



Technology Optimization Center Monthly Sample Report



This document is a highly confidential which contains all the information regarding the red team engagement that was done by Infopercept Team on ABC Company.

Table of Contents

Copyright

| | |
|---|----|
| Disclaimer | 4 |
| 1.Request Volume Trend | 5 |
| 2.Average Resolution Time (Month wise) | 5 |
| 3. SLA Compliance Vs Breached Trend – Technician | 5 |
| 4.Site wise Request | 6 |
| 5.Email Statistics | 6 |
| 6.DMARC Compliance - Email Volume..... | 6 |
| 7.DMARC Compliance - Email Rejection – Threat Protection | 7 |
| 8.DMARC Compliance - Email Rejection – Threat Protection | 8 |
| 9.Proactive Measure Taken | 9 |
| 20+ blacklisted IPs were blocked on Firewall, Phishing Sender ID were blocked on Office 365 tenants | 9 |
| 10.Proactive Measure Taken | 10 |
| Monitor Failed Login Attempts and Blocking them | 10 |
| 11.Endpoints – Morphisec..... | 10 |
| 3 Attacks prevented by Windows Defender | 10 |
| 3 Attacks prevented by Windows Defender | 10 |
| 12.Endpoints – Symantec | 11 |
| Identify Computer at Risk and Run Full Scan on the System. | 11 |
| 13.ESET – End Point Security for Windows 7 | 11 |
| 14.Web Site Status | 12 |
| 15.On Going Activities..... | 12 |
| 16.On Going Activities_contd..... | 13 |
| 17.Current Project Status | 13 |
| 18.Pending Decision | 14 |
| 19.DARKWEB Monitoring | 15 |
| 20 Dark web Monitoring | 15 |
| Cybersquatting Risk | 15 |
| Email Address Compromise Risk | 16 |
| Email Address Compromise Risk | 16 |
| 21. What Next? | 17 |

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.

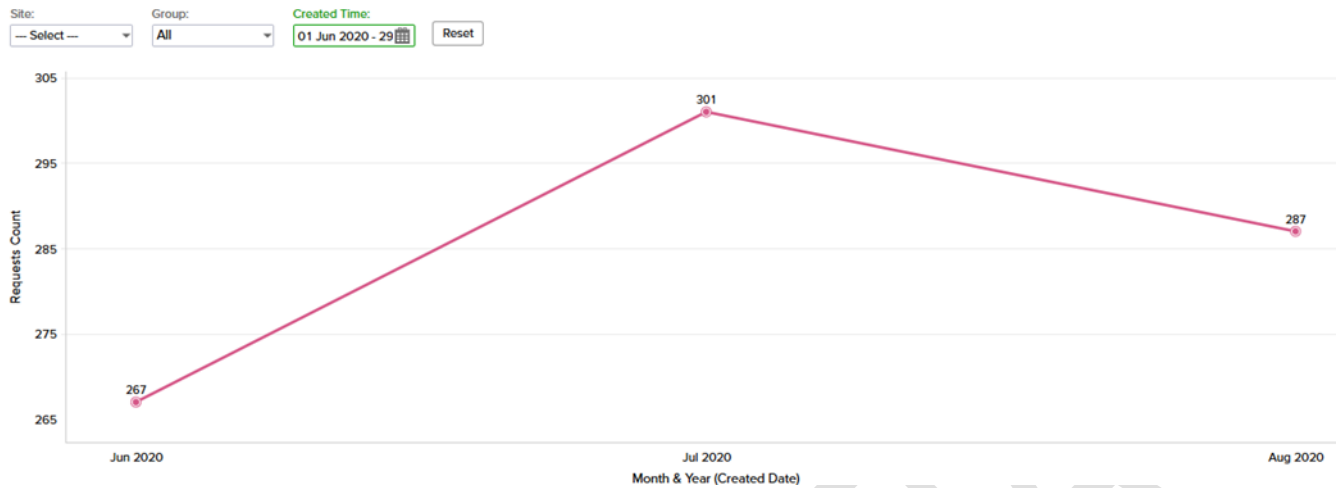


Disclaimer

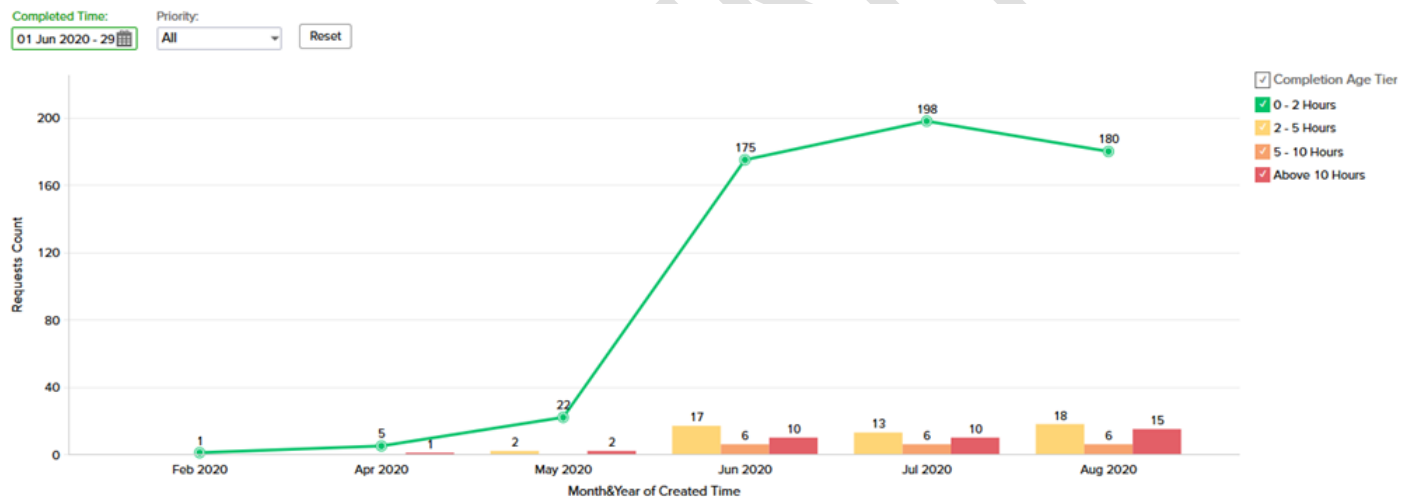
By accessing and using this report you agree to the following terms and conditions and all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property 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.



