Threat analytics solution

[Comprehensive protection for detecting and mitigating sophisticated cyber threats]

Today's security solutions are necessary but not sufficient

In recent years, as the threat from cyber attacks has grown, many businesses have come to realize that the security solutions they have in place are necessary, but no longer sufficient. Their security infrastructures provide good defense against generic or known cyber attacks, but what about customized, multi-faceted targeted attacks? These attacks are routinely circumventing existing security defenses and there is a growing concern amongst businesses that it is this undetected cyber activity that could do the most damage to their organizations. The longer it remains unnoticed, the worse the financial damage and loss of sensitive data will be.

For some businesses, the subsequent need to ensure that their business operations and the data under their control is fully protected, coupled with the need to avoid any reputational loss or expensive breach notification costs, now mandates that they require additional security solutions to complement their existing security infrastructures. The threat analytics solution from BAE Systems has been designed to fulfill this need. Leveraging our rich heritage in data analytics and drawing upon our extensive experience gained in providing cyber protection to governments and businesses worldwide, we have built an enterprise threat analytics platform that uses a combination of threat intelligence and complex behavioral analytics to detect the unknown threats that your current security solutions cannot.

A solution to address today's outstanding security challenges

Our threat analytics solution helps businesses detect the most sophisticated cyber threats. To do this it recognizes and addresses the challenges faced by most security managers and analysts today:

Threat: New cyber threats may go undetected by products that only recognize previously encountered attacks.

Threat Intelligence: Threat intelligence can be helpful, but sifting through it all and making it actionable is a huge challenge for organizations. Plus, it doesn't help catch true 'zero day' attacks.

Efficiency and Decision Making: Analysts and current tools are too often overwhelmed by security alert data. The contextual information needed to assess alerts is also often distributed across several toolsets: by bringing this all into a central platform analysts would be able to triage and process more alerts, faster, enabling them to focus on the alerts that matter most, and leading to greater protection from the threats that could impact their business.

Investigation: Security analysts need greater capability to triage and investigate alerts and to more quickly query, visualize and derive connections between data points, in order to determine those which are indicative of new or evolving cyber threats.

Platform/Storage: All significant network metadata and data must be collected and stored and the architecture of the analytics platform must enable rapid data querying, retrieval and analysis. The ultimate challenge is to enable 'speed-of-thought' investigation where analysts are able to manipulate data and pursue thought processes in real time. This presents several key challenges: Cost/Processing Power/Architecture.

Effective solution integration

Our integrated solution addresses these challenges to enable the effective detection, analysis and investigation of insider threats and sophisticated targeted attacks. The solution comprises:

Threat Analytics Platform and Threat Detection Engine

- Using advanced behavioral analytics to analyse data on a massive scale, we are able to detect and generate customizable alerts on anomalous network activity which is indicative of both known and new and evolving threats.

Additional Integrated Bundled Modules:

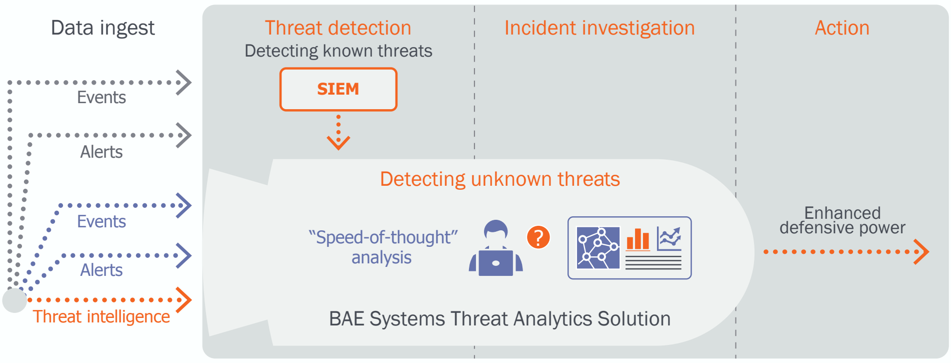
- Threat Intelligence Management – We facilitate the ingesting and management of multiple threat intelligence sources, enabling you to quickly transform threat intelligence into actions which enhance your cyber defense.
- Analyst Investigation Solution – We enable analysts to triage, investigate and manage large volumes of alerts under a single pane of glass, before recording their work in a ticket management system and sharing their conclusions with peers.

Features

- As threats evolve, new analytic algorithms can be added to detect them which provides a future-proof platform for the detection of sophisticated, targeted cyber threats.
- Provides security analysts with a single view of network activity across the whole IT estate.
- Detects attackers by their behaviour and activity patterns, not just by the signatures of previously encountered attacks.
- Prioritizes suspicious activity and enriches security alerts with business, open-source and third-party data to power our Advanced Threat Detection managed security service.

Benefits

- Threat: Finds the most sophisticated, targeted threats and can be extended to monitor any threat.
- Efficiency: Significantly improves analyst productivity and drives more value from existing security monitoring systems.
- Scale: Scales to any organization, affordably.
- Decision making: Allows security analysts to make informed decisions, fast.
- Control: Gives analysts greater control over alert generation in response to threat detection.



Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

BAE Systems, 265 Franklin Street, Boston, MA 02110, USA
T: +1 (617) 737 4170
E: learn@baesystems.com | W: baesystems.com/businessdefense

linkedin.com/company/baesystemsai
twitter.com/baesystems_ai

CREST
CESG Certified Service
Cyber Incident Response
CPNI Centre for the Protection of National Infrastructure