SECURITY ASSESSMENT FOR XXX

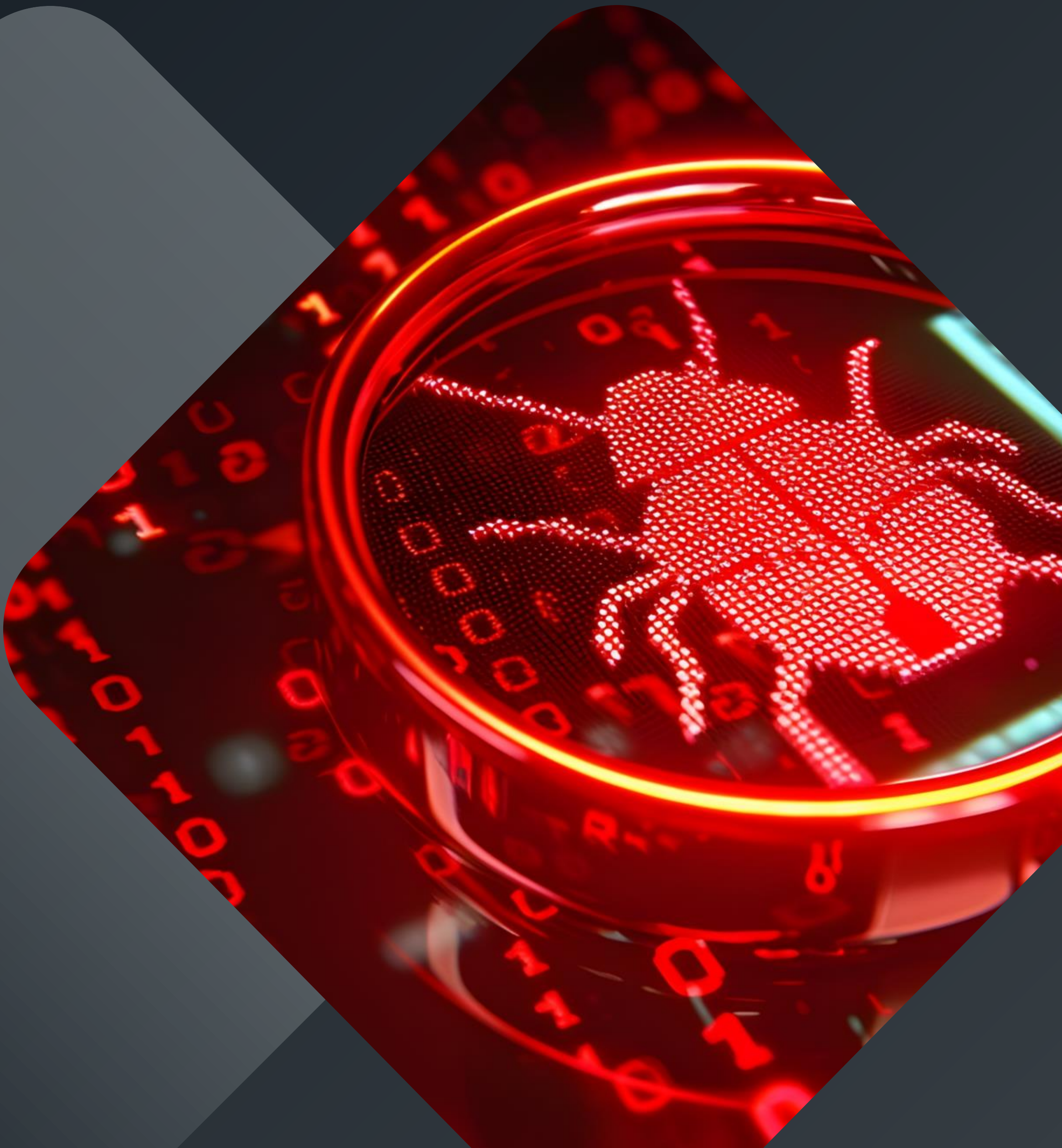
Date: 8. Oct 2024

CONTENTS

The Infoblox Security Assessment analyzes DNS traffic to deliver comprehensive visibility into potential threats and risks associated with all network assets and communication with malicious domains, high-risk applications and content.

BACK TO CONTENTS

EXECUTIVE SUMMARY



BACK TO CONTENTS

EXECUTIVE SUMMARY

KEY FINDINGS AND RISKS

CRITICAL
40.7K

HIGH-RISK EVENTS

Number of malicious domains accessed

CRITICAL
>300K

HIGH-RISK WEBSITES

Illegal or policy-violating sites associated with potential data theft and other risks

HIGH
1.5k

DGAs

Domain Generation Algorithms

HIGH
387

LOOKALIKE DOMAINS

Hit on Look A Like Domains

288

ZERO DAY DNS

Domains registered and launched within a small window – typically indicative of spearphishing

36k

SUSPICIOUS DOMAINS

Detected domains that are likely to be used in a future malicious campaign

RECOMMENDATIONS TO MITIGATE RISK

- Enable blocking of detected malicious and suspicious domains for proactive protection
- Add custom lookalike domain monitoring and Infoblox Domain Mitigation service to address brand reputation risks if required
- Leverage SOC Insights to reduce the number of security events, surfacing critical and actionable threats

Domain takedown within 24 hours

50% alert reduction on EDR and NGFW

Up to 500 SOC Hours Saved

63 days avg Proactive protection

SECURITY INDICATOR SUMMARY

Your DNS traffic has been reviewed over the past 30 days, uncovering the following:

18.1M
DNS Requests

Total volume of individual requests/traffic analyzed

40.7k
High-Risk Events

Number of high-risk malicious domains accessed

0
Medium-Risk Events

Number of medium-risk malicious domains accessed

16
Insights

Actionable insights based on aggregated and correlated security event data

6
Custom Lookalike Domains

Created to impersonate your brand for malicious purposes

9k
DoH

DNS over HTTPS (DoH) is encrypted traffic, which can hide malicious activity

288
Zero Day DNS

Domains registered and launched within a small window – typically indicative of spearphishing

36k
Suspicious Domains

Detected domains that are likely to be used in a future malicious campaign

22.9k
Newly Observed Emergent Domains

A type of, domain that has only recently been observed within customer traffic.

1.5k
Domain Generated Algorithms

Indicative that malware exists and is looking to communicate "home"

0
DNS Tunneling

DNS tunneling can be indicative of data exfiltration or C2

89
Unique Applications

Number of applications to verify against sanctioned list

300k
High-Risk Web Categories

Illegal or policy-violating sites associated with potential data theft and other risks

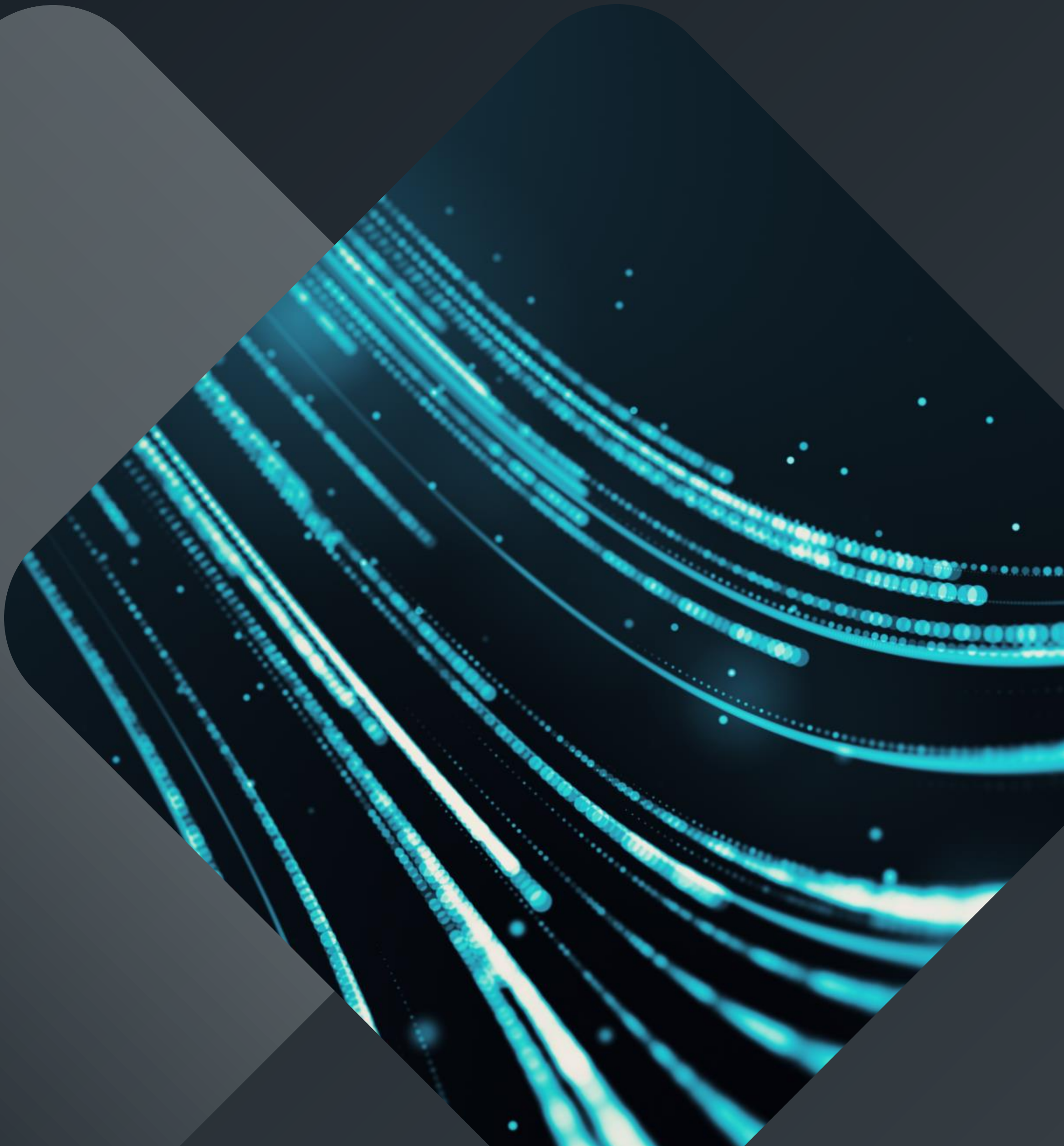
4
Threat Actors

Known DNS threat actors detected with activity in your network

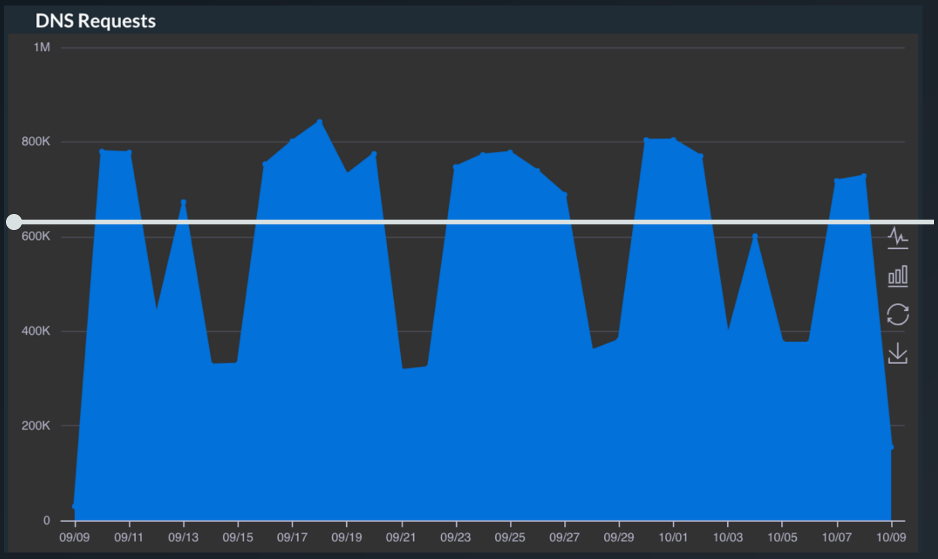
1.6k events per day on avg.

