Integrating WhiteHat Scans With BIG-IP ASM

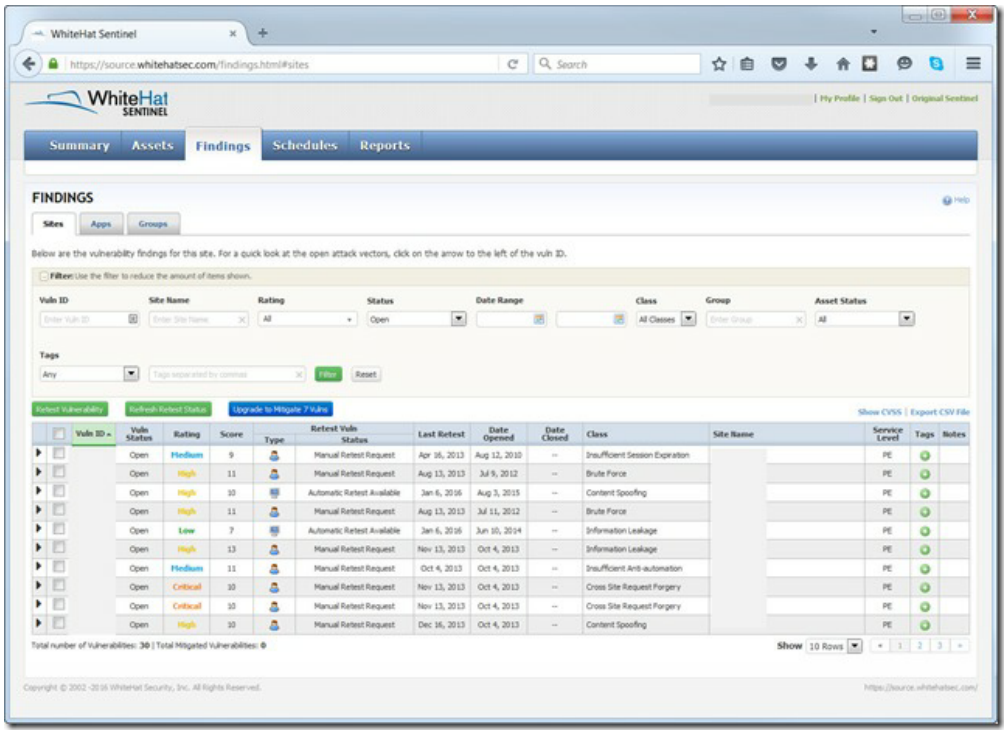
John Wagnon, 2016-25-02

Today's web applications are under constant attack, and it's critical to keep those applications secure at all times for the protection of yourself and your customers. Ideally, you would utilize a team of perfect web developers who create perfectly secure applications that have no bugs and no security vulnerabilities. But that's fantasy. In the real world, web applications are deployed every day with a litany of vulnerabilities that provide a target-rich environment for online adversaries. Fortunately, there are companies that specialize in securing web applications, and they provide a way to scan your applications and find critical vulnerabilities. WhiteHat Security has long been a leader in this space, and they protect organizations by identifying website vulnerabilities that the bad guys exploit to cause harm.

WhiteHat employs a world-class team of security professionals who constantly research and monitor current threats to web applications. Using this expertise, they develop fully customized tests to run against any web application in the world. These robust tests can be run automatically or manually by the WhiteHat team, and -- rest assured -- if your web application has any vulnerability at all, WhiteHat will find it.

WhiteHat offers custom remediation guidance as well as metrics and reports on all the vulnerabilities they find. This allows you to easily and confidently remediate the vulnerabilities as they are discovered. From personal experience, let me say that it's much better to have a trusted partner like WhiteHat find a vulnerability before a nefarious attacker finds it first.

