LOGPOINT

THREAT INTELLIGENCE

Is the capacity to identify the signs of compromise in an infrastructure on which the organization must act.

Enterprise Log-Data is valuable when analysed in and by itself

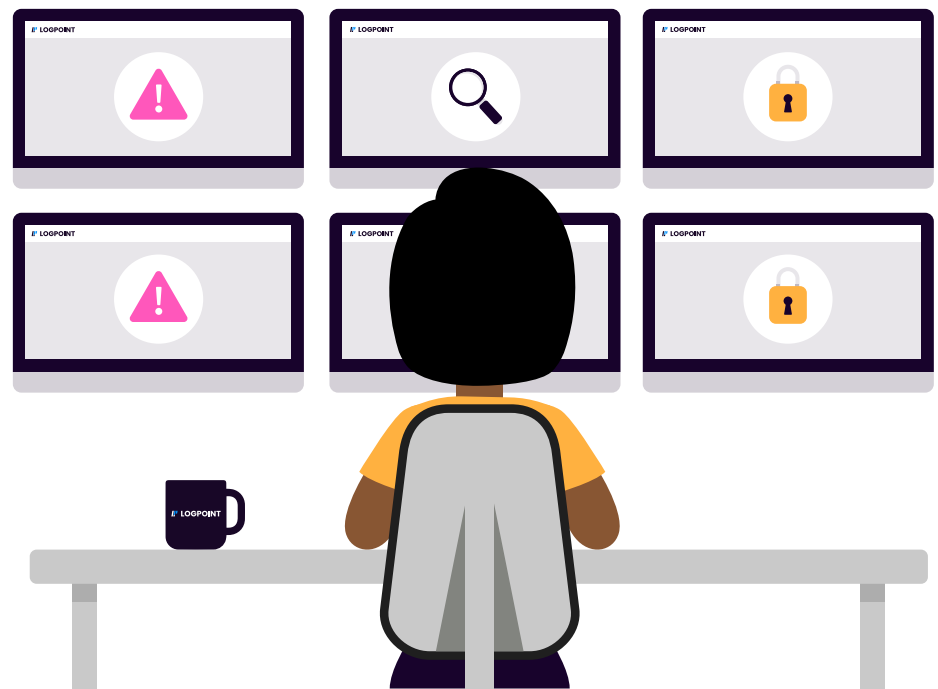
Thanks to the analysis of events generated in the network and by the footprints they leave, fraud, external attacks and errors can be discovered.

By correlating your internal data with indicators of compromise, seemingly innocent data can hint at a potential issue. With pre-canned analytics in the form of alert-rules, dashboards and data mappings running out of the box, the Logpoint Threat Intelligence application is a turn-key application.

The Threat Intelligence application sources data from best-in-class ProofPoint and the large collection of indicators from Critical Stack. With these sources ingested, Logpoint can analyze structured and unstructured data, alerting if any match between the known-bad indicators and collected enterprise data is identified.

Logs: Essential for correlation and investigation

In order to facilitate the detection of abnormal activity, logs in the infrastructure must be analyzed. Having logs for correlation and investigation is fundamental for every organization. These logs supply data on everything that happens in a network, whether it is tight knit or spread out; on workstations, servers and applications.