The number of requests in total (1. Pos) shows the importance of the DNS protocol for the IT infrastructure and the unique vantage point for visibility and security

TRAFFIC USAGE ANALYSIS



TRAFFIC USAGE ANALYSIS

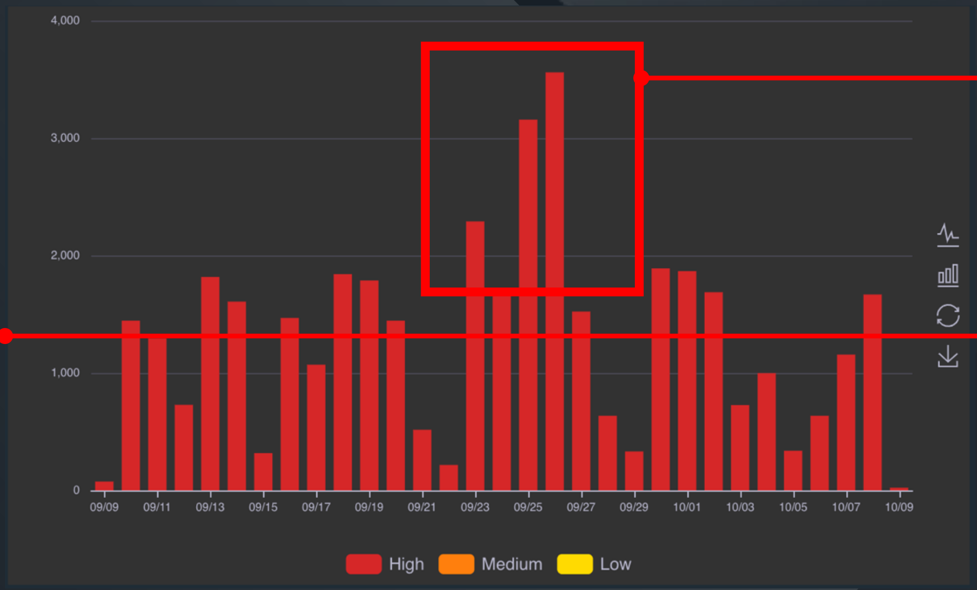


requests/day avg. 603k

The visualization shows an expected drop during the weekends.
> Investigation recommended if unexpected increases are occurring.

The amount of DNS request in total pointing out the core network functionality of the protocol for the organization.

TRAFFIC USAGE ANALYSIS



Increase of High-Risk Events

Avg. 1.3k Firewall Events per day

The average of 1.3k events per day which got blocked over the last month aligns with expected low false positive rate of the threat intelligence service Infoblox offers with no impact on the daily business and easy to manage user experience.

BACK TO CONTENTS

KEY INSIGHTS

BACK TO CONTENTS

KEY INSIGHTS

All security events are aggregated, correlated, analyzed, and extrapolated into actionable, prioritized insights.

SUMMARY

INSIGHT SEVERITY

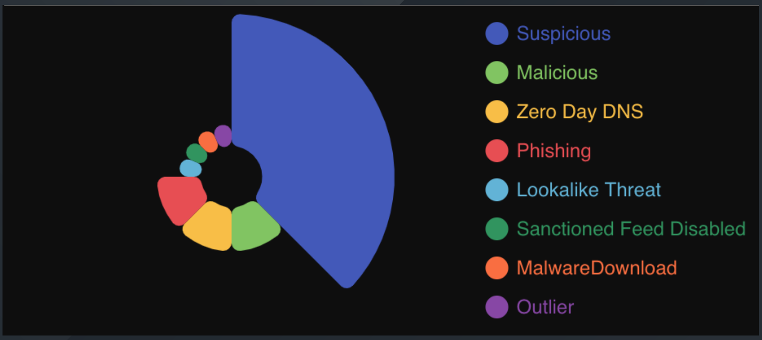
16
Total Open Insights

12
Medium Priority Insights

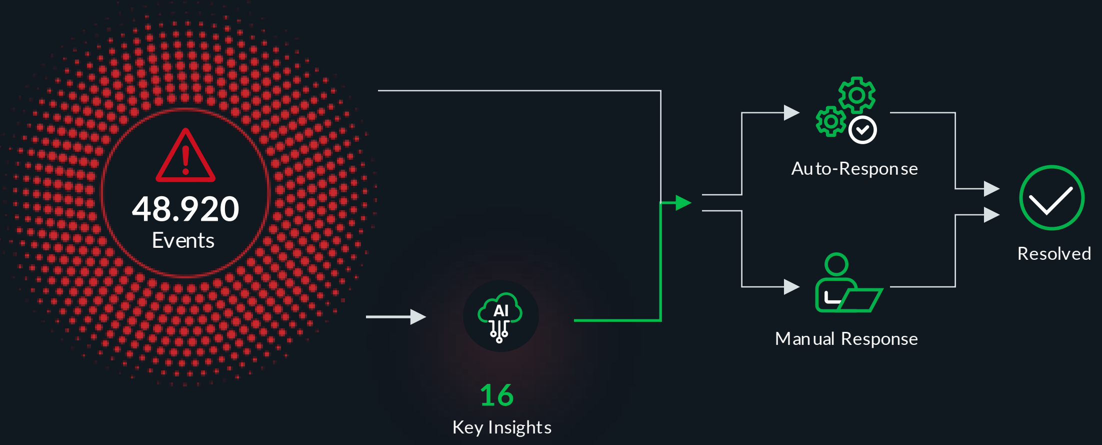
1
High Priority Insights

1
Critical Priority Insights

INSIGHT DISTRIBUTION BY THREAT TYPE

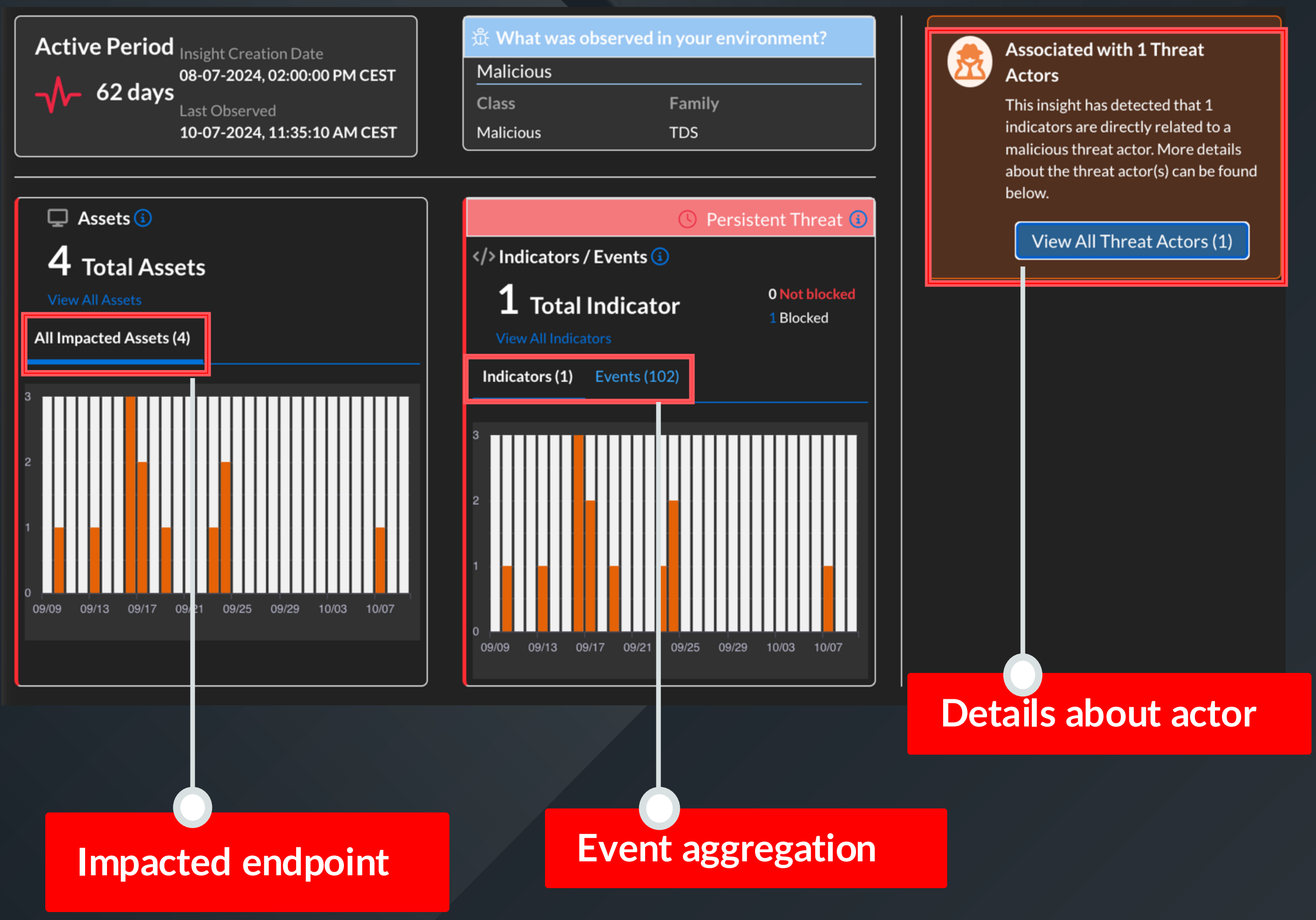


EVENT TO INSIGHT AGGREGATION



BACK TO CONTENTS

MALICIOUS INSIGHT DETAILS



Active Period
62 days
Insight Creation Date
08-07-2024, 02:00:00 PM CEST
Last Observed
10-07-2024, 11:35:10 AM CEST

What was observed in your environment?
Malicious

Class	Family
Malicious	TDS

Associated with 1 Threat Actors

This insight has detected that 1 indicators are directly related to a malicious threat actor. More details about the threat actor(s) can be found below.

