infoblox®

Infoblox Threat Defense: Cyberangriffe blockieren, bevor sie beginnen: Der Schlüssel liegt in DNS Security

Stephan Fritsche
Central Europe Security Lead, Infoblox

16.09.2025, Congress Park Hanau

infoblox®

Stephan Fritsche
Central Europe Security Lead
Mobil: +49 170 58 52 443
sfritsche@infoblox.com
www.infoblox.com

https://www.infoblox.com/products/bloxone-ddi/
https://www.infoblox.com/products/bloxone-threat-defense/

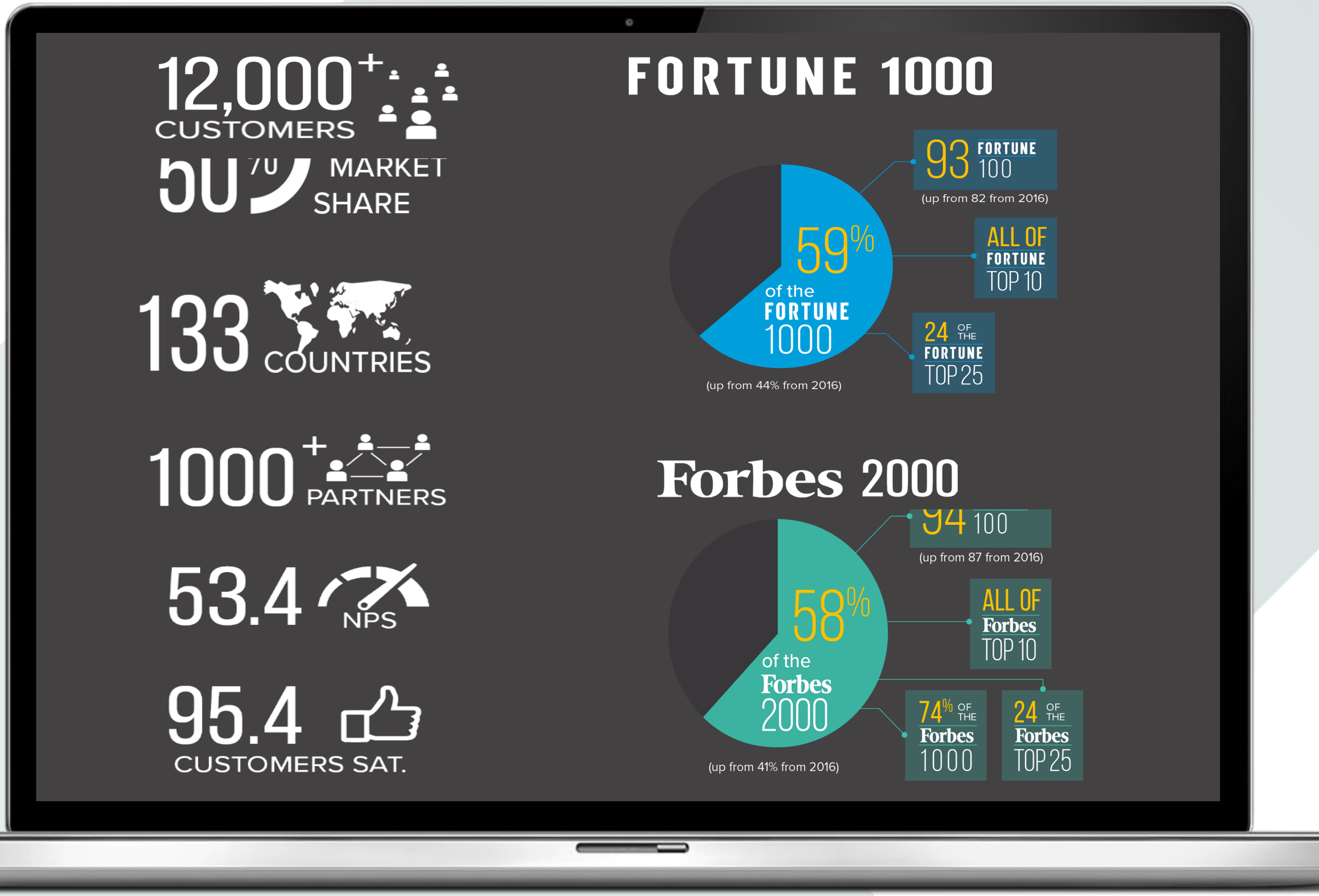
Leading the Industry

MISSION

Empowering organizations to manage their continuously evolving growing networks simply and securely.

OFFERINGS

Core Network Services, Cybersecurity, Secure Edge Services



12,000+ CUSTOMERS

50% MARKET SHARE

133 COUNTRIES

1000+ PARTNERS

53.4 NPS

95.4 CUSTOMERS SAT.

FORTUNE 1000

59% of the FORTUNE 1000

(up from 44% from 2016)

93 FORTUNE 100

(up from 82 from 2016)

ALL OF FORTUNE TOP 10

24 OF THE FORTUNE TOP 25

Forbes 2000

58% of the Forbes 2000

(up from 41% from 2016)

94 100

(up from 87 from 2016)

ALL OF Forbes TOP 10

74% OF THE Forbes 1000

24 OF THE Forbes TOP 25

infoblox

A LEADER IN CLOUD NETWORKING AND SECURITY SERVICES

INTEGRATED DDI

UNITE DNS, DHCP, IPAM

Manage from the cloud with BloxOne® DDI or on-prem with NIOS DDI.

DNS DETECTION & RESPONSE

ACHIEVE SECURITY EVERYWHERE

Deploy hybrid DNS-layer security with BloxOne® Threat Defense.

HYBRID MULTI-CLOUD INTEGRATION

MANAGE HYBRID WORKLOADS

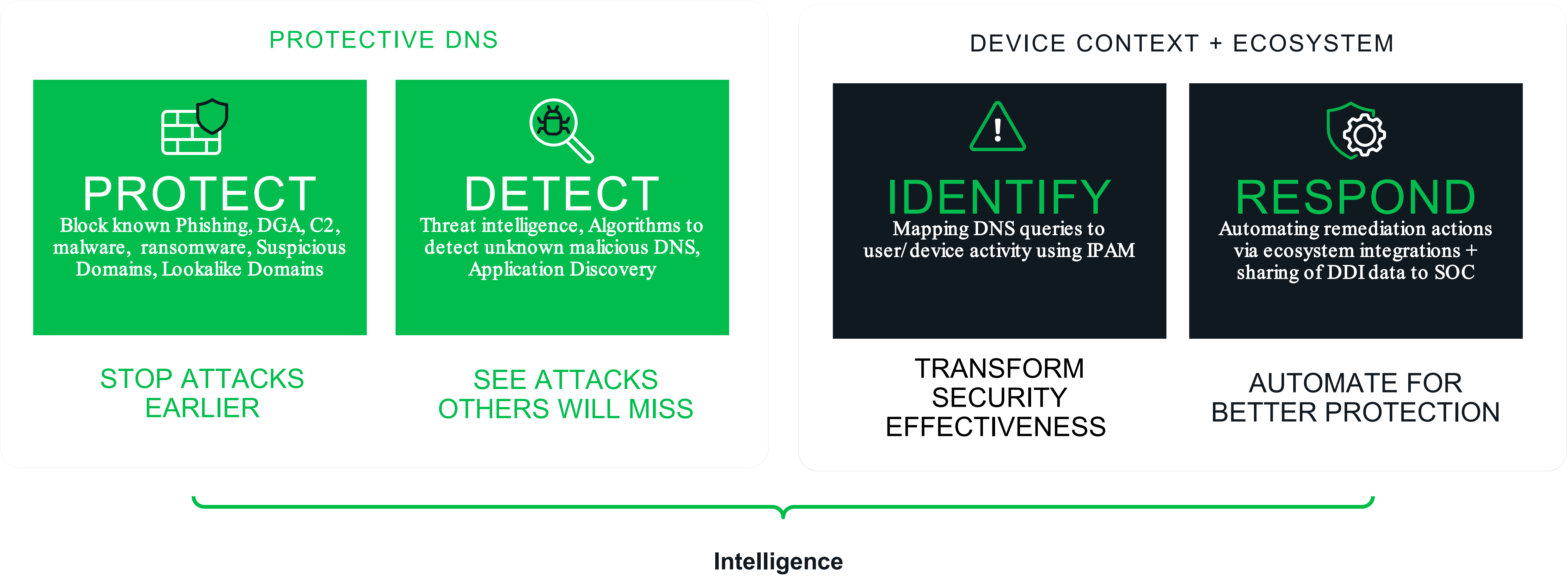
Maintain complex multi-cloud networks with automated processes.

