The time window between the disclosure of a new cyber vulnerability and its use by cybercriminals has been getting smaller and smaller over time. A recent episode, such as Log4j vulnerability, exemplifies this well. Within hours after the exploit being released, attackers started scanning the internet looking for vulnerable hosts to deploy threats like crypto currency miners and ransomware on vulnerable systems. Thus, it becomes imperative for the cyber security defense strategy to detect threats and their capabilities as early as possible to maximize success of prevention actions. Although crucial, discovering new threats is a challenging activity for security analysts due to the immense volume of data and information sources to be analyzed for signs that a threat is emerging. In this sense, we present a framework for automatic identification and profiling of emerging threats using Twitter messages as a source of events and MITRE ATT&CK as a source of knowledge for threat characterization. The framework comprises three main parts: identification of cyber threats and their names; profiling the identified threat in terms of its intentions or goals by employing two machine learning layers to filter and classify tweets; and alarm generation based on the threat’s risk. The main contribution of our work is the approach to characterize or profile the identified threats in terms of its intentions or goals, providing additional context on the threat and avenues for mitigation. In our experiments the profiling stage reached a F1 score of 77% in correctly profiling discovered threats.