# API security moves mainstream

DUBAI, UNITED ARAB EMIRATES, July 29, 2022 /EINPresswire.com/ -- Cameron Camp, Security Researcher at ESET explains that the heavyweights are now moving into API security, cementing it as "A Thing".

As swarms of IoT gear, seeking richer data retrieval from their cloud mother ships, the more robust – and more potentially dangerously hackable – API interfaces get a fresh push toward center stage.
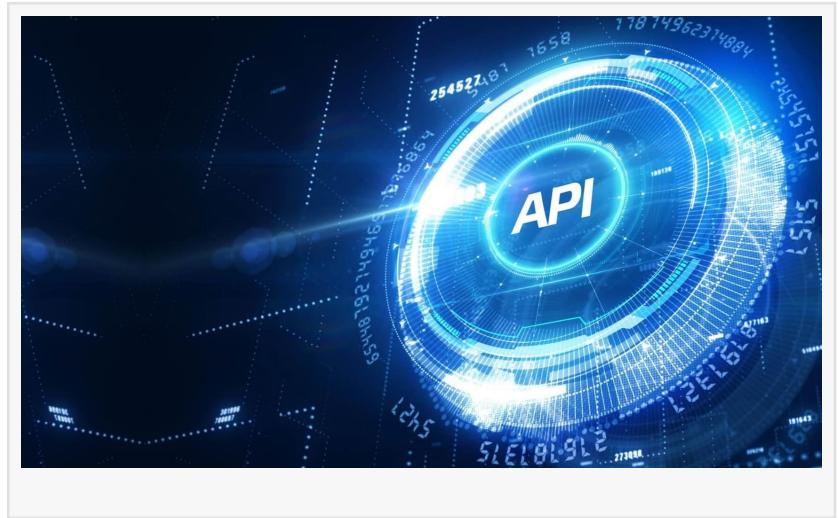
With Google's API security initiative Apigee, API security is growing up. And it's not just IoT. Machine-to-machine data behind super-slick UX designs needs seamless interfaces that help move its masses of data with less friction, offering more responsive mashups of tech polled from locations far and wide.

But to make this all "just work", those more robust interfaces bake in more robust attack possibilities to potentially slurp data wholesale to parts unknown and at record speed.

Recently, we wrote about the spate of new startups at this year's RSA Conference that tried to get attendees to wrap their heads around how to make sure an API doesn't suddenly start misbehaving or does stuff no one knows about until it's too late. It's not just us: our friends at DarkReading purport to tally the mounting business losses associated with API hacks.

And now the heavyweights are moving into this space too, cementing API security as "A Thing". Google's Apigee Advanced API Security for Google Cloud aims to let organizations identify API misconfigurations and thwart malicious bots, the former being one of the main culprits of API security incidents.

Luckily, there are tools from folks like the OWASP API Security Project where you can do a health check on your own APIs, or on those you interface with, which can serve as a baseline. They also have a drill-down about the most common misconfigurations and how to avoid them, so it's a great place to start.

As we mentioned in our previous post, there were a bevy of API security startups darkening the halls at RSA, so you may also have some commercial options, with more coming in the future.

Expect to continue to see API hacks ramp up as companies wrestle with the prospect of securing yet-another-interface, this time an industrial one that sits at the heart of the cloud and big data, and – configured wrong – can allow vast troves of data to be siphoned off around the world to parts unknown. Just make sure it's not your data.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here