



vicarius



The Speed of Vulnerability Remediation

Michael Assraf, CEO of Vicarius, on Enterprise
IT Vulnerability Challenges



Michael Assraf

Prior to co-founding Vicarius, Assraf was a hands-on developer and vice president of research and development at multiple technology startups.

As enterprise IT infrastructures become more complex, the faster vulnerabilities can be identified – and especially remediated – the better, says **Michael Assraf**, CEO and co-founder of Vicarius. “We see organizations using five or six tools and still not getting to where they need to be” in their vulnerability remediation, he says.

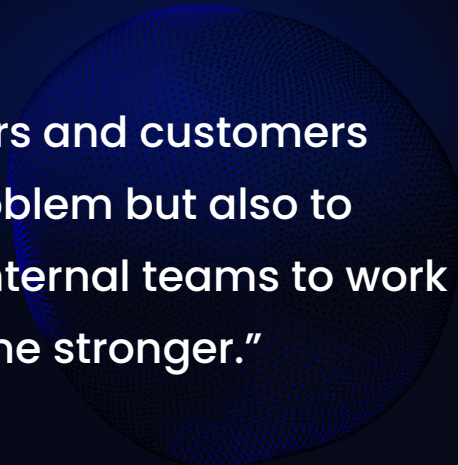
In a video interview with Information Security Media Group at [RSA Conference 2022](#), Assraf also discusses:

- The shift from vulnerability management to vulnerability remediation;
- The changing nature of enterprise infrastructures;
- Why speed is critical to the vulnerability remediation process.

Drivers for Vicarius

Anna Delaney: Talk to us about some of the drivers behind the launch of Vicarius.

Michael Assraf: In 2016, my co-founder Roy told me that he was managing the vulnerabilities and the cybersecurity hygiene for a big insurance company in Israel. He said they were overwhelmed with the amount of vulnerabilities they had and didn’t know where to start or how to fix them. So we thought about the best way to accomplish that, and we worked very closely with design partners



“We worked very closely with design partners and customers to not only provide the right tools for the problem but also to provide the best collaborative way for the internal teams to work on this process and make their cyber hygiene stronger.”

and customers to not only provide the right tools for the problem but also to provide the best collaborative way for the internal teams to work on this process and make their cyber hygiene stronger.

The first part of vulnerability remediation is scanning, where network scanners provide a list and a report of vulnerabilities. Then you have a prioritization process, and then you have the remediation process. We identified two main problems there. The first one was that the process was not efficient. Because the two teams – security, which is in charge of identifying and prioritizing vulnerabilities, and IT – were not working together, they were working almost against each other. The second problem was that the process was always reactive, meaning that the customer had to find the vulnerability in his assets and only then he could even start to think about fixing it. We had to make the process efficient and proactive, and we also had to provide the customer with next-generation technologies to allow them to respond faster, even before a certain vulnerability had been identified and found on their network or on their infrastructure.

Too Many Tools

Delaney: What is at the root of not knowing where to begin with vulnerability management?

Assraf: At the root is the way the infrastructure has been changed throughout. When we had a router and all the computers sat in one office, with the servers on-premises, a scanner would scan all the assets. You were provided with a certain static subnet. But then we started to add AWS and Azure, and then people started working from home and then we had VPN-connected devices. All this made the process of scanning from the network much harder. And then instead of ripping and replacing everything, we just started to build on top of that more products to help us cope with the problem. We didn't stop and build the whole process from scratch. We just added more and more tools. And now we see organizations using five or six tools and still not getting to where they need to be.

Vicarius' Topia Suite

Delaney: How does your Topia suite work?

Assraf: With Topia, we took the first step in vulnerability remediation – vulnerability identification and scanning – and based it off asset inventory, which is quite different. And on top of that, we added a prediction layer toward yet-to-be-discovered vulnerabilities. The first step allows customers to see which CVEs and threats they have based on previous information that was publicly available. But we also provide software composition analysis and a glimpse into the future on how the software can be hijacked.

The second phase is vulnerability prioritization. For that, we combine the usage of each software on each asset and then we provide very interesting insight. For example, rather than giving you a vulnerability report with 12,000 vulnerabilities for 100 computers, we tell you, “You have these vulnerabilities, but we found out that these three are easier to exploit because they’re running on a machine that has an open port. They’re more highly used than the others. They have communication with the DMZ and all sorts of things that are

related to how we execute the software on a specific machine.”

Last, the remediation all comes under one consolidated platform so you don’t need to integrate to different platforms. It’s all under one license. You can do the patching, scripting, and custom development called patchless protection, which allows customers to protect yet-to-be-discovered vulnerabilities from exploitation, without a software vendor update.

Vicarius' Altruism

Delaney: Talk to me about the altruistic side of Vicarius and how you give back to the security community.