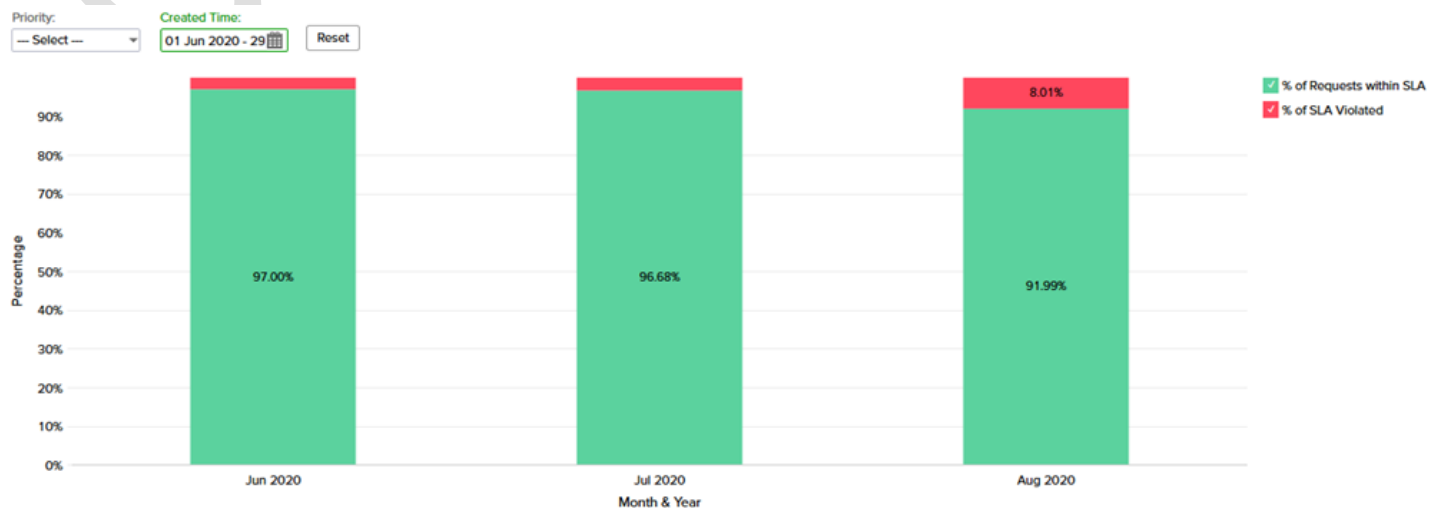
1. Request Volume Trend



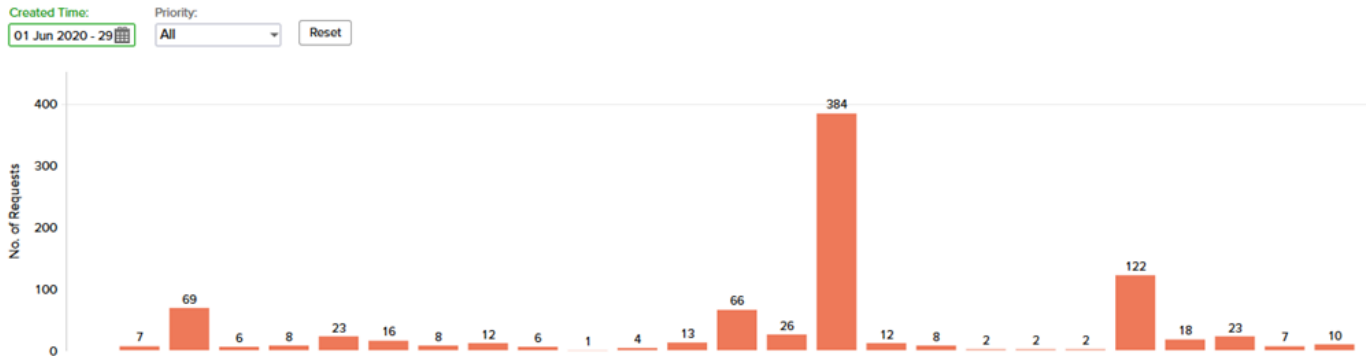
2. Average Resolution Time (Month wise)



