



Technology Optimization Center Monthly Sample Report

INFOPERCEPT
Sample Report 2020

YOUR DATE HERE

COMPANY NAME
Authored by: Your Name

 **Infopercept**

Contents

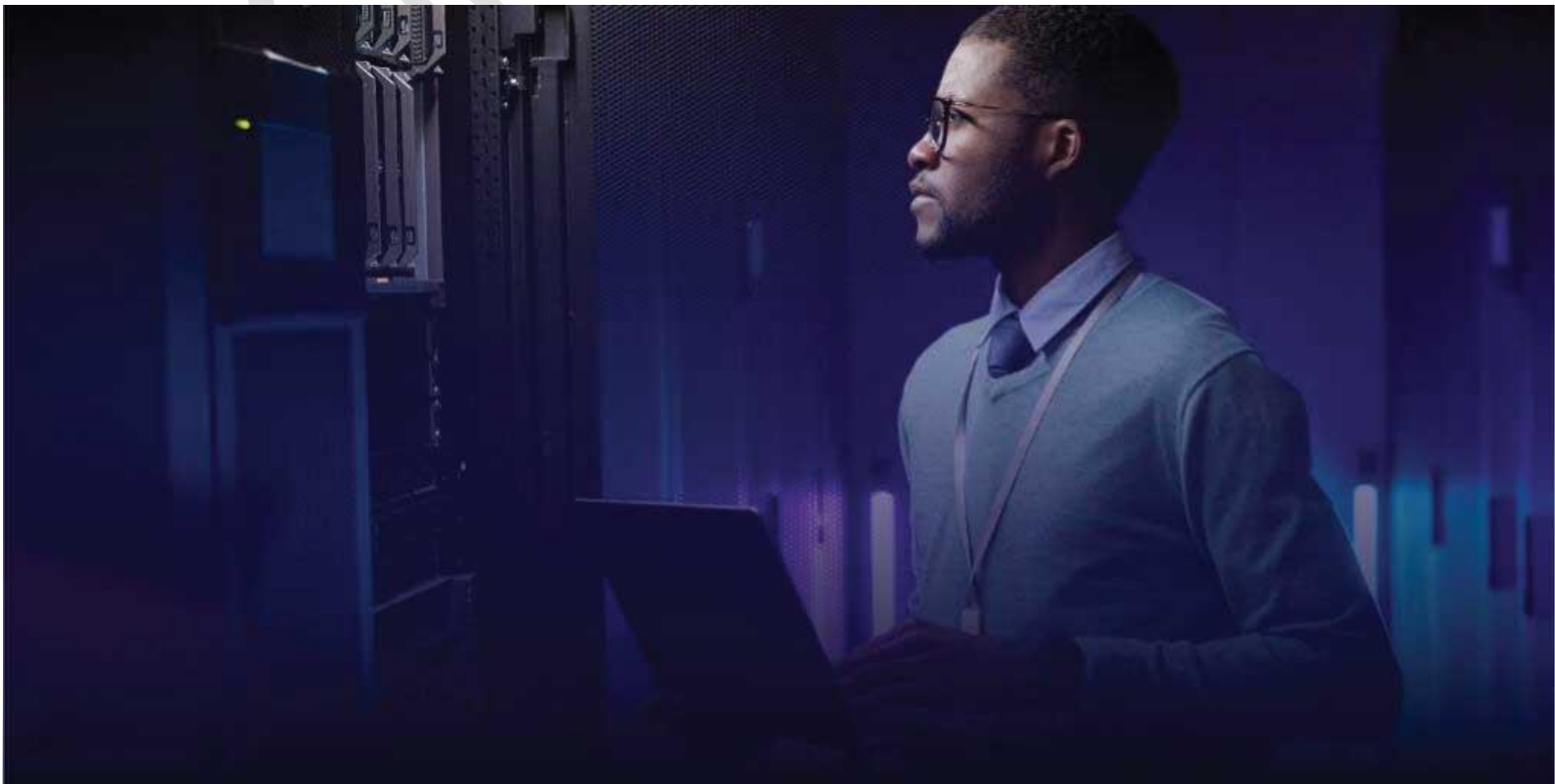
Copyright	3
Disclaimer.....	4
1. Request Volume Trend	5
2. Average Resolution Time (Month wise)	6
3. SLA Compliance Vs Breached Trend – Technician.....	7
4. Site wise Request	8
5. Email Statistics	9
6. DMARC Compliance – Email Volume	10
7. DMARC Compliance – Email Rejection – Threat Protection	11
8. DMARC Compliance – Email Rejection – Threat Protection	12
9. Proactive Measure Taken	13
10. Proactive Measure Taken	14
11. Endpoints – Morphisec	15
12. Endpoints – Symantec.....	16
13. ESET – End Point Security for Windows 7	17
14. Web Site Status	18
15. On Going Activities	19
16. On Going Activities_contd.....	20
17. Current Project Status	21
18. Pending Decision	22
19. DARKWEB Monitoring	23
20. Dark web Monitoring	24
21. What Next?	26
About Infopercept.....	Error! Bookmark not defined.

Copyright

The copyright in this work is vested in Infopercept Consulting Pvt. Ltd, and the document is issued in confidence for the purpose for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under agreement or with the consent in writing of Infopercept Consulting Pvt. Ltd. and then only on condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of Infopercept Consulting Pvt. Ltd.

© Infopercept Consulting Pvt. Ltd. 2020.

