Castellum Labs

WHITE PAPER 2021

Advanced AppSec. Staying Ahead!

www.castellumlabs.com

A lot of focus in application security is towards testing software surfaces (web, mobile and API) and ensuring fixes are done and regressed before release hits the production environment. And, then some organization go beyond the corrective steps and work on embedding the process of vulnerability detection, within their engineering life cycle.

This could be just limited to embedding or throwing the scanners & tools into the build process or it could be an advance level orchestration of the tools at various stages of development process, and, then using them in synchronized way, to preempt vulnerabilities from creeping in your software. In addition to doing the obvious, there are advanced measures organization can take, to outsmart the bad threat actors.

Most Attacks are "Spray and Pray"

As the world of cyber criminals shifts towards plug and play model of attack launch, the tools and infra being used in attacks are predictable. A lot of attacks today, are, not hard labor of misplaced mind/priorities. They are industrial model assemblies combed through multiple things available on darkweb and other open forums. Most of the attacks, will:

- Take a prepared attack tools from one of the forums on darkweb
- Some time also take the pre-config attack configuration of these tools (for specific env)
- And, use a set of botnets to launch a large scale scanning modeled attacks on web surface

Category	Item for Sale	Average Sale Price
	Password Hacking Tool Custom Files	$ 1.96
	Keylogger	$ 2.07
	Phishing Page	$ 2.28
	WiFi Hacking Software	$ 3.00
	Bluetooth Hacking Software	$ 3.48
	FBI/NSA Hacking Tools	$ 5.64
	Cryptocurrency Fraud Malware	$ 6.07
	Hacking Software	$ 8.77
	Remote Access Trojan	$ 9.74
	Anonymity Tools	$ 13.19
	Carding Software	$ 44.37
	Malware	$ 44.99
	Fraudulent Account	$ 145.05
	Cell Tower Simulator Kit	$ 28,333.33

This new rent model of cyber crime, though increases the volumes of attacks across the surfaces, has some brighter aspect at the end of the tunnel. The fact that these volumes of cyber criminals are made possible, through ready made tools and pre configured attack composition can help you do custom modeled security in your software surface.

Counter Intelligence #1 - Look for the "Attack Tools" | Create an Inventory

Search for the automated tools which are commonly used for software surface attacks. Some of the common ones are related to credential stuffing. And, develop an understanding of their working. Look for specific attack model they follow.

Tools:

https://spyse.com/ - OSINT search engine that provides fresh data about the entire web, storing all data in its own DB, interconnect finding data and has some cool features.

http://www.metasploit.com/ - World's most used penetration testing software.

https://findsubdomains.com - Online subdomains scanner service with lots of additional data. Works using OSINT.

https://github.com/bjeborn/basic-auth-pot - HTTP Basic Authentication honeyPot.

http://ww.arachni-scanner.com/ - Web Application Security Scanner Framework.

https://github.com/sullo/nikto - Nikto web server scanner.

http://www.tenable.com/products/nessus-vulnerability-scanner - Nessus Vulnerability Scanner.

http://www.portswigger.net/burp/intruder.html - Burp Intruder is a tool for automating customized attacks against web apps.

http://www.openvas.org/ - The world's most advanced Open Source vulnerability scanner and manager.