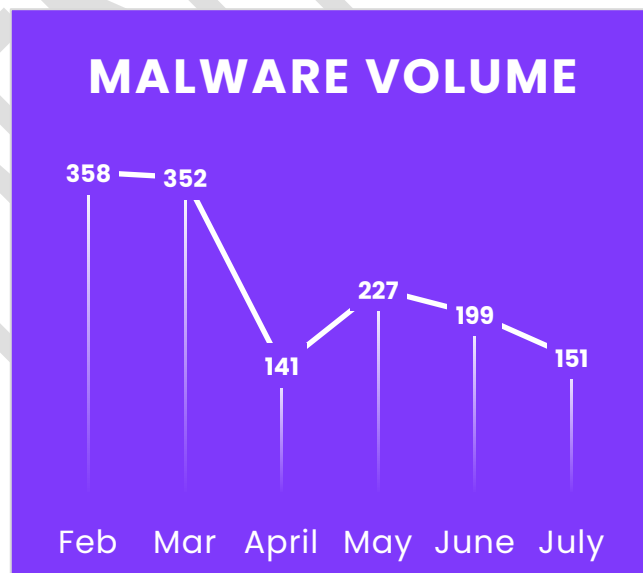
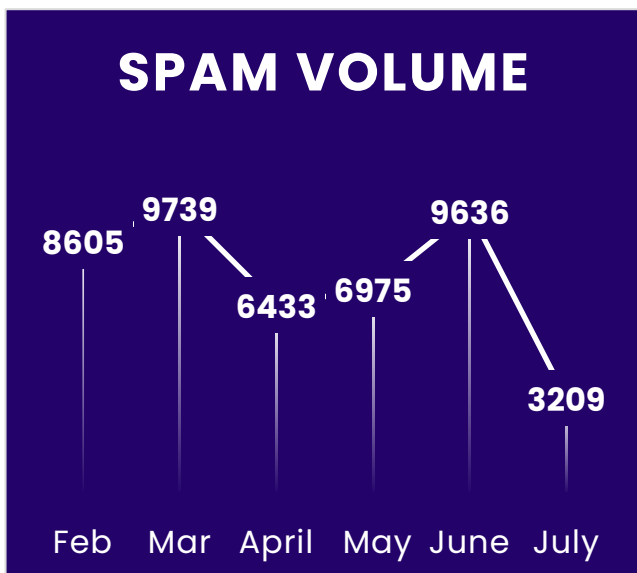
3. SLA Compliance Vs Breached Trend – Technician



4.Site wise Request



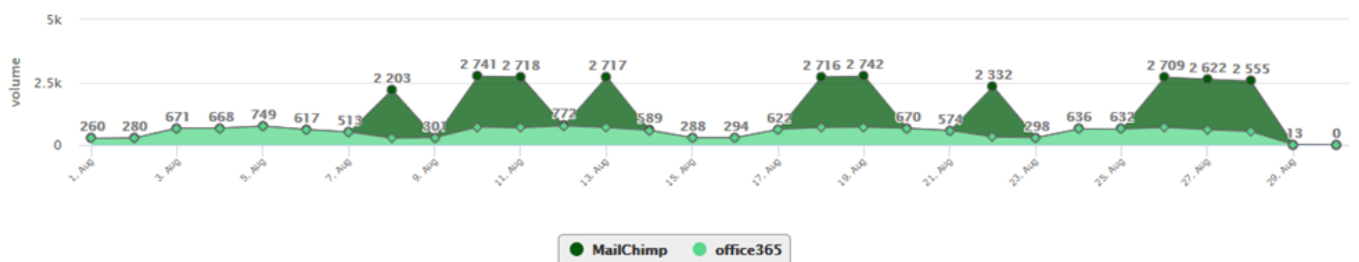
5.Email Statistics



6.DMARC Compliance - Email Volume

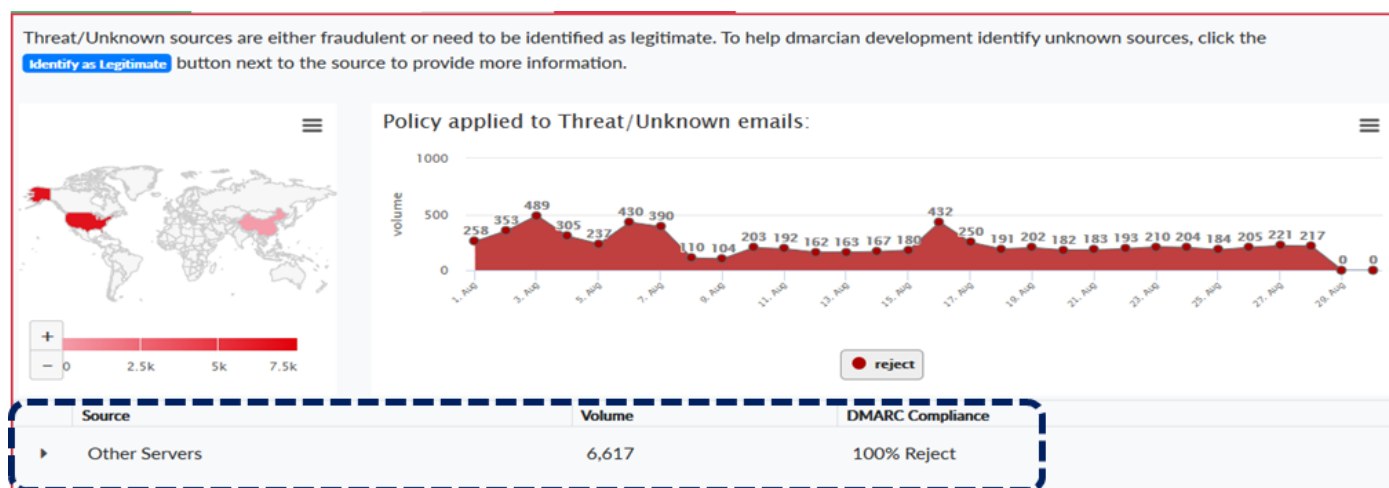
DMARC Capable can send DMARC compliant email. Technical staff can attend to your organization's servers. External emailers listed here can send DMARC compliant email.