Like Finding A Needle In A Haystack

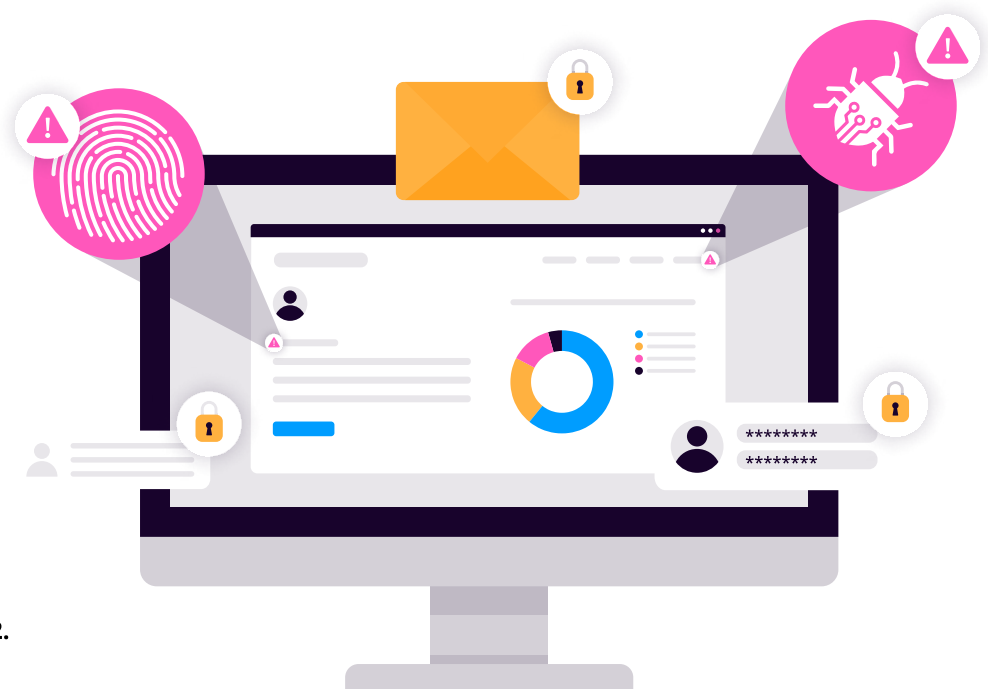
The sorting of collected information is like finding a needle in a haystack.

- Which of these records are the important ones?
- How do you figure out if something that seems to be working normally is in fact a malicious activity or the clue that an attack is taking place?

Fundamental aspect of Cyber Security

Obtaining the analysis of useful information that allow the countering of diverse threats is always a more complex challenge, taking into account the permanent evolution of risk and methods of attack. That is why Threat Intelligence is an aspect of cyber security that no one in charge of a network can afford to ignore or leave aside.

Its role in network defence is proven, and the threat data collected has an indisputable value for organisations. In effect, they provide decision-makers a reliable basis to help confirm the benefits and consequences of their decisions.