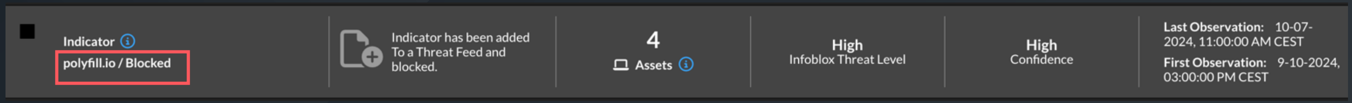
Assets
4 Total Assets

Persistent Threat
Indicators / Events
1 Total Indicator
0 Not blocked
1 Blocked

Details about actor

Impacted endpoint

Event aggregation



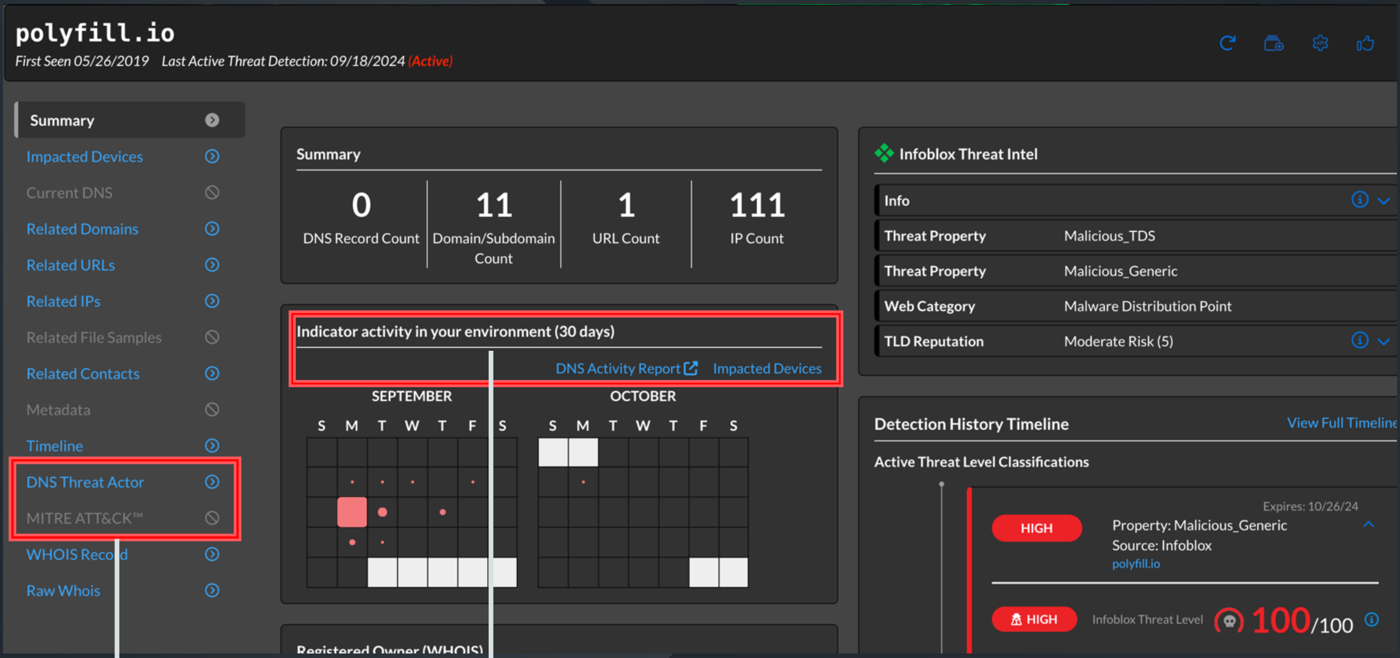
Indicator polyfill.io / Blocked	Indicator has been added To a Threat Feed and blocked.	4 Assets	High Infoblox Threat Level	High Confidence	Last Observation: 10-07-2024, 11:00:00 AM CEST First Observation: 9-10-2024, 03:00:00 PM CEST

SOC Insights supports a guided threat investigation process to quickly answer the imported key asks.

Other included features in the Bloxone Threat Defense product suite supports further the investigation process. (TIDE & Dossier – s. next page)

DOSSIER

An integrated threat research portal to look up Indicators of Compromise (IoC). Can also be used for example to look up IoCs of other infrastructure/security systems.



polyfill.io

First Seen 05/26/2019 Last Active Threat Detection: 09/18/2024 (Active)

Summary

0	11	1	111
DNS Record Count	Domain/Subdomain Count	URL Count	IP Count

Indicator activity in your environment (30 days)

DNS Activity Report · Impacted Devices

Registered Owner (WHOIS)

Infoblox Threat Intel

Info	
Threat Property	Malicious_TDS
Threat Property	Malicious_Generic
Web Category	Malware Distribution Point
TLD Reputation	Moderate Risk (5)

Detection History Timeline · View Full Timeline

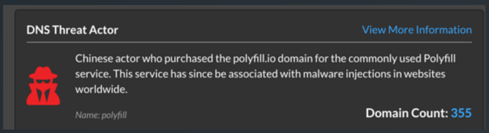
Active Threat Level Classifications

HIGH · Expires: 10/26/24 · Property: Malicious_Generic · Source: Infoblox · polyfill.io

HIGH · Infoblox Threat Level 100/100

If an IoC is linked to an Advanced Persitend Threat (APT) or Threat Actor the avialble information are easy to access to get more information about the Tactics, Techniques, and Procedures (TTPs).

Shows frequenz of access attempts in your enviorment and allow to pull a direct report about impacted devices

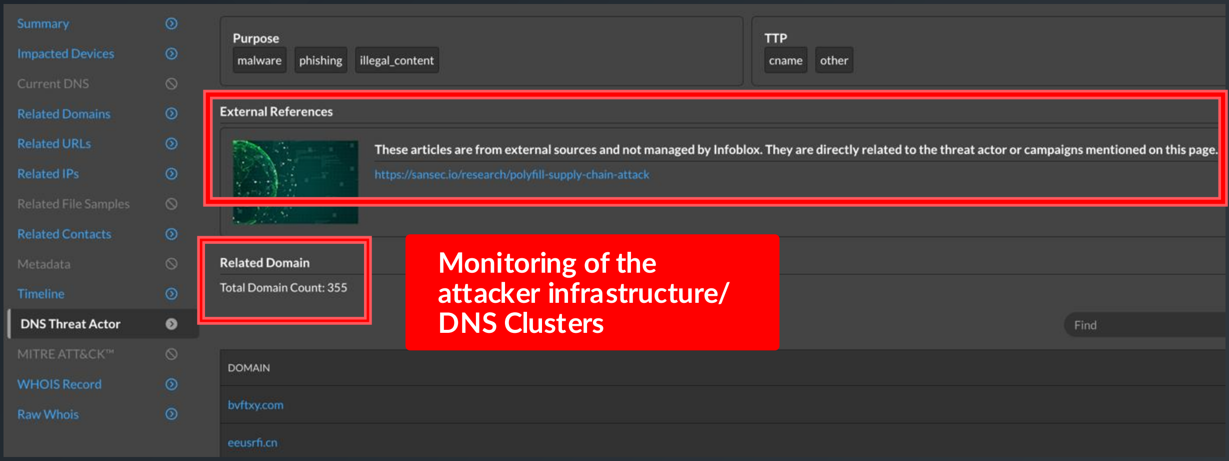


DNS Threat Actor · View More Information

Chinese actor who purchased the polyfill.io domain for the commonly used Polyfill service. This service has since be associated with malware injections in websites worldwide.

Name: polyfill

Domain Count: 355



Purpose: malware · phishing · illegal_content

TTP: cname · other

External References

These articles are from external sources and not managed by Infoblox. They are directly related to the threat actor or campaigns mentioned on this page.

https://sansec.io/research/polyfill-supply-chain-attack

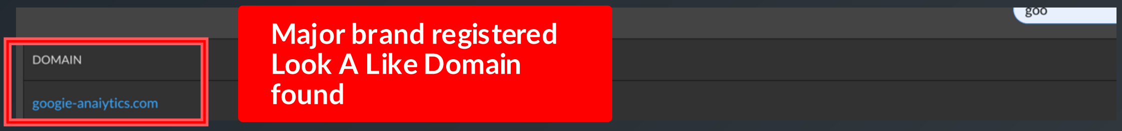
Related Domain

Total Domain Count: 355

Monitoring of the attacker infrastructure/ DNS Clusters

Find

DOMAIN
bvftxy.com
eeusrfi.cn



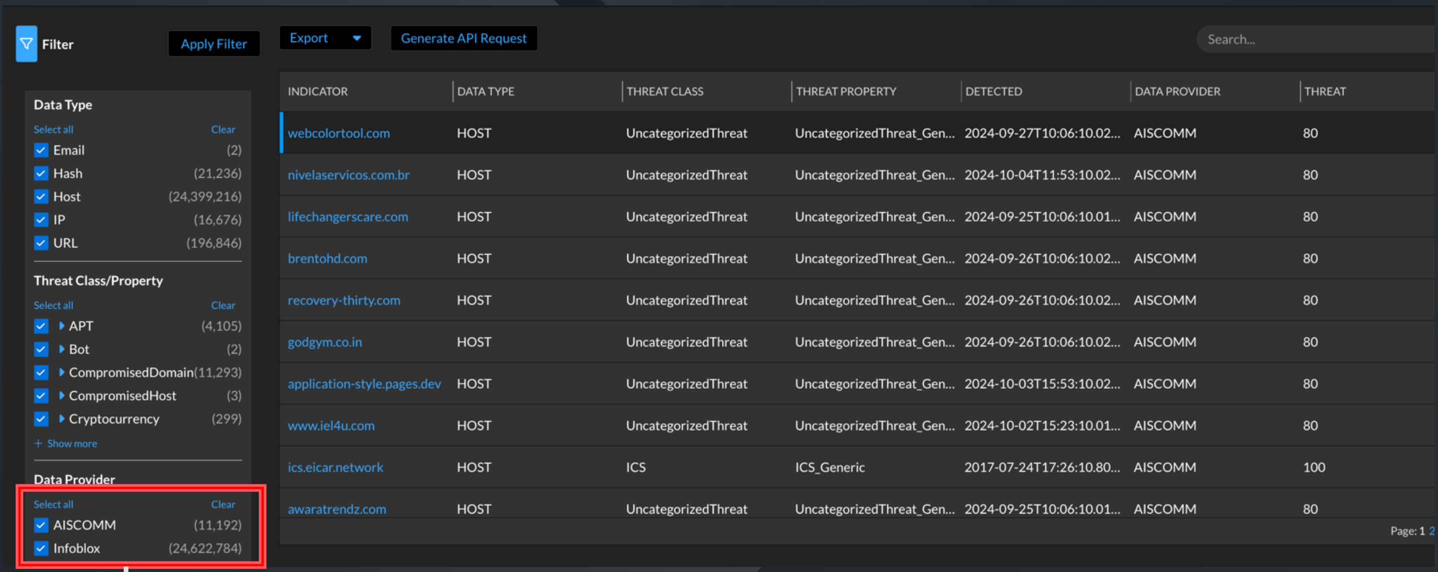
goo

DOMAIN
googie-anaiytics.com

Major brand registered Look A Like Domain found

TIDE

An integrated threat intelignece exchange database. Allow look ups, uploads and can be used to utilize the listed iocs to be shared accross the it security stack.



Data Type

Select all — Clear

- ☑ Email (2)
- ☑ Hash (21,236)
- ☑ Host (24,399,216)
- ☑ IP (16,676)
- ☑ URL (196,846)

Threat Class/Property

Select all — Clear

- ☑ APT (4,105)
- ☑ Bot (2)
- ☑ CompromisedDomain (11,293)
- ☑ CompromisedHost (3)
- ☑ Cryptocurrency (299)
- + Show more

Data Provider

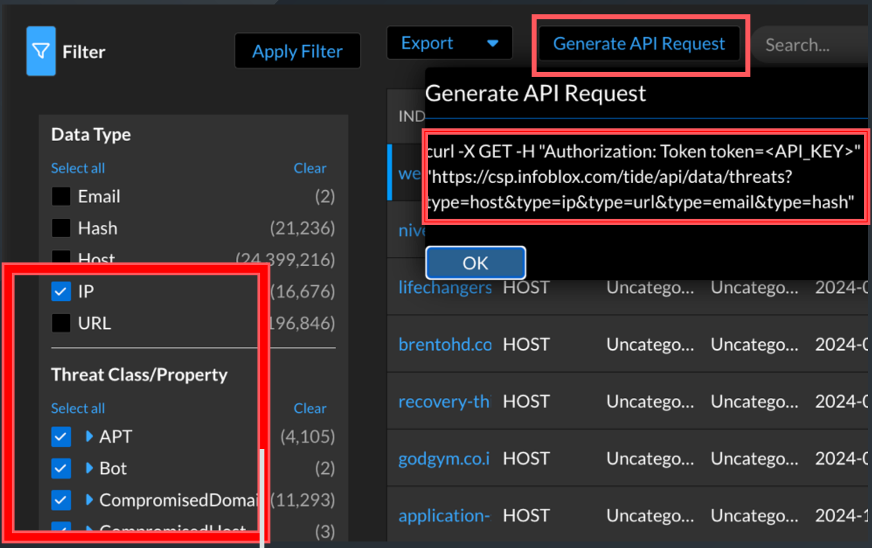
Select all — Clear

- ☑ AISCOMM (11,192)
- ☑ Infoblox (24,622,784)