DMARC Capable by Email Volume

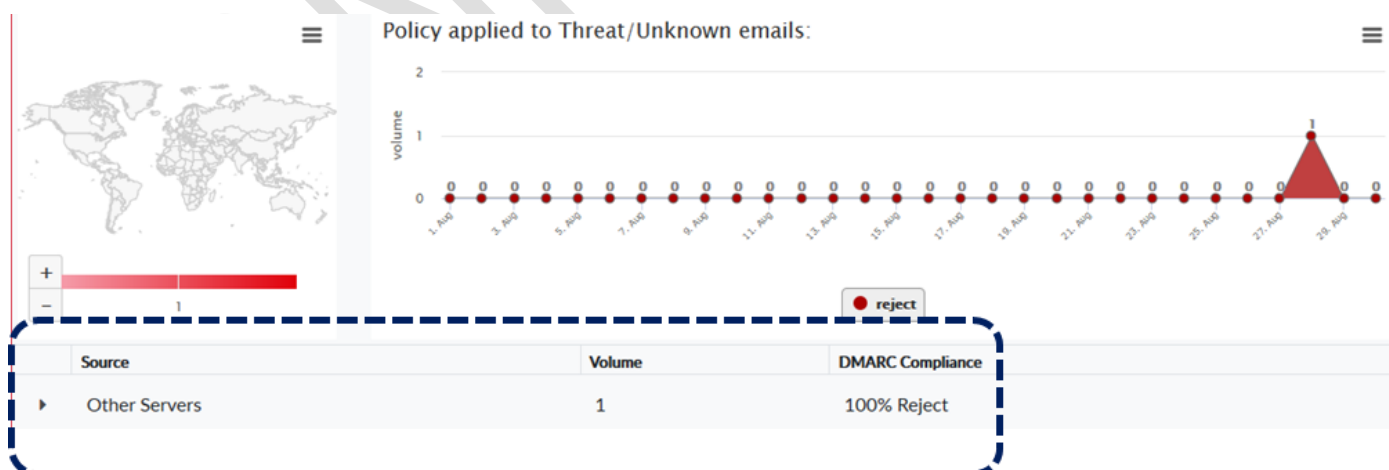


| Source | Volume | DMARC Compliance | SPF Alignment | DKIM Alignment |
|----------------------|--------|------------------|---------------|----------------|
| MailChimp | 20,205 | 100% | SPF Incapable | DKIM 100% |
| Microsoft Office 365 | 15,297 | 100% | SPF 100% | DKIM 99.84% |

7.DMARC Compliance - Email Rejection – Threat Protection

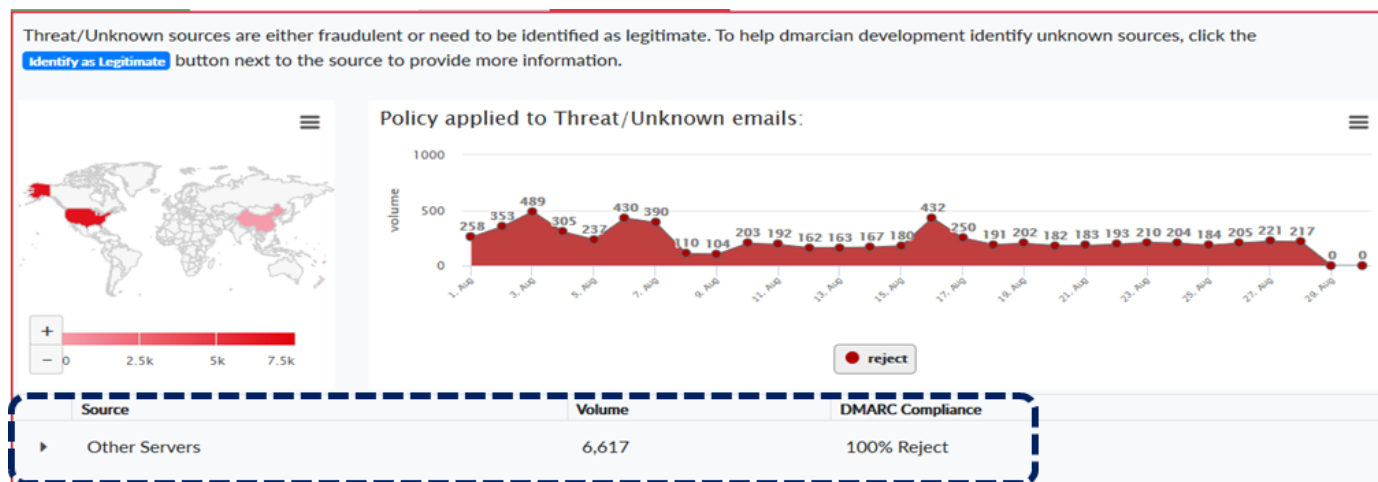


| Server Name | Country | From: domain count | Message count |
|------------------|---------|--|---------------|
| *.nikiz.com | | Identify as Legitimate | 1 |
| nxdomain | | 1 | 4 |
| *.mia.bi | | Identify as Legitimate | 1 |
| *.163data.com.cn | | Identify as Legitimate | 1 |