CONFIDENTIAL

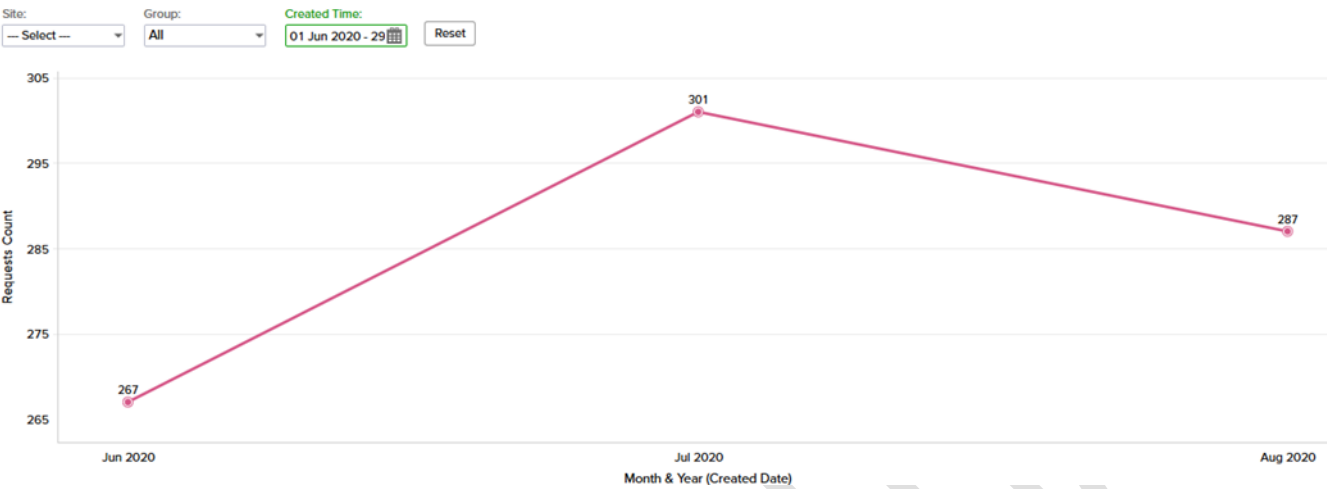


Disclaimer

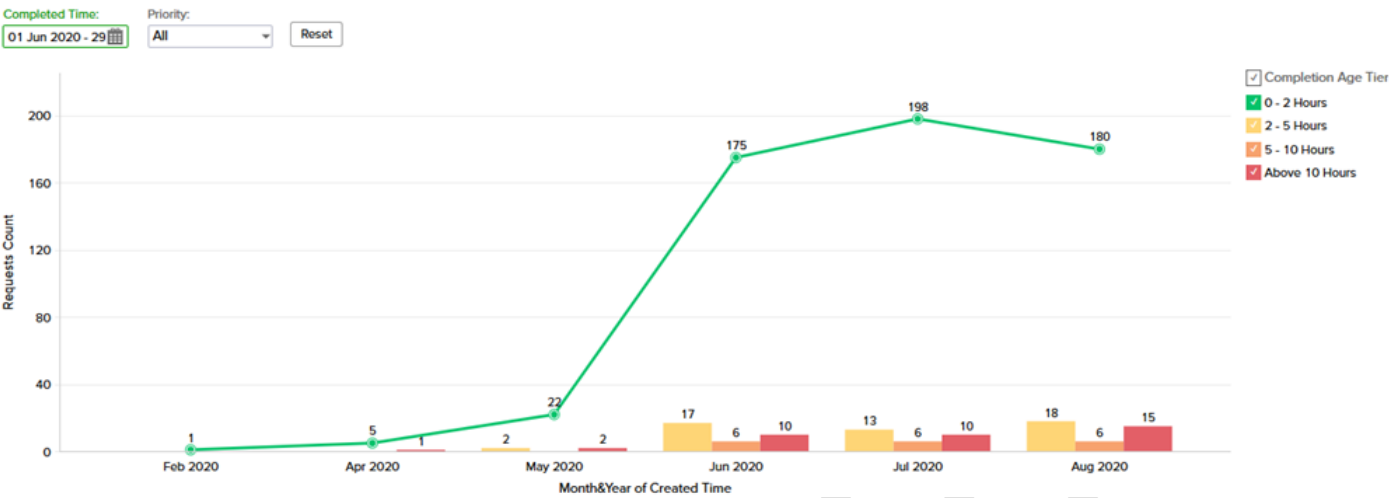
By accessing and using this report you agree to the following terms and conditions and all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property of Infopercept Consulting Pvt Ltd (Infopercept). Nothing contained in this document shall be construed as conferring by implication, estoppel, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of Infopercept or any third party. This document and its contents including, but not limited to, graphic images and documentation may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, without the prior written consent of Infopercept. Any use you make of the information provided, is at your own risk and liability. Infopercept makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information, products, services, and related graphics contained in this document. All such information products, services, related graphics and other contents are provided 'as is' without warranty of any kind. The relationship between you and Infopercept shall be governed by the laws of the Republic of India without regard to its conflict of law provisions. You and Infopercept agree to submit to the personal and exclusive jurisdiction of the courts located at Mumbai, India. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws. You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so.



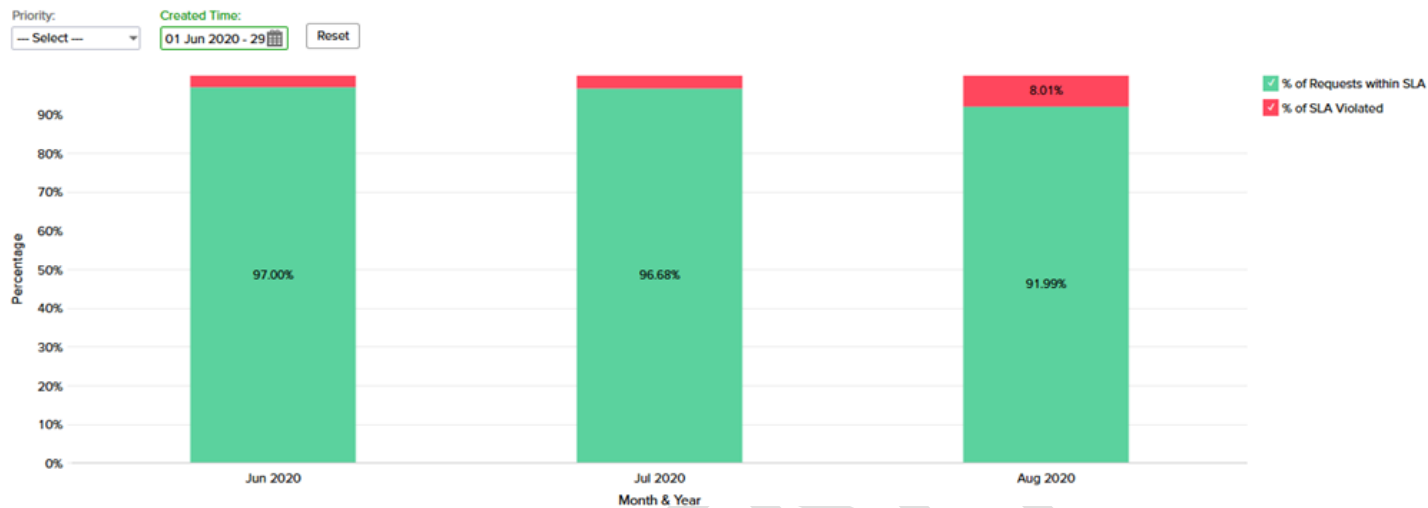
1. Request Volume Trend



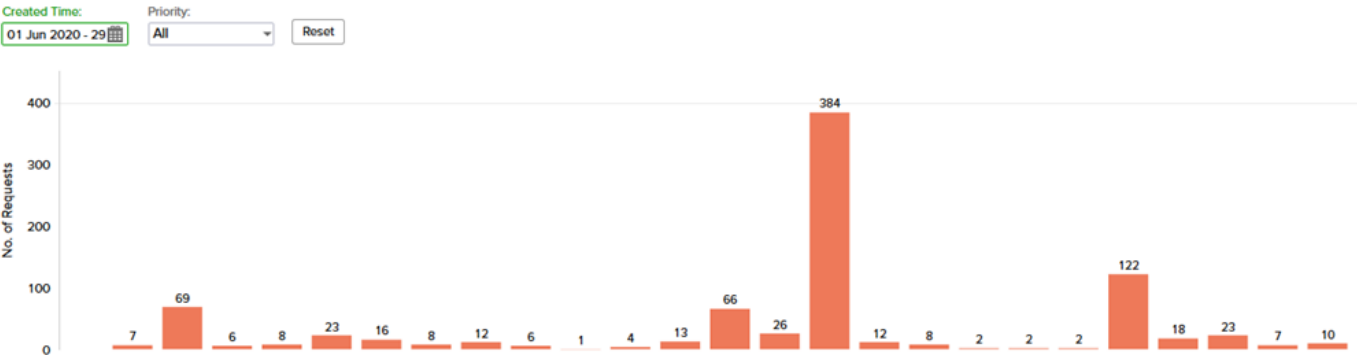
2. Average Resolution Time (Month wise)



