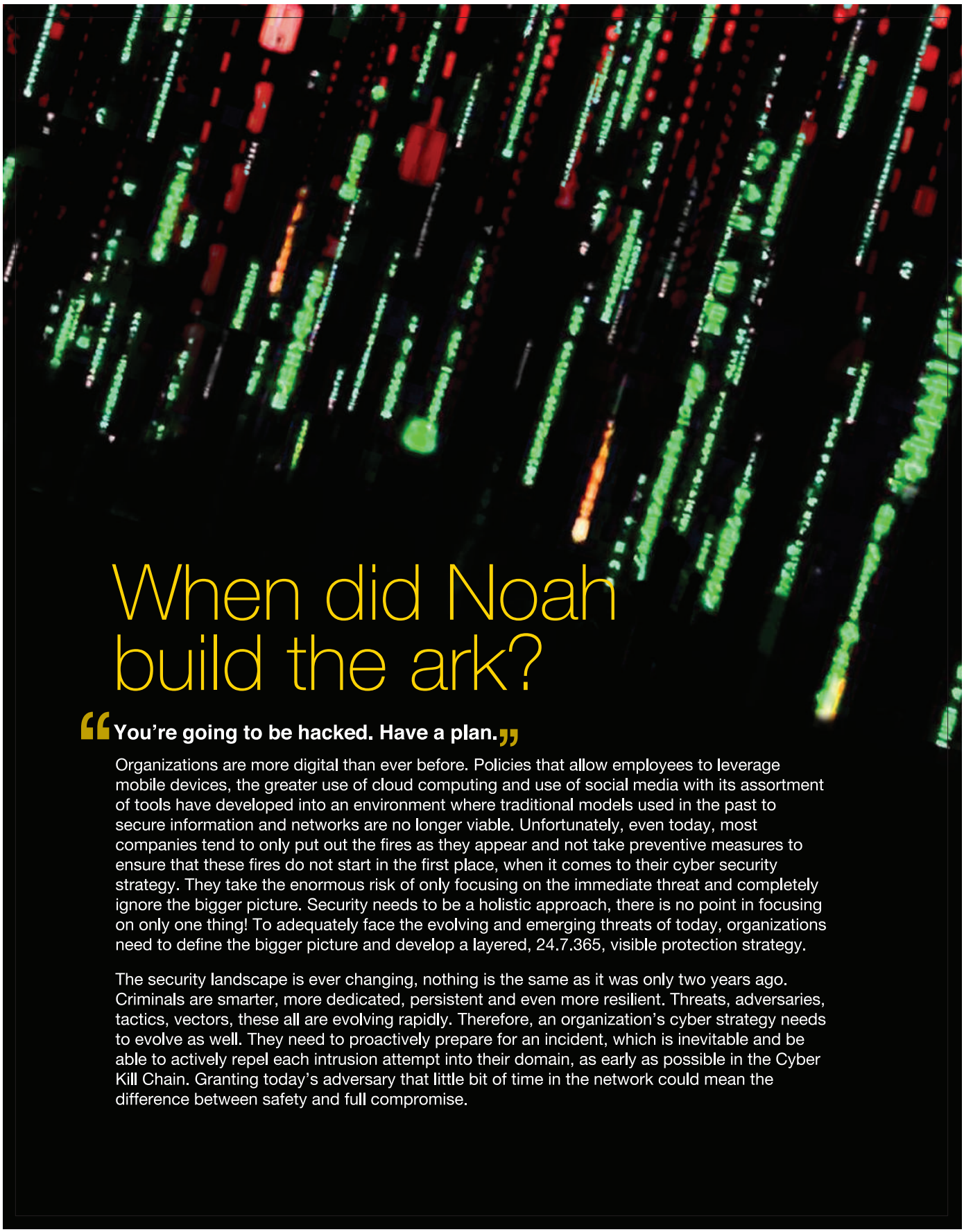


When did Noah build the ark?

“You’re going to be hacked. Have a plan.”

Organizations are more digital than ever before. Policies that allow employees to leverage mobile devices, the greater use of cloud computing and use of social media with its assortment of tools have developed into an environment where traditional models used in the past to secure information and networks are no longer viable. Unfortunately, even today, most companies tend to only put out the fires as they appear and not take preventive measures to ensure that these fires do not start in the first place, when it comes to their cyber security strategy. They take the enormous risk of only focusing on the immediate threat and completely ignore the bigger picture. Security needs to be a holistic approach, there is no point in focusing on only one thing! To adequately face the evolving and emerging threats of today, organizations need to define the bigger picture and develop a layered, 24.7.365, visible protection strategy.

The security landscape is ever changing, nothing is the same as it was only two years ago. Criminals are smarter, more dedicated, persistent and even more resilient. Threats, adversaries, tactics, vectors, these all are evolving rapidly. Therefore, an organization’s cyber strategy needs to evolve as well. They need to proactively prepare for an incident, which is inevitable and be able to actively repel each intrusion attempt into their domain, as early as possible in the Cyber Kill Chain. Granting today’s adversary that little bit of time in the network could mean the difference between safety and full compromise.