THREAT INTELLIGENCE

PROTECT AGAINST EVOLVING THREATS

Uplift security stacks with DNS threat intel that’s hunted, not gathered.

DNS DETECTION AND RESPONSE



PROTECTIVE DNS

PROTECT
Block known Phishing, DGA, C2, malware, ransomware, Suspicious Domains, Lookalike Domains

STOP ATTACKS EARLIER

DETECT
Threat intelligence, Algorithms to detect unknown malicious DNS, Application Discovery

SEE ATTACKS OTHERS WILL MISS

DEVICE CONTEXT + ECOSYSTEM

IDENTIFY
Mapping DNS queries to user/ device activity using IPAM

TRANSFORM SECURITY EFFECTIVENESS

RESPOND
Automating remediation actions via ecosystem integrations + sharing of DDI data to SOC

AUTOMATE FOR BETTER PROTECTION

Intelligence

DNS is important

DOMAIN DEMAND

- 61B Internet-connected devices in 2023 (~ ⅔ IoT)
- 351M second-level domains
- 200K new domains are created every day

DOMAIN RISK

- 85% of newly registered domains are malicious
- Average PC sends ~3,000 DNS queries per day
- 92% of Malware and C2s depend on DNS
- It only takes one DNS query to compromise a network

DOMAIN ABUSE

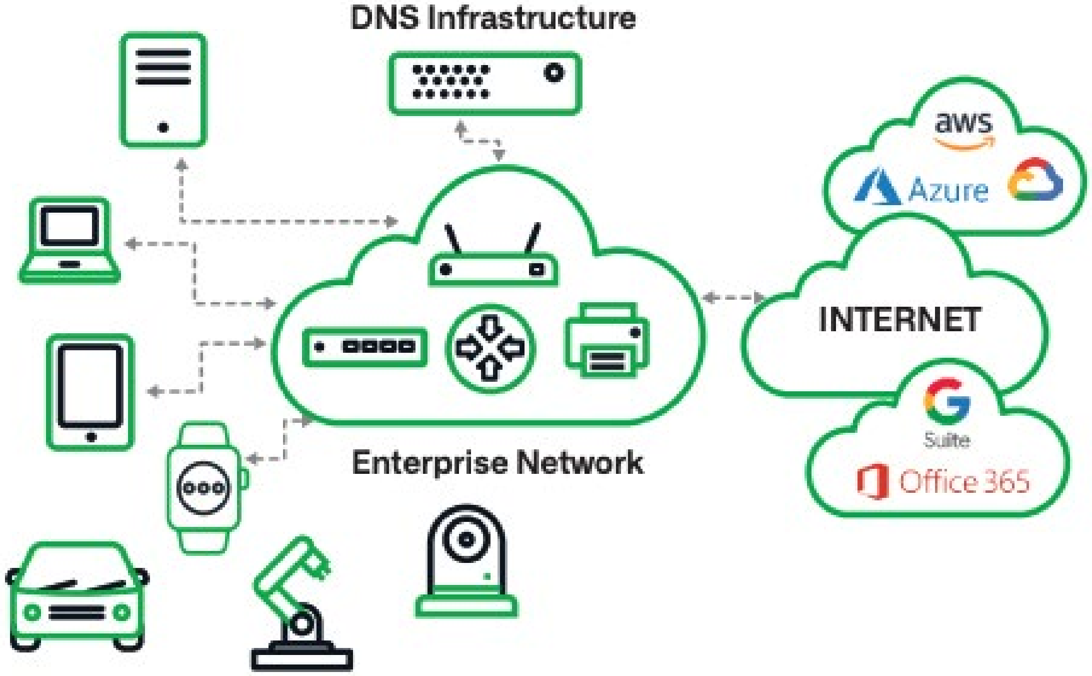
- 76% of Orgs. in 2022 targeted by ransomware
- Traffic Distribution Systems (TDSs) are increasingly being used in phishing distribution to evade detection
- Fake gov't domains increased 30-40% in 2023
- >300K lookalike domains detected in ~1 year

infoblox

DNS IS FRONT AND CENTER FOR RISK REDUCTION

A Strategic Solution with a Unique View

- DNS spans entire organization
- Sees/records all user/device activity
- Closest to all network assets
- Unique position to block threats missed by others



92% Of Cyber Attacks Utilize DNS Protocol

EASIEST WAY TO PROVIDE THREAT PROTECTION, BENEFITS OF SHIFT LEFT SECURITY

You have already DNS in place

Protect all devices, any system anywhere including IoT/OT, included Application discovery

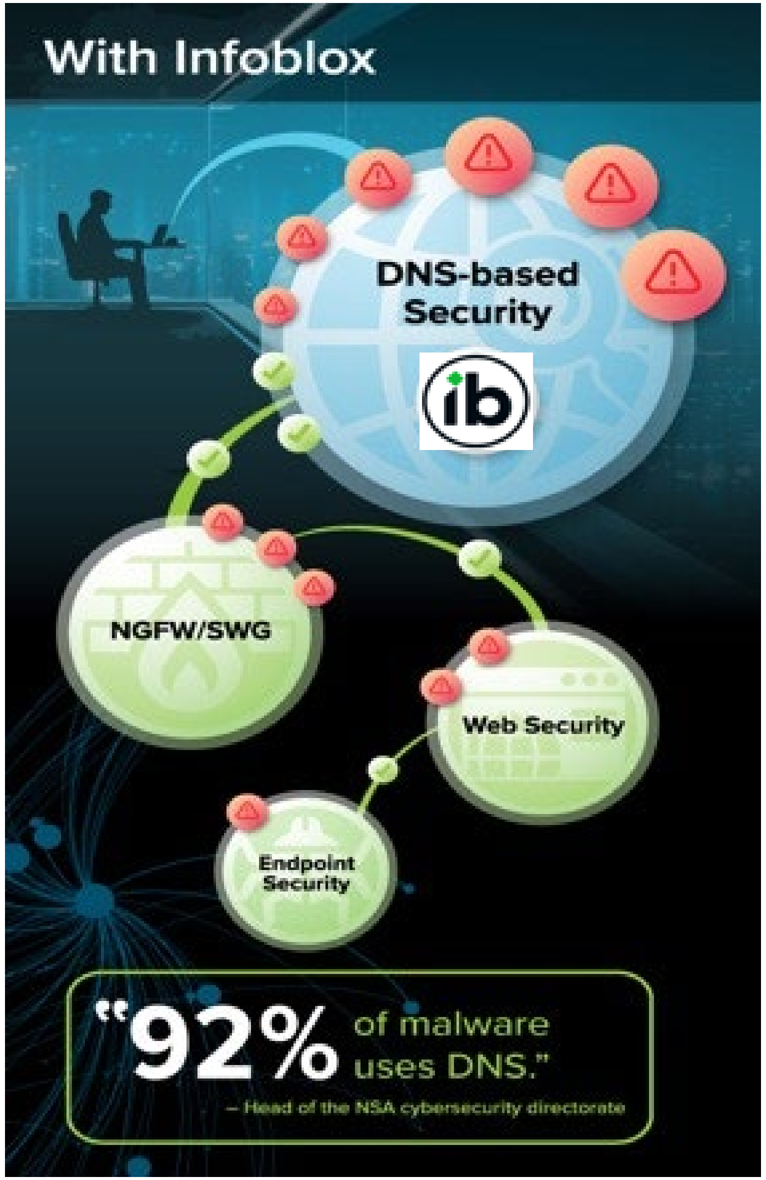
Reduce load on downstream security devices, increase ROI.

