Product Newsletter

May 2018 Edition

We have enhanced number of product areas and our backend infrastructure used by MSS teams over the last month.

Indusface Web Application Security (WAS) Scanner Updates:

(Adds benefits to Indusface WAS, TAS & AppTrana Customers)

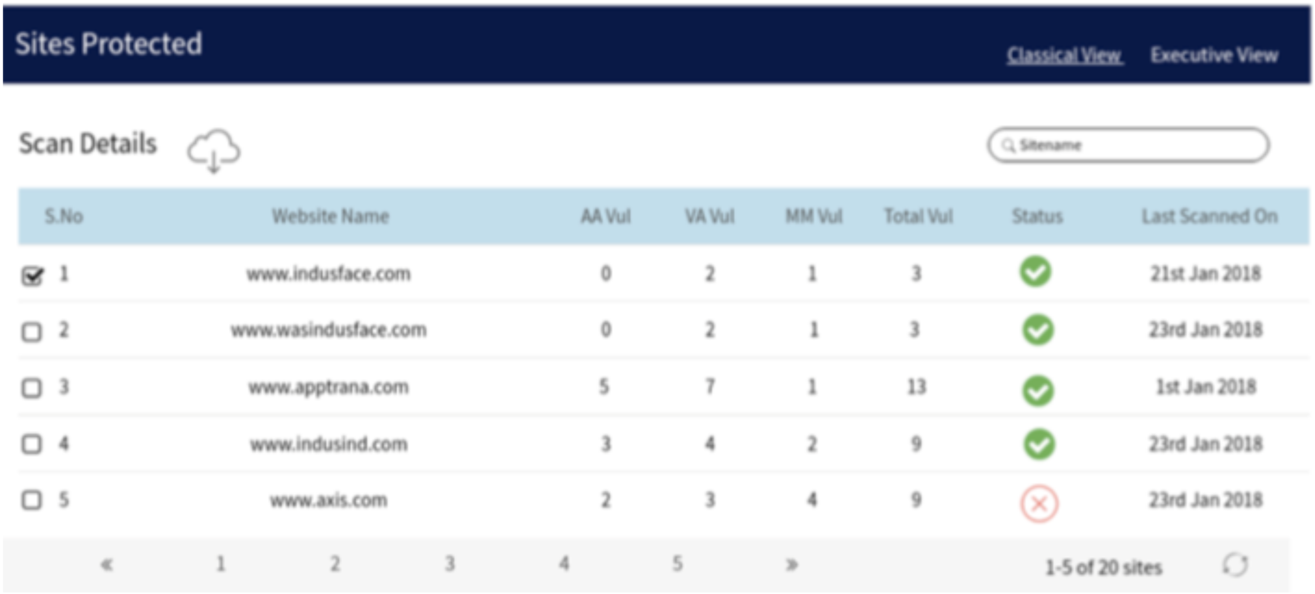
WAF to Scanner Integrations:

Enabled deeper integration between WAF and WAS modules. With this, our automated self-learning technology will analysis real user traffic flowing through WAF and would improve WAS scanner coverage by finding hard to reach / sections of the application.