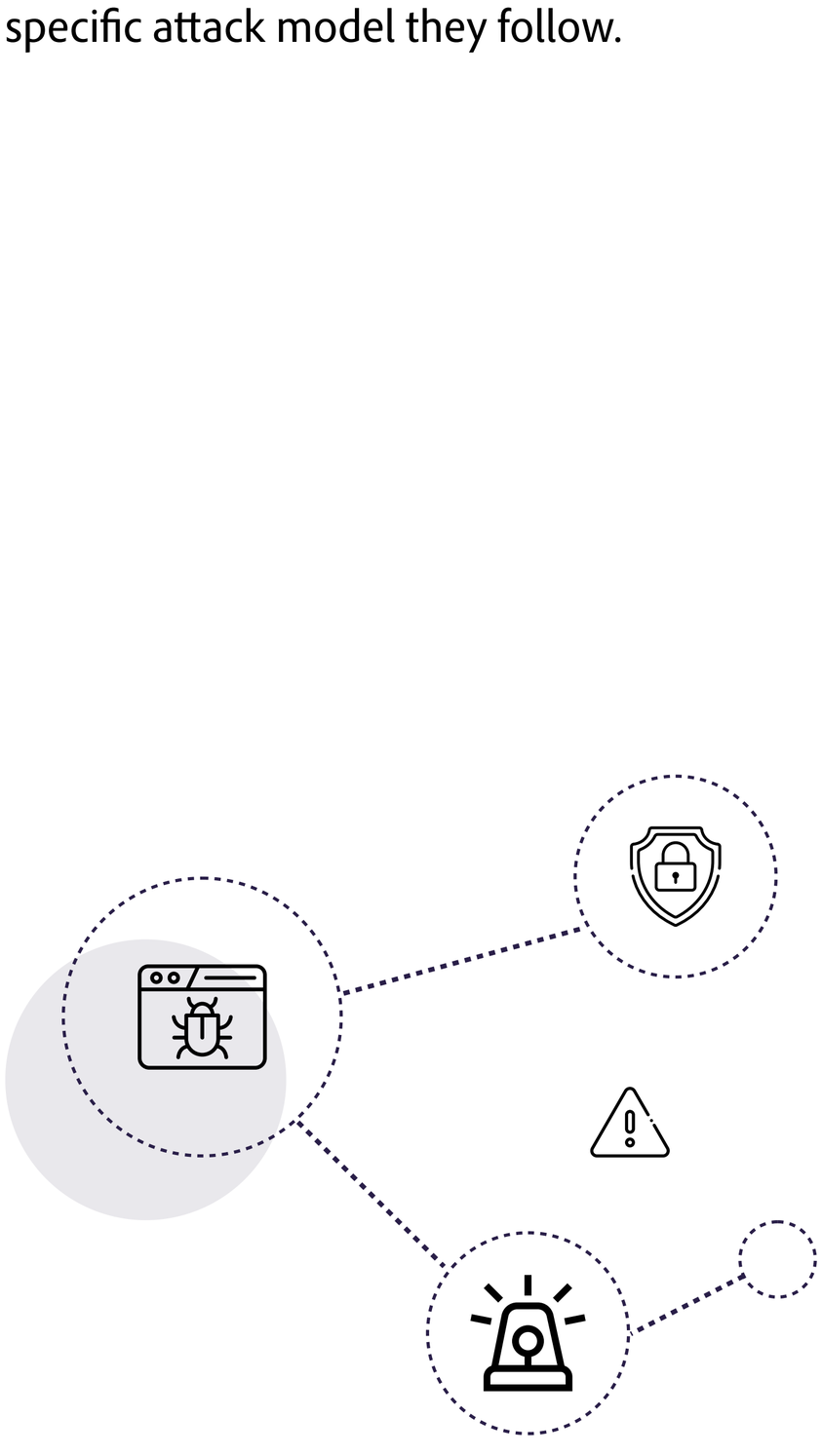
https://github.com/iSECPartners/Scout2 - Security auditing tool for AWS environments.

https://www.owasp.org/index.php/ZAP - The Zed Attack Proxy is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

https://guithub.com/tecknicaltom/dsniff - dsniff is collection of tools for network auditing and penetration testing.

https://github.com/DanMclnerney/dnsspoof - DNS spoofer. Drops DNS responses from the router and replaces it with the spoofed DNS response.