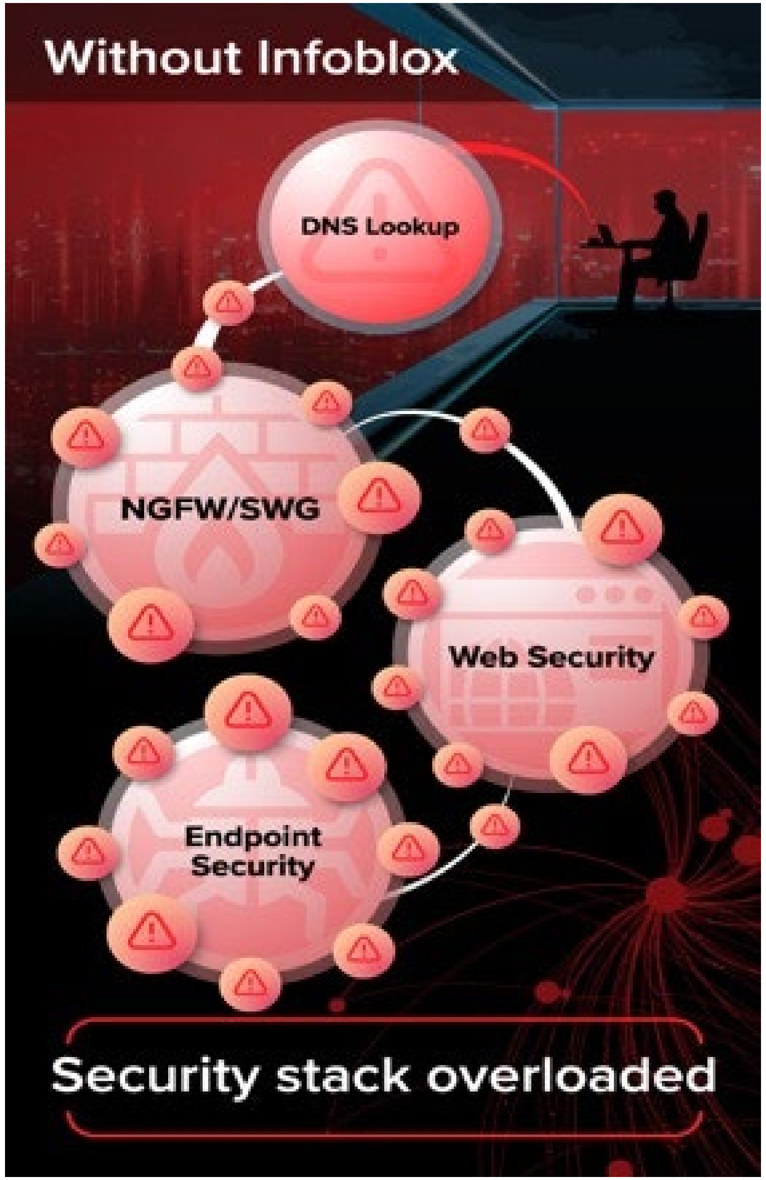
Reduce security alerts to SecOps and SIEMs, increase efficiency

DNS based threat hunting to track adversary infrastructure before actual attack starts – e.g., Pre-crime/suspicious domains, DGAs, lookalike d

PAYBACK
<6 months

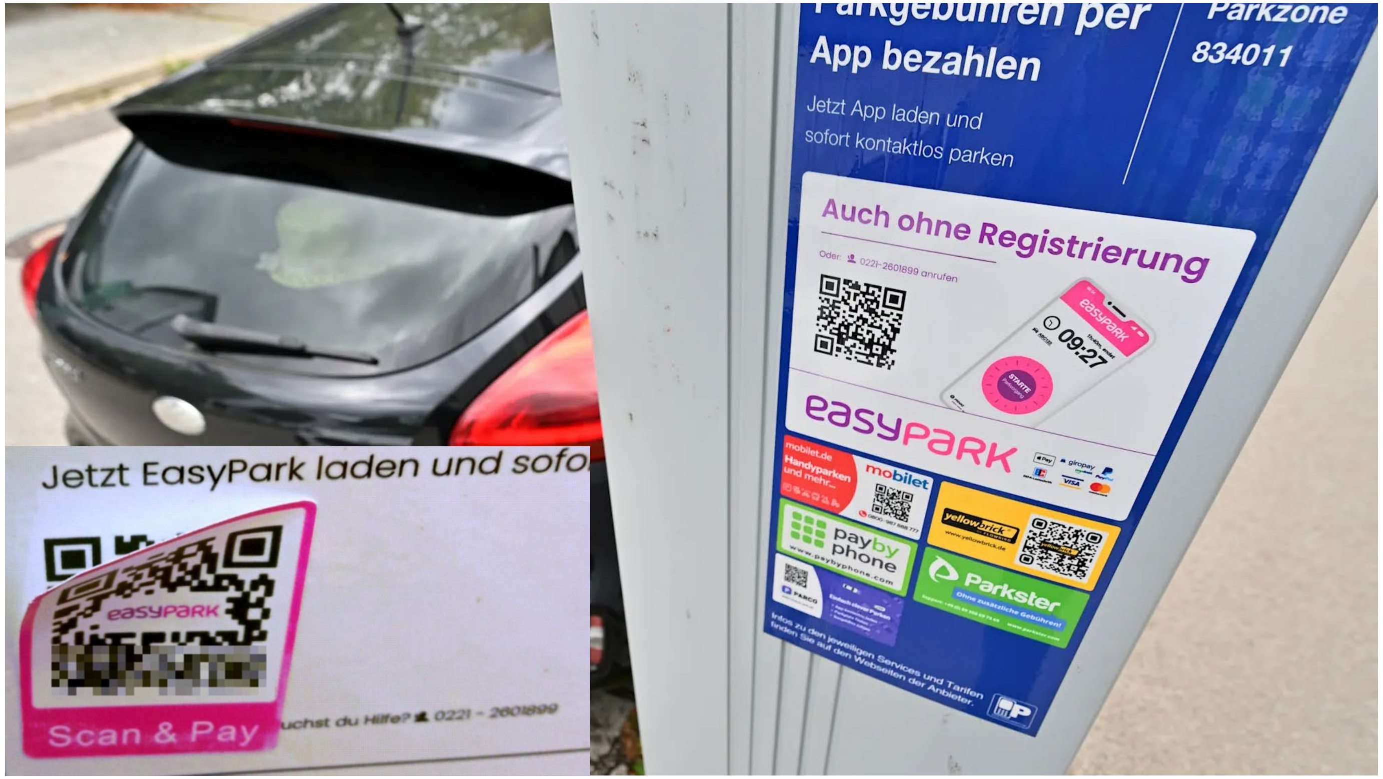
ROI
243%

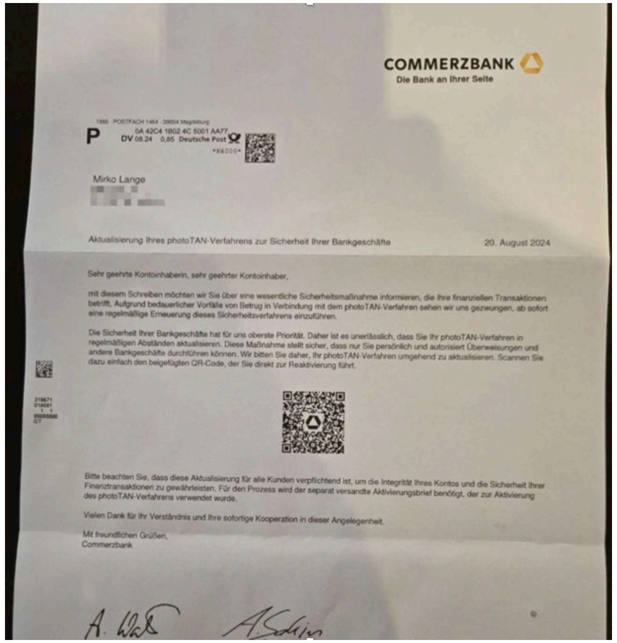




Fraud scam with QR codes: Quishing at parking machines

- Parking machines
- Charging stations
- Menus (restaurant, delivery service)
- Letter from the bank
- Timetable
- …




COMMERZBANK
Die Bank an Ihrer Seite

1886 · POSTFACH 1464 · 39004 Magdeburg
P
0A 42C4 1B02 4C 5001 AA77
DV 08.24 0,85 Deutsche Post
K4000

Mirko Lange
[redacted]

Aktualisierung Ihres photoTAN-Verfahrens zur Sicherheit Ihrer Bankgeschäfte

20. August 2024

Sehr geehrte Kontoinhaberin, sehr geehrter Kontoinhaber,

mit diesem Schreiben möchten wir Sie über eine wesentliche Sicherheitsmaßnahme informieren, die Ihre finanziellen Transaktionen betrifft. Aufgrund bedauerlicher Vorfälle von Betrug in Verbindung mit dem photoTAN-Verfahren sehen wir uns gezwungen, ab sofort eine regelmäßige Erneuerung dieses Sicherheitsverfahrens einzuführen.

