an independent security research institute, around 350,000 malware instances are created each day. To combat these, having access to a reliable database of malicious domains detected across the globe is vital. This can help you figure out if a suspicious source that's intruding in your network is known to be malicious.

Log360, ManageEngine's SIEM solution, comes with built-in threat intelligence capabilities to detect malicious domains, IPs, and URLs intruding in a network. These suspicious sources are flagged by correlating data from external threat feeds. In addition, Log360 can assess the seriousness of the threat, get the geolocation, intercept an attack, and more.

How threat feeds compile data



Product features

Reputation-based scoring

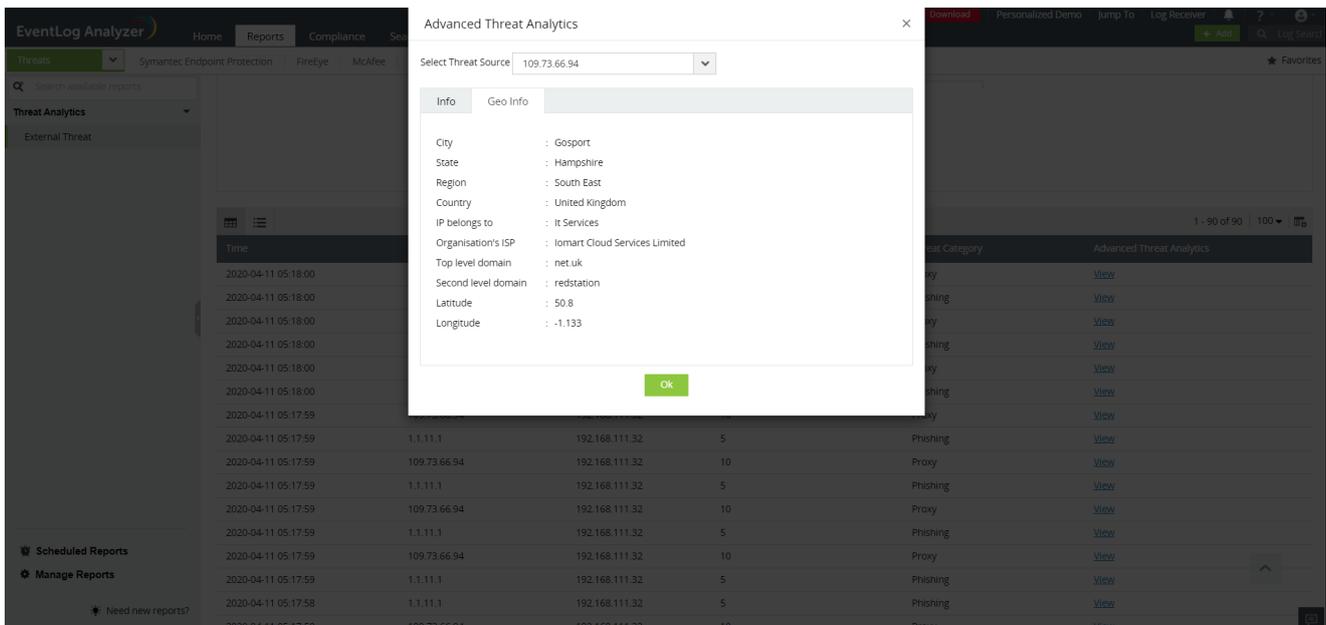
The screenshot shows the 'Advanced Threat Analytics' window in EventLog Analyzer. The window displays the IP address 109.73.66.94 with a 'High Risk' status and a 'Reputation Score = 7' on a scale from 0 to 100. The window also shows the following information:

- Domain name: 109.73.66.94
- Domain age: 24
- Flagged as malicious on: 2015-11-19 23:32:00
- Last occurrence on threat list: 2019-08-18 12:31:41
- No. of times it occurred on threat list: 3
- Category: Proxy

A message at the bottom of the window states: 'This source has been whitelisted. [Click Here](#) to remove from whitelisted source.' The background shows a table of threat data with columns for Time, IP, and Category.

If you have multiple suspicious domains, which ones pose the greatest risk? This is something reputation-based scoring can help you figure out. If a domain or URL has no recorded history of malicious activity, the reputation score will be high. On the other hand, if the source has been flagged for malicious behavior or is associated with suspicious domains, the reputation score will be low. This information can be useful in setting firewall policies to determine what domains will be allowed or blocked in a network.

Geolocation for threats



The screenshot displays the Log360 Advanced Threat Analytics interface. A modal window titled "Advanced Threat Analytics" is open, showing geolocation information for a selected threat source (IP: 109.73.66.94). The "Geo Info" tab is active, displaying the following details:

- City : Gosport
- State : Hampshire
- Region : South East
- Country : United Kingdom
- IP belongs to : It Services
- Organisation's ISP : Iomart Cloud Services Limited
- Top level domain : net.uk
- Second level domain : redstation
- Latitude : 50.8
- Longitude : -1.133

The background interface shows a list of threat events with columns for Time, IP, and Category. The "Category" column lists various threat types such as Phishing and Proxy.

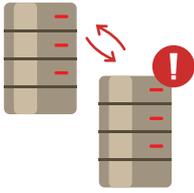
When a network is under attack, every bit of information to determine from where the malicious source originated can be crucial. With the Log360's Advanced Threat Analytics module, information on the location of the domain, the ISP of the organization that owns the domain, and more will be displayed.

Intercepting callback servers



In many advanced attacks, when a system gets infected, it often comes under the control of an external server, also known as a callback or command-and-control server. Since Log360 constantly scans outgoing connections, this communication with a suspicious source can be intercepted and flagged with advanced threat intelligence. Once an attack is discovered, aside from getting an alert, you can automate the appropriate response using workflows.

Malware detection



Sophisticated malware can sometimes evade signature-based antivirus software. In cases like these, their point of origin could raise red flags even if the file appears innocuous. For instance, if software downloaded from a source with a low reputation proceeds to make critical changes in a system, the chances are that it's an attack. If this sequence of events is detected, an alert will be raised and the appropriate mitigating action can be automated as well.

By combining the wealth of information from the collected logs and the database of global threat feeds, Log360 helps you take preemptive action against network threats. Aside from advanced threat intelligence, Log360 can also help mitigate attacks by automating your incident response with easy-to-build workflows. Download the solution to see it in action. If you need help, you can schedule a demo with one of our product experts. We're more than happy to help.

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities. For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

ManageEngine
Log360

\$ Get Quote

↓ Download