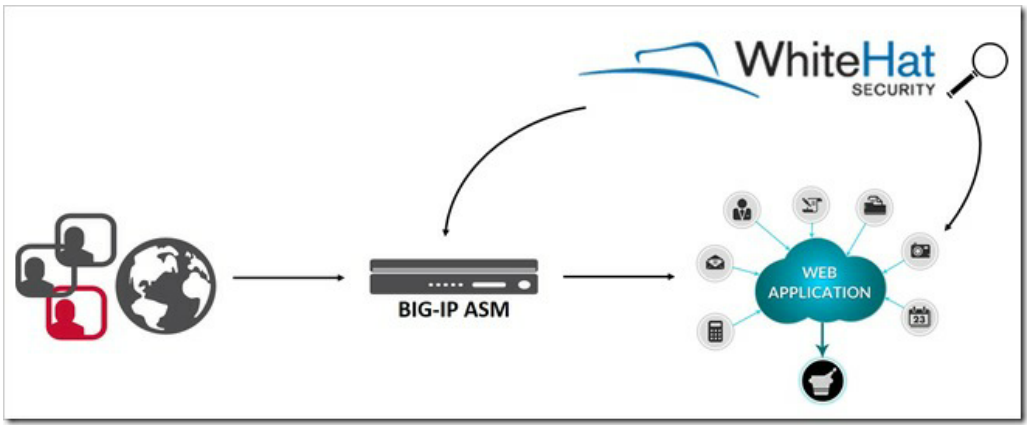
WhiteHat Sentinel, the company's flagship cloud-based application security product, offers a very user-friendly web interface that outlines all the findings from a given scan. The screenshot below shows an example list of vulnerabilities that were found from a WhiteHat security scan. Notice that WhiteHat ranks each finding with a "rating" scale that allows you to know how severe a particular vulnerability is. Also, notice that each finding receives a numeric score that shows how likely this vulnerability is to be exploited. So, if you have a finding with a high score and a critical vulnerability, it's time to take some action on getting that one fixed!



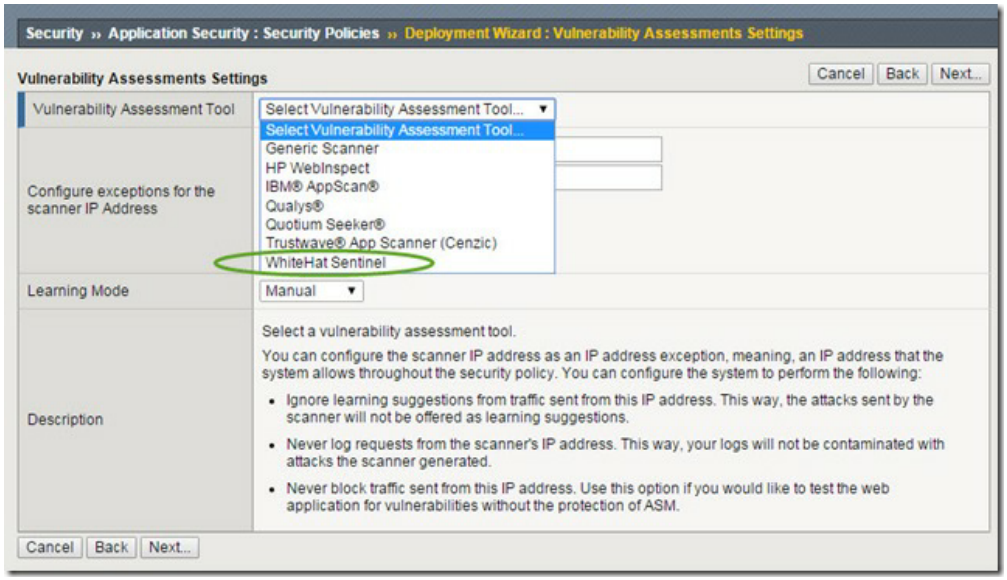
Imagine this scenario: WhiteHat Sentinel has done a fantastic job of scanning your web applications for current vulnerabilities, and you now have an awesome list of findings to mitigate. But, what if it takes some time to mitigate those findings? What if some of them are so extensive that you might not ever get time to fix them? How will your web application stay secure in the meantime? Of course, I'm glad you asked!

F5's BIG-IP Application Security Manager (ASM) is a Web Application Firewall that is specifically designed to protect your web applications from the exact threats that are found by these WhiteHat scans. One of the powerful features of the ASM is that it has the capability to talk directly to WhiteHat Sentinel via the WhiteHat API and build a custom security policy for your specific web application based on the results of your WhiteHat scan. Here's how it works (also, see the picture below):

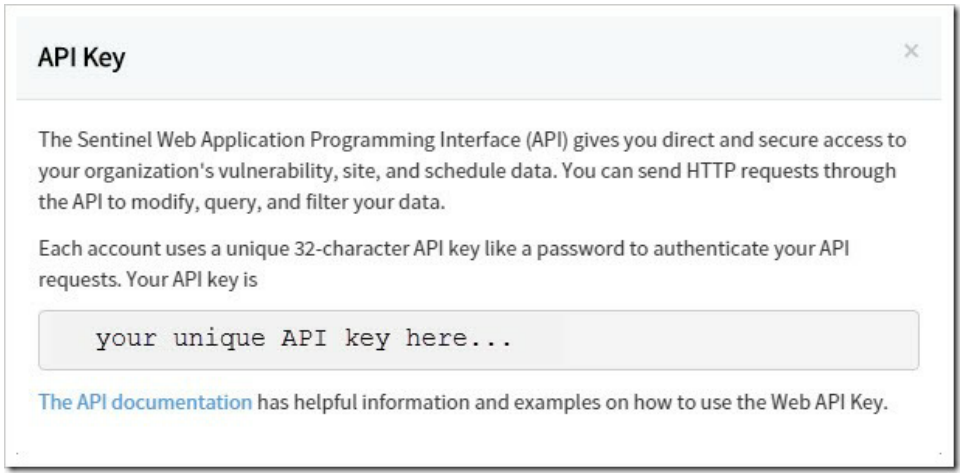
- The BIG-IP ASM sits in front of your web applications and protects them from attack
- WhiteHat Sentinel scans your web applications and sends a list of vulnerabilities to the BIG-IP ASM
- The BIG-IP ASM configures a security policy based on the actual findings from the WhiteHat scan