Die Sicherheit Ihrer Bankgeschäfte hat für uns oberste Priorität. Daher ist es unerlässlich, dass Sie Ihr photoTAN-Verfahren in regelmäßigen Abständen aktualisieren. Diese Maßnahme stellt sicher, dass nur Sie persönlich und autorisiert Überweisungen und andere Bankgeschäfte durchführen können. Wir bitten Sie daher, Ihr photoTAN-Verfahren umgehend zu aktualisieren. Scannen Sie dazu einfach den beigefügten QR-Code, der Sie direkt zur Reaktivierung führt.

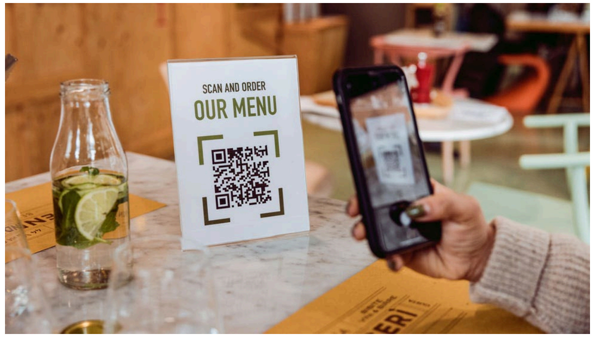
319671
018091
1 1
00000000
GT

Bitte beachten Sie, dass diese Aktualisierung für alle Kunden verpflichtend ist, um die Integrität Ihres Kontos und die Sicherheit Ihrer Finanztransaktionen zu gewährleisten. Für den Prozess wird der separat versandte Aktivierungsbrief benötigt, der zur Aktivierung des photoTAN-Verfahrens verwendet wurde.

Vielen Dank für Ihr Verständnis und Ihre sofortige Kooperation in dieser Angelegenheit.

Mit freundlichen Grüßen,
Commerzbank

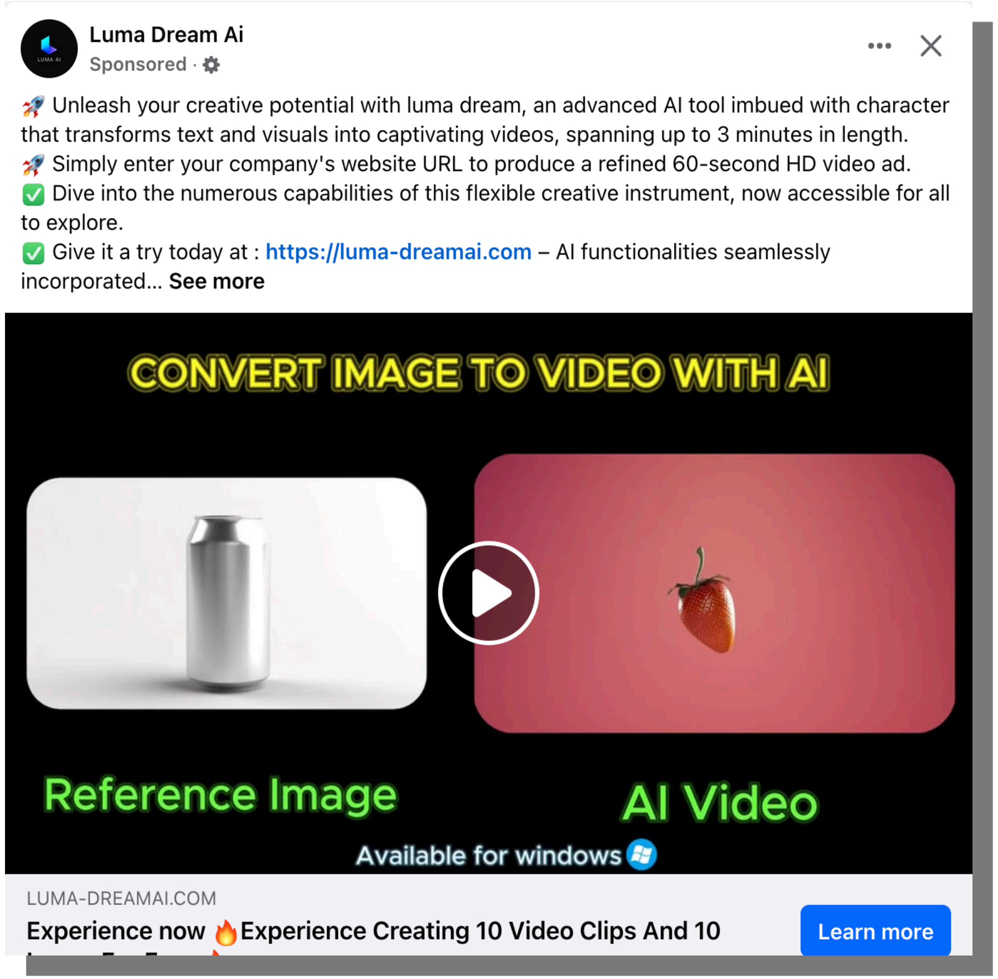
A. W A. S



infoblox

FREE AI VIDEO TOOLS

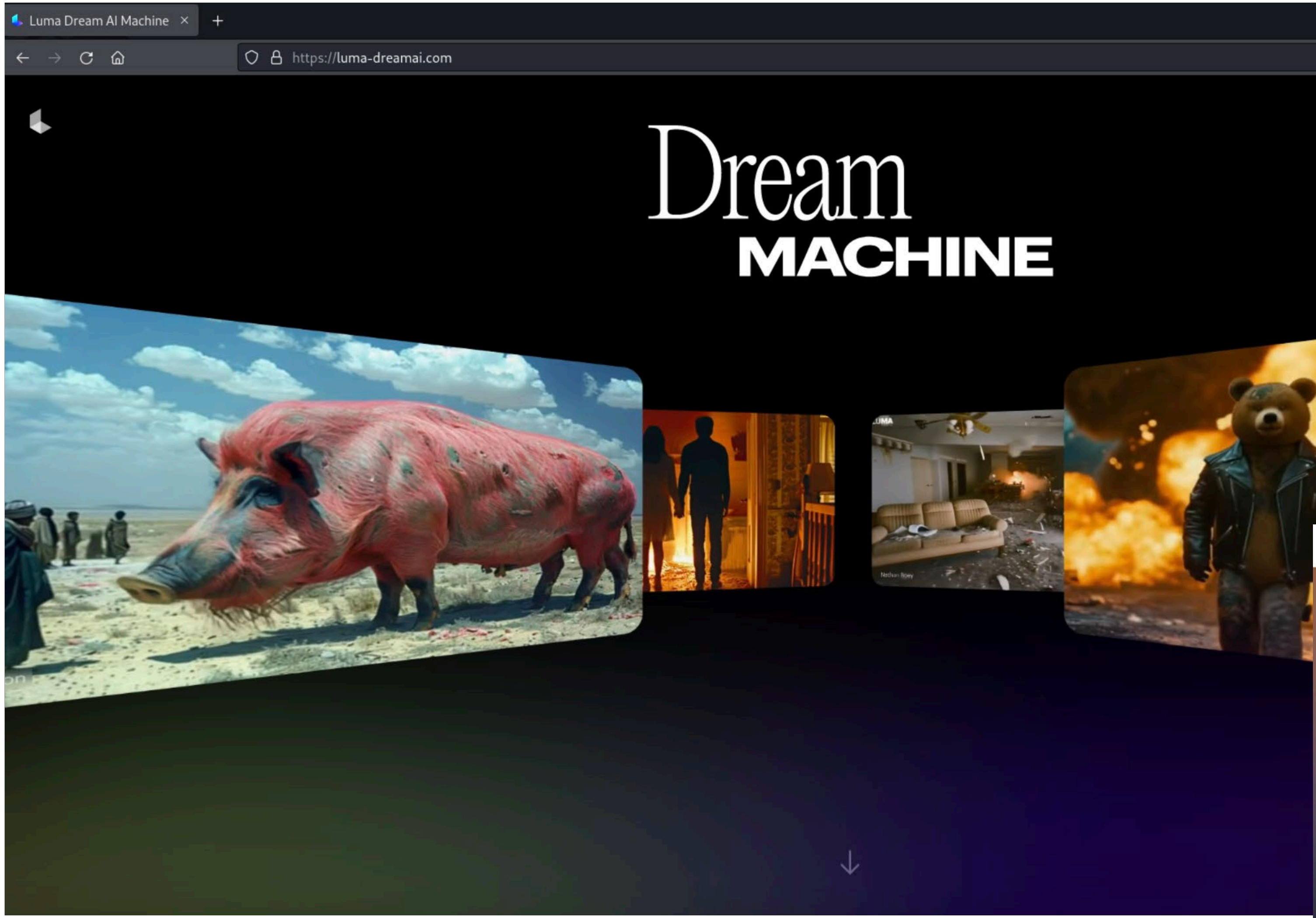
https://lumalabs.ai/dream-machine



Luma Dream Ai
Sponsored · ⚙

🚀 Unleash your creative potential with luma dream, an advanced AI tool imbued with character that transforms text and visuals into captivating videos, spanning up to 3 minutes in length.
🚀 Simply enter your company's website URL to produce a refined 60-second HD video ad.
✅ Dive into the numerous capabilities of this flexible creative instrument, now accessible for all to explore.
✅ Give it a try today at : https://luma-dreamai.com – AI functionalities seamlessly incorporated... See more