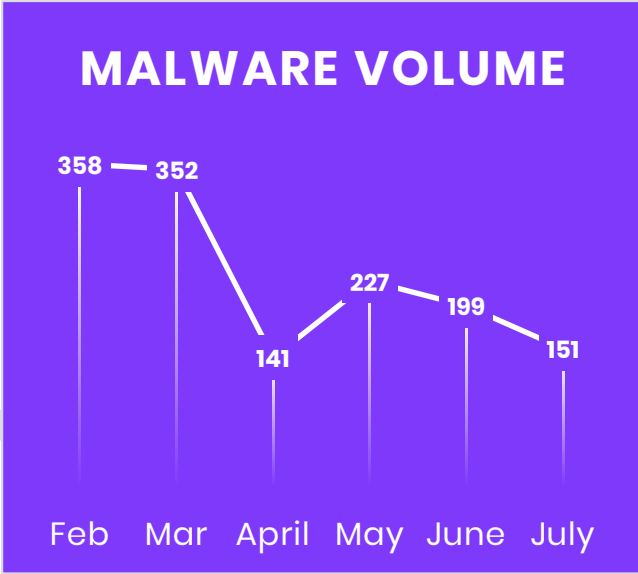
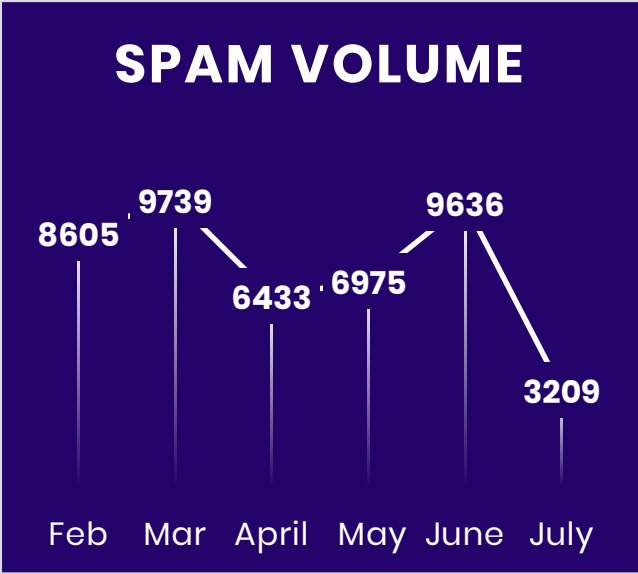
3. SLA Compliance Vs Breached Trend – Technician



4. Site wise Request

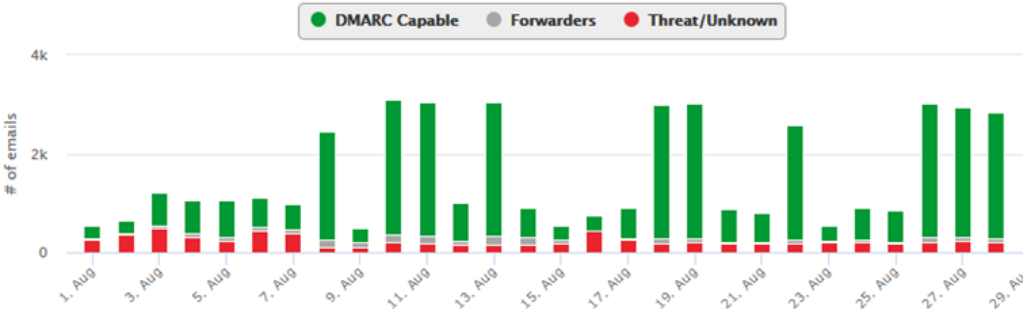
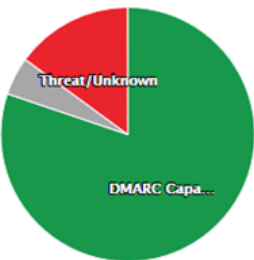


5. Email Statistics



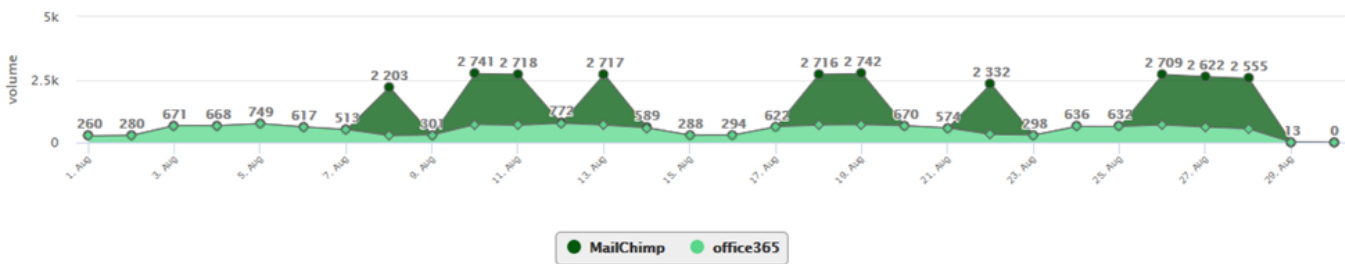
6. DMARC Compliance – Email Volume

Email Volume by Category



DMARC Capable can send DMARC compliant email. Technical staff can attend to your organization's servers. External emailers listed here can send DMARC compliant email.