Logpoint is EAL3+ certified

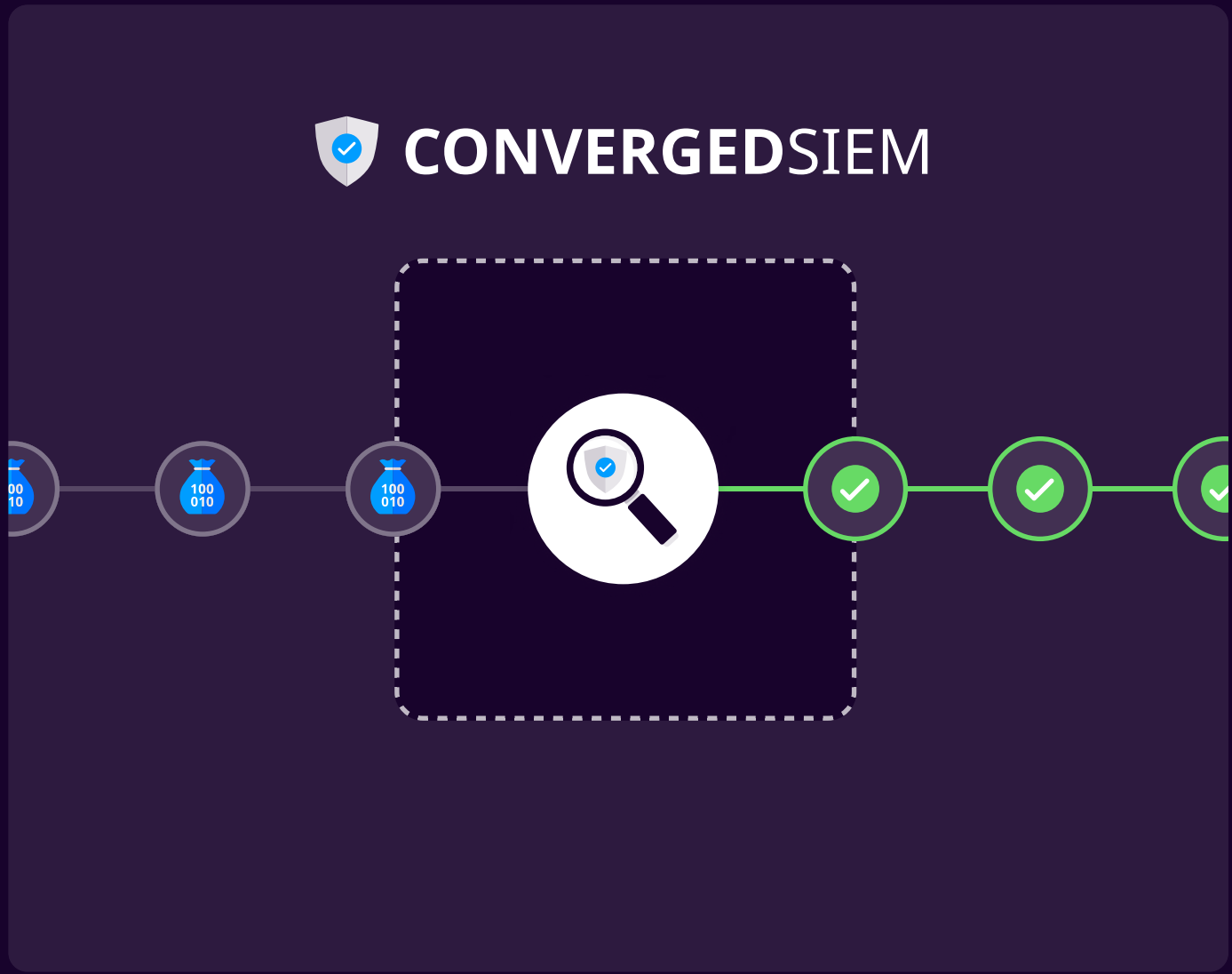
The EAL3+ certification indicates that the Logpoint solution has been examined, checked and documented according to the Common Criteria standard (www.commoncriteriaportal.org) and also according to ISO/IEC IS 15408.

Use-Case Example

A group of hackers is using a new method to attack the most widespread electronic messaging system in the world. This type of attack has never been used before and no safety measure to combat the situation is in place. Anti-virus, firewall and IDS systems are blind and don't recognize the attack.

Through the use of SIEM, these attacks are captured, analyzed and their methodology identified. This methodology is described in a common language and distributed to other SIEMs or incident management platforms. This description can then be transmitted automatically and used to detect the faintest signs of the attack when it occurs.

Thanks to Threat Intelligence, the attacks have been captured, described and shared throughout the team – at the same time taking into account the context that is essential to monitor the evolution of attacks from day to day.