LUMA-DREAMAI.COM
Experience now 🔥Experience Creating 10 Video Clips And 10



Luma Dream AI Machine

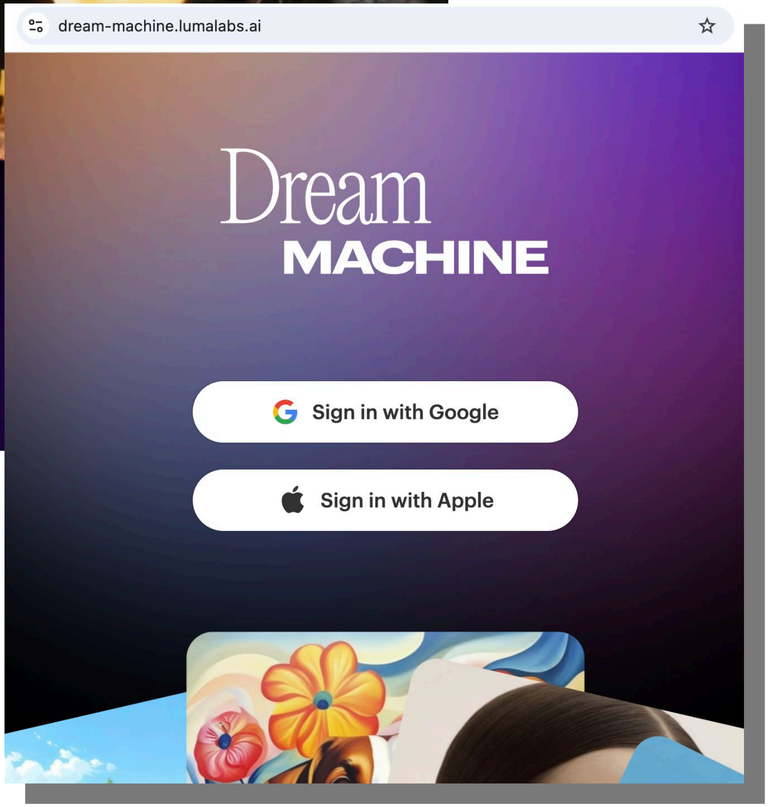
https://luma-dreamai.com

Private browsing

Start Free Now

Dream MACHINE

Fake



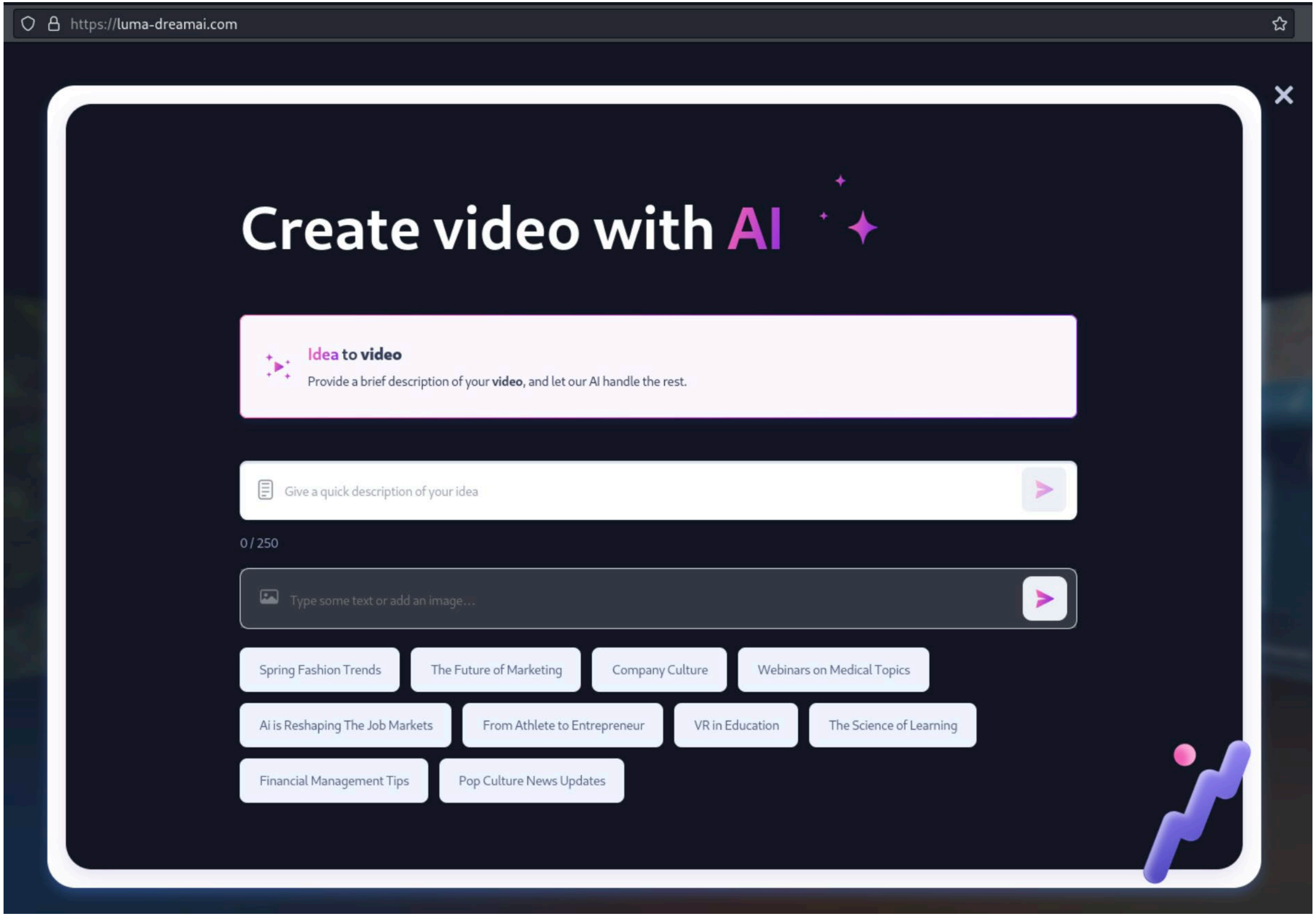
dream-machine.lumalabs.ai

Dream MACHINE

Sign in with Google

Sign in with Apple

Correct



https://luma-dreamai.com

Create video with AI

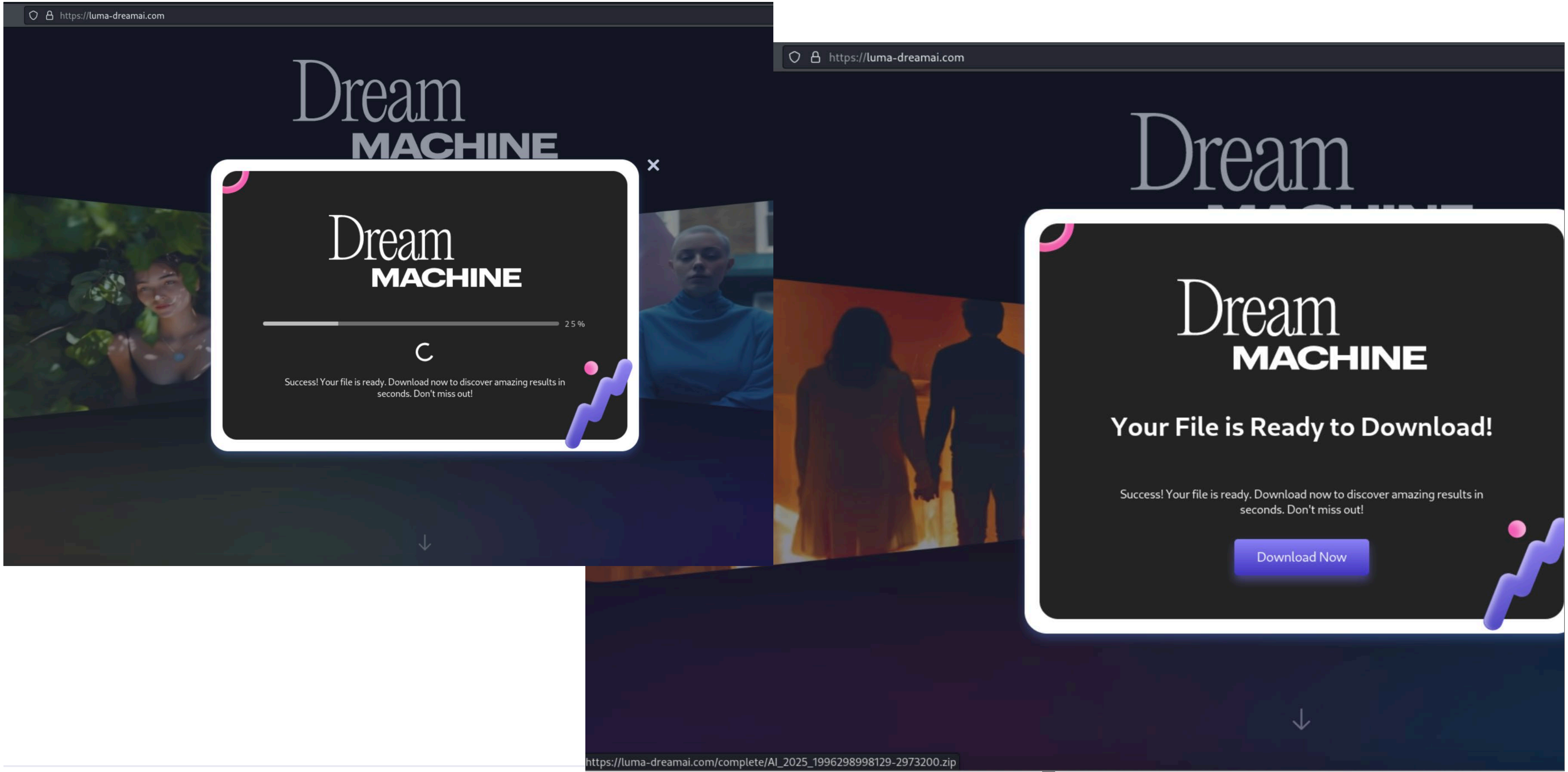
Idea to video

Provide a brief description of your **video**, and let our AI handle the rest.

Give a quick description of your idea

0 / 250

Type some text or add an image...