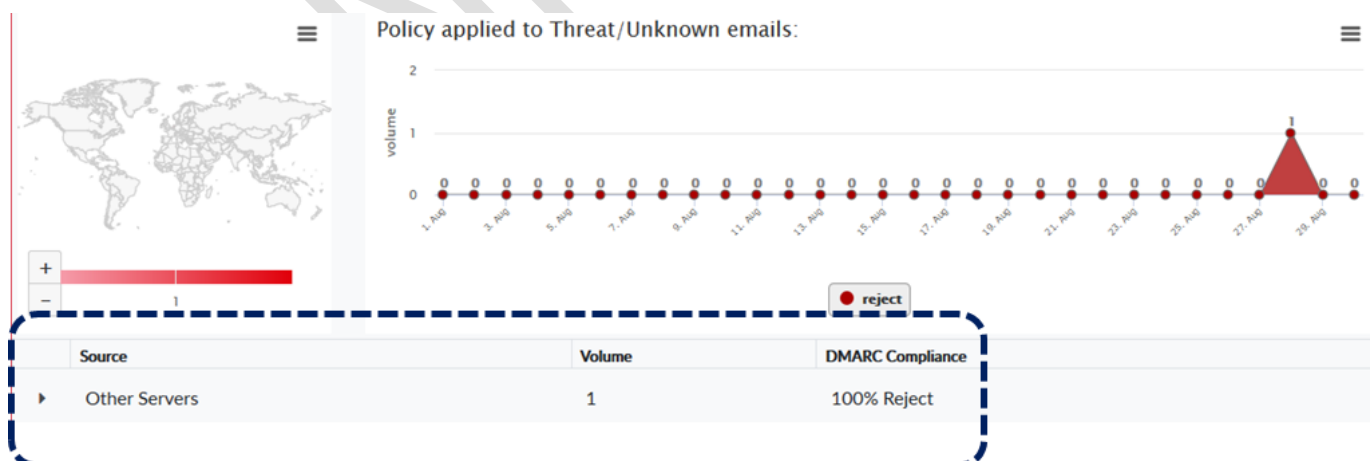


| Server Name | Country | From: domain count | Message count |
|--------------|---------|--|---------------|
| *.nubilus.nl | | Identify as Legitimate | 1 |

8. DMARC Compliance - Email Rejection – Threat Protection



| 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 agroserv@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 notificacionssl@mejiayasociadosab r-fukada@nomura-kensetsu.co.jp contato@bissoliferramentas.com arief.rahmadiansyah@dieselone.co.3</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 mrodgers@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 expont@tccsun.com</p> |
|--|--|---|

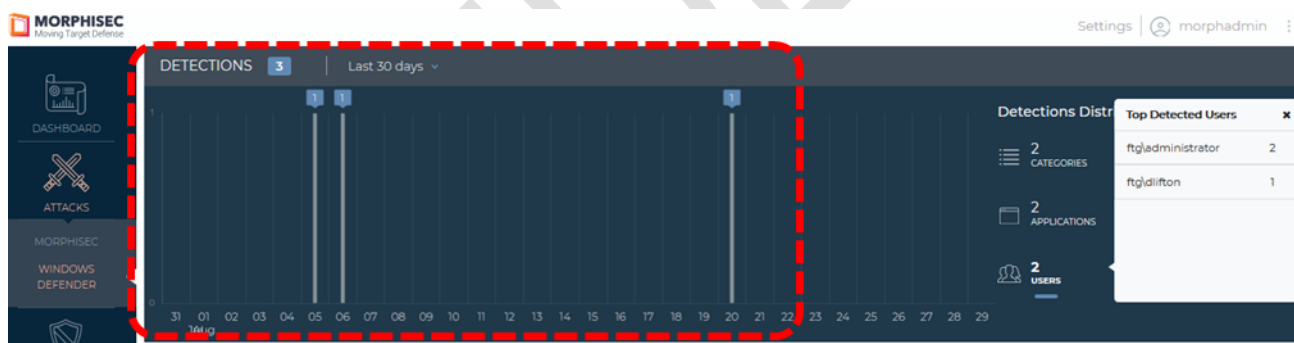
10.Proactive Measure Taken

Monitor Failed Login Attempts and Blocking them

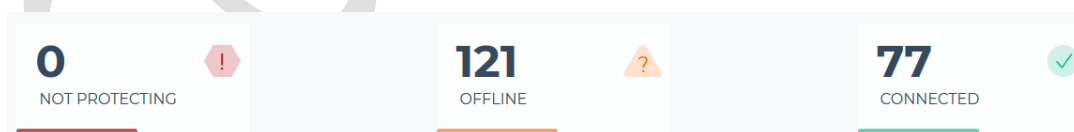
| | | | | |
|-----------------------|----------|---------------------|---------|----------------|
| 8/28/2020, 4:59:13 PM | 973bf1b: | Office 365 Exchange | Failure | 115.84.112.138 |
| 8/28/2020, 4:57:00 PM | 4335999 | Office 365 Exchange | Failure | 72.221.232.144 |
| 8/28/2020, 4:56:55 PM | cb17a8a: | Office 365 Exchange | Failure | 72.221.232.144 |
| 8/28/2020, 4:52:28 PM | a109235 | Office 365 Exchange | Failure | 191.97.1.40 |
| 8/28/2020, 4:52:24 PM | a259067 | Office 365 Exchange | Failure | 191.97.1.40 |
| 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

