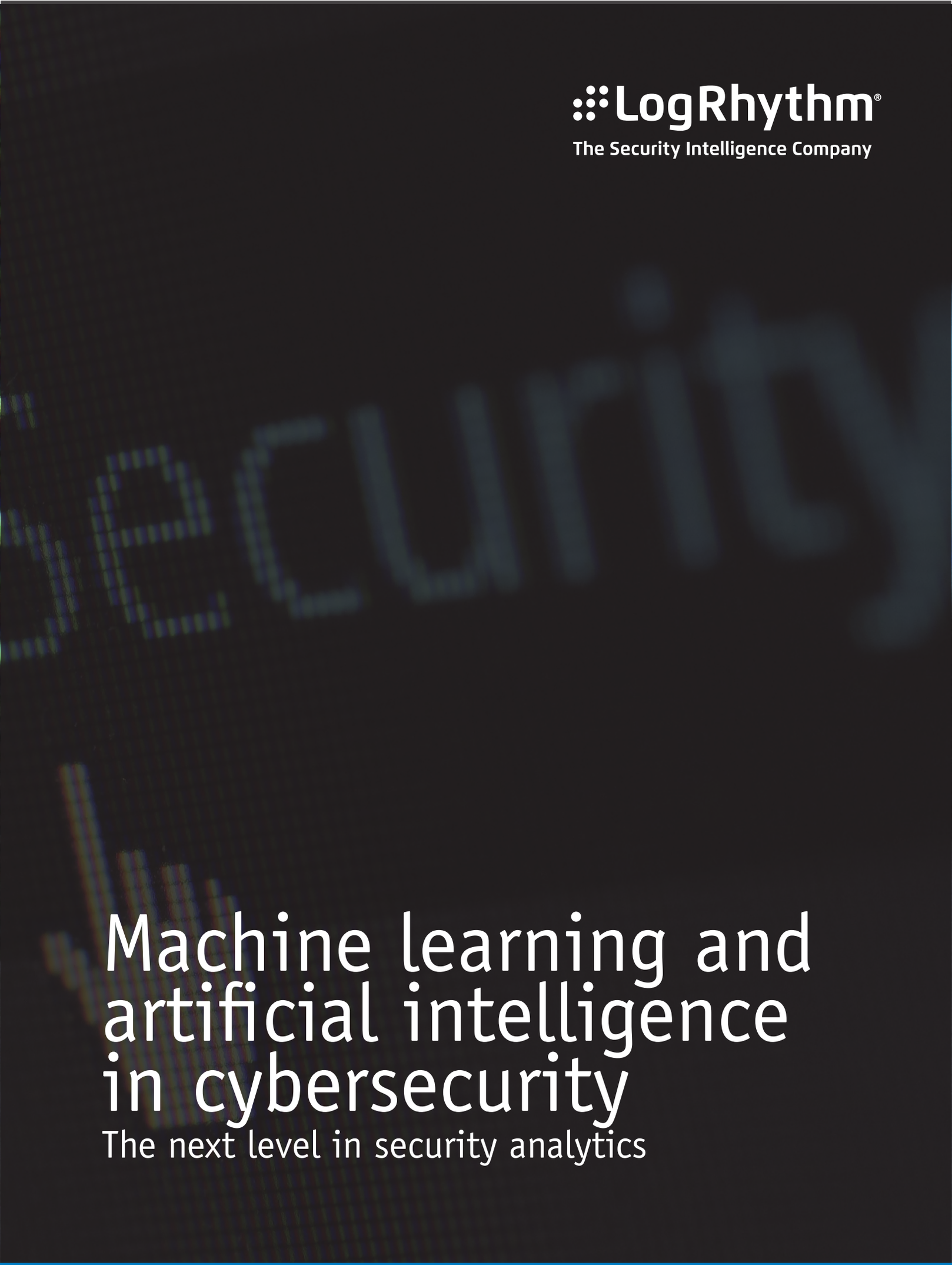
LogRhythm®
The Security Intelligence Company



Machine learning and artificial intelligence in cybersecurity

The next level in security analytics

LogRhythm
The Security Intelligence Company

Next-generation threats need next-generation solutions

One of the most common problems for enterprise security teams is how to respond effectively to the sheer volume of alarms they face every day. With so much noise, it can be hard for personnel to filter out false positives and find the real dangers to company systems, as well as the root problems underlying them.

