INSIDER PRO
FROM IDG

SEPTEMBER 17, 2019 | INSIDERPRO.COM

Home > Security

Review: Blue Hexagon may make you rethink perimeter security

This fully functional, fully trained cybersecurity tool is ready on day 1 to spot threats on whatever network it's charged with protecting.

By John Breeden II

Over the past few years, CSO has reviewed several cybersecurity programs that incorporated artificial intelligence, machine learning or deep learning in one form or another as part of their overall offering. Blue Hexagon differs from all of them in several ways. One big one is the fact that with this platform, deep learning is basically the whole package, not just a small component.

How Blue Hexagon is used and deployed also sets it apart from other cybersecurity programs that dabble in deep learning. For one, most every other program with learning capabilities is installed within an environment and then takes several days, weeks or months to learn about the traffic patterns of the host network.

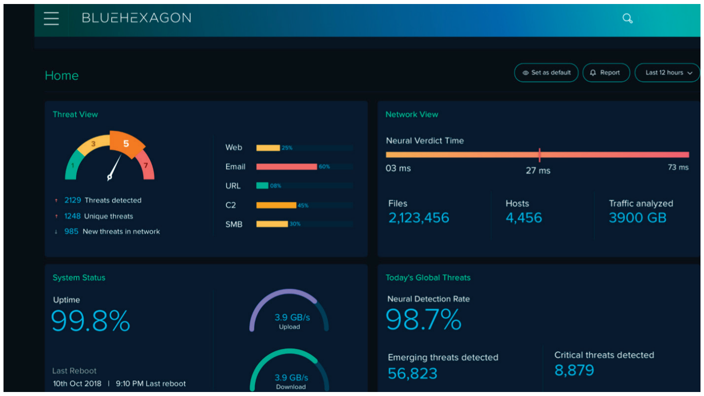
Once a baseline is established, they can help to flag anomalous activity as an indicator of compromise, which is how most programs try and discover previously unknown threats. With Blue Hexagon, users get a fully functional, fully trained cybersecurity tool from day one that is ready to spot threats regardless of the network it's charged with protecting. It's the difference between deploying a smart student who knows nothing but is ready to learn the ropes and a professor who already has years of experience doing their job.

But there is also a more subtle difference with Blue Hexagon, though it's probably the biggest differentiator. While most platforms with machine learning look for anomalies in things like traffic or user behavior, Blue Hexagon actually looks for threats. And it will make a determination about whether a file, process, document or other program is malicious in under one second every time. There is no gray area with Blue Hexagon. Things are either threats or not. Its ability to spot threats so quickly can close many of the gaps that hackers try to exploit, leaving them without enough time to capitalize on any foothold they may briefly establish.

The Blue Hexagon platform is installed as an appliance or a virtual appliance right behind the firewall on a network. You need a separate appliance for each gateway a network has, but each one can handle up to 10 Gbps of traffic. All traffic coming into a network is copied and sent to the appliance for analysis. If something is found to be a threat by the Blue Hexagon appliance, it can link up with any existing cybersecurity program to take actions like blocking or quarantining the threat. In this way, it does not need to deploy its own agents or add more clutter to the environment, but can instead use whatever agents, plus firewalls and other appliances, are already in place to halt malware very quickly.

For example, many organizations use enterprise antivirus these days that installs software agents on endpoints, though they are rarely any good against unknown threats. Connecting them with Blue Hexagon, can really enhance their performance. This approach makes sense given the crowded nature of cybersecurity defenses today.

By making Blue Hexagon work with everything else, it can add its considerable deep learning capabilities to those other platforms, though this also means that you really can't use Blue Hexagon by itself for cybersecurity as it would not have any remediation functions on its own. Luckily, most networks today are packed with cybersecurity software and hardware.