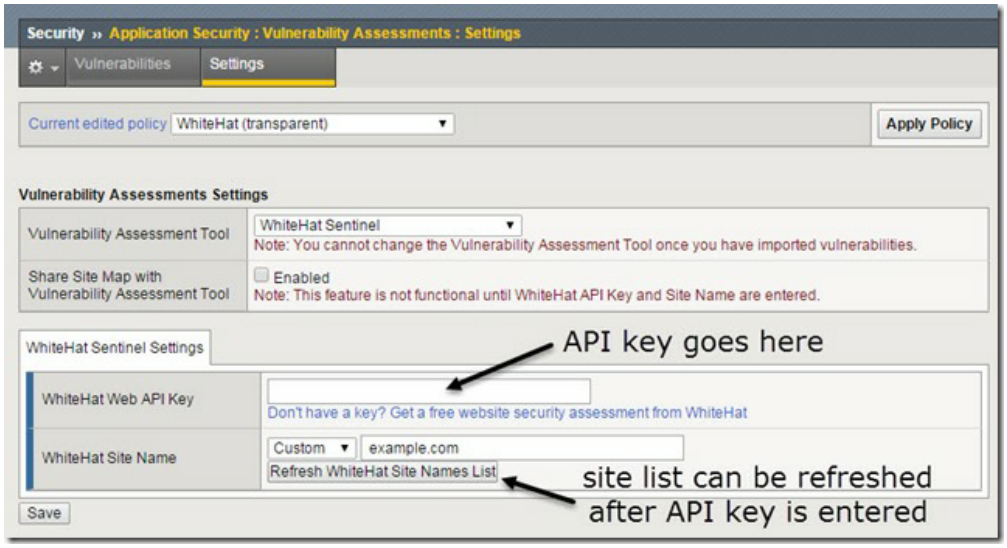
When you create a security policy on the BIG-IP ASM, there are several options to choose from. This specific article won't go into every detail of policy building because it can get fairly extensive, but you can read this article for more details on policy building. As you build a security policy, you can select the "Vulnerability Assessment Tool" option, and you can see in the screenshot below that one of the scanning tools that integrates with the BIG-IP ASM is the WhiteHat Sentinel tool. Simply select that option from the dropdown box and then you'll have an option to add an IP address and Netmask for the scanner. This tells the BIG-IP ASM that it should not block that IP address because it's the one used by the WhiteHat Sentinel scanner. *Note: WhiteHat will need to give you the specific IP address and Netmask they will be using for their scans.*



After you set up the security policy on the BIG-IP ASM, you will need to load in the API key from WhiteHat. This allows the BIG-IP and WhiteHat Sentinel to talk to one another and make updates automatically. The WhiteHat API is unique to your WhiteHat account and will not change. This is nice because you won't ever need to reload this key once you initially set it up on the BIG-IP ASM. To retrieve the key, you login to your WhiteHat account and navigate to your profile page and you will see a link for the API key. The screenshot below shows the popup message you will see when displaying your API key.



Now that you have your WhiteHat API key, you simply copy/paste it into the BIG-IP ASM (see screenshot below). Once you input the key, you should be able to click the "Refresh WhiteHat Site Names List" button and a list of all the sites on your WhiteHat account will auto-populate so that you can simply select the one(s) you want. You also have the option of selecting the "custom" option from the dropdown menu and typing in the site name yourself.



When the BIG-IP ASM is protecting your web applications and WhiteHat Sentinel is constantly scanning them for new vulnerabilities, you can rest assured that your web applications are secure. WhiteHat will alert you when a vulnerability is found, and the BIG-IP ASM will protect that vulnerability from the bad guys. It's a match made in heaven…

Learn more about BIG-IP ASM and WhiteHat Sentinel by visiting these resources:

- https://f5.com/products/modules/application-security-manager
- https://f5.com/solutions/service-provider/reference-architectures/application-layer-security
- https://www.whitehatsec.com/offerings.html#sast

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com