Threat *intelligence* management

Convert threat intelligence into defensive power

The need for effective operationalized threat intelligence

All the security defenses in the world will not prevent a determined, knowledgeable and well-resourced attacker from compromising your organizations. To focus resources and build more effective defenses, you need to be better informed about the threats you face. However, a regular supply of threat information is not enough to improve company defenses: you must dedicate resources to understanding, analyzing and relating it to your organization and to the processes and assets that you are trying to protect. Further action must then be taken to transform it into defensive power that can protect your business from new and evolving threats. Without this last step, your network defense will not be improved and your exposure to the cyber threat remains the same.

Getting threat intelligence does not protect you: it's what you do with it once you have it that really counts.

Fast track to informed cyber defense

Our threat intelligence management solution is designed to help:

- process threat information and turn it into relevant intelligence upon which analysts can take action

- help analysts by making their jobs easier and more efficient, and helping them to interact more effectively with other teams who will implement security protection.

To streamline the process of turning threat information into informed defense, our platform implements a workflow that provides automation of repeatable processes, whilst supporting rapid real-time analysis by experienced human operators.

Convert threat intelligence into defensive power

Acquire   Process   Store   Analyze   Action

The solution enables analysts to distill threat intelligence and quickly action it to improve your defense. Using this solution, when new threat information is received by your organization, we will help you reduce the time it takes to:

- store, triage and process the data

- analyse the data and transform it into threat intelligence

- generate threat reports and new threat signatures

- share these with security managers who can then conduct sensor enrichment to protect your business from new and evolving threats.

On premise, within your control

Our solution is immediately available without the headache, start-up costs, and planning commonly associated with trying to build a solution in-house. Management is simple. Delivered on-premise, it is straightforward to adapt the solution to fit within your current business processes and richly integrate into your organization, enabling your analysts to be as efficient and as well informed as possible.

Features and benefits

Our advanced threat intelligence management solution provides the following key functionality and benefits as listed in the table on the right. A full list of features is available on request.

Summary

To learn more about the advanced threat intelligence management solution and to fast track your way to a more effective, informed cyber defense, please contact your local BAE Systems representative or visit us at www.baesystems.com/threatintel

Features	Benefits
Central intelligence repository	Product provides a real-time single view of intelligence for multiple users
Automated ingest	Reduced friction for adding information to the central repository. Easy integration with existing threat information sources, including via email, API, folder or user upload
Signature export	Indicators that have been identified and associated with a potential threat can be quickly harnessed to protect your network
Ad-hoc search	Easy access to all corporate threat knowledge
External/internal context	Provides related information from external/internal sources that can influence the assessment of the report, enabling analysts to block the associated IP addresses as well as the host names referenced in the threat intelligence
Related documents	Helps users to understand each piece of threat information in the context of other related information
Ticketing integration	Rapidly create tickets for ongoing incidents or attach threat intelligence to existing incident tickets

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

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

CREST

CESG Certified Service

CPNI Centre for the Protection of National Infrastructure

Cyber Incident Response