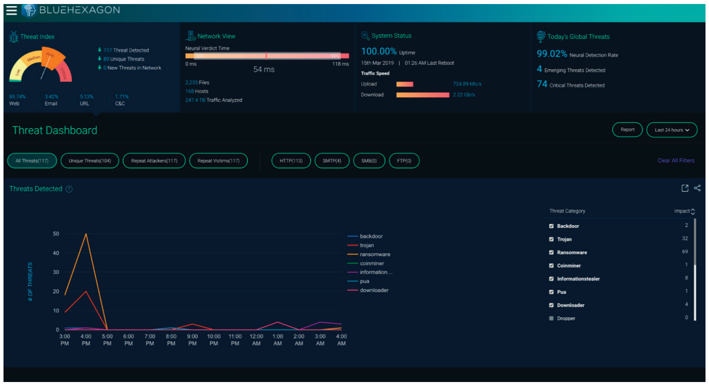
CSO

In addition to all the normal information one would expect to see in a cybersecurity dashboard, Blue Hexagon compares new global threat data to its engine's detection rate, so users can see how effective overall the platform is at stopping unknown threats. That self-tattling stat is dynamic, and updated each morning.

There is also a version of Blue Hexagon that works in the cloud with Amazon Web Services (AWS), though that was not tested as part of this review. With AWS deployments, all of the remediation services are already provided by Amazon in their cloud. Blue Hexagon simply links up with them and uses the AWS tools to remediate any threats it finds. And of course, in either deployment type, all of the threat data can be sent to a central repository for more analysis, training or threat hunting.

Testing Blue Hexagon

Working with the on-prem version of the platform within a demo environment, several emerging threats from a virus zoo were pre-positioned and set to try and run the Blue Hexagon gauntlet. Everything thrown at Blue Hexagon was created, or at least captured, the same day as the test. So, it was all very new, and at least in terms of variants, very much unknown by most cybersecurity programs. For example, many of the most recent threats used in the testing were able to slip right by signature-based antivirus.


BLUEHEXAGON

Threat Index
117 Threat Detected
89 Unique Threats
0 New Threats in Network
89.74% Web
3.42% Email
5.13% URL
1.71% C&C

Network View
Neural Verdict Time
0 ms 54 ms 118 ms
2,233 Files
168 Hosts
247.4 TB Traffic Analyzed

System Status
100.00% Uptime
15th Mar 2019 | 01:26 AM Last Reboot
Traffic Speed
Upload 724.89 Mb/s
Download 2.22 Gb/s

Today's Global Threats
99.02% Neural Detection Rate
4 Emerging Threats Detected
74 Critical Threats Detected

Threat Dashboard

All Threats(117) Unique Threats(104) Repeat Attackers(117) Repeat Victims(117) HTTP(113) SMTP(4) SMB(0) FTP(0)

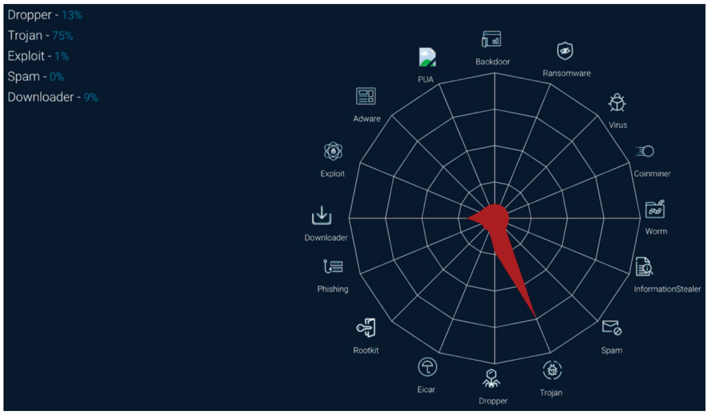
Threats Detected

Threat Category	Impact
☑ Backdoor	2
☑ Trojan	32
☑ Ransomware	69
☑ Coinminer	1
☑ Informationstealer	8
☑ Pua	1
☑ Downloader	4
■ Dropper	0

CSO

In addition to tracking overall threats, Blue Hexagon can break them down by both type and the pathways used by attackers when trying to exploit the network. This can lead to interesting insights about what adversaries are trying to accomplish.