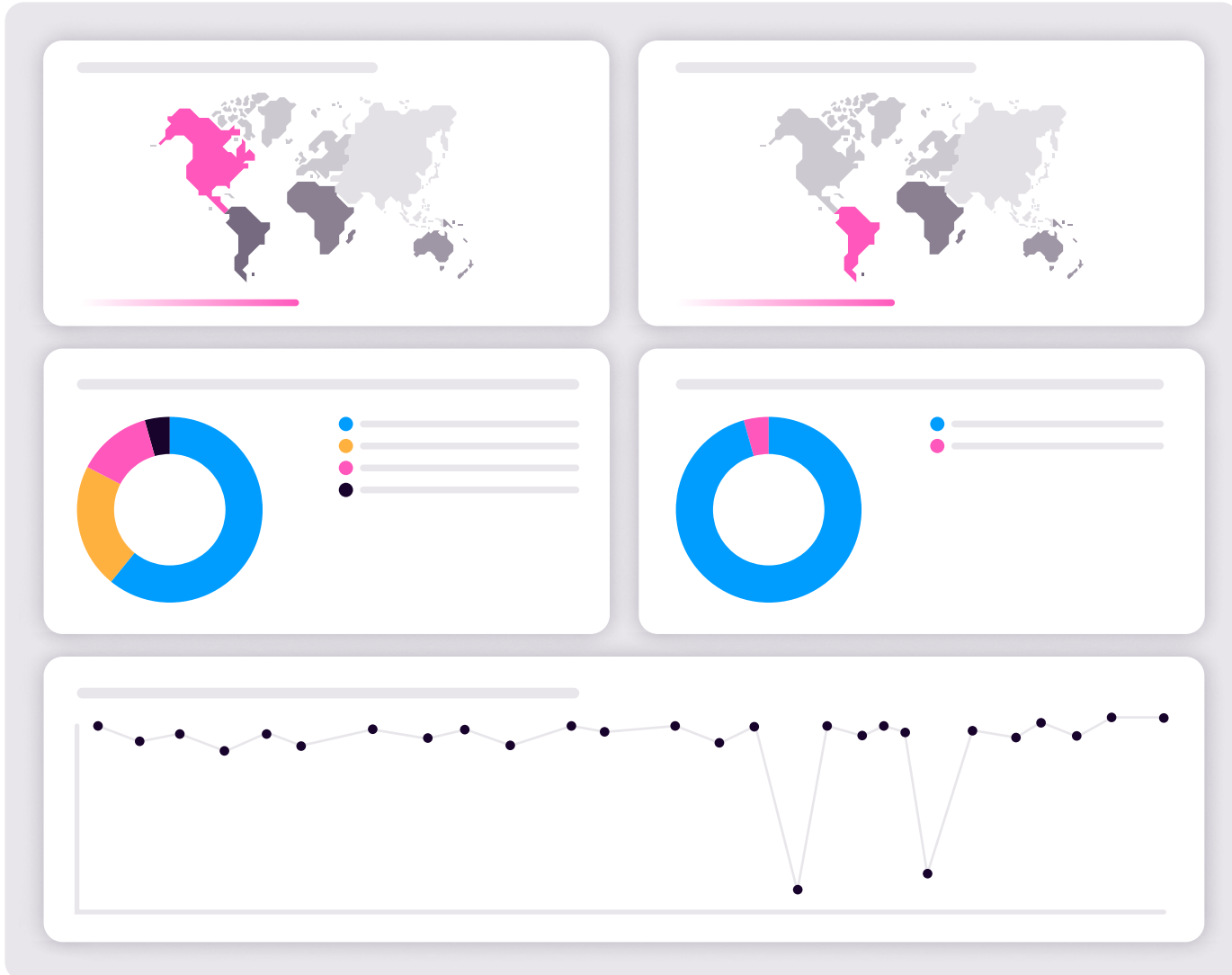
Getting Started With Threat Intelligence

With this application, Logpoint offers a simple and efficient module for providing contextual attack information to observations from sensor data in your network

Logpoint allows the integration of more than 100 data sources on threats, relying on Critical Stack or ProofPoint among others. Everything is normalized in a common language. Starting from this, analysts can automate event interrogation, screening hundreds of thousands of indications of compromise to evaluate the data based on known attacks. The effectiveness of skills an organisation possesses to protect the infrastructure, must rely on a knowledge of the characteristics or techniques threats employ, so as to identify and collect data on that attack methodology or other proof aof compromise.

With Logpoint, the sharing of this information can be at top speed, almost in real time.

As a Logpoint customer, the Threat Intelligence application is included in your existing license and downloadable directly from our Help Center.



About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers Converged SIEM: an end-to-end security platform that combines SIEM, SOAR, threat intelligence, UEVBA and EDR capabilities. Logpoint Converged SIEM accelerates threat detection, investigation and response while minimizes false positives and autonomously prioritizes risks to improve SOC team's efficiency.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information, visit logpoint.com

LOGPOINT.COM