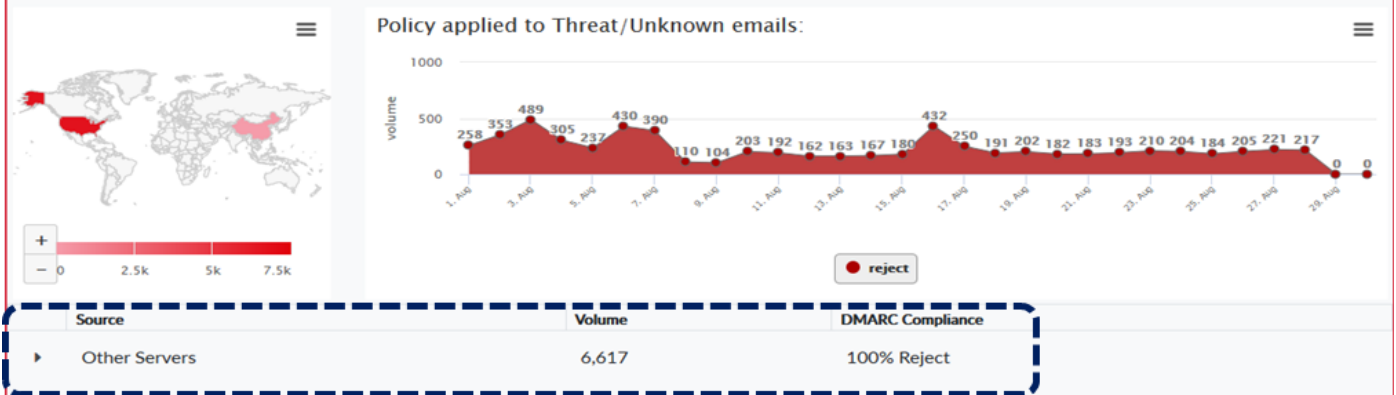
DMARC Capable by Email Volume



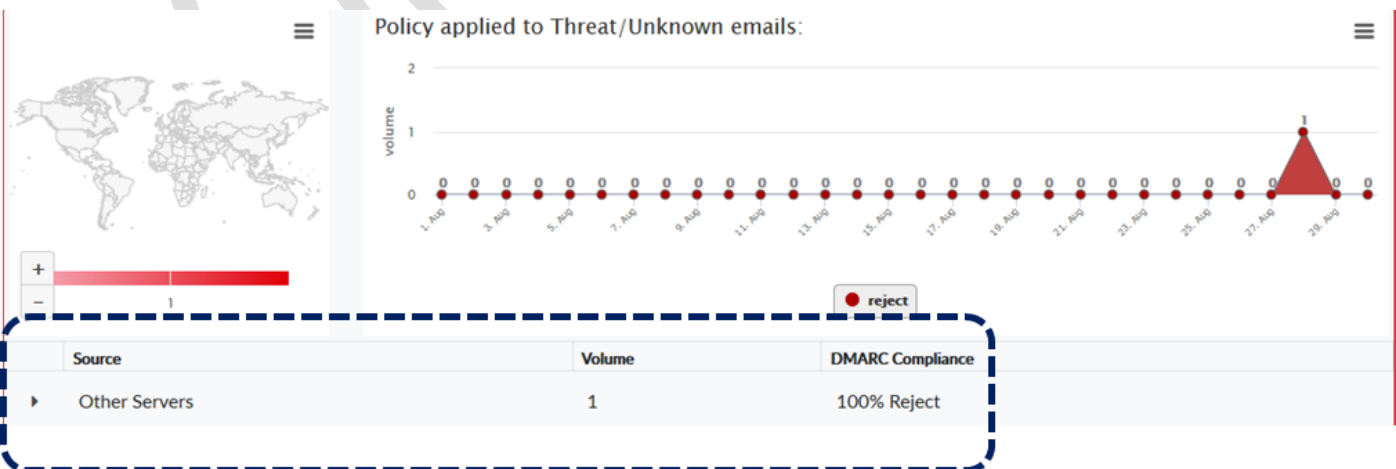
Source	Volume	DMARC Compliance	SPF Alignment	DKIM Alignment
MailChimp	20,205	100%	SPF Incapable	DKIM 100%
Microsoft Office 365	15,297	100%	SPF 100%	DKIM 99.84%

7. DMARC Compliance – Email Rejection – Threat Protection

Threat/Unknown sources are either fraudulent or need to be identified as legitimate. To help dmardian development identify unknown sources, click the [Identify as Legitimate](#) button next to the source to provide more information.



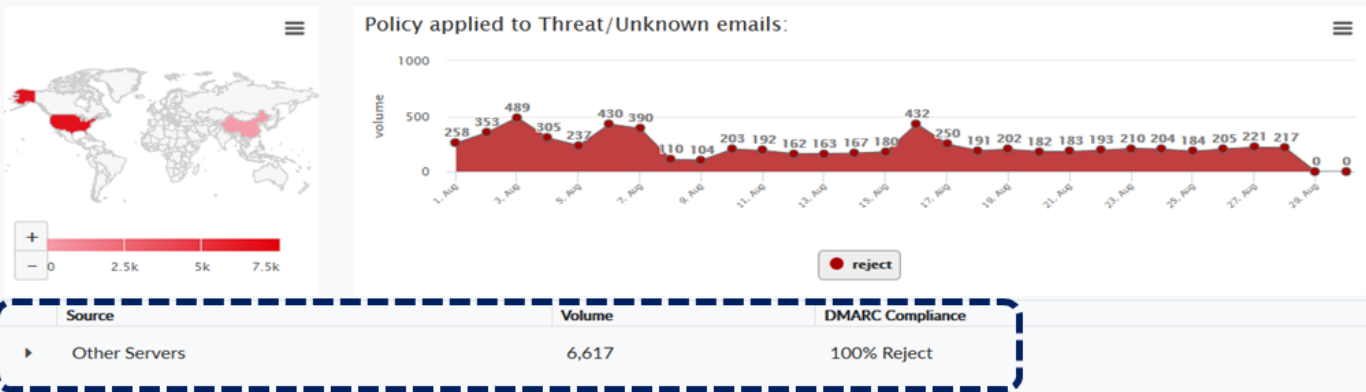
Server Name	Country	From: domain count	Message count
*.nikiz.com		1	6,610
*.nxdomain		1	4
*.mia.bi		1	2
*.163data.com.cn		1	1



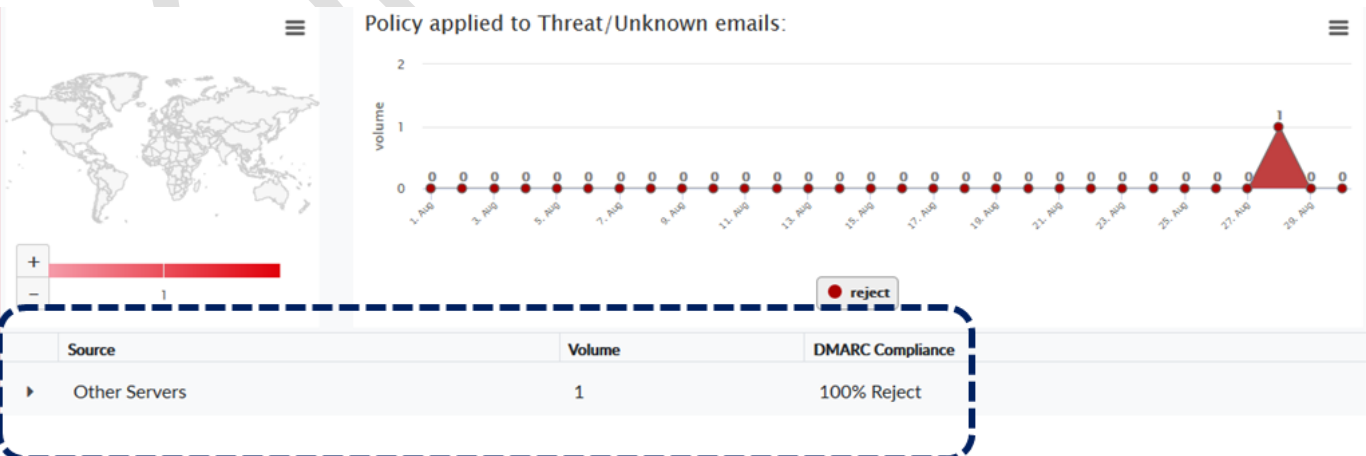
Server Name	Country	From: domain count	Message count
*.nubilus.nl		1	1