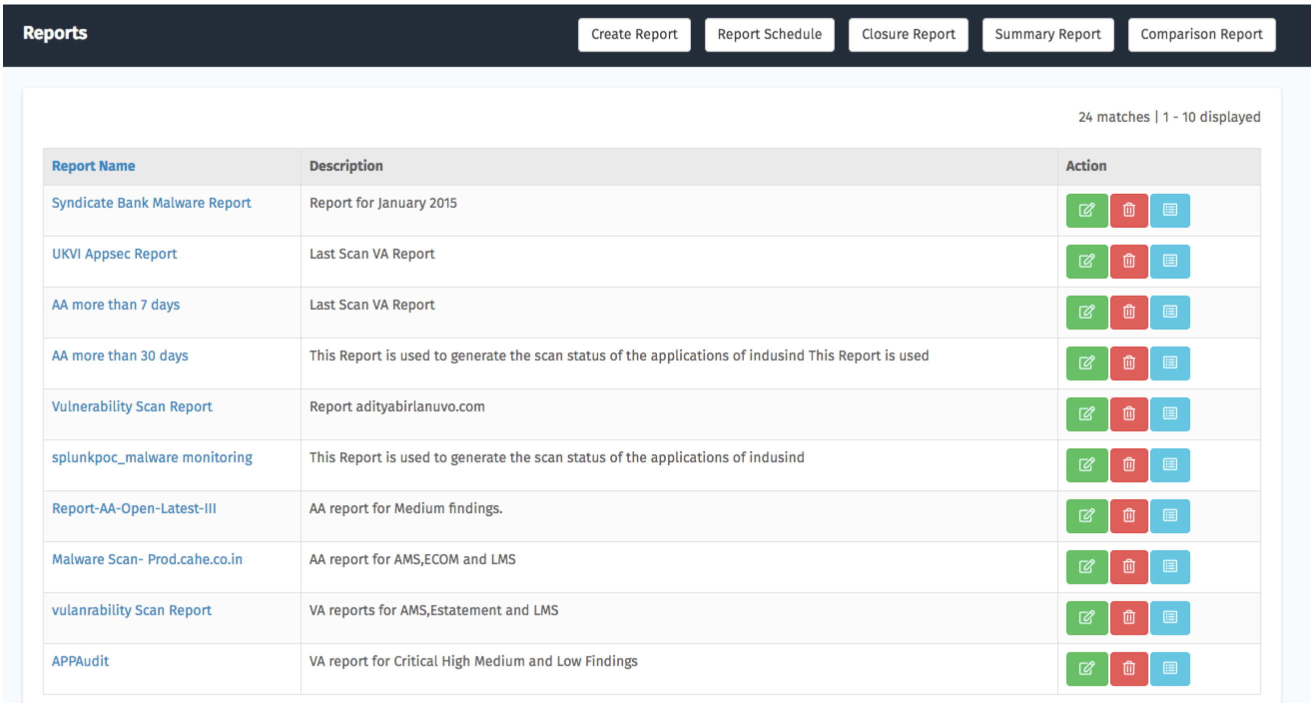
New WAS Portal:

New information rich and user-friendly WAS portal will go beta in coming few weeks. With this, customers will have easy access to useful information in a more intuitive manner.

Here's a sneak preview.