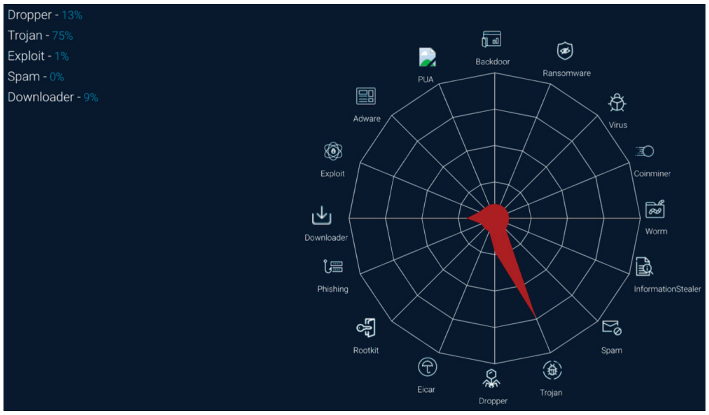
One thing that was both interesting and noticeable during the testing was that Blue Hexagon is using machine learning and a tightly focused intelligence to find new and even polymorphed threats that defy easy categorization. Even if an adversary can rapidly change their malware to avoid detection and signatures, Blue Hexagon could still probably spot it. That means, essentially, that Blue Hexagon can reestablish effective perimeter security from its spot right behind the network gateway. Thanks to its fully trained machine learning capabilities, Blue Hexagon could spot even the newest and most camouflaged threats as we tried to slip them into a protected network.



CSO

Although most threats are stopped long before they can do damage, the platform still analyzes anything it deems to be malware, and shares its thought process by defining the characteristics of discovered malware. Here an uncovered threat is shown to be mostly a trojan, but also has a few other properties. Data like this could be invaluable for later threat hunting.

For example, as brand new malware variants were loaded up and sent into the test network, the Blue Hexagon platform flagged them and sent enforcement actions to firewalls and other security devices to stop them, all of which was accomplished in under a second each time. It was impressive to see the Blue Hexagon dashboard responding to threats in almost real time. And keep in mind that these threats were so new at the time of the testing that a few of them didn't score higher than 40 percent with the VirusTotal site that tracks the effectiveness of antivirus platforms.



CSO

The Blue Hexagon platform can show how dangerous threats it uncovers truly are, and where in the kill chain they were when remediated. Almost nothing in our testing got very far down the kill chain.

This doesn't mean you won't still need a traffic anomaly program. Blue Hexagon is not designed to catch every kind of threat. For example, a valid user suddenly downloading terabytes of proprietary information from a database server would not trigger a response from Blue Hexagon even though that is clearly a red flag kind of action. Instead, Blue Hexagon is designed to do one thing very well, and that is spotting known and unknown threats as they try to sneak into a network. The fact that it also collects metadata on those threats is just a bonus.

Any organization that has given up on perimeter security and instead adopted the mindset of "it's not if, but when you will be hacked" should give Blue Hexagon a look. Not only can it spot the newest, most hidden threats trying to compromise a network, but also it enhances other security platforms, like antivirus, that may already be installed. It can take on a very specific role in cybersecurity, watching the ubiquitous perimeter for threats and do it in a unique and effective way that many people probably thought was no longer possible.

John Breeden II is an award-winning journalist and reviewer with over 20 years of experience covering technology. He is the CEO of the Tech Writers Bureau, a group that creates technological thought leadership content for organizations of all sizes.

BLUEHEXAGON

For more information about the Blue Hexagon network threat protection,
visit www.bluehexagon.ai or email inquiries@bluehexagon.ai