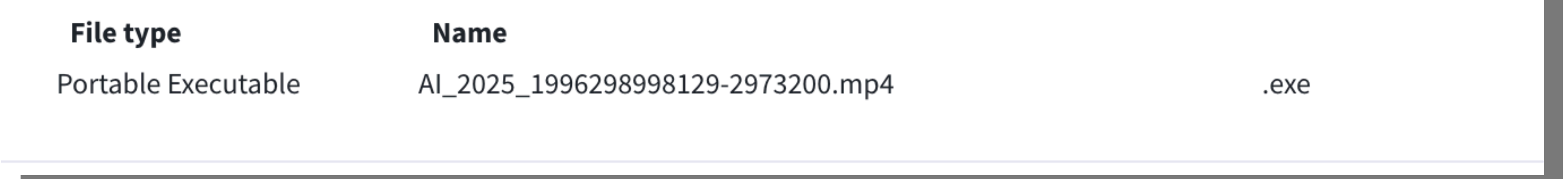


Success! Your file is ready. Download now to discover amazing results in seconds. Don't miss out!

Your File is Ready to Download!

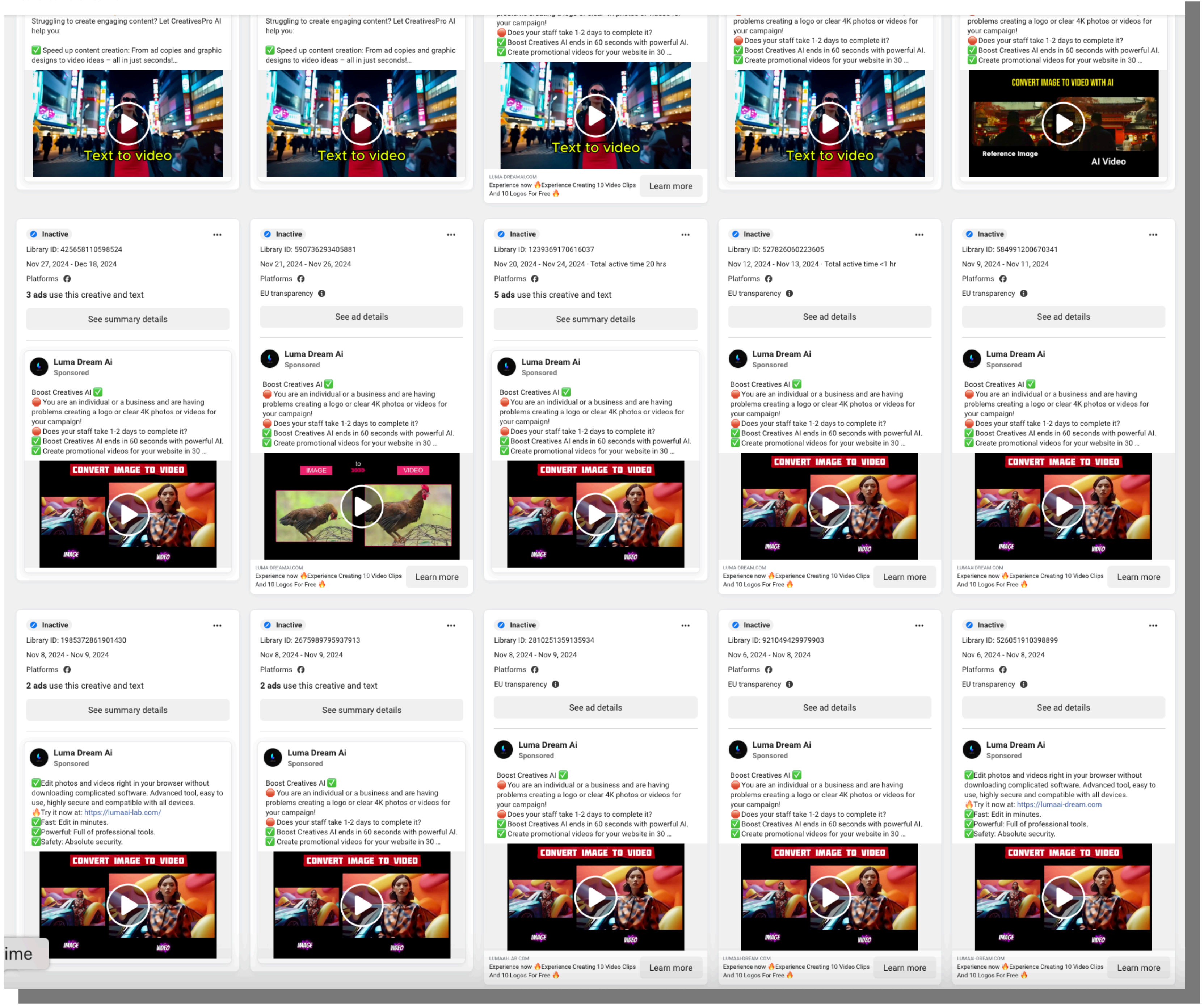
Success! Your file is ready. Download now to discover amazing results in seconds. Don't miss out!

https://luma-dreamai.com/complete/AI_2025_1996298998129-2973200.zip



File type	Name	
Portable Executable	AI_2025_1996298998129-2973200.mp4	.exe

Launched November 2024



Struggling to create engaging content? Let CreativesPro AI help you:

✅ Speed up content creation: From ad copies and graphic designs to video ideas – all in just seconds!...