8. DMARC Compliance – Email Rejection – Threat Protection

Threat/Unknown sources are either fraudulent or need to be identified as legitimate. To help dmarcian development identify unknown sources, click the [Identify as Legitimate](#) button next to the source to provide more information.



Server Name	Country	From: domain count	Message count
*.nikiz.com		1	6,610
*.nxdomain		1	4
*.mia.bi		1	2
*.163data.com.cn		1	1



Server Name	Country	From: domain count	Message count
*.nubilus.nl		1	1

9. Proactive Measure Taken

20+ blacklisted IPs were blocked on Firewall, Phishing Sender ID were blocked on Office 365 tenants

111	Deny	Remote IP range...	172.104.86.207/32
112	Deny	Remote IP range...	192.241.237.68/32
113	Deny	Remote IP range...	178.128.197.35/32
114	Deny	Remote IP range...	192.241.205.86/32
115	Deny	Remote IP range...	192.241.227.106/32
116	Deny	Remote IP range...	164.90.223.18/32
117	Deny	Remote IP range...	137.135.242.205/32
118	Deny	Remote IP range...	167.71.237.18/32
119	Deny	Remote IP range...	59.126.193.85/32
120	Deny	Remote IP range...	220.135.43.81/32
121	Deny	Remote IP range...	152.249.191.123/32
122	Deny	Remote IP range...	159.65.86.54/32
123	Deny	Remote IP range...	164.90.192.79/32
124	Deny	Remote IP range...	157.230.119.122/32
125	Deny	Remote IP range...	165.22.82.135/32

<p>ticket # 3753 - Notepad</p> <p>File Edit Format View Help</p> <p>sunshine@yamazen.com.ph cfalcinelli@segrup.com.ar agroserve@arnetbiz.com.ar ulises@trademarket.com.mx irene.tagsip@cebudaitocorp.com mariceldiaz@ariesautomotores.com hieu.hd@lilama-sh1.com.vn cbautista@liconsa.gob.mx tanmoy.pramanick@tikona.co.in notificacionesssl@mejiayasociadosabc r-fukada@nomura-kensetsu.co.jp contato@bissoliferramentas.com arief.rahmadiansyah@dieselone.co.j</p>	<p>ticket # 3815 - Notepad</p> <p>File Edit Format View Help</p> <p>huyennt@fujiseiko.com.vn info@skillsetapi.live ahmad.ramdhani@starconcord.co.id goran.nedeljkovic@actimtronic.co.rs sinisa@bomi10.com.mk Sanda.Kozinda@nutricia.com furkan.s@dardanos.com purchases@suncoastmarketing.com fernandez@heras.co.uk arek.wozniak@carrara.it linxw@coscol.com.cn agencyqhd@hoscogroup.com corporation@marico.com.sg mrogers@onfonmedia.com bookings@bundletrip.com desmond.kaeni@satsol.net info@nnmed.com</p>	<p>ticket # 3958 - Notepad</p> <p>File Edit Format View Help</p> <p>info.vincolinwilliam1@yahoo.com hr@darong.tw mail@info.compramostucoche.es babajide.johnson@medburymedicals.com.ng ash.zhang@ugslogistics.com galsync@homeessentialsindia.com zagorka.vukadinovic@bokirus.rs marketing08@wingchunhk.com analistap11@integra.com.ve sales@exceltech-solutions.com tech@yako-uganda.com milan@travelana.co.uk elpi@elpi.com.pl jumutoni@epcafrica.com gucci.cashes@sinteks.com nak@naksystem.com brenda@quantummetal.com ymedina@mlj.mx export@tccsun.com</p>
--	---	---