Assraf: Hackers work in a very collaborative manner. They share information on Twitter and have dark web places where they can exchange information about previous hacks. And on GitHub, you can find frameworks that are very popular among hackers. But we don’t see that very often on the good side. We don’t see vendors sharing information back to the community about what they’ve found so others can fix it. That is exactly what we’re trying to do. The first

“We launched vsociety, which is a social platform specifically for security and IT admins that helps them first figure out in easy language what a vulnerability is and then provides them with a script for remediation. This is completely outsourced.”

part is helping organizations to find threats they have in the best way they can. For that purpose, we launched our version of Nmap, and we provided our dashboard as a free tool for Nmap users that use Nmap with our instructions to help them figure out what the threats are. This is completely free; we don't charge any money for it.

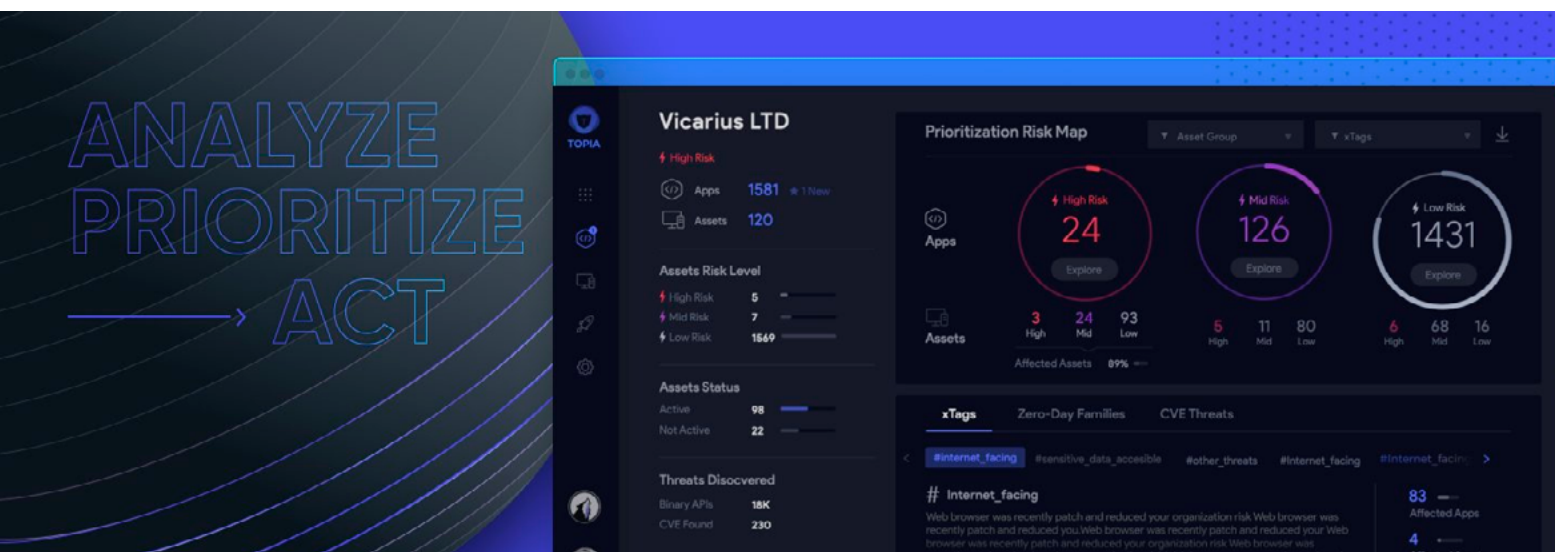
The second part is the collaborative part. Now, when a vulnerability comes out, everyone talks about the analysis: "This is how it affected my network. This is what it can harm. These are the technical details." We figured out that there is a very big gap between analyzing the vulnerability and fixing it. For that purpose, we launched vsociety, which is a social platform specifically for security and IT admins that helps them first figure out in easy language what a vulnerability is and then provides then with a script for remediation. This is completely outsourced. We sometimes push information there, but everything is available for everyone. Sometimes, we also share popular vulnerabilities that everyone is talking about. We push them back to the

community, and everyone will be able to see them, even without logging in. They won't have even have to sign up for the platform.

Joining vsociety

Delaney: How can security pros join and help it grow?

Hassold: It's very simple. You just go to the website and register to the social platform. From that moment on, you will see all of our content. You can also register for notification, so every time there is a vulnerability that affects one of your assets or your software, you will automatically receive an email alert. Every time you enter there, you will see all the popular and recent vulnerabilities, and you will be able to click on them and see the best way to remediate them. In later phases, every vulnerability that has been remediated using vsociety, through our approved script, will be pushed back to Topia, and our users will be able to use the remediation scripts in order to strengthen their cyber hygiene.





Hello, we're Vicarius.

We're on a mission to prevent hackers from exploiting corporate devices—and restore your sleep.

More information is available at www.vicarius.io

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

 **BANK INFO SECURITY®**  Just for Credit Unions **CU INFO SECURITY®**  **GOV INFO SECURITY®**  **HEALTHCARE INFO SECURITY®**

 **infoRisk**
TODAY

 **CAREERS INFO SECURITY®**

Data Breach.
Prevention. Response. Notification. TODAY

CyberEd.io


ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io