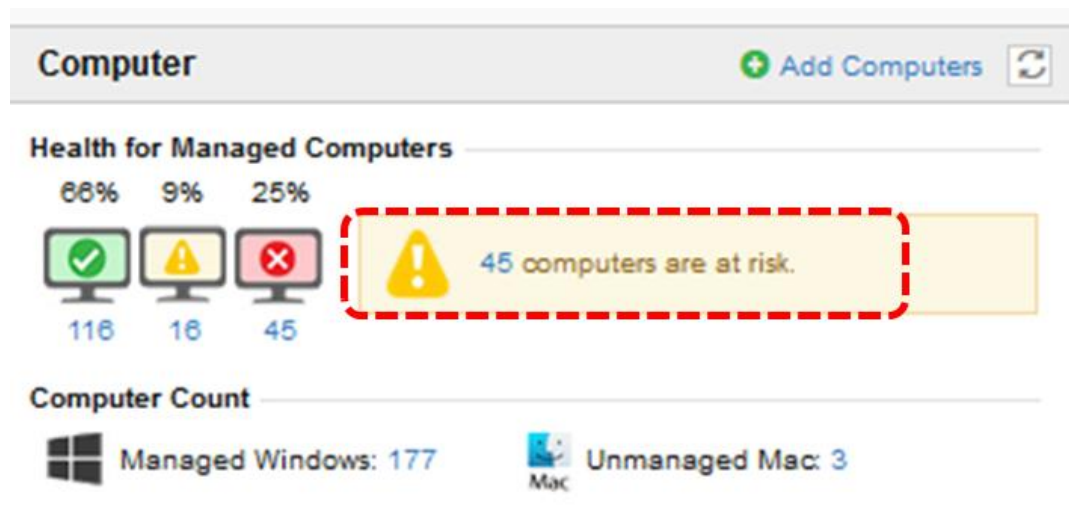


155 Clients till July



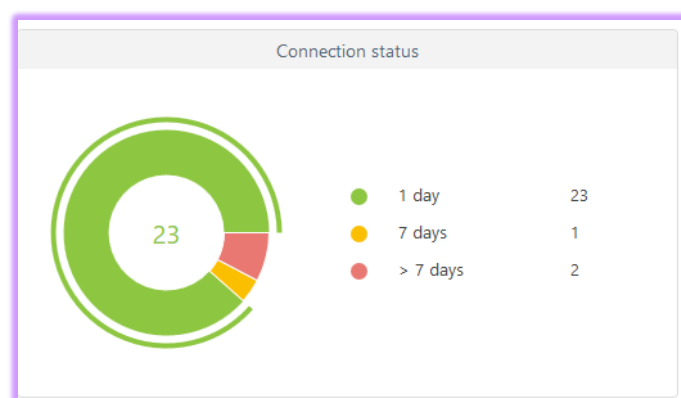
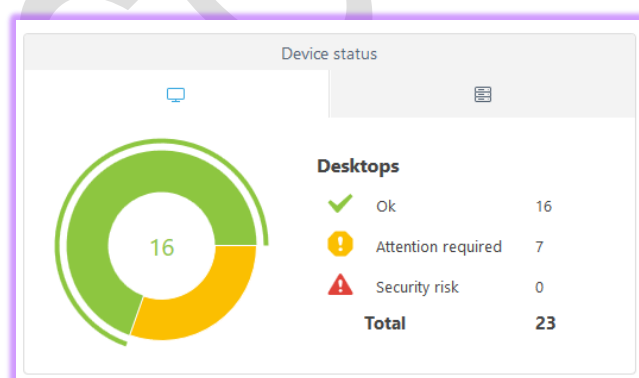
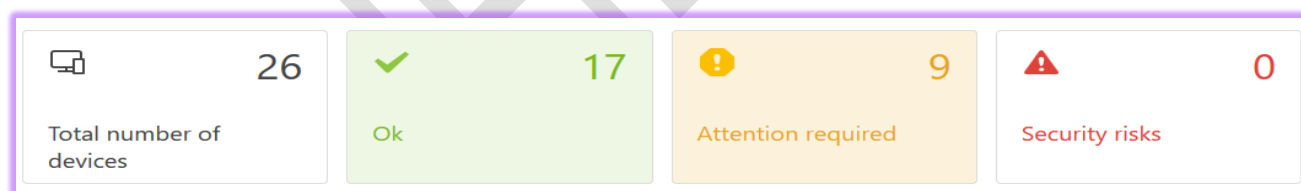
12.Endpoints – Symantec