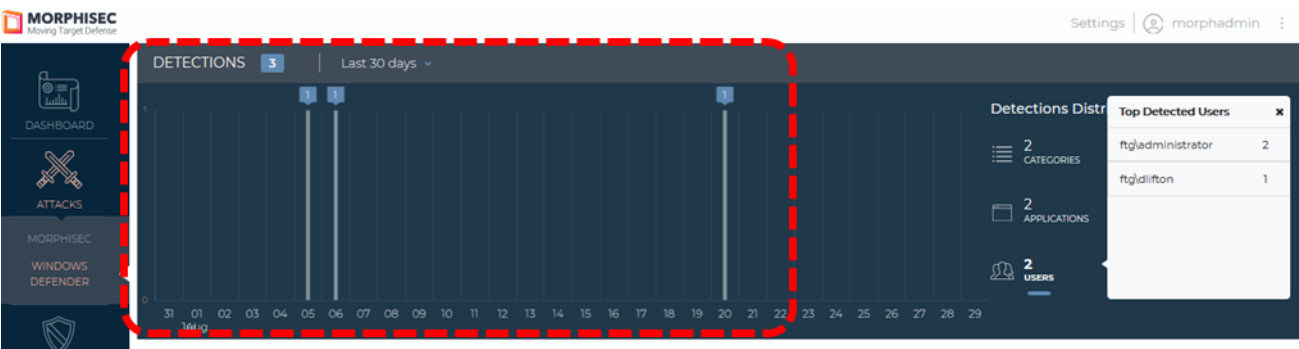
10. Proactive Measure Taken

Monitor Failed Login Attempts and Blocking them

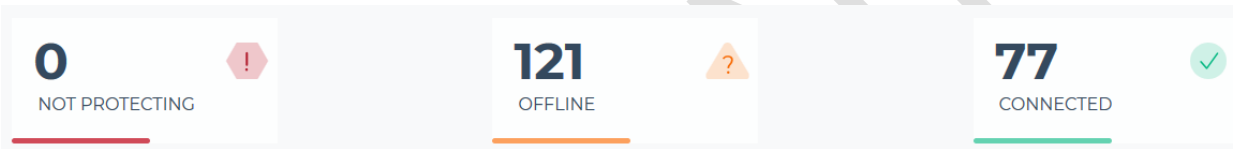
8/28/2020, 4:59:13 PM	973bf1b:	Office 365 Exchange	Failure	115.84.112.138
8/28/2020, 4:57:00 PM	4335999	Office 365 Exchange	Failure	72.221.232.144
8/28/2020, 4:56:55 PM	cb17a8a:	Office 365 Exchange	Failure	72.221.232.144
8/28/2020, 4:52:28 PM	a109235	Office 365 Exchange	Failure	191.97.140
8/28/2020, 4:52:24 PM	a259067	Office 365 Exchange	Failure	191.97.140
8/28/2020, 4:50:25 PM	ce65f29f	Office 365 Exchange	Failure	115.84.112.138
8/28/2020, 4:50:21 PM	00eaa9a:	Office 365 Exchange	Failure	115.84.112.138
8/28/2020, 4:47:08 PM	65d7e6c	Office 365 Exchange	Failure	72.221.232.147
8/28/2020, 4:47:03 PM	3944215	Office 365 Exchange	Failure	46.43.176.10
8/28/2020, 4:46:48 PM	aaeb847	Office 365 Exchange	Failure	103.28.38.166
8/28/2020, 4:44:04 PM	749cd60	Office 365 Exchange	Failure	82.129.113.81
8/28/2020, 4:41:51 PM	889eea8	Office 365 Exchange	Failure	82.129.113.81

11. Endpoints – Morphisec

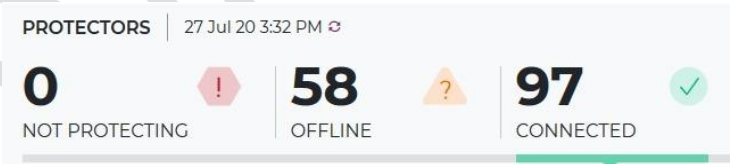
3 Attacks prevented by Windows Defender



3 Attacks prevented by Windows Defender



155 Clients till July 2020



12. Endpoints – Symantec

Identify Computer at Risk and Run Full Scan on the System.

Computer

Add Computers

Health for Managed Computers

66%9%25%

116

16

45

45 computers are at risk.

Computer Count

Managed Windows: 177

Unmanaged Mac: 3

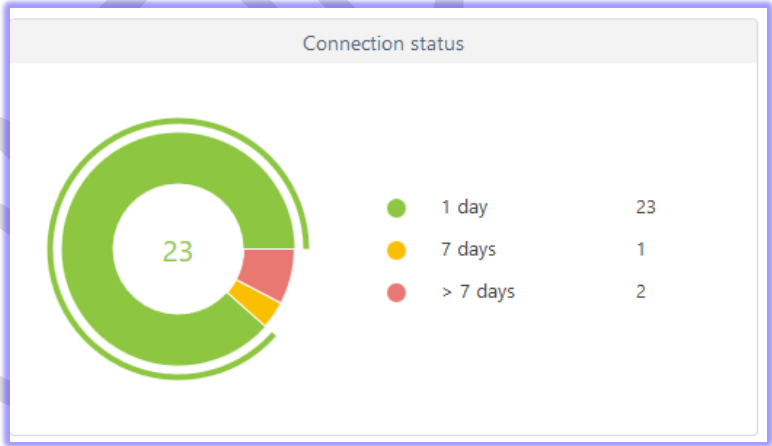
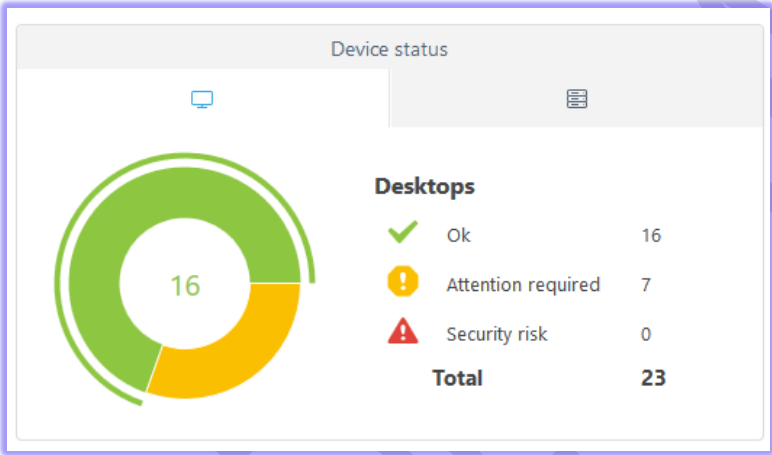
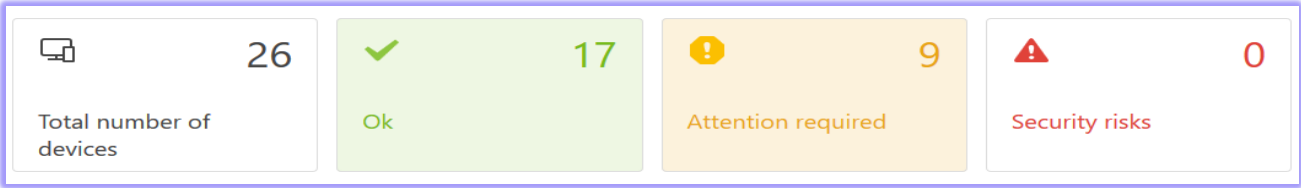
Top Risks Detected		
Severity	Name	Detections
Information	Tracking Cookies	16

INFOPERCEPT
TOC Sample Report 2020


"Infopercept Proprietary Material - Please do not copy or distribute".

16 | Page

13. ESET – End Point Security for Windows 7




14. Web Site Status



Warning: Malware Detected

Infected with malware. Immediate action is required

Request Cleanup



IP address: 185.119.173.118

Hosting: Unknown

Running on: Apache

CMS: WordPress 5.4.1

Powered by: Unknown

[More Details](#)

MinimalLowMediumHighCritical Security Risk

Malware Found

[Known javascript malware: spam-seo.sape?1](#)

Malware Found

[Known javascript malware: spam-seo.sape?1](#)

Malware Found

[Known javascript malware: spam-seo.sape?1](#)

Malware Found

CONFIDENTIAL

15. On Going Activities

No.	Activity Details	SITE A	SITE B
01	Fine Tune Folder Rights <ul style="list-style-type: none"> All shared folder rights being fine-tuned according to the current user department and role. 	●	●
02	Active Directory user and groups' monitor <ul style="list-style-type: none"> Until we have a full-fledged monitoring systems is in place, we have started monitoring and recording (in some cases) users and groups information at all locations 	●	●
03	Updating the User List <ul style="list-style-type: none"> Users, left the organization shall be removed from the Active Directory, Office 365 and shared resources post approval). 	●	●
04	Data Management of ex-staff members <ul style="list-style-type: none"> In those cases wherein data is left behind is moved to separate folder and only administrators have access to those folders 	●	●
05	Malware and other infections' Monitoring <ul style="list-style-type: none"> Removed the suspicious malware files based on the alerts we received from Firewall and Antivirus (Symantec) Software. 	●	●
06	Windows updates for all locations <ul style="list-style-type: none"> All security and critical updates will be pushed to all the computers in every single location. 	●	●
07	Application Server Backup Issue. <ul style="list-style-type: none"> APP03 Server backup is happening with Warning State. 	●	●
08	Website Restriction Policies <ul style="list-style-type: none"> Fine tune current Website restriction policies across all the firewalls. 	●	●