Counter Intelligence #2 - Check Pre-Defined Attack Configurations

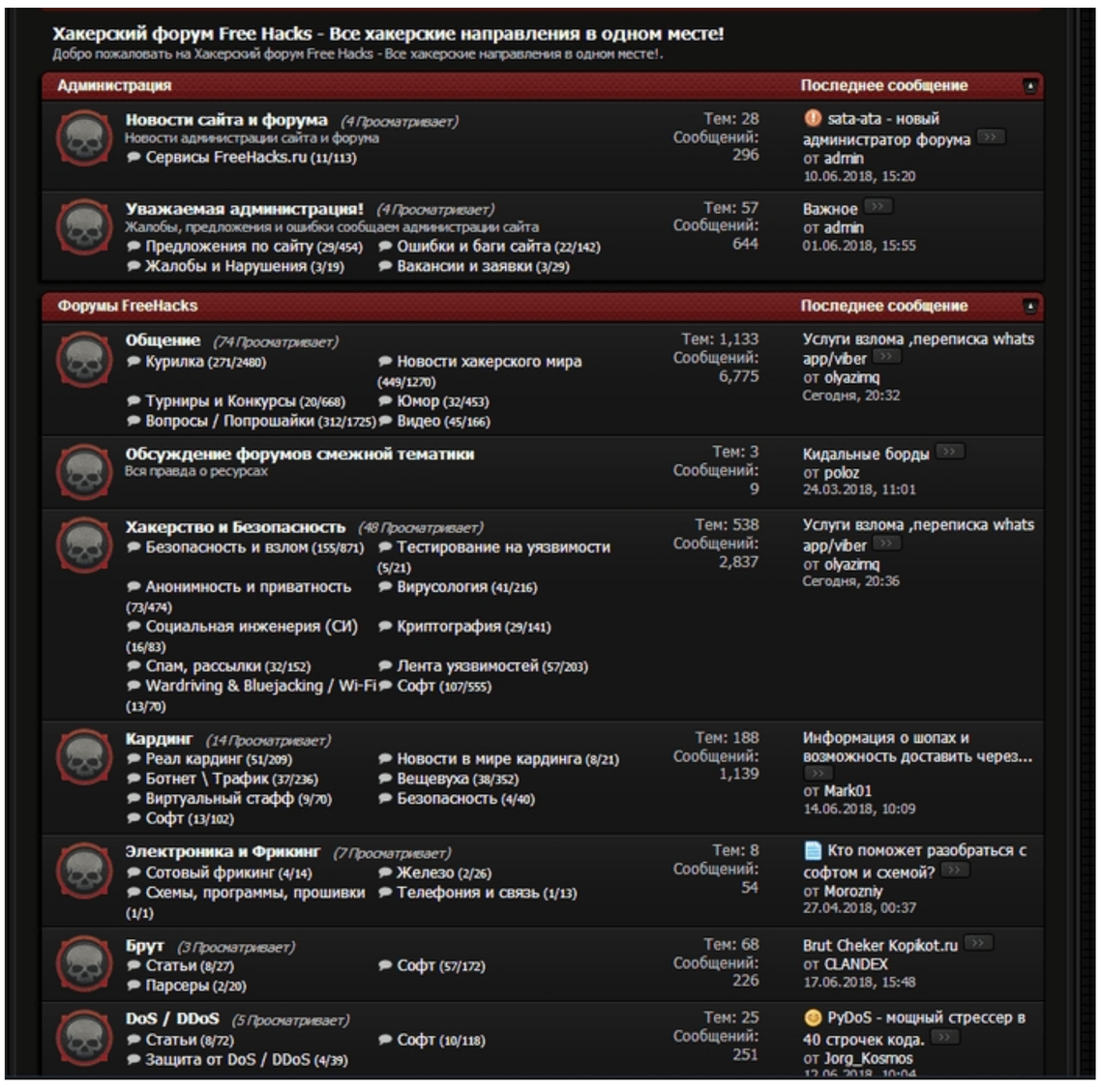


While you look for these tools, check the attack configurations which already exist in these tools. They come pre-loaded with certain attack configurations, meant for specific exploitation model for specific gaps in web surfaces.

Once you develop good understanding of these attack configurations, go back to your software logic and software behavior and change it to deal with these attack configuration.

Counter Intelligence #3 - Check Forums and Chat Threads on Darkweb

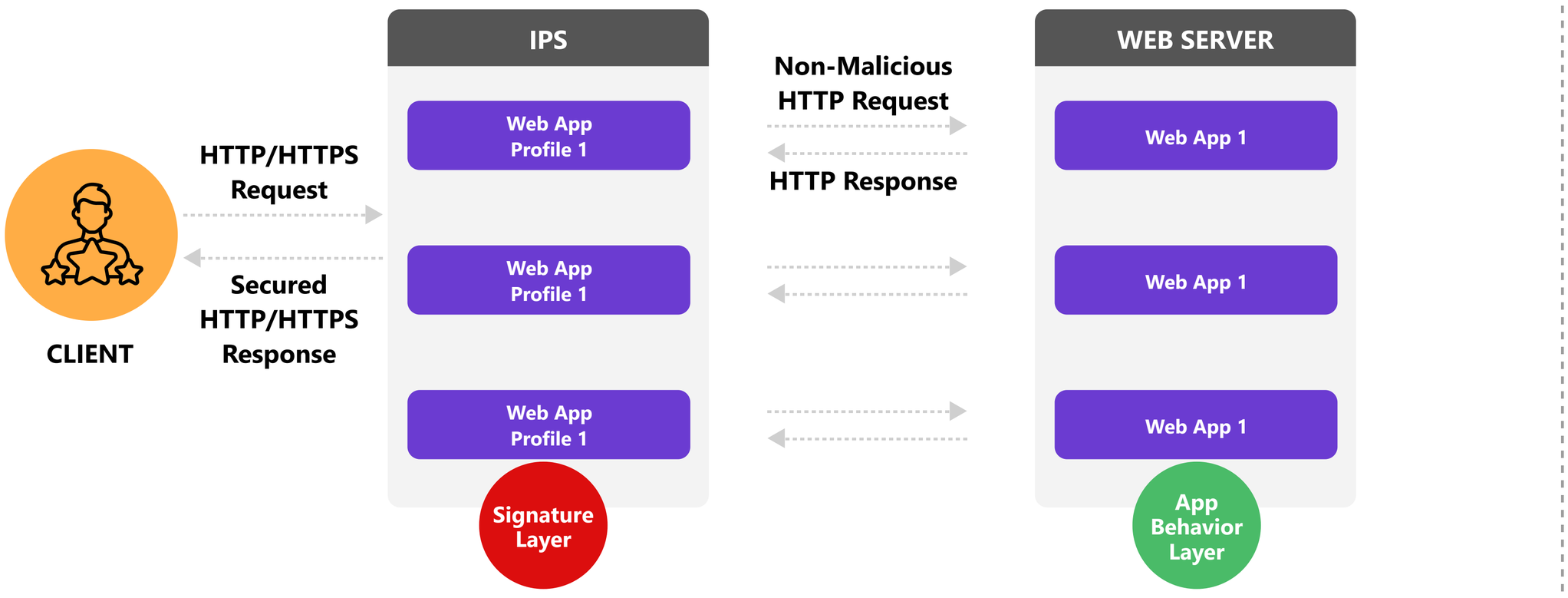
Further, go to forums and look for specific pre-built attack configs which are targeted against your organization. These target modeled attack configs are made to exploit your kind of network and software surface. These have been developed with an attack intent for your organization. Possibility is, you will find them on the market places on darkweb.