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

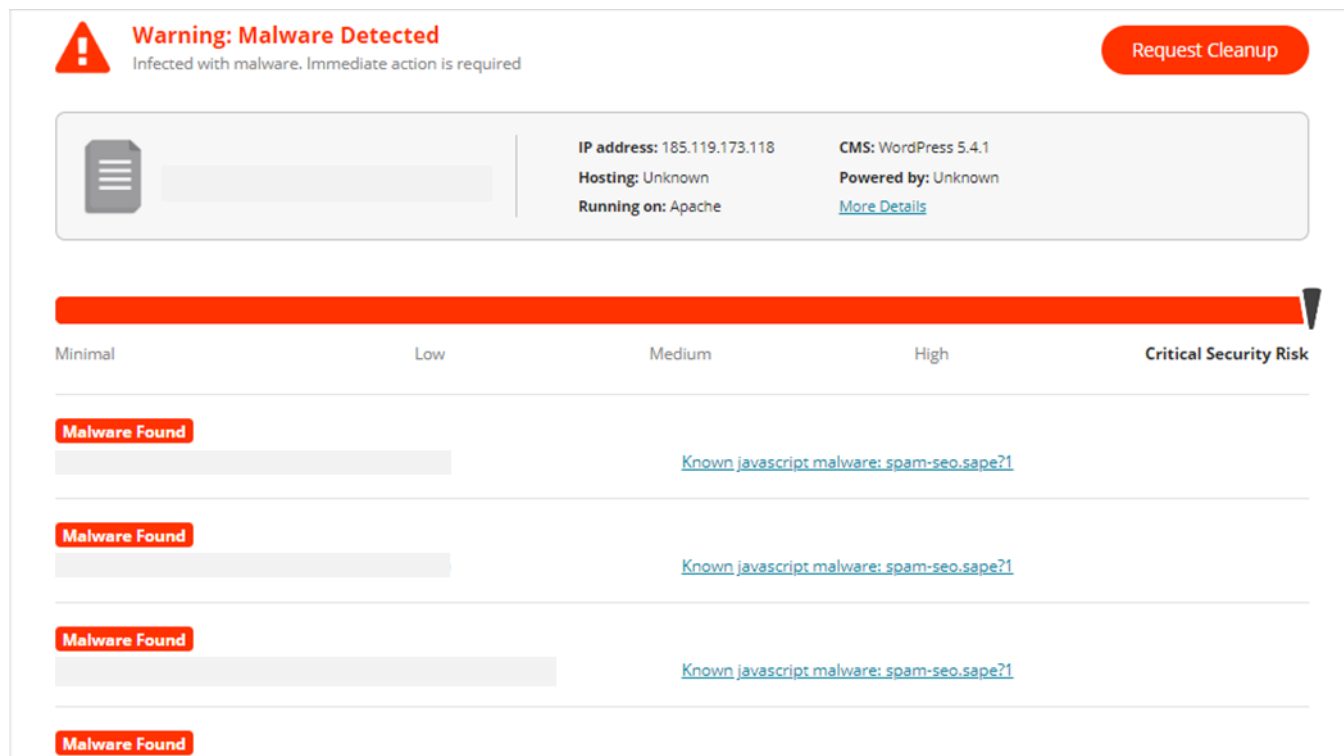


| Top Risks Detected | | |
|--------------------|------------------|------------|
| Severity | Name | Detections |
| Information | Tracking Cookies | 16 |

13.ESET – End Point Security for Windows 7



14. Web Site Status



15. On Going Activities

| No. | Activity Details | SITE A | SITE B |
|-----|--|--------|--------|
| 01 | Fine Tune Folder Rights All shared folder rights being fine-tuned according to the current user department and role. | ● | ● |
| 02 | Active Directory user and groups' monitor 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 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 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 Removed the suspicious malware files based on the alerts we received from Firewall and Antivirus (Symantec) Software. | ● | ● |
| 06 | Windows updates for all locations All security and critical updates will be pushed to all the computers in every single location. | ● | ● |
| 07 | Application Server Backup Issue. APP03 Server backup is happening with Warning State. | ● | ● |
| 08 | Website Restriction Policies 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 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 perform weekly checks of our important websites and document them with ticket | ● | ● |
| 11 | Email security and monitoring 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 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 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 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 | 2 FA On O365 Office 365 for charity was activated with help from Microsoft | ● | ● | |
| 04 | Morphisec Client Roll out | ● | ● | 198 out of 200 Lic. Installed. |
| 05 | ESET AV For Windows 7 | ● | ● | 26 /42 Lic. installed |
| 06 | SPICEWORKS (Inventory Management Tool) | ● | ● | |
| 07 | Web Application Firewall for Online Portal | ● | ● | |
| 08 | Security Assessment of Portal | ● | ● | |
| 09 | Server Consolidation | ● | ● | |

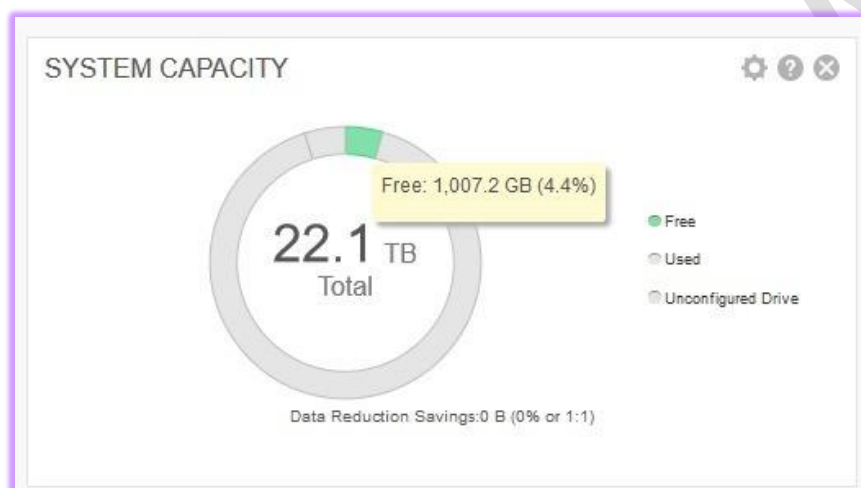
● COMPLETED

● IN PROGRESS

● PENDING

18.Pending Decision

| No. | Activity Details | Status / Remarks |
|-----|---|---|
| 01 | Disaster Recovery on Cloud. Restoration of Current Backed up Data to Cloud | Decision Pending. |
| 02 | HP Store Once Renewal (Backup Storage) Contract is already expired | Decision Pending. |
| 03 | EMC Storage Capacity 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

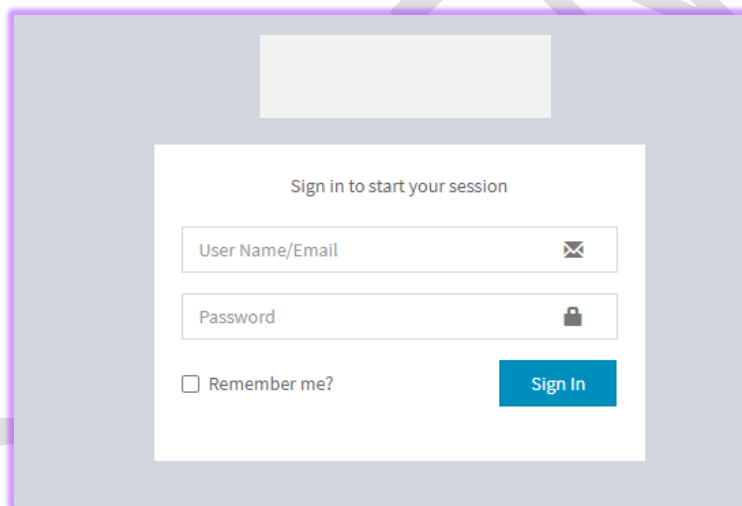
Email Address Compromise Risk

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

- [redacted] LinkedIn, Spambot]
- [redacted] [onliner spambot]
- [redacted] [Adobe, onliner spambot]
- [redacted] [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.