INDICATOR	DATA TYPE	THREAT CLASS	THREAT PROPERTY	DETECTED	DATA PROVIDER	THREAT
webcolortool.com	HOST	UncategorizedThreat	UncategorizedThreat_Gen...	2024-09-27T10:06:10.02...	AISCOMM	80
nivelaservicos.com.br	HOST	UncategorizedThreat	UncategorizedThreat_Gen...	2024-10-04T11:53:10.02...	AISCOMM	80
lifechangerscare.com	HOST	UncategorizedThreat	UncategorizedThreat_Gen...	2024-09-25T10:06:10.01...	AISCOMM	80
brentohd.com	HOST	UncategorizedThreat	UncategorizedThreat_Gen...	2024-09-26T10:06:10.02...	AISCOMM	80
recovery-thirty.com	HOST	UncategorizedThreat	UncategorizedThreat_Gen...	2024-09-26T10:06:10.02...	AISCOMM	80
godgym.co.in	HOST	UncategorizedThreat	UncategorizedThreat_Gen...	2024-09-26T10:06:10.02...	AISCOMM	80
application-style.pages.dev	HOST	UncategorizedThreat	UncategorizedThreat_Gen...	2024-10-03T15:53:10.02...	AISCOMM	80
www.iel4u.com	HOST	UncategorizedThreat	UncategorizedThreat_Gen...	2024-10-02T15:23:10.01...	AISCOMM	80
ics.eicar.network	HOST	ICS	ICS_Generic	2017-07-24T17:26:10.80...	AISCOMM	100
awaratrendz.com	HOST	UncategorizedThreat	UncategorizedThreat_Gen...	2024-09-25T10:06:10.01...	AISCOMM	80

Page: 1 2

24.6 Million active indicators next to the dynamic detection features for tunneling, zero day dns and Domain Generation Alg. (DGAs)



Data Type

Select all — Clear

- ■ Email (2)
- ■ Hash (21,236)
- ■ Host (24,399,216)
- ☑ IP (16,676)
- ■ URL (196,846)

Threat Class/Property

Select all — Clear

- ☑ APT (4,105)
- ☑ Bot (2)
- ☑ CompromisedDomai (11,293)
- ☑ CompromisedHost (3)

Generate API Request

```
curl -X GET -H "Authorization: Token token=<API_KEY>"
'https://csp.infoblox.com/tide/api/data/threats?
type=host&type=ip&type=url&type=email&type=hash"
```

IND				
we				
nive				
lifechangers	HOST	Uncatego...	Uncatego...	2024-(
brentohd.co	HOST	Uncatego...	Uncatego...	2024-(
recovery-th	HOST	Uncatego...	Uncatego...	2024-(
godgym.co.i	HOST	Uncatego...	Uncatego...	2024-(
application-	HOST	Uncatego...	Uncatego...	2024-1

Easy filtering and API call generation

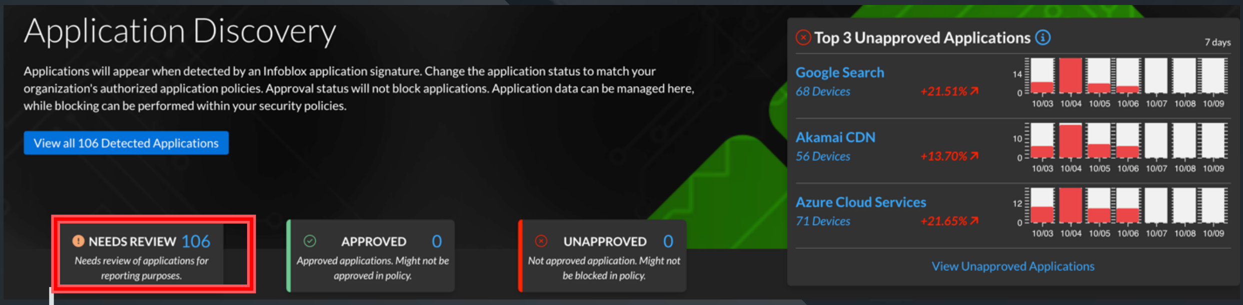
The TIDE DB or Dossier information allows to parse source code for unwanted IoCs.
In example to support the identification of compromised GIT projects or libraries.

BACK TO CONTENTS

APPLICATION DETECTION

APPLICATION DETECTION

All application traffic is categorized, providing full visibility into authorized and potential unauthorized usage. Unauthorized usage increases risk and exposure.



Application Discovery

Applications will appear when detected by an Infoblox application signature. Change the application status to match your organization's authorized application policies. Approval status will not block applications. Application data can be managed here, while blocking can be performed within your security policies.

View all 106 Detected Applications

NEEDS REVIEW 106
Needs review of applications for reporting purposes.

APPROVED 0
Approved applications. Might not be approved in policy.

UNAPPROVED 0
Not approved application. Might not be blocked in policy.

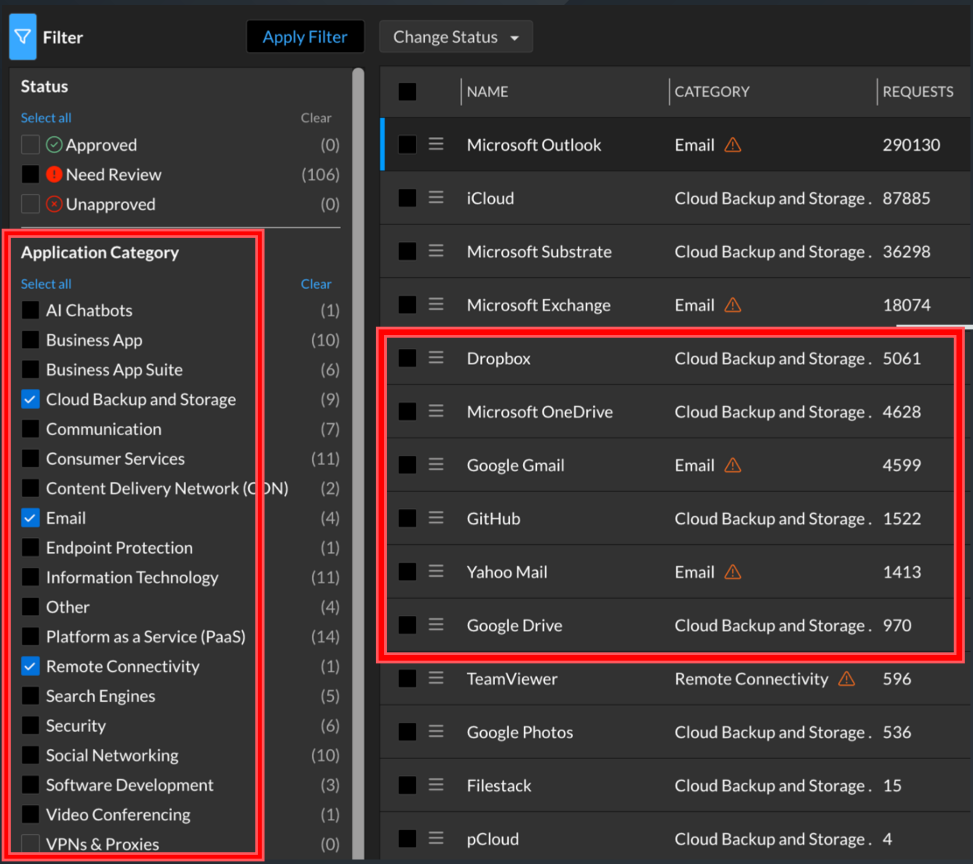
Top 3 Unapproved Applications — 7 days

Application	Devices	Change
Google Search	68 Devices	+21.51% ↗
Akamai CDN	56 Devices	+13.70% ↗
Azure Cloud Services	71 Devices	+21.65% ↗

View Unapproved Applications

Often also known as shadow IT. With regard to 106 applications used in the environment, the questions arise:

Are these applications managed by the IT department?
What about licensing?
What about protection against data loss?
What about infection risks?



Filter — Apply Filter — Change Status

Status — Select all — Clear

□ Approved	(0)
■ Need Review	(106)
□ Unapproved	(0)

Application Category — Select all — Clear

■ AI Chatbots	(1)
■ Business App	(10)
■ Business App Suite	(6)
☑ Cloud Backup and Storage	(9)
■ Communication	(7)
■ Consumer Services	(11)
■ Content Delivery Network (CDN)	(2)
☑ Email	(4)
■ Endpoint Protection	(1)
■ Information Technology	(11)
■ Other	(4)
■ Platform as a Service (PaaS)	(14)
☑ Remote Connectivity	(1)
■ Search Engines	(5)
■ Security	(6)
■ Social Networking	(10)
■ Software Development	(3)
■ Video Conferencing	(1)
■ VPNs & Proxies	(0)

NAME	CATEGORY	REQUESTS
Microsoft Outlook	Email ⚠	290130
iCloud	Cloud Backup and Storage .	87885
Microsoft Substrate	Cloud Backup and Storage .	36298
Microsoft Exchange	Email ⚠	18074
Dropbox	Cloud Backup and Storage .	5061
Microsoft OneDrive	Cloud Backup and Storage .	4628
Google Gmail	Email ⚠	4599
GitHub	Cloud Backup and Storage .	1522
Yahoo Mail	Email ⚠	1413
Google Drive	Cloud Backup and Storage .	970
TeamViewer	Remote Connectivity ⚠	596
Google Photos	Cloud Backup and Storage .	536
Filestack	Cloud Backup and Storage .	15
pCloud	Cloud Backup and Storage .	4

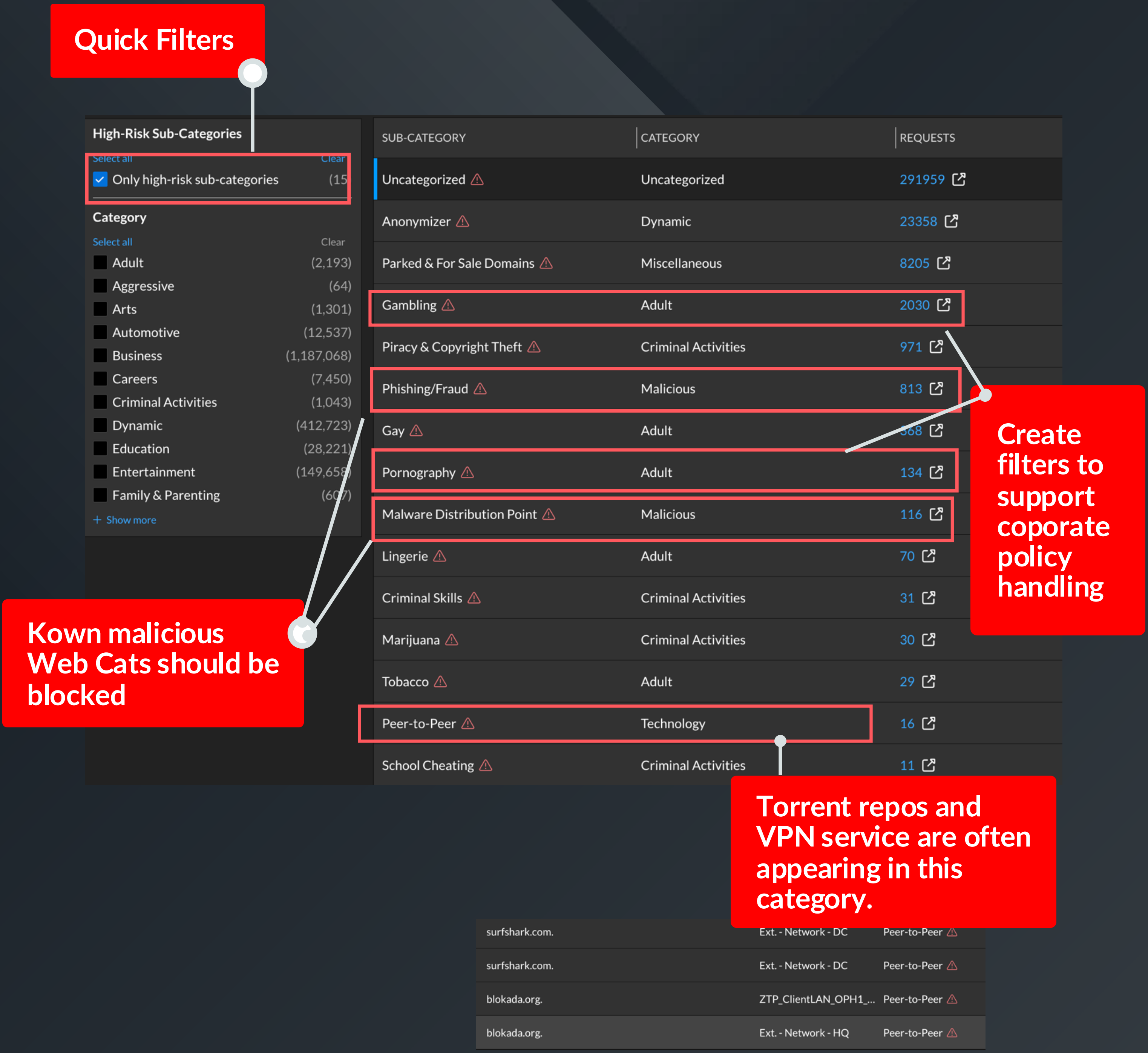
Examples of data loss and infection risks: Unmanaged or open-access storage platforms are often not under the control of the IT department, e.g. for malware scans and data protection policy checks.