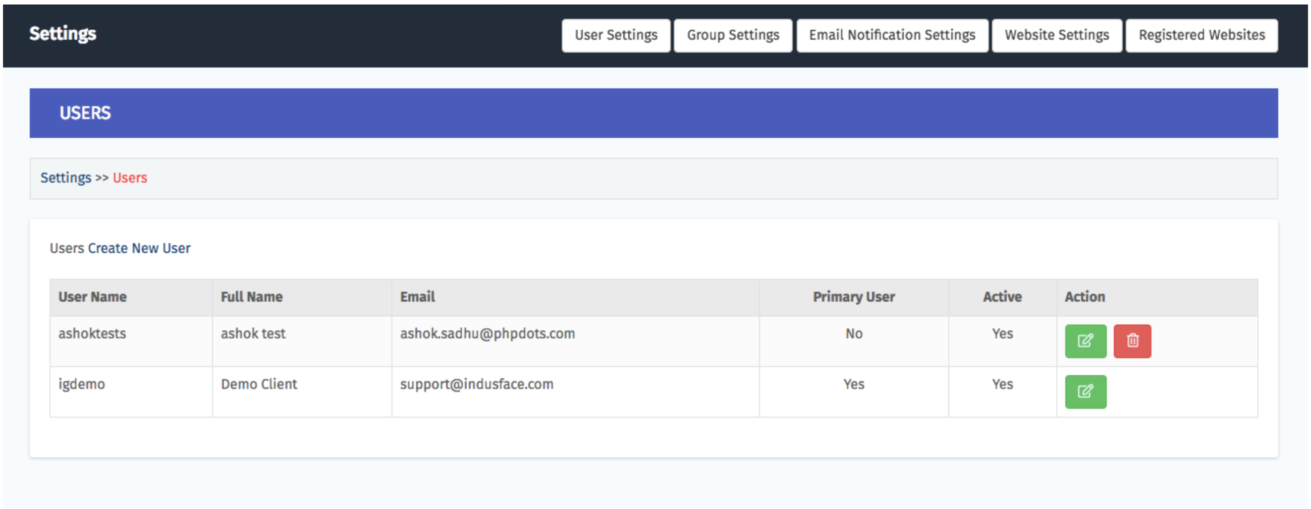


S.No	Website Name	AA Vul	VA Vul	MM Vul	Total Vul	Status	Last Scanned On
☑ 1	www.indusface.com	0	2	1	3	✓	21st Jan 2018
□ 2	www.wasindusface.com	0	2	1	3	✓	23rd Jan 2018
□ 3	www.apptrana.com	5	7	1	13	✓	1st Jan 2018
□ 4	www.indusind.com	3	4	2	9	✓	23rd Jan 2018
□ 5	www.axis.com	2	3	4	9	☒	23rd Jan 2018



24 matches | 1 - 10 displayed

Report Name	Description	Action
Syndicate Bank Malware Report	Report for January 2015	✎ 🗑 ☰
UKVI Appsec Report	Last Scan VA Report	✎ 🗑 ☰
AA more than 7 days	Last Scan VA Report	✎ 🗑 ☰
AA more than 30 days	This Report is used to generate the scan status of the applications of indusind This Report is used	✎ 🗑 ☰
Vulnerability Scan Report	Report adityabirlanuvo.com	✎ 🗑 ☰
splunkpoc_malware monitoring	This Report is used to generate the scan status of the applications of indusind	✎ 🗑 ☰
Report-AA-Open-Latest-III	AA report for Medium findings.	✎ 🗑 ☰
Malware Scan- Prod.cahe.co.in	AA report for AMS,ECOM and LMS	✎ 🗑 ☰
vulanrability Scan Report	VA reports for AMS,Estatement and LMS	✎ 🗑 ☰
APPAudit	VA report for Critical High Medium and Low Findings	✎ 🗑 ☰



User Name	Full Name	Email	Primary User	Active	Action
ashoktests	ashok test	ashok.sadhu@phpdots.com	No	Yes	✎ 🗑
igdemo	Demo Client	support@indusface.com	Yes	Yes	✎

Signatures added/improved:

Added: Web Server Default Web Page Detected

This plugin detects if any web server’s default test page is found. If such page is found, then it may disclose information about the web-server that can be leveraged by hackers to launch attack. Such pages should not be exposed

Enhancements were also made to following Platform based Signatures

Joomla, Drupal, PHP, WordPress, IBM WebSphere, MySQL.

Indusface Web Application Firewall (WAF) Updates

(Adds benefits to Indusface WAS, TAS & AppTrana Customers)

Traffic and event analytics infrastructure:

One of the major challenges around security events monitoring process is to filter out noise and provide actionable alerts to the team. We have made big investments in building traffic and event analytics infrastructure on our backend. This new analytics infrastructure filters out noise and alerts MSS team on security events that need closer monitoring or further mitigation actions. This helps us deliver better protection and various other MSS service more efficiently to our customers.

New DDoS protection

As promised last time, improved DDOS protection rules are incrementally made live for all our customers starting with our SaaS customers.

Block Bots identification

Improved our technology behind bad bot identification using a mix of approaches which include more frequent updates from public sources as well using our own research. This helps us better protect sites against bots used commonly by Email harvesters, Content Scrappers, Spam bots, bots linked to viruses or malwares.

Similarly, we will be rolling out following updates in the next few weeks.

Client fingerprints based DDOS protection: Our DDOS protection technologies will use advanced client finger printing which will uniquely identify a traffic from a particular user session. This will enhance our ability to surgically block distributed attacks without affecting legitimated users accessing site from common IP like same company firewall or same ISP.

HoneyPot Bot Defender Rule: We have enhanced our Bot defender rules which can now identify malicious bots through honeypots and block them. If a new malicious bot is identified when it attacks one of the protected site, this information will be registered in our global threat intelligence database and attack from same botnet on any other sites under our protection will be blocked faster.