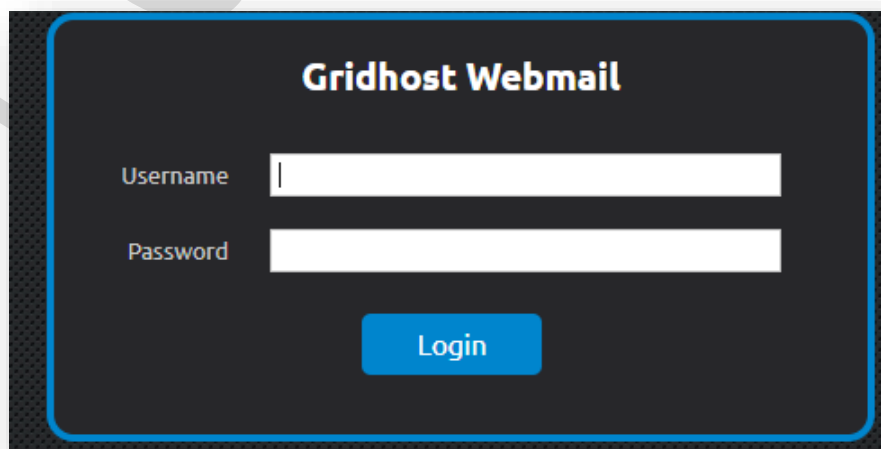
Sign in to start your session

User Name/Email

Password

☐ Remember me?

Sign In



Gridhost Webmail

Username

Password

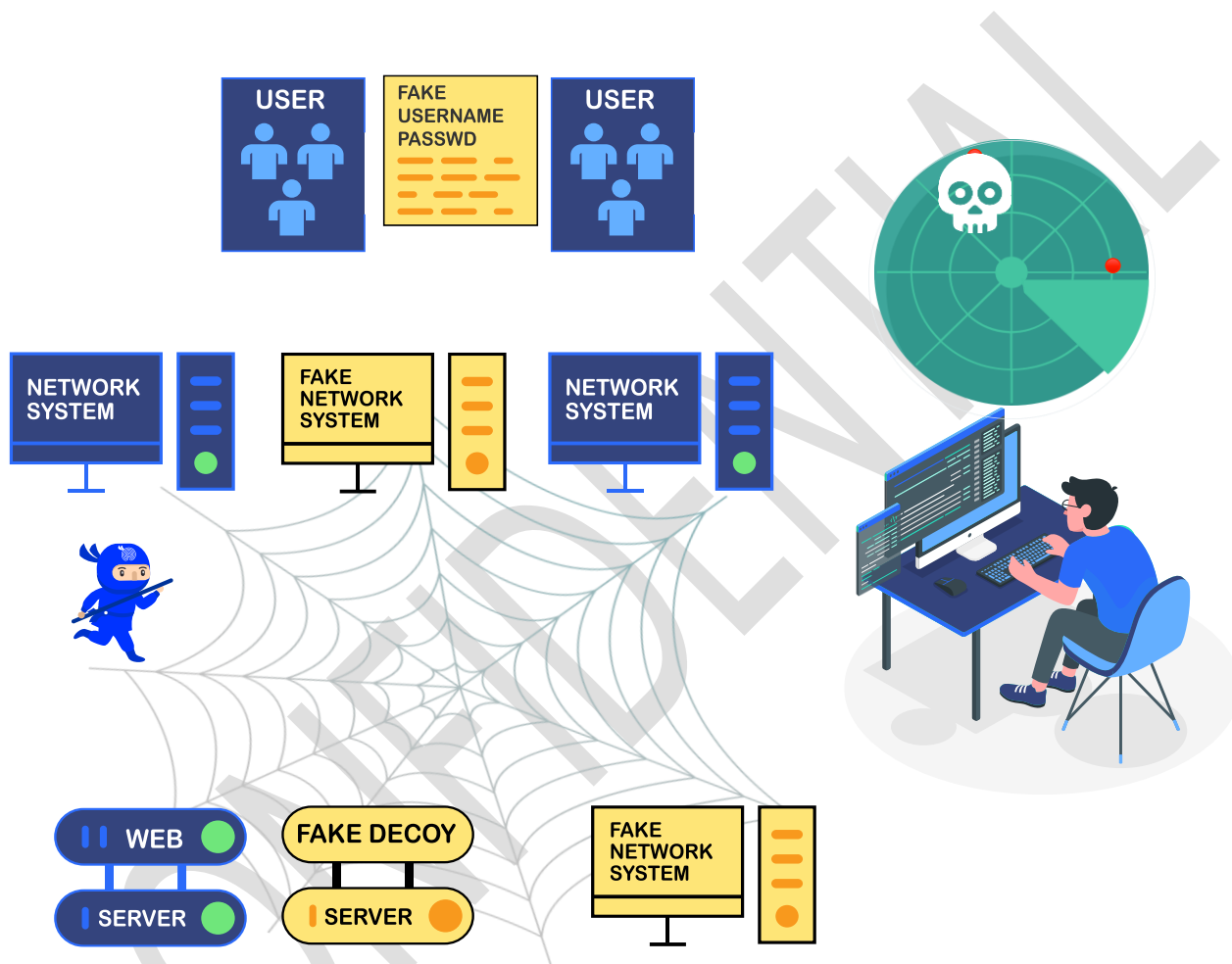
Login

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



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.

Imprint

© Infopercept Consulting Pvt. Ltd.

Created Date

Oct 2023

Contact Detail

sos@infopercept.com

www.infopercept.com/sample-report