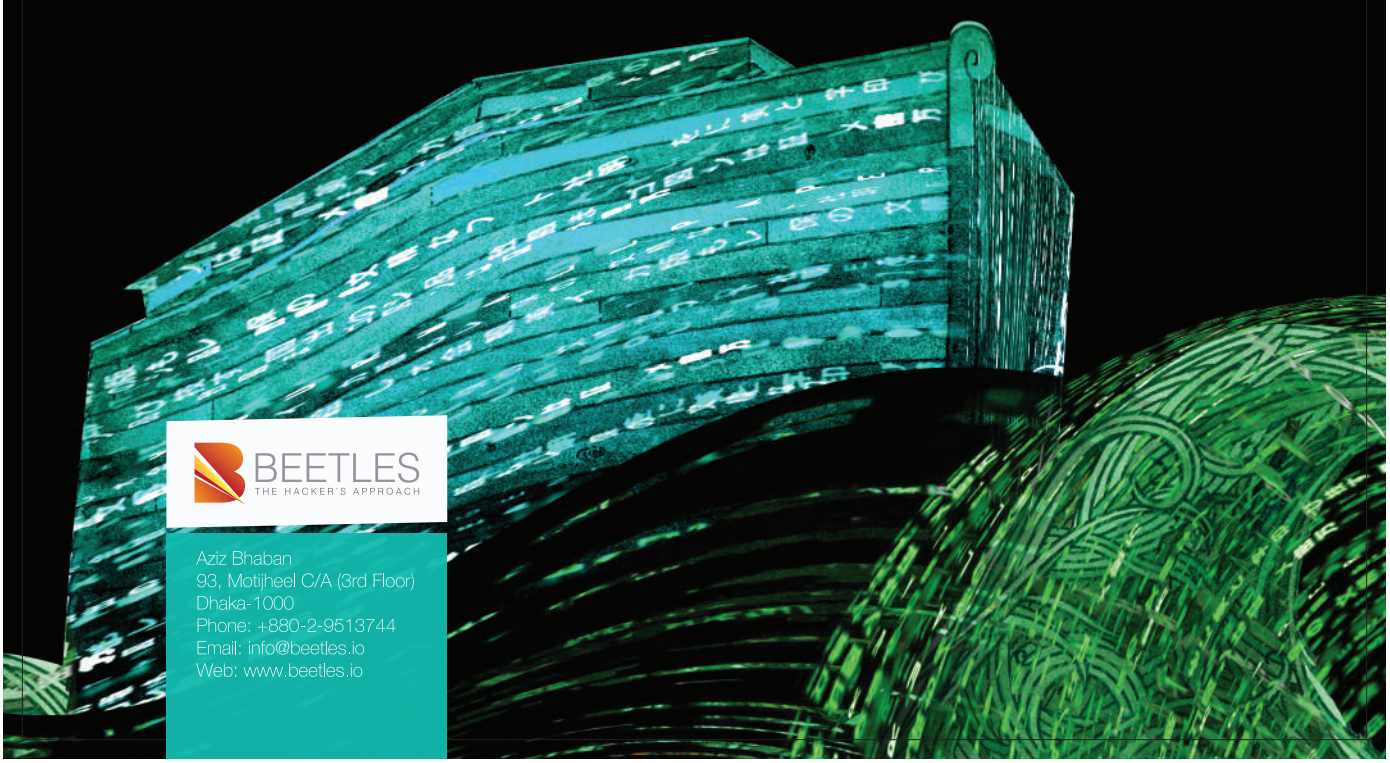
True security needs to be proactive, not reactive. Noah built the ark BEFORE the rains!

Threats can come from any direction, at any time. Not only do we need to be one step ahead and ready for the enemy outside, but we need to be prepared for the enemy within. As an organization, you need to know and understand who is accessing your data, why, from where and for how long.

A security operations center (SOC) is a centralized location for monitoring, detecting and responding to security issues and incidents that an organization may face. Whatever the size of the organization, it is always valuable to have a dedicated team whose job is to constantly monitor security operations and incidents and respond to any issues that may arise. By centralizing various sources of data into a singular security monitoring system, the SOC can gain actionable intelligence into possible anomalies that are indicative of threat activity. Based on these findings, automated and manual interventions can be made to respond to the event

You need a partner who can help you keep calm in the midst of an incident, who can help make sense of the chaos that ensues an attack attempt, a professional team with the experience and the capacity to help you process, understand, analyze and react to incidents that exceed the skill level and capacity of your internal staff.

The Beetles Security Operations Center (SOC) has been set up with a clear management, to handle events, make decisions, bring situations to resolution and provide a service to the organization. The Beetles SOC will ensure that you have a real-time view into your security status, assure you that the systems are not being negatively affected and has the ability to execute agreed upon protocols and processes in a consistent manner with issues arise all the while providing a live support to your infrastructure. The Beetles SOC ensures that you are not blindfolded on the battlefield.



BEETLES
THE HACKER'S APPROACH

Aziz Bhaban
93, Motijheel C/A (3rd Floor)
Dhaka-1000
Phone: +880-2-9513744
Email: info@beetles.io
Web: www.beetles.io