16. On Going Activities_contd.

No.	Activity Details	SITE A	SITE B
09	Websites monitoring <ul style="list-style-type: none"> All websites are constant under monitoring and if and when, there will be any issue, it will be notified and perhaps rectified within short while 	●	●
10	Website Security and updates checks <ul style="list-style-type: none"> perform weekly checks of our important websites and document them with ticket 	●	●
11	Email security and monitoring <ul style="list-style-type: none"> All emails from hotels domain and foods domain are under monitor and any and all security updates necessary are to be performed in coming days, with quite a few security changes being implemented already 	●	●
12	Email retention policy applied <ul style="list-style-type: none"> Anytime (since Nov 2019) an email account deleted, then its emails are retained for next 7 years, to be recovered in case of need. 	●	●
13	Malware and other infections' Monitoring <ul style="list-style-type: none"> we monitor status and health of both these infrastructures since they have all our production servers and user data backups 	●	●
14	VMware Vcenter live activity <ul style="list-style-type: none"> we monitor live status of all our host server, as that affects our production capability and is highly critical 	●	●

17. Current Project Status

No.	Activity Details	SITE A	SITE B	Remarks
01	Windows Group Policy Roll Out	●	●	
02	User Data Migration to Central Storage	●	●	
03	<ul style="list-style-type: none"> 2 FA On O365 Office 365 for charity was activated with help from Microsoft 	●	●	
04	<ul style="list-style-type: none"> Morphisec Client Roll out 	●	●	198 out of 200 Lic. Installed.
05	<ul style="list-style-type: none"> ESET AV For Windows 7 	●	●	26 /42 Lic. installed
06	<ul style="list-style-type: none"> SPICEWORKS (Inventory Management Tool) 	●	●	
07	<ul style="list-style-type: none"> Web Application Firewall for Online Portal 	●	●	
08	<ul style="list-style-type: none"> Security Assessment of Portal 	●	●	
09	<ul style="list-style-type: none"> Server Consolidation 	●	●	

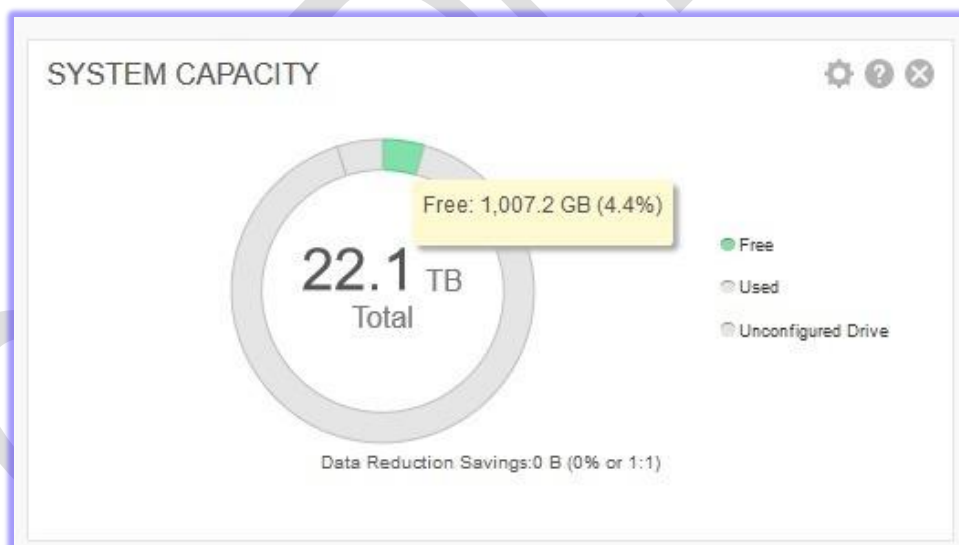
● COMPLETED

● IN PROGRESS

● PENDING

18. Pending Decision

No.	Activity Details	Status / Remarks
01	Disaster Recovery on Cloud. <ul style="list-style-type: none"> Restoration of Current Backed up Data to Cloud 	Decision Pending.
02	HP Store Once Renewal (Backup Storage) <ul style="list-style-type: none"> Contract is already expired 	Decision Pending.
03	EMC Storage Capacity <ul style="list-style-type: none"> ONLY 1 TB Space is available. 	Post Approval, we can ask supplier to submit the quotation.
04	Web Application Firewall	PoC Completed. Technical report is submitted



19. DARKWEB Monitoring



20. Dark web Monitoring

Cybersquatting Risk

During the monthly dark web monitoring assessment we identified following 6 domains that creates Cybersquatting Risk for Customer.

1. [Spamming Domain)
2. [Domain is for sale)
3. [Spamming Domain)
4. (looks genuine but still team will look into
5. [spamming Domain)

A well-protected domain name is certainly immensely helpful for security, worldwide prominence, and profitability of a business, quite like an internationally protected trademark or service mark. Hence, proper registration and protection of both the trademark and domain name are advisable and imperative. Infopercept recommends Customer to register its website [www](#) Trademark or Servicemark

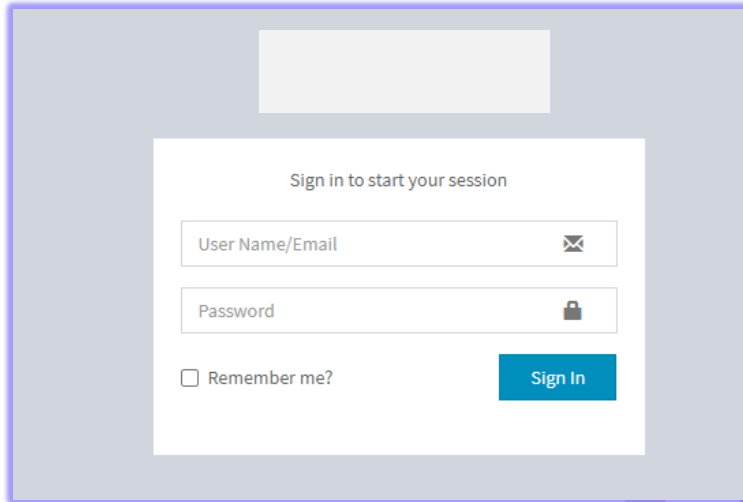
Email Address Compromise Risk

During the monthly dark web monitoring assessment we identified 4 email address that creates compromise risk for Customer.