BACK TO CONTENTS

WEB CONTENT DISCOVERY

WEB CONTENT DISCOVERY

All web traffic is categorized, highlighting illegal or policy-violating content, such as hacking, gambling, pornography, etc. browsing questionable content increases exposure to credential/data stealing and other threats.



Quick Filters

High-Risk Sub-Categories

Select all Clear

☑ Only high-risk sub-categories (15

Category

Select all Clear

□ Adult	(2,193)
□ Aggressive	(64)
□ Arts	(1,301)
□ Automotive	(12,537)
□ Business	(1,187,068)
□ Careers	(7,450)
□ Criminal Activities	(1,043)
□ Dynamic	(412,723)
□ Education	(28,221)
□ Entertainment	(149,658)
□ Family & Parenting	(607)

+ Show more

SUB-CATEGORY	CATEGORY	REQUESTS
Uncategorized ⚠	Uncategorized	291959
Anonymizer ⚠	Dynamic	23358
Parked & For Sale Domains ⚠	Miscellaneous	8205
Gambling ⚠	Adult	2030
Piracy & Copyright Theft ⚠	Criminal Activities	971
Phishing/Fraud ⚠	Malicious	813
Gay ⚠	Adult	368
Pornography ⚠	Adult	134
Malware Distribution Point ⚠	Malicious	116
Lingerie ⚠	Adult	70
Criminal Skills ⚠	Criminal Activities	31
Marijuana ⚠	Criminal Activities	30
Tobacco ⚠	Adult	29
Peer-to-Peer ⚠	Technology	16
School Cheating ⚠	Criminal Activities	11

Create filters to support coporate policy handling

Kown malicious Web Cats should be blocked

Torrent repos and VPN service are often appearing in this category.

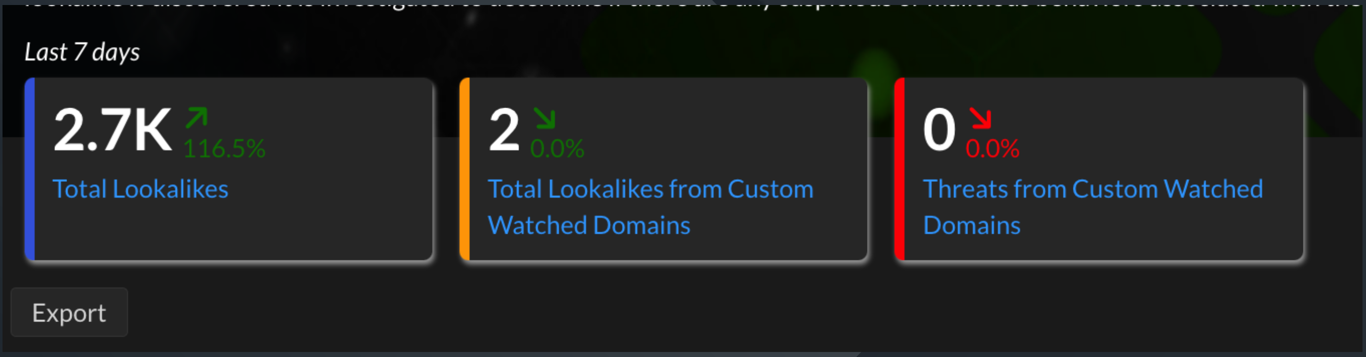
surfshark.com.	Ext. - Network - DC	Peer-to-Peer ⚠
surfshark.com.	Ext. - Network - DC	Peer-to-Peer ⚠
blokada.org.	ZTP_ClientLAN_OPH1_...	Peer-to-Peer ⚠
blokada.org.	Ext. - Network - HQ	Peer-to-Peer ⚠

LOOKALIKE DOMAINS

LOOKALIKE DOMAINS

Active monitoring for lookalike domains of major brands, including common typosquats. Custom monitoring for lookalikes impersonating your brand for malicious purposes.

SUMMARY



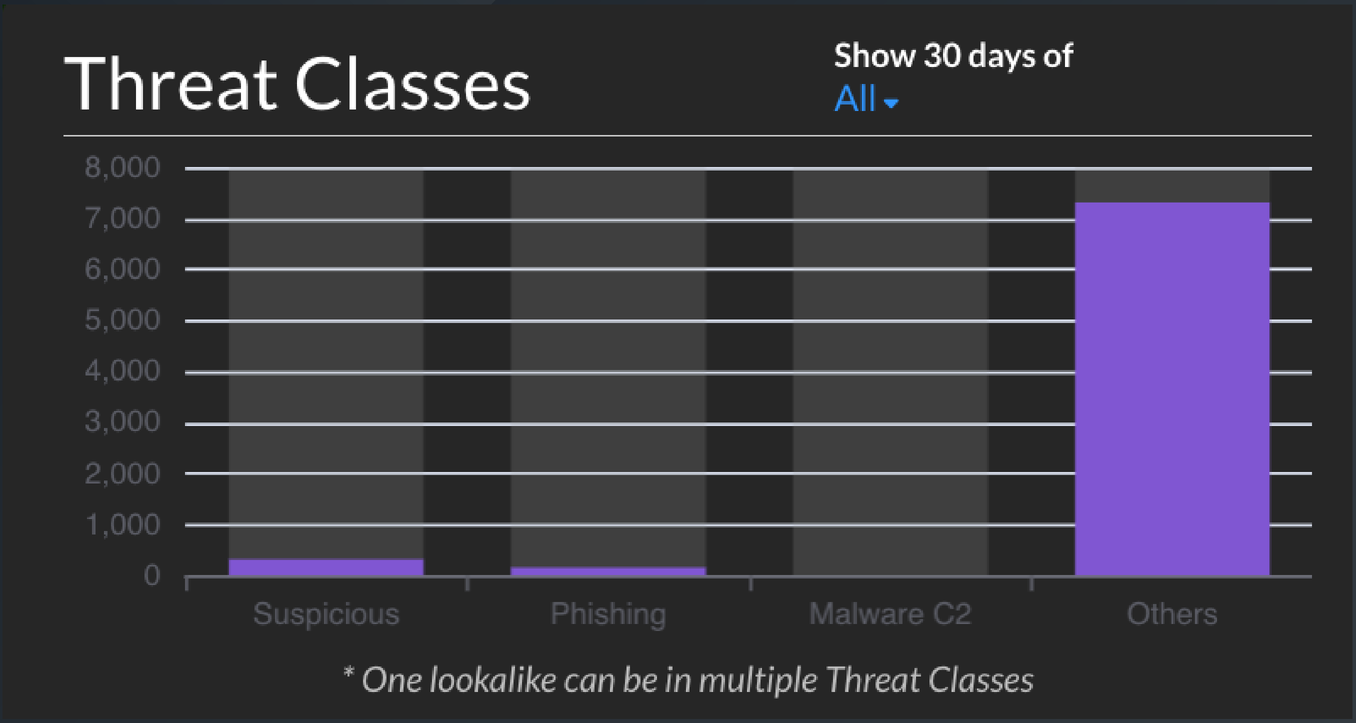
Last 7 days

2.7K ↗ 116.5%
Total Lookalikes

2 ↘ 0.0%
Total Lookalikes from Custom Watched Domains

0 ↘ 0.0%
Threats from Custom Watched Domains

LOOKALIKES BY THREAT TYPES



Threat Classes

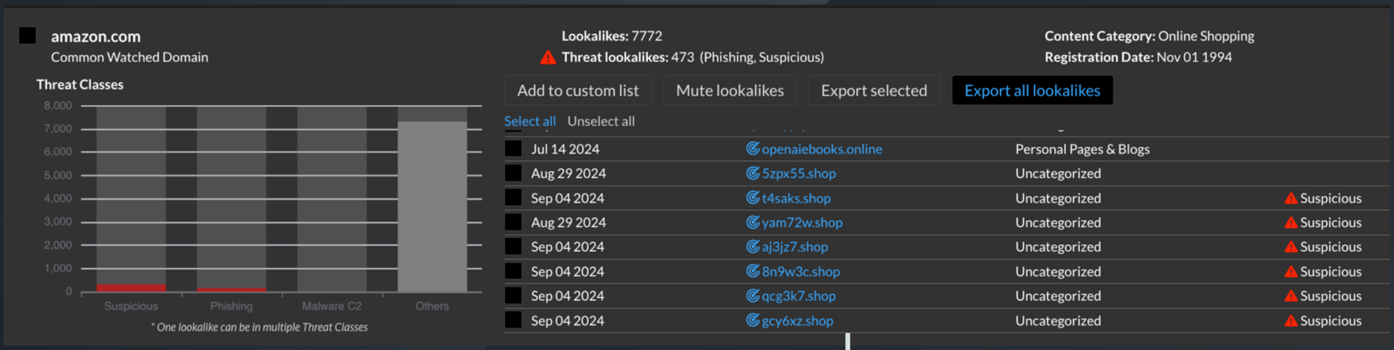
Show 30 days of
All ▾

** One lookalike can be in multiple Threat Classes*

BACK TO CONTENTS

LOOKALIKE DOMAINS ANALYSIS

Review and request a domain take-down (professional service offer) if the organization's reputation is at risk.