It's a problem that's exacerbated by the difficulty and expense of dealing with skills shortages and overworked staff.

The role of artificial intelligence

Artificial Intelligence (AI) can help solve these challenges. By offering real-time analytics for threat detection and prevention using algorithms and statistical rules around normal behaviour, AI can help automate security processes.

While often used interchangeably, machine learning and AI are different technologies that are used in different ways.

Machine learning allows security systems to be taught context; once they have that context, AI allows them to use log data, user behaviour and data flows to create a 'whitelist' of normal behaviour unique to each organisation. The AI can then react instantly to any behaviour, by a machine or by a user, that strays too far from the company's norms.

AI can help detect and prevent threats in other ways, too. Sophisticated malware attacks can often sit for months within a company's systems before being activated. Using AI to spot the attack before it becomes a problem can spare the organisation many hours of work restoring systems and mitigating the damage after the event.

Artificial intelligence can also help prevent attacks from known sources or those with recognised software signatures, acting autonomously to isolate systems or users that have been compromised or begin behaving in a suspicious way. The organisation can choose whether the system takes action entirely on its own or it can set alerts for staff to approve or investigate further.

By logging events and creating algorithms around standard user behaviour, LogRhythm's AI Engine can generate templates that customers can use to build their own bespoke defences. LogRhythm's SmartResponse™ plug-in also allows actions to be taken once threats have been identified, such as allowing a compromised system to be automatically isolated.

It's predicted that there will be 350,000 more cybersecurity jobs than skilled workers by 2020[1]

LogRhythm
The Security Intelligence Company

The future of artificial intelligence

The next stage for AI security will be a shift to the cloud. Hosted systems will offer more scalability – unlike on-premise systems that can quickly become overloaded when searching for suspect behaviour further back into logs, cloud-based systems will be able to inspect a data lake and quickly provide results.

Using the cloud will also hugely increase the data available to AI systems and accelerate their learning rates. It will allow the creation of peer-based profiling – instead of looking at typical behaviour within an organisation, AI will be able to compare an organisation with its regional peers, such as similar companies or even people performing comparable jobs in other industries. With the wealth of information available, AI systems will help companies create better, more effective detection rules customised to their organisation and industry.

And, as AI's capabilities build, it will increasingly free up security analysts to focus on other priorities, including staying ahead of the curve on attacks, monitoring new and emerging hacker groups, and keeping their skills and knowledge up to date.

UK businesses deal with over 5,000 security incidents every year[2]

What's normal for your organisation?

Security systems can easily find anomalous behaviour on a network but every organisation is different. What's suspicious for one organisation may be the standard order of business for another.

That's where AI really proves its worth: artificial intelligence can learn to recognise the unique way that users, hosts, applications and devices behave on an organisation's network, and so flag up when any activity is outside what would be expected.

By combining AI with pattern recognition software and whitelisting, AI can help detect security incidents without creating unnecessary false positive or negatives.

How can you use AI for security? One solution is **LogRhythm AI Engine**, which delivers real-time visibility to risks, threats and critical operations issues.

In the longer term, AI will allow security teams to take a more strategic and proactive approach to cybersecurity instead of just reacting to the latest attack.

LogRhythm
The Security Intelligence Company

As threats grow more sophisticated it is becoming ever more important for security teams to have their time and skills move away from reacting to the last attack, and instead look forward, taking steps to defend against the next threat on the horizon.

At LogRhythm, our mission is to help organisations detect, respond to, and neutralise threats using the best technology tools available.

To find out more about how AI and machine learning can help improve your security profile, contact us.

About LogRhythm

LogRhythm is the pioneer in Threat Lifecycle Management™ (TLM) technology, empowering organisations on six continents to rapidly detect, respond to and neutralise damaging cyberthreats. LogRhythm's TLM platform unifies leading-edge data lake technology, artificial intelligence, security analytics and security automation and orchestration in a single end-to-end solution. LogRhythm serves as the foundation for the AI-enabled security operations centre, helping customers secure their cloud, physical and virtual infrastructures for both IT and OT environments. Among other accolades, LogRhythm is positioned as a Leader in Gartner's SIEM Magic Quadrant.

www.logrhythm.com

[1] 2017 Global Information Security Workforce Study: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf
[2] PwC Global State of Information Security Survey 2017: https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/global-state-of-information-security-survey-2017.html

01628 918300 | europe@logrhythm.com | www.logrhythm.com