Change Application Behavior

Based on your observations and analysis of three things mentioned above, modify your application response and behavior. you can build intelligence in your software, to deal with mal-intent request & reject requests or divert request to a sink hole. One such behavior modification will be changing the way credential requests are entertained by the application.

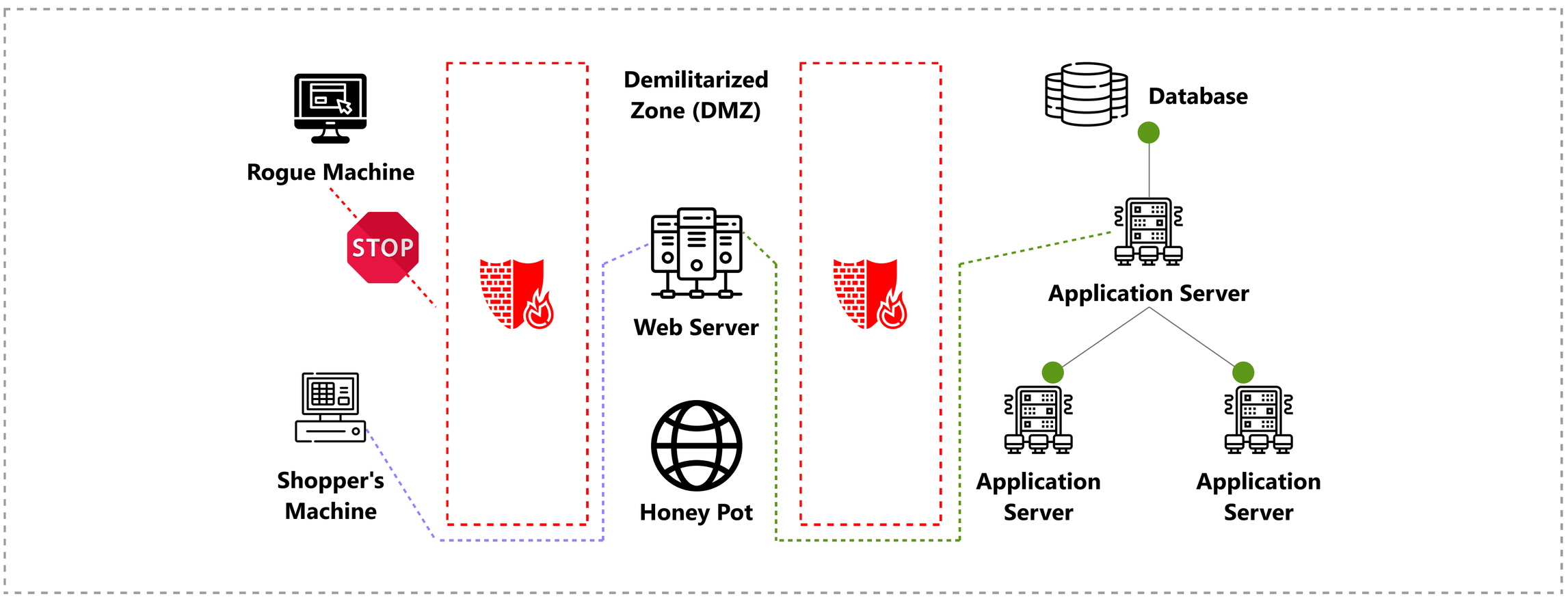
- Don't allow a request if it contains specific header composition, similar to an attack tool
- Fine tune the lock out mechanism of the account, to beat the fragment model attack patterns of tools