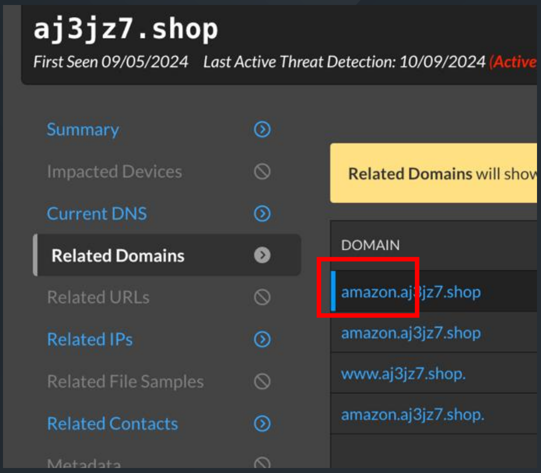
amazon.com
Common Watched Domain

* One lookalike can be in multiple Threat Classes

Lookalikes: 7772
Threat lookalikes: 473 (Phishing, Suspicious)

Content Category: Online Shopping
Registration Date: Nov 01 1994

■	Jul 14 2024	openaiebooks.online	Personal Pages & Blogs	
■	Aug 29 2024	5zpx55.shop	Uncategorized	
■	Sep 04 2024	t4saks.shop	Uncategorized	Suspicious
■	Aug 29 2024	yam72w.shop	Uncategorized	Suspicious
■	Sep 04 2024	aj3jz7.shop	Uncategorized	Suspicious
■	Sep 04 2024	8n9w3c.shop	Uncategorized	Suspicious
■	Sep 04 2024	qcg3k7.shop	Uncategorized	Suspicious
■	Sep 04 2024	gcy6xz.shop	Uncategorized	Suspicious



aj3jz7.shop

First Seen 09/05/2024 Last Active Threat Detection: 10/09/2024 (Active

Related Domains will show

DOMAIN
amazon.aj3jz7.shop
amazon.aj3jz7.shop
www.aj3jz7.shop.
amazon.aj3jz7.shop.

Example of a major brand

BACK TO CONTENTS

SECURITY ACTIVITIES

SECURITY ACTIVITIES

All DNS queries are logged, categorized, and attributed by severity to surface security-related events requiring further forensic analysis.

SUMMARY

48.9K
Security Events

48.9K
DNS Firewall

>300K
High Risk Web Content

92
Threat Insight

12
Threat View

16
Insights

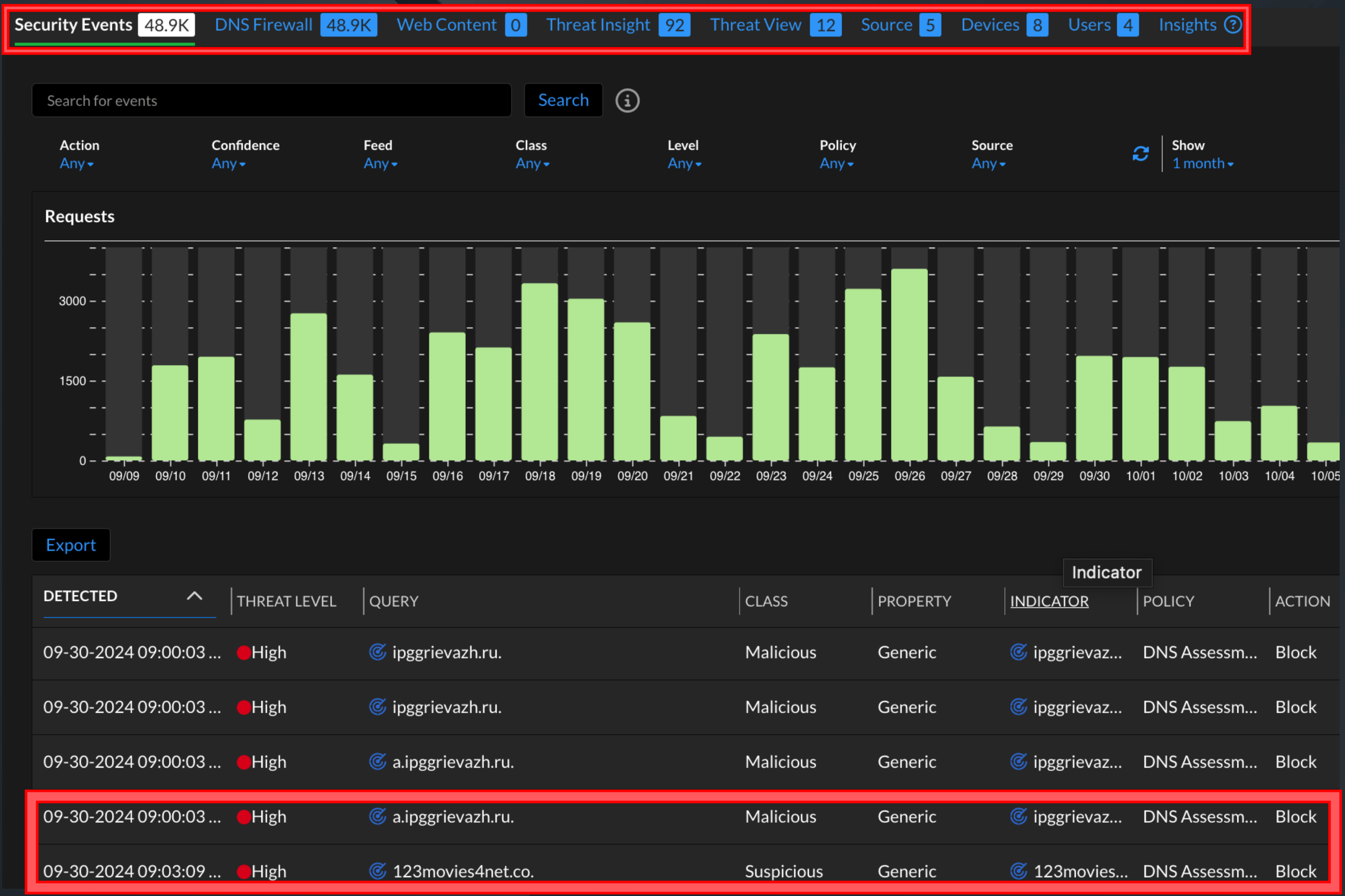
8
Devices

4
Users

5
Source

Depends on deployment options (s. APPENDICES)

SECURITY ACTIVITIES ANALYSIS



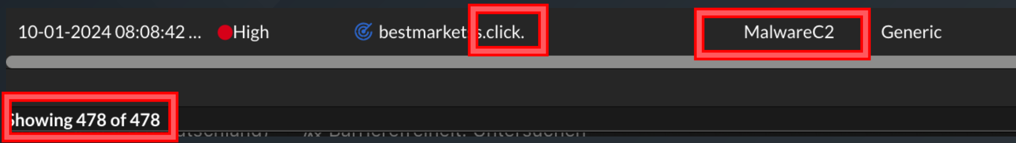
Security Events 48.9K | DNS Firewall 48.9K | Web Content 0 | Threat Insight 92 | Threat View 12 | Source 5 | Devices 8 | Users 4 | Insights

Search for events | Search

Action	Confidence	Feed	Class	Level	Policy	Source	Show
Any	Any	Any	Any	Any	Any	Any	1 month

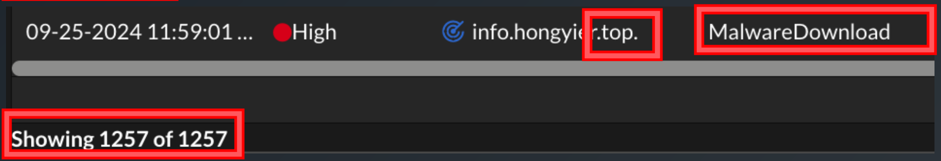
Requests

DETECTED	THREAT LEVEL	QUERY	CLASS	PROPERTY	INDICATOR	POLICY	ACTION
09-30-2024 09:00:03 ...	● High	ipggrievazh.ru.	Malicious	Generic	ipggrievaz...	DNS Assessm...	Block
09-30-2024 09:00:03 ...	● High	ipggrievazh.ru.	Malicious	Generic	ipggrievaz...	DNS Assessm...	Block
09-30-2024 09:00:03 ...	● High	a.ipggrievazh.ru.	Malicious	Generic	ipggrievaz...	DNS Assessm...	Block
09-30-2024 09:00:03 ...	● High	a.ipggrievazh.ru.	Malicious	Generic	ipggrievaz...	DNS Assessm...	Block
09-30-2024 09:03:09 ...	● High	123movies4net.co.	Suspicious	Generic	123movies...	DNS Assessm...	Block



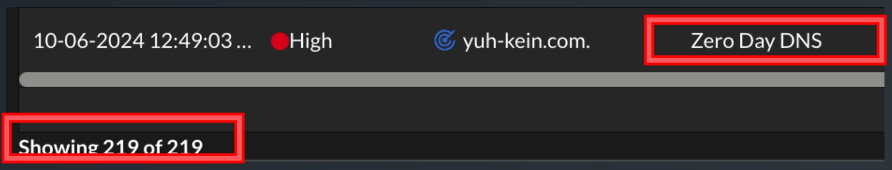
10-01-2024 08:08:42 ... ● High bestmarkets.click. MalwareC2 Generic

howing 478 of 478



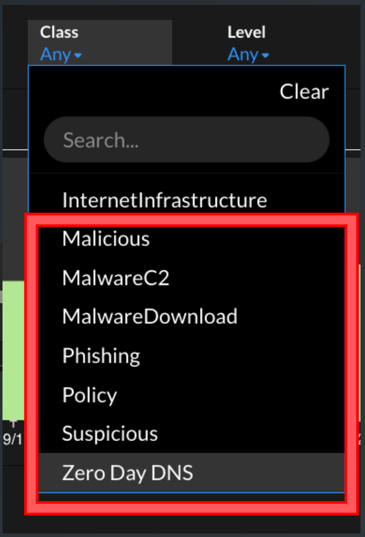
09-25-2024 11:59:01 ... ● High info.hongyier.top. MalwareDownload

Showing 1257 of 1257



10-06-2024 12:49:03 ... ● High yuh-kein.com. Zero Day DNS

Showing 219 of 219



Class	Level
Any	Any

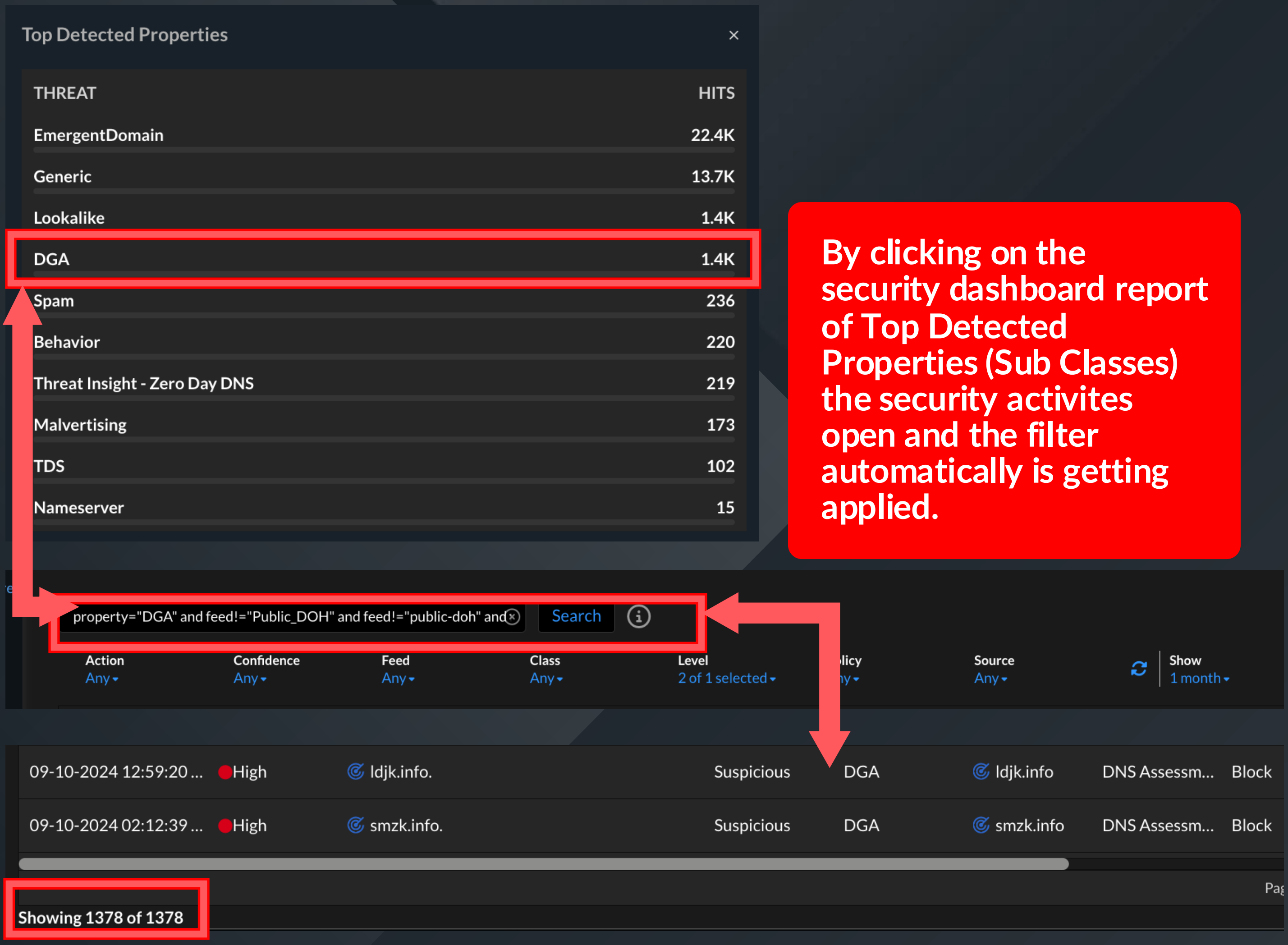
Clear

Search...