Struggling to create engaging content? Let CreativesPro AI help you:

✅ Speed up content creation: From ad copies and graphic designs to video ideas – all in just seconds!...

your campaign!
🛑 Does your staff take 1-2 days to complete it?
✅ Boost Creatives AI ends in 60 seconds with powerful AI.
✅ Create promotional videos for your website in 30 ...

LUMA-DREAMAI.COM
Experience now 🔥Experience Creating 10 Video Clips And 10 Logos For Free 🔥
Learn more

problems creating a logo or clear 4K photos or videos for your campaign!
🛑 Does your staff take 1-2 days to complete it?
✅ Boost Creatives AI ends in 60 seconds with powerful AI.
✅ Create promotional videos for your website in 30 ...

problems creating a logo or clear 4K photos or videos for your campaign!
🛑 Does your staff take 1-2 days to complete it?
✅ Boost Creatives AI ends in 60 seconds with powerful AI.
✅ Create promotional videos for your website in 30 ...

Inactive
Library ID: 425658110598524
Nov 27, 2024 - Dec 18, 2024
Platforms
3 ads use this creative and text
See summary details

Luma Dream Ai
Sponsored

Boost Creatives AI ✅
🛑 You are an individual or a business and are having problems creating a logo or clear 4K photos or videos for your campaign!
🛑 Does your staff take 1-2 days to complete it?
✅ Boost Creatives AI ends in 60 seconds with powerful AI.
✅ Create promotional videos for your website in 30 ...

Inactive
Library ID: 590736293405881
Nov 21, 2024 - Nov 26, 2024
Platforms
EU transparency
See ad details

Luma Dream Ai
Sponsored

Boost Creatives AI ✅
🛑 You are an individual or a business and are having problems creating a logo or clear 4K photos or videos for your campaign!
🛑 Does your staff take 1-2 days to complete it?
✅ Boost Creatives AI ends in 60 seconds with powerful AI.
✅ Create promotional videos for your website in 30 ...

LUMA-DREAMAI.COM
Experience now 🔥Experience Creating 10 Video Clips And 10 Logos For Free 🔥
Learn more

Inactive
Library ID: 1239369170616037
Nov 20, 2024 - Nov 24, 2024 · Total active time 20 hrs
Platforms
5 ads use this creative and text
See summary details

Luma Dream Ai
Sponsored

Boost Creatives AI ✅
🛑 You are an individual or a business and are having problems creating a logo or clear 4K photos or videos for your campaign!
🛑 Does your staff take 1-2 days to complete it?
✅ Boost Creatives AI ends in 60 seconds with powerful AI.
✅ Create promotional videos for your website in 30 ...

Inactive
Library ID: 527826060223605
Nov 12, 2024 - Nov 13, 2024 · Total active time <1 hr
Platforms
EU transparency
See ad details

Luma Dream Ai
Sponsored

Boost Creatives AI ✅
🛑 You are an individual or a business and are having problems creating a logo or clear 4K photos or videos for your campaign!
🛑 Does your staff take 1-2 days to complete it?
✅ Boost Creatives AI ends in 60 seconds with powerful AI.
✅ Create promotional videos for your website in 30 ...

LUMA-DREAM.COM
Experience now 🔥Experience Creating 10 Video Clips And 10 Logos For Free 🔥
Learn more

Inactive
Library ID: 584991200670341
Nov 9, 2024 - Nov 11, 2024
Platforms
EU transparency
See ad details

Luma Dream Ai
Sponsored

Boost Creatives AI ✅
🛑 You are an individual or a business and are having problems creating a logo or clear 4K photos or videos for your campaign!
🛑 Does your staff take 1-2 days to complete it?
✅ Boost Creatives AI ends in 60 seconds with powerful AI.
✅ Create promotional videos for your website in 30 ...

LUMAAIDREAM.COM
Experience now 🔥Experience Creating 10 Video Clips And 10 Logos For Free 🔥
Learn more

Inactive
Library ID: 1985372861901430
Nov 8, 2024 - Nov 9, 2024
Platforms
2 ads use this creative and text
See summary details

Luma Dream Ai
Sponsored

✅Edit photos and videos right in your browser without downloading complicated software. Advanced tool, easy to use, highly secure and compatible with all devices.
🔥Try it now at: https://lumaai-lab.com/
✅Fast: Edit in minutes.
✅Powerful: Full of professional tools.
✅Safety: Absolute security.

Inactive
Library ID: 2675989795937913
Nov 8, 2024 - Nov 9, 2024
Platforms
2 ads use this creative and text
See summary details

Luma Dream Ai
Sponsored

Boost Creatives AI ✅
🛑 You are an individual or a business and are having problems creating a logo or clear 4K photos or videos for your campaign!
🛑 Does your staff take 1-2 days to complete it?
✅ Boost Creatives AI ends in 60 seconds with powerful AI.
✅ Create promotional videos for your website in 30 ...

Inactive
Library ID: 2810251359135934
Nov 8, 2024 - Nov 9, 2024
Platforms
EU transparency
See ad details

Luma Dream Ai
Sponsored

Boost Creatives AI ✅
🛑 You are an individual or a business and are having problems creating a logo or clear 4K photos or videos for your campaign!
🛑 Does your staff take 1-2 days to complete it?
✅ Boost Creatives AI ends in 60 seconds with powerful AI.
✅ Create promotional videos for your website in 30 ...

LUMAAI-LAB.COM
Experience now 🔥Experience Creating 10 Video Clips And 10 Logos For Free 🔥
Learn more

Inactive
Library ID: 921049429979903
Nov 6, 2024 - Nov 8, 2024
Platforms
EU transparency
See ad details

Luma Dream Ai
Sponsored

Boost Creatives AI ✅
🛑 You are an individual or a business and are having problems creating a logo or clear 4K photos or videos for your campaign!
🛑 Does your staff take 1-2 days to complete it?
✅ Boost Creatives AI ends in 60 seconds with powerful AI.
✅ Create promotional videos for your website in 30 ...

LUMAAI-DREAM.COM
Experience now 🔥Experience Creating 10 Video Clips And 10 Logos For Free 🔥
Learn more

Inactive
Library ID: 526051910398899
Nov 6, 2024 - Nov 8, 2024
Platforms
EU transparency
See ad details

Luma Dream Ai
Sponsored

✅Edit photos and videos right in your browser without downloading complicated software. Advanced tool, easy to use, highly secure and compatible with all devices.
🔥Try it now at: https://lumaai-dream.com
✅Fast: Edit in minutes.
✅Powerful: Full of professional tools.
✅Safety: Absolute security.

LUMAAI-DREAM.COM
Experience now 🔥Experience Creating 10 Video Clips And 10 Logos For Free 🔥
Learn more

ime

Burglar / Thief want to get into a company

“Safe company”

Mahlzeit!!
MOTION SENSOR
???

Attackers want to get into a company

IDS

"Safe company"

