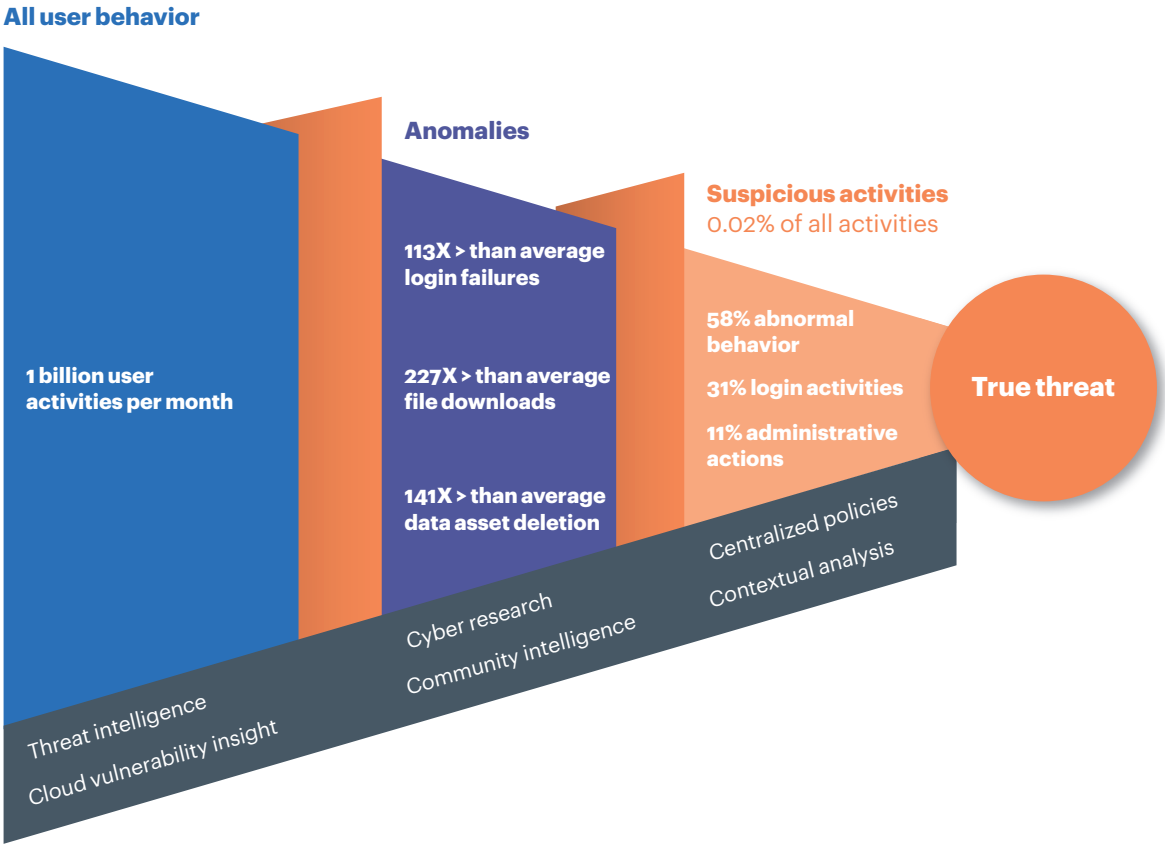
The Australian Cyber Security Research Institute (ACSRI) has been set up and funded by the Australian government. ACSRI combines private companies, public agencies, and universities with a focus on leading cyber research. ACSRI participants have committed about $90 million, and the Australian government has augmented this with an additional $50 million. ACSRI is industry led—minimizing the risk of wasting research funds on areas that are being done commercially elsewhere or where Australia does not have a competitive advantage. ACSRI aims to support about 600 postgraduate research personnel over seven years.

Automation and artificial intelligence

According to Cisco's 2017 Annual Cybersecurity Report, only one in 5,000 user activities (0.02 percent) connected with third-party cloud applications is suspicious. The challenge for security teams is to pinpoint that one instance. Only with automation can security teams cut through the noise of security alerts and focus their resources on investigating true threats. The multistage process of identifying normal and potentially suspicious user activities hinges on the use of automation, with algorithms applied at every stage (see figure 29).

AI and machine learning have the power to disrupt the industry. Security leaders should explore innovative technologies that turn defenses into learning systems. Unsupervised machine-learning approaches, such as those focused on user and entity behavior analytics, work at the intersection of human behavior and big data analytics. Solutions should focus on removing people from the

Figure 29
Identifying user patterns with automation



Source: A.T. Kearney analysis