- InternetInfrastructure
- Malicious
- MalwareC2
- MalwareDownload
- Phishing
- Policy
- Suspicious
- Zero Day DNS

BACK TO CONTENTS

SECURITY ACTIVITIES ANALYSIS



Top Detected Properties ×

THREAT	HITS
EmergentDomain	22.4K
Generic	13.7K
Lookalike	1.4K
DGA	1.4K
Spam	236
Behavior	220
Threat Insight - Zero Day DNS	219
Malvertising	173
TDS	102
Nameserver	15

By clicking on the security dashboard report of Top Detected Properties (Sub Classes) the security activites open and the filter automatically is getting applied.

property="DGA" and feed!="Public_DOH" and feed!="public-doh" and

Action	Confidence	Feed	Class	Level	licy	Source	Show
Any	Any	Any	Any	2 of 1 selected	ny	Any	1 month

09-10-2024 12:59:20 ...	●High	ldjk.info.	Suspicious	DGA	ldjk.info	DNS Assessm...	Block
09-10-2024 02:12:39 ...	●High	smzk.info.	Suspicious	DGA	smzk.info	DNS Assessm...	Block

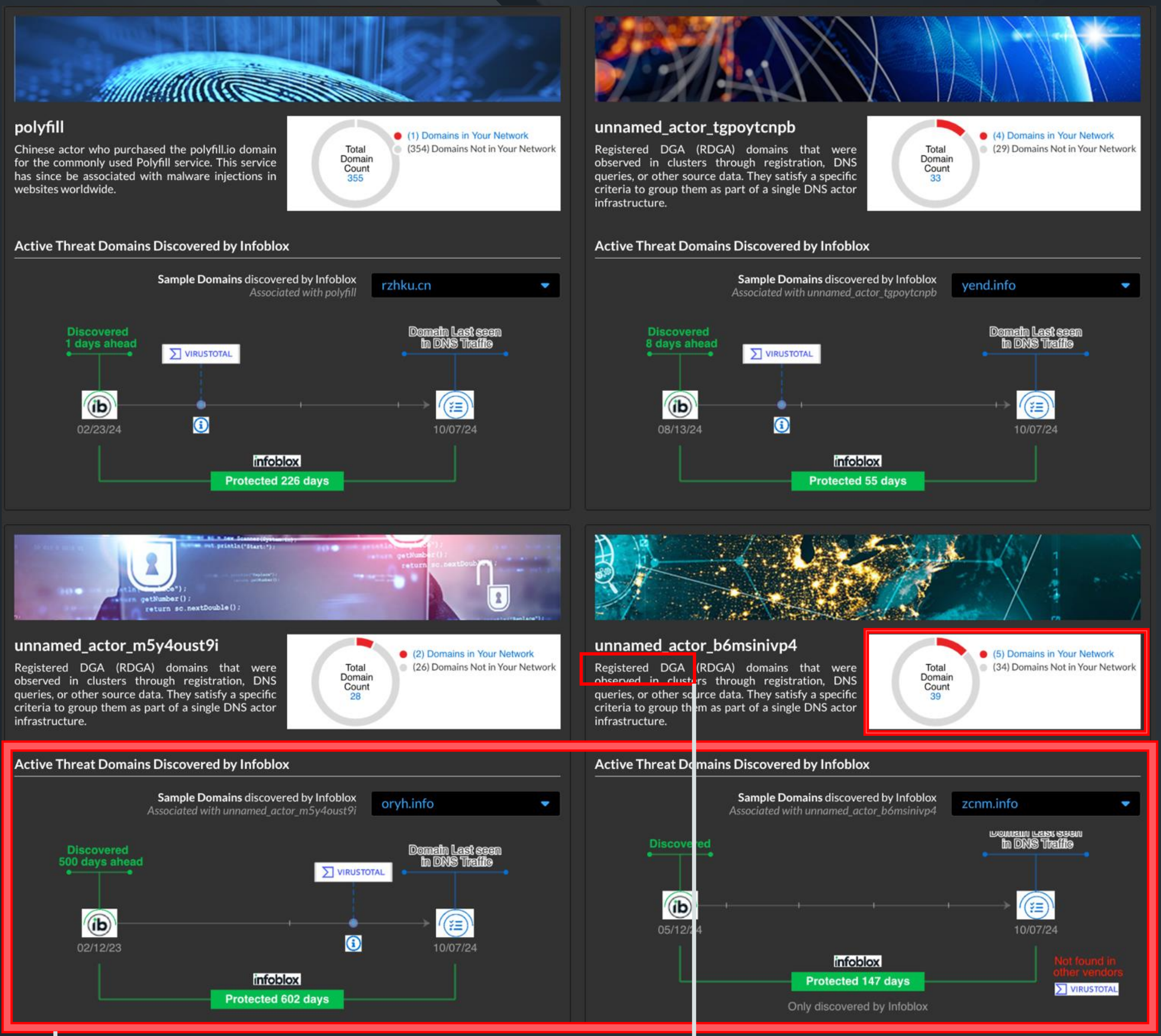
Showing 1378 of 1378

THREAT ACTORS

BACK TO CONTENTS

THREAT ACTORS

Specific active threat actors discovered in the assessment environment, including their activity timeline, correlated indicators, and a synopsis of their targets and techniques.



polyfill

Chinese actor who purchased the polyfill.io domain for the commonly used Polyfill service. This service has since be associated with malware injections in websites worldwide.

Total Domain Count 355

- ● (1) Domains in Your Network
- ● (354) Domains Not in Your Network

Active Threat Domains Discovered by Infoblox

Sample Domains discovered by Infoblox
Associated with polyfill

rzhku.cn

unnamed_actor_tgpoytcnpb

Registered DGA (RDGA) domains that were observed in clusters through registration, DNS queries, or other source data. They satisfy a specific criteria to group them as part of a single DNS actor infrastructure.

Total Domain Count 33

- ● (4) Domains in Your Network
- ● (29) Domains Not in Your Network

Active Threat Domains Discovered by Infoblox

Sample Domains discovered by Infoblox
Associated with unnamed_actor_tgpoytcnpb

yend.info

unnamed_actor_m5y4oust9i

Registered DGA (RDGA) domains that were observed in clusters through registration, DNS queries, or other source data. They satisfy a specific criteria to group them as part of a single DNS actor infrastructure.

Total Domain Count 28

- ● (2) Domains in Your Network
- ● (26) Domains Not in Your Network

Active Threat Domains Discovered by Infoblox

Sample Domains discovered by Infoblox
Associated with unnamed_actor_m5y4oust9i

oryh.info

unnamed_actor_b6msinivp4

Registered DGA (RDGA) domains that were observed in clusters through registration, DNS queries, or other source data. They satisfy a specific criteria to group them as part of a single DNS actor infrastructure.

Total Domain Count 39

- ● (5) Domains in Your Network
- ● (34) Domains Not in Your Network

Active Threat Domains Discovered by Infoblox

Sample Domains discovered by Infoblox
Associated with unnamed_actor_b6msinivp4

zcnm.info

Early prevention capabilities relate to a DNS-based threat intelligence service

DGAs are often hard-coded into malware

BACK TO CONTENTS

RECOMMENDATIONS & NEXT STEPS

RECOMMENDATIONS

Based on the key findings listed below, we're proposing the following set of recommendations.

KEY FINDINGS

Seen Potentials:

Client Misconfiguration
Mobile Devices At Risk
Potential Unwanted SaaS Applications
Data Loss Risk
Evasion/ Security Bypass Risk
Malware Infection Risk
Unwanted User Behaviour
Potential Infected Clients

Specific DNS Risks:

- DoH (8.8k Hits)
- Suspicious LookALike (431 Hits)
- Suspicious Domains (12k Hits)
- Suspicious NOED (22.3k Hits)
- DGA (1.3k Hits)
- Zero Day DNS (219 Hits)
- Threat Actor DNS Clusters (12 IoCs)

RECOMMENDATIONS

- Enhance visibility by combining deployment options
- Employee Awareness Training
- Make use of the threat intelligence feeds to inspect your source code
- Keep Alive DNS Request and Response Logging for investigation demands
- Employee Threat Investigation & Response Training
- Keep-Alive DNS Threat Analytics
- Keep-Alive DNSDR
- Keep-Alive Event Aggregation Engine
- Start Application approval and filtering

BACK TO CONTENTS

FOR MORE INFORMATION CONTACT:

NAME

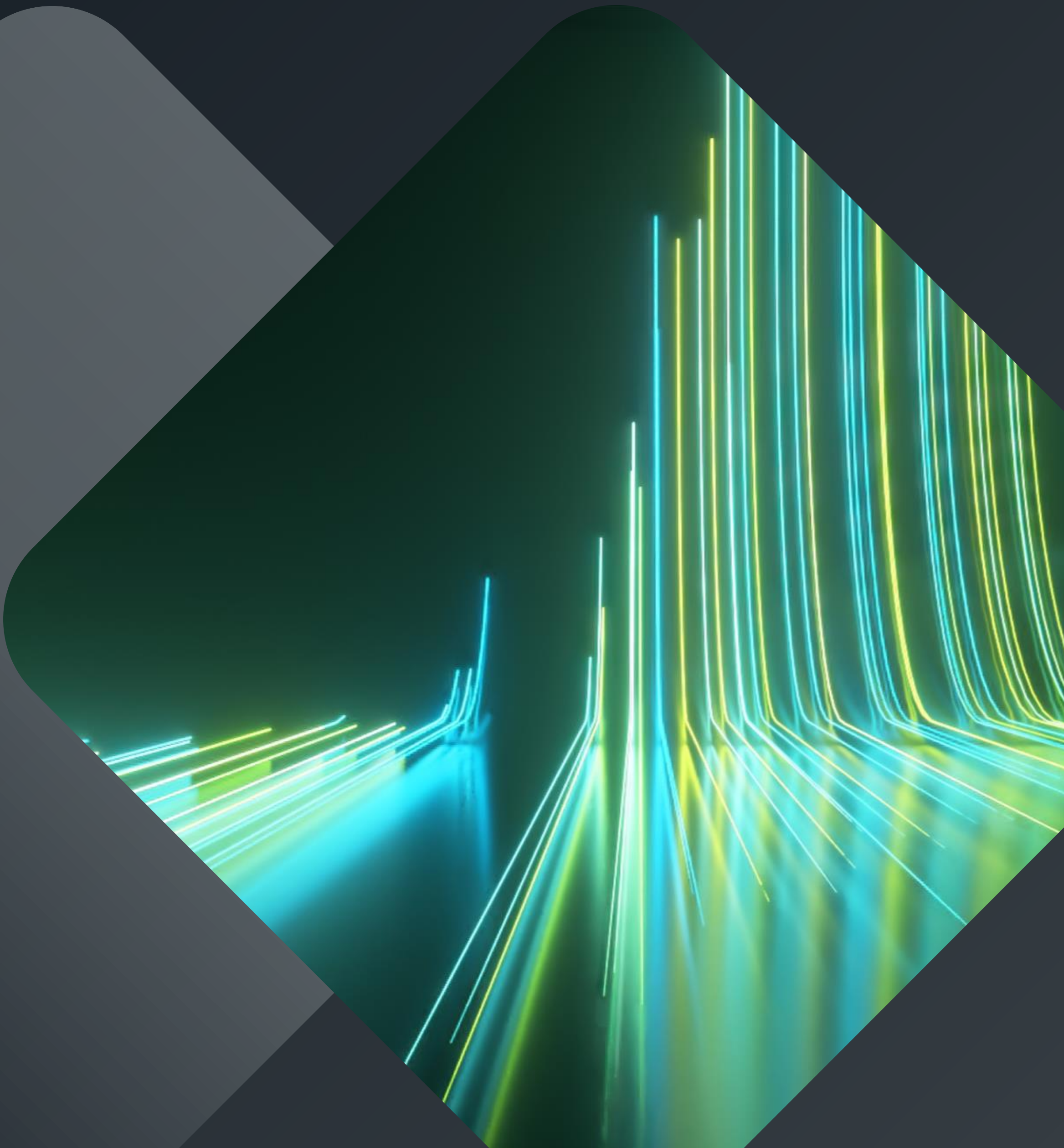
TITEL

EMAIL:

PHONE NUMBER:

This Infoblox Security Assessment report is based on information provided to Infoblox and our own observations during the assessment period. We have conducted the assessment in accordance with generally accepted cybersecurity auditing standards. However, our assessment has limitations, and we cannot guarantee that all vulnerabilities and security issues have been identified. This report is provided for informational purposes only and should not be relied upon as a complete representation of the security of the organization's information systems. We do not accept responsibility for any losses or damages that may arise from the use of this report or any reliance on the findings contained herein. It is important to note that cybersecurity threats are constantly evolving, and the organization's security posture may change at any time. Our findings are accurate as of the date of the assessment and may not reflect the current state of the organization's security posture.

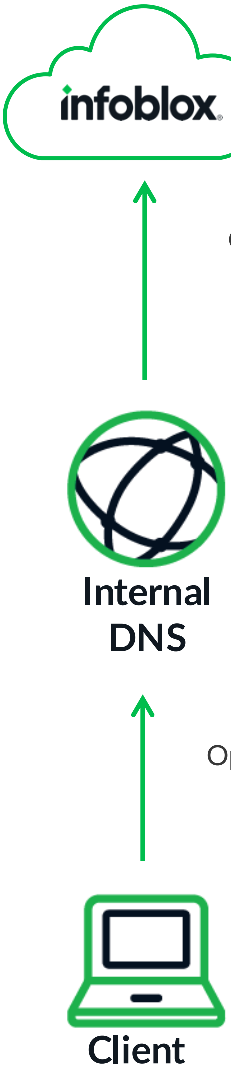
APPENDICES



ASSESSMENT METHODOLOGY

We used the following methodology to perform the assessment:

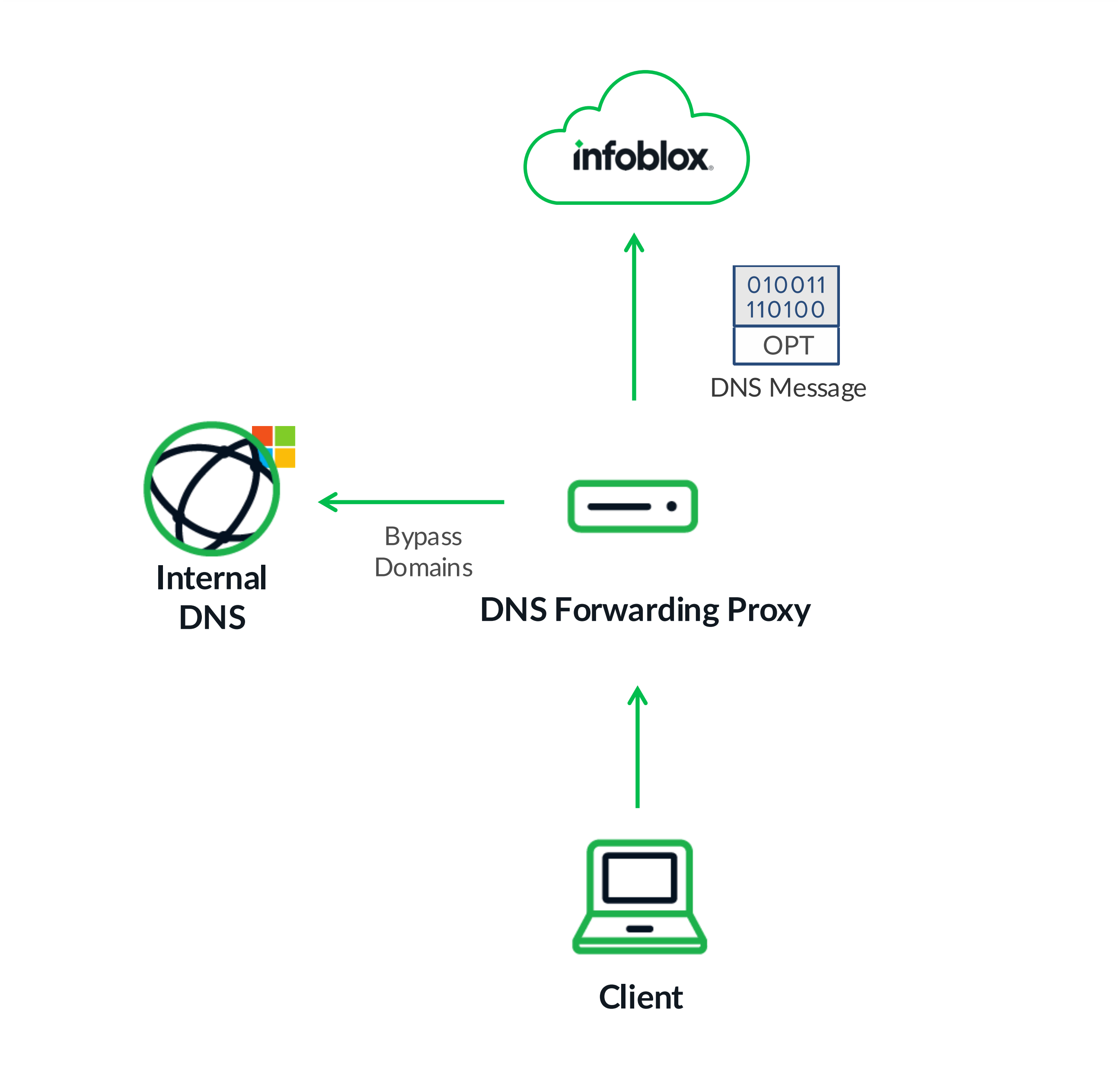
DIRECT FORWARDING



ASSESSMENT METHODOLOGY

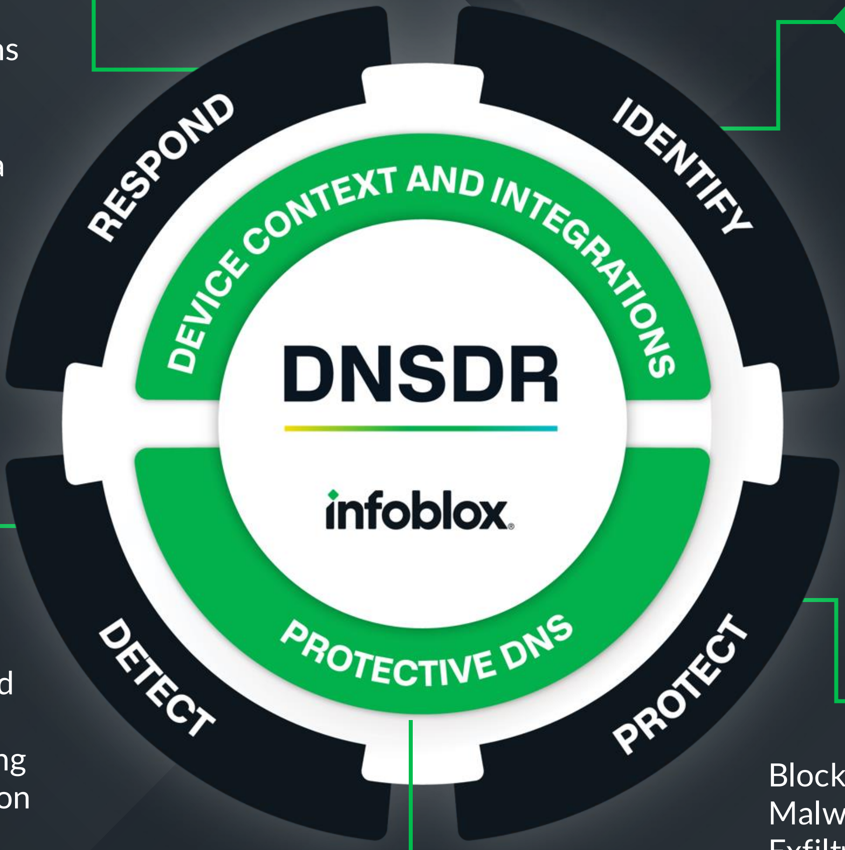
We used partly the following methodology to perform the assessment:

DNS FORWARDING PROXY



SECURITY SOLUTIONS

DNS DETECTION AND RESPONSE



RESPOND
Automates remediation actions via ecosystem integrations and shares of DDI data to SOC

IDENTIFY
Automates responses based on user and device context

DETECT
Detects suspicious and malicious actor infrastructure, including near-real time detection of many threats

PROTECT
Blocks phishing, DGA, C2, Malware, Ransomware, Exfiltration and Suspicious Domains

Blocks at the intent to communicate

> “DNS is the unsung hero in cybersecurity, transforming threat detection and intelligence with every query. **Infoblox elevates DNS from a basic network function to a cornerstone of cybersecurity strategy”.** – Christopher Kissel, Research Vice President, Security and Trust at IDC

SECURITY SOLUTIONS

INFOBLOX THREAT DEFENSE

Protective DNS

Block phishing, ransomware, malware C2

Block suspicious domains

Threat Insight

Real-time streaming analytics to detect/block data exfiltration, DGAs, and Zero Day DNS

Examines all DNS records (e.g., A, AAAA, CNAME, MX, NS, SOA, TXT, etc.)

Lookalike Domain Monitoring

Monitor and alert on lookalike domains used for phishing, spear phishing, and brand damage

SOC Insights

Leverage AI to turn vast event, network, ecosystem, and unique DNS intelligence data into a manageable set of actionable insights

Dossier

Context on threat indicators (e.g., hostnames, URLs, IPs)

Easy view of impacted devices

Infoblox Ecosystem

Automate security event response via API-based integrations

Share contextual data (IPAM/DHCP) for prioritization

Ingest custom/third-party threat intel feeds for broader distribution

BACK TO CONTENTS

ABOUT INFOBLOX

Uniting networking and security to deliver unmatched performance and protection.

TOP 25 Cybersecurity Companies in 2020 (#6)

63 Patents Granted. 25 Pending

13000+ Customers

154 Countries

1140+ partners

92 Fortune 100 List (up from 82 in 2016)

540 employees supporting Engineering & Product development

93.3 Customer Satisfaction

DDI market share is **48.7%** per IDC's 2021

47.7 NPS Score