IPS

IPS

MOTION SENSOR

IDS

Next Generation Firewall

Sandbo
xing

Firewall

DNS Data Infiltration

DNS Data Exfiltration

infoblox

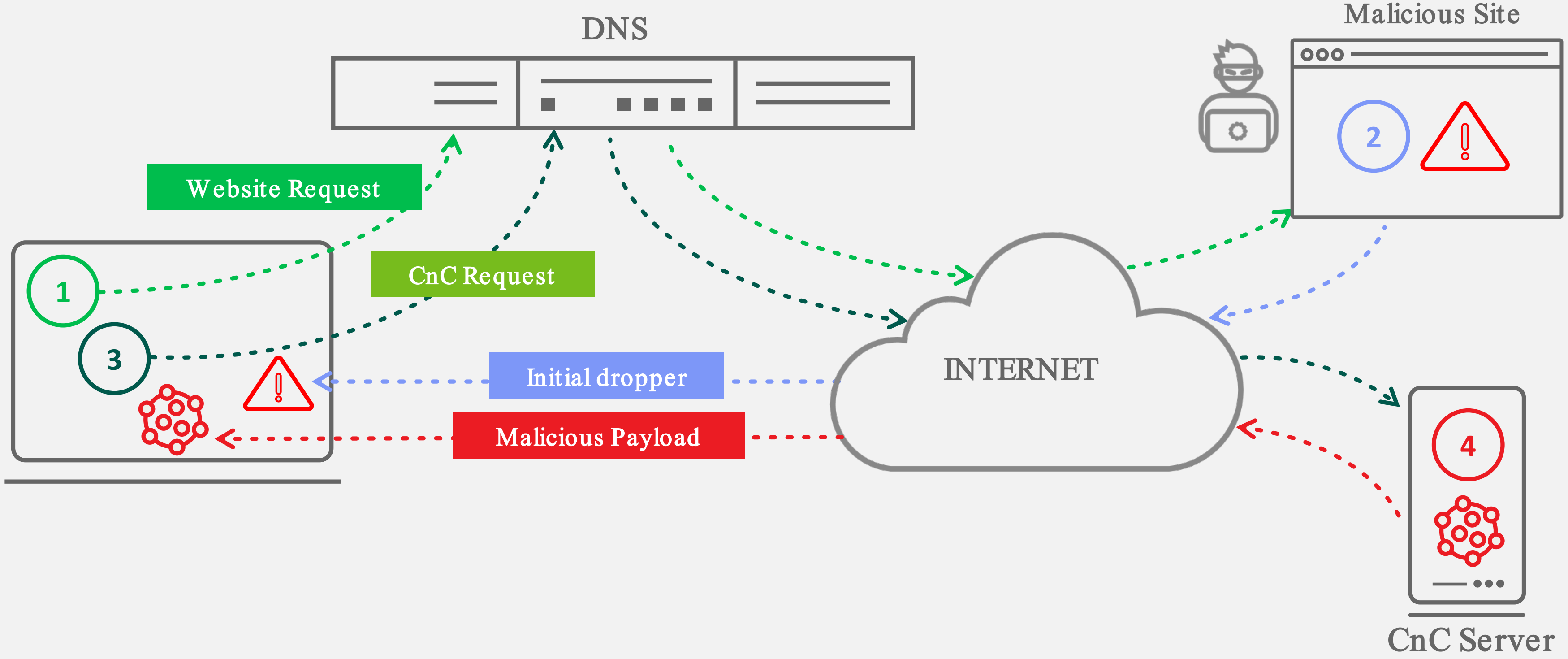
Common Attack Steps Review

1 User directed to malicious site

2 Website delivers initial exploit

3 Exploit contacts Command and Control (CnC) server

4 Malicious payload downloaded



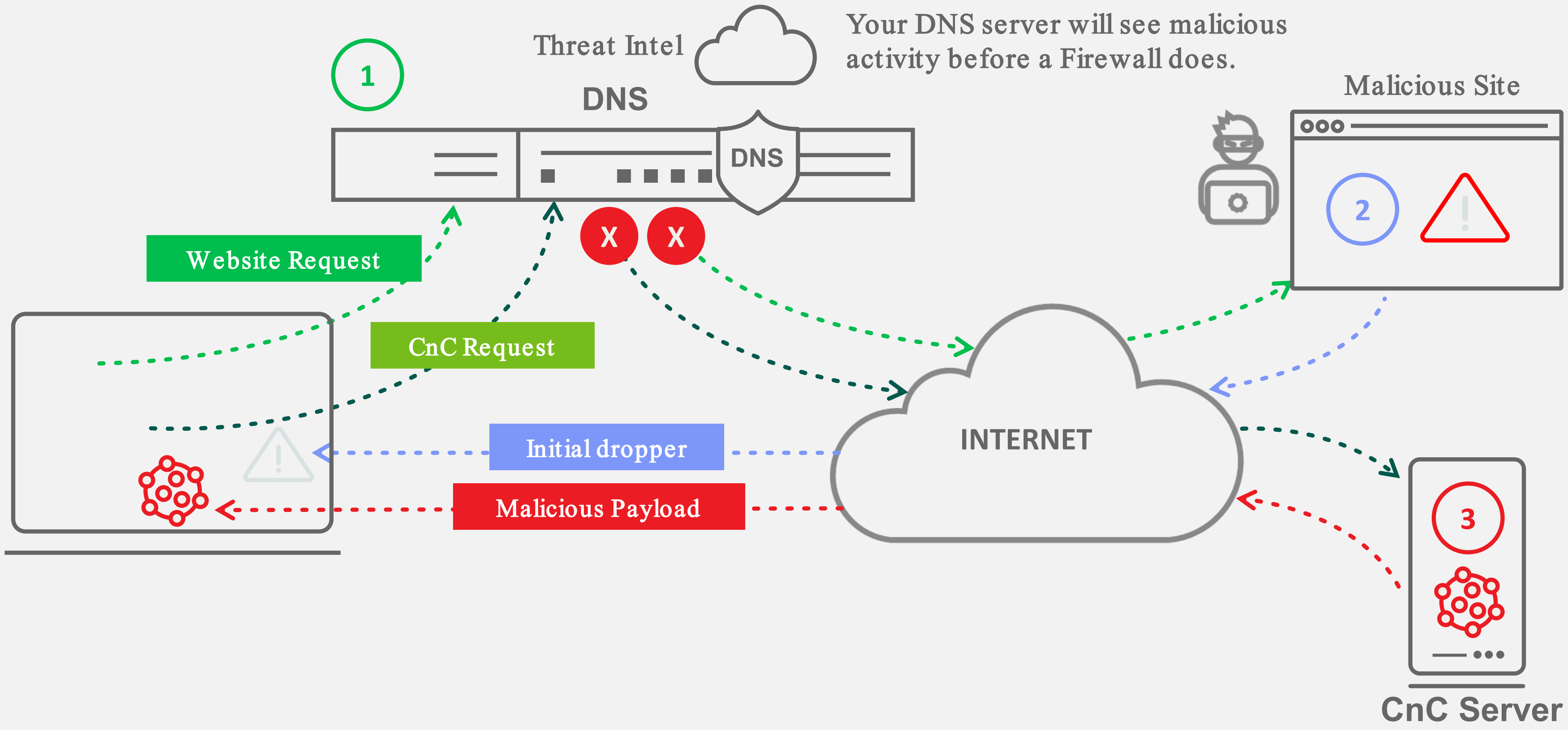
DNS is used for all outbound traffic requests

Leveraging DDI Intelligence for Foundational Security

1 Curated threat intelligence for DNS

2 Connection to malicious website blocked at DNS

3 If already infected, system blocked from connecting to CnC at DNS



Secure DNS breaks the attack chain from the start

Infoblox
Threat Intel

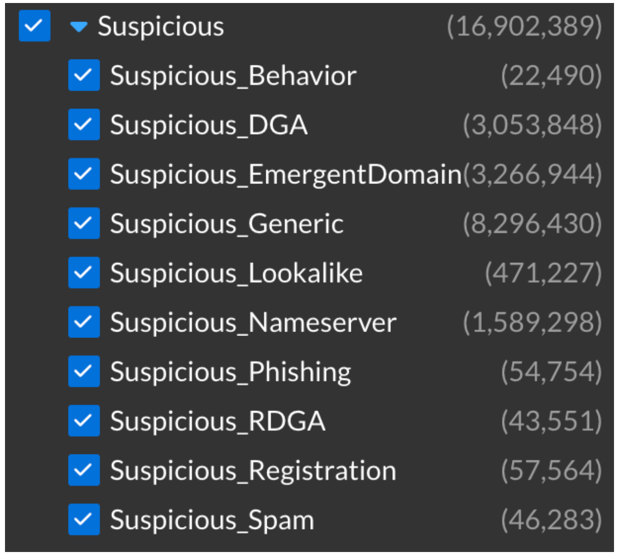
SUSPICIOUS DOMAINS

DETECTION

- Cybercriminals use aging techniques to bypass New Domain Quarantine feeds.
- Infoblox categorizes suspicious new domains, lookalikes and others based on their construction and/ or behavior reputation scores (Infoblox patented algorithm)
- When: before confirmation of any malicious activity.
- The Suspicious Feed allows our customers to optimize the chances of stopping major attacks before they happen and respond quickly to the ever-changing threat landscape

In total in 2024, the customer-reported false positive rate was below 0.0002%

Infoblox has identified 16 million suspicious domains as of August 2024



☑ ▾ Suspicious	(16,902,389)
☑ Suspicious_Behavior	(22,490)
☑ Suspicious_DGA	(3,053,848)
☑ Suspicious_EmergentDomain	(3,266,944)
☑ Suspicious_Generic	(8,296,430)
☑ Suspicious_Lookalike	(471,227)
☑ Suspicious_Nameserver	(1,589,298)
☑ Suspicious_Phishing	(54,754)
☑ Suspicious_RDGA	(43,551)
☑ Suspicious_Registration	(57,564)
☑ Suspicious_Spam	(46,283)

DNS THREAT HUNTING - DNS FINGERPRINTS (SIGNATURES)