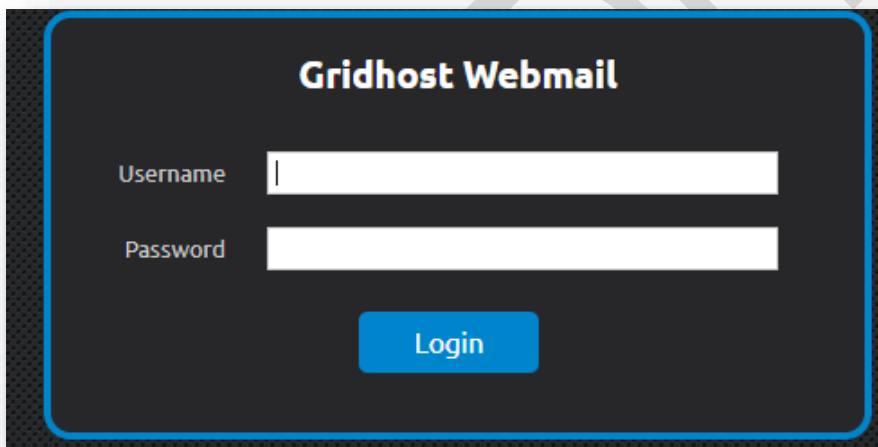
- [LinkedIn, Spambot]
- [onliner spambot]
- [Adobe, onliner spambot]
- [onliner spambot, canva]

Email Address Compromise Risk

During our Dark web Scan we have observed that webmail portal and Portal is accessible publicly which can lead to Brute force or Dictionary Attack.



A screenshot of a webmail login interface. At the top, there is a grey rectangular box. Below it, the text "Sign in to start your session" is centered. There are two input fields: "User Name/Email" with an envelope icon on the right, and "Password" with a lock icon on the right. Below the password field is a checkbox labeled "Remember me?". To the right of the checkbox is a blue button labeled "Sign In".



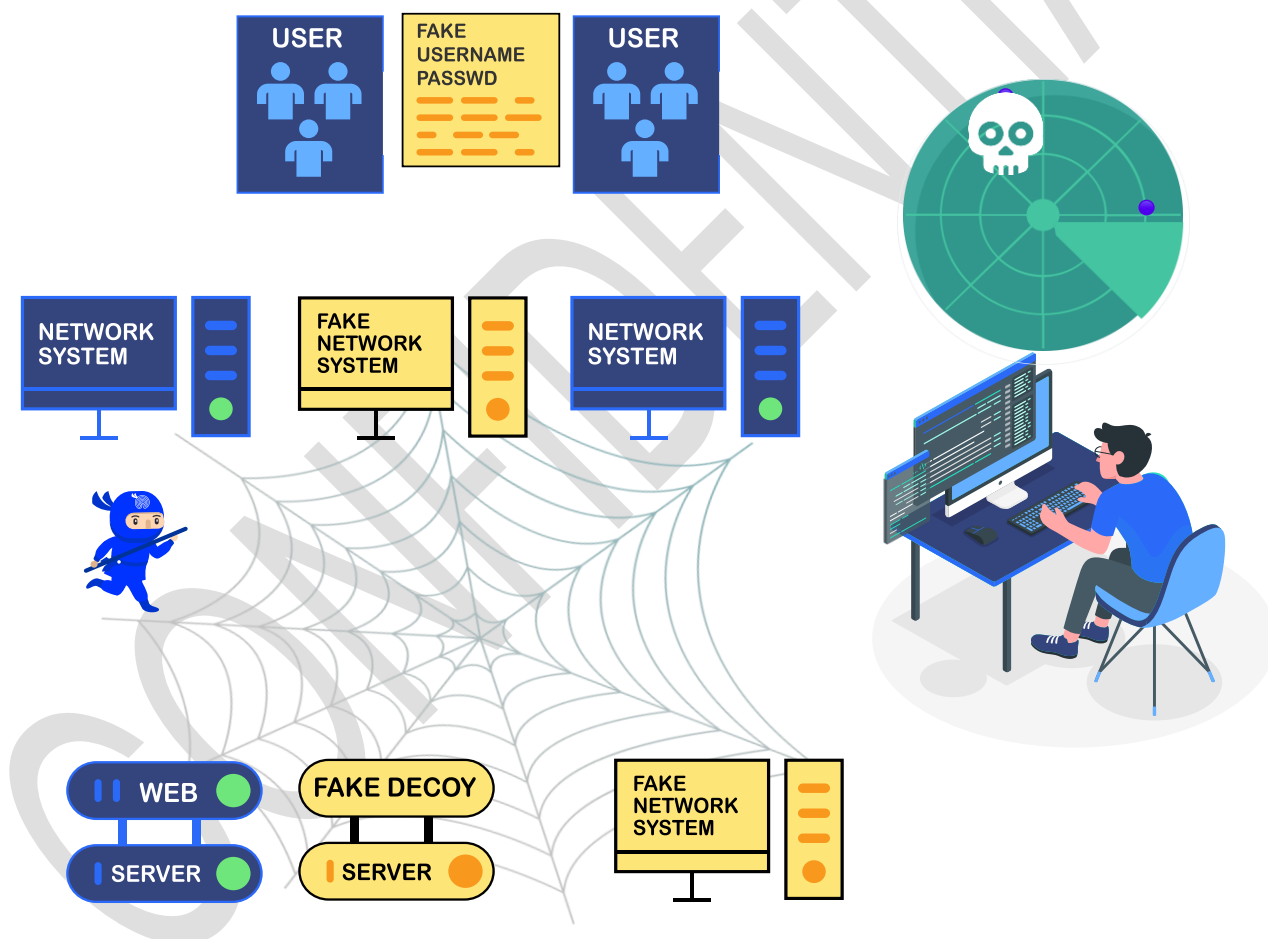
A screenshot of the "Gridhost Webmail" login interface. The title "Gridhost Webmail" is at the top in white text on a dark background. Below the title are two input fields: "Username" and "Password". Below these fields is a blue button labeled "Login".

21. What Next?

- Dark Web Monitoring for All the Domains
- Implementation of Open-Source **Deception Technology** within the Network.
- Implementation of Open Source **SIEM Solution**.

Have Shared the pre-requisites with David to Initiate the Installation.

Reduced False Positives



Personalized Threat Intelligence

About INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

Imprint

© Infopercept Consulting Pvt. Ltd. 2021

Publisher

H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info

M: +91 9898857117

W: www.infopercept.com

E : sos@infopercept.com

Global Offices

UNITED STATES OF AMERICA

+1 516 713 5040

UNITED KINGDOM

+44 2035002056

SRI LANKA

+94 702 958 909

KUWAIT

+965 6099 1177

INDIA

+91 9898857117

By accessing/ proceeding further with usage of this platform / tool / site / application, you agree with the Infopercept Consulting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions, kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.

