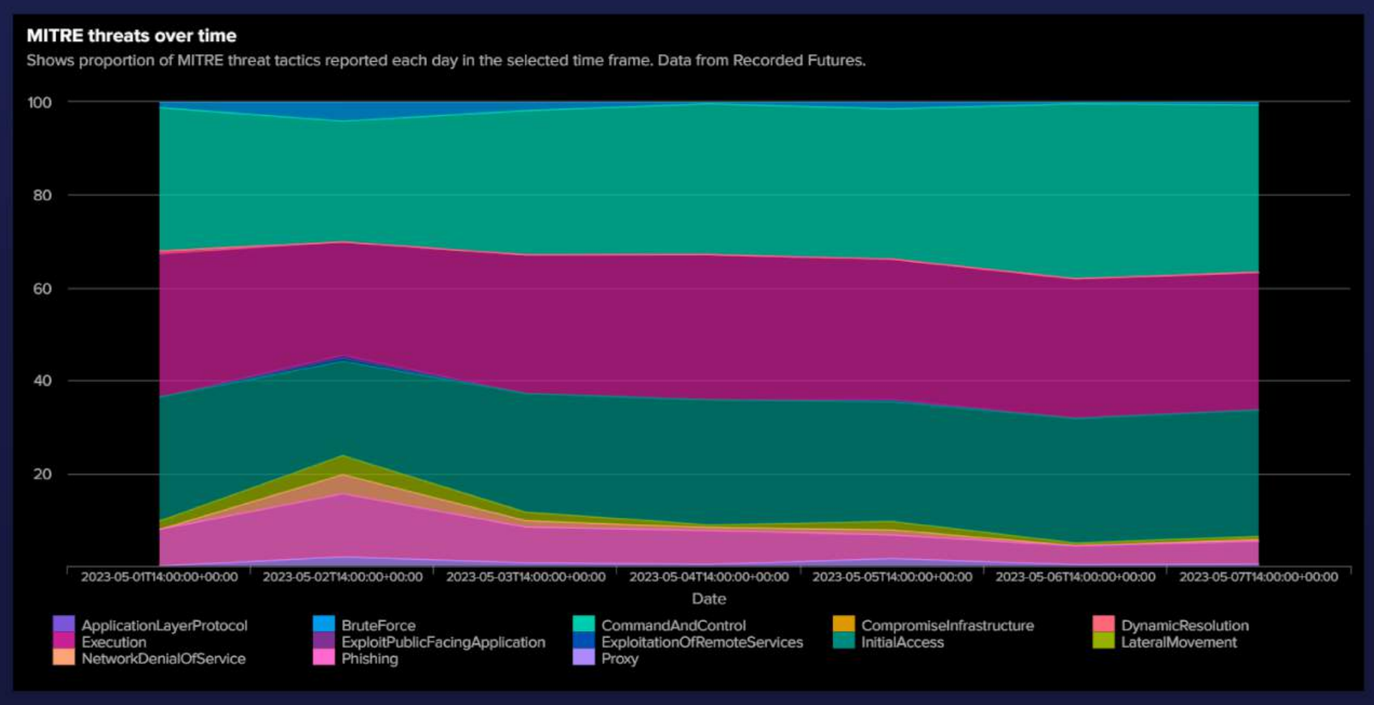
Boosting cyber security at KPMG

Using new sources of intelligence to detect ever-evolving cyber threats

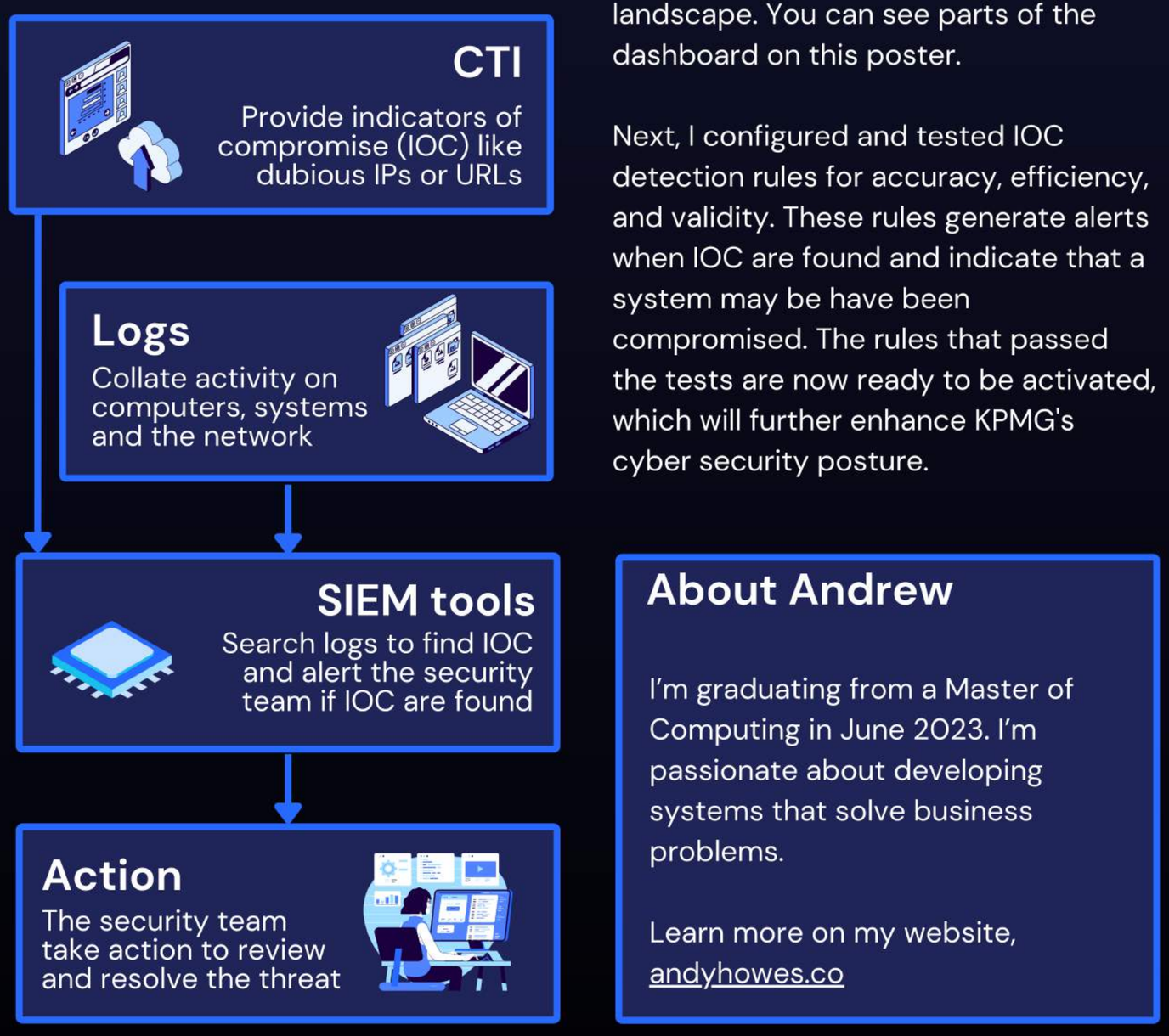
To stay cyber secure, organisations need to have robust Security Information and Event Management (SIEM) systems in place. My internship with KPMG helped achieve just that by strengthening their SIEM capabilities.



SIEM and CTI

SIEM tools provide real time threat monitoring by analysing network traffic and log feeds to find indicators of compromise (IOC). IOC are signs that a system may have been breached. Looking for IOC in logs enables organisations to respond quickly to real-time alerts of suspected breaches.

SIEM tools are powered by cyber threat intelligence (CTI), which provide the IOC to search for. KPMG recently invested in a new source of CTI that they wanted to integrate into their SIEM tool.



Using new CTI sources

I was tasked by KPMG's Cyber Security Operations team with integrating this new CTI source into their SIEM tool, with the aim of boosting the system's threat detection capabilities and empowering the team with insights into emerging threats.

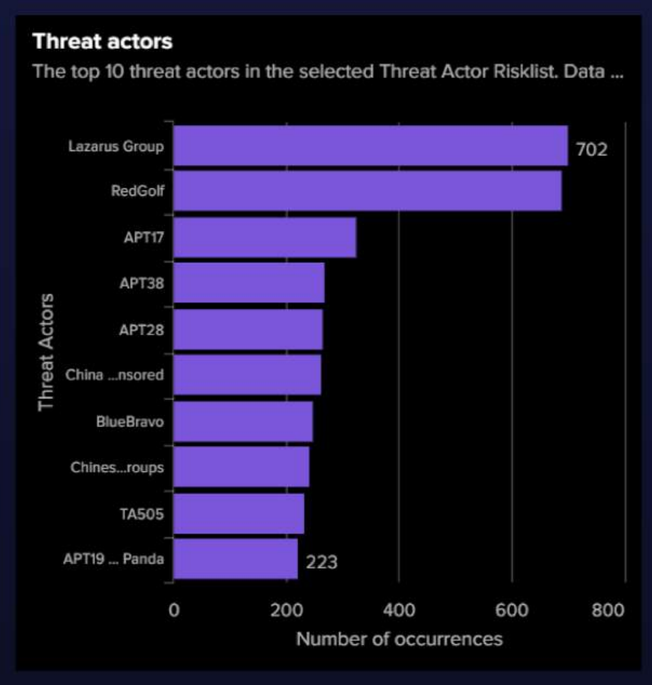
I used the source's API to integrate the the new data source into KPMG's SIEM environment. Next, I assessed the threat data to determine the kinds of insights I could extract from it. Based on this analysis, I developed a threat intelligence dashboard which enabled KPMG to easily understand the threat landscape. You can see parts of the dashboard on this poster.

Next, I configured and tested IOC detection rules for accuracy, efficiency, and validity. These rules generate alerts when IOC are found and indicate that a system may be have been compromised. The rules that passed the tests are now ready to be activated, which will further enhance KPMG's cyber security posture.

About Andrew

I'm graduating from a Master of Computing in June 2023. I'm passionate about developing systems that solve business problems.

Learn more on my website, andyhowes.co



Results and benefits

Integrating this CTI source into KPMG's SIEM tool benefited multiple stakeholders. The security team gained enhanced cyber security capabilities, and their management gained additional oversight. KPMG employees now have added protection, and KPMG's clients have peace of mind about their data and systems.

I have strengthened KPMG's SIEM system by integrating new CTI sources, configuring detection rules, and developing insightful dashboards. These efforts have bolstered the organisation's ability to resist ever-evolving cyber threats.

Learn more

andyhowes.co/SIEM