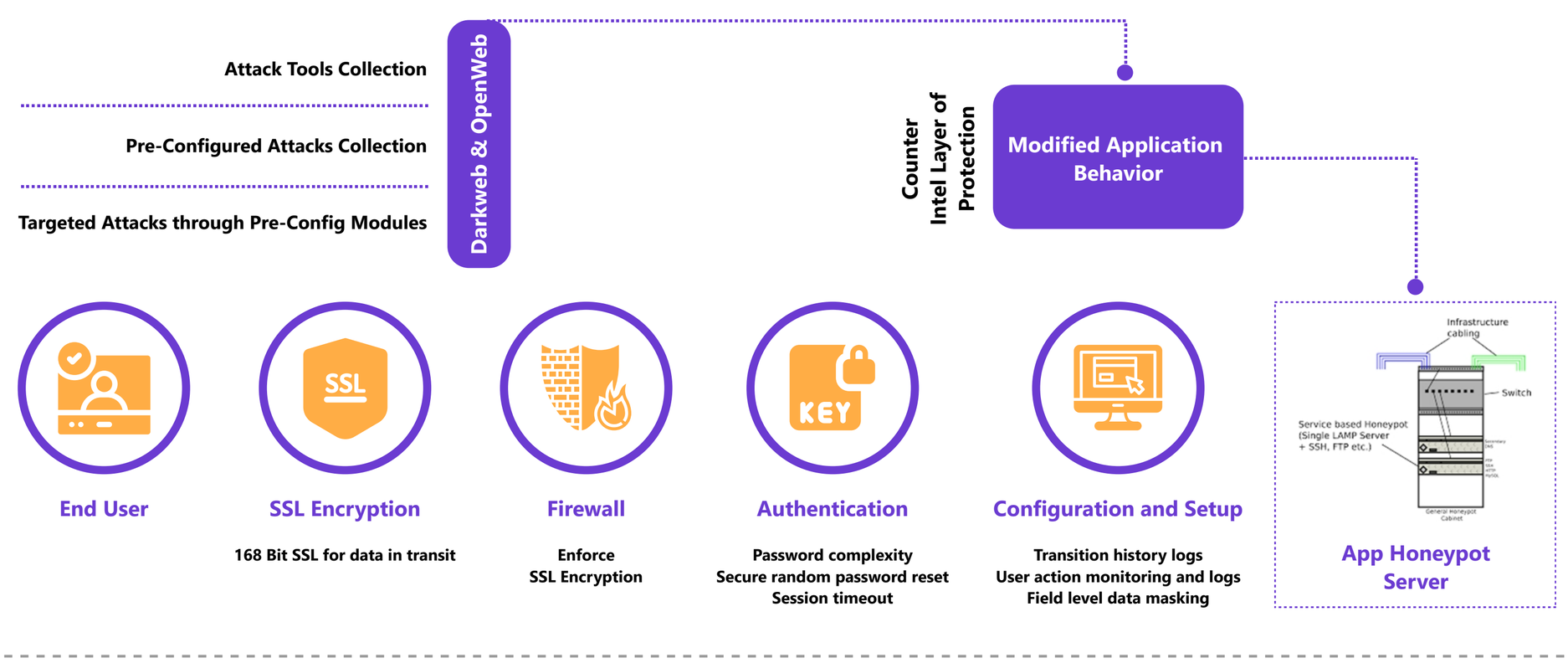
Create a Honeypot

If you would like to take this a step further and not only build application behavior around the attack tools or pre-defined attack configs, you can establish a honeypot, and, re-direct all malicious request to the honeypot.

That will help you collect more and dynamic info about request formats and request mechanism, which will come handy in making your applications change the behavior even further to accommodate these new attack intelligence collected at the run-time.



Create a software surface, which is not only protected using inline testing and detection mechanism, but one, which can work on thwarting the potential attack, by understanding the nature of threats and responding to the requests and traffic in context of the native behavior change.



Most of the time software surface is neglected surface in the organization. And, most of the time, this is the surface which can inflict maximum damage, if exploited by the attackers.

Castellum Labs

+91 97009 70397 info@castellumalbs.com www.castellumlabs.com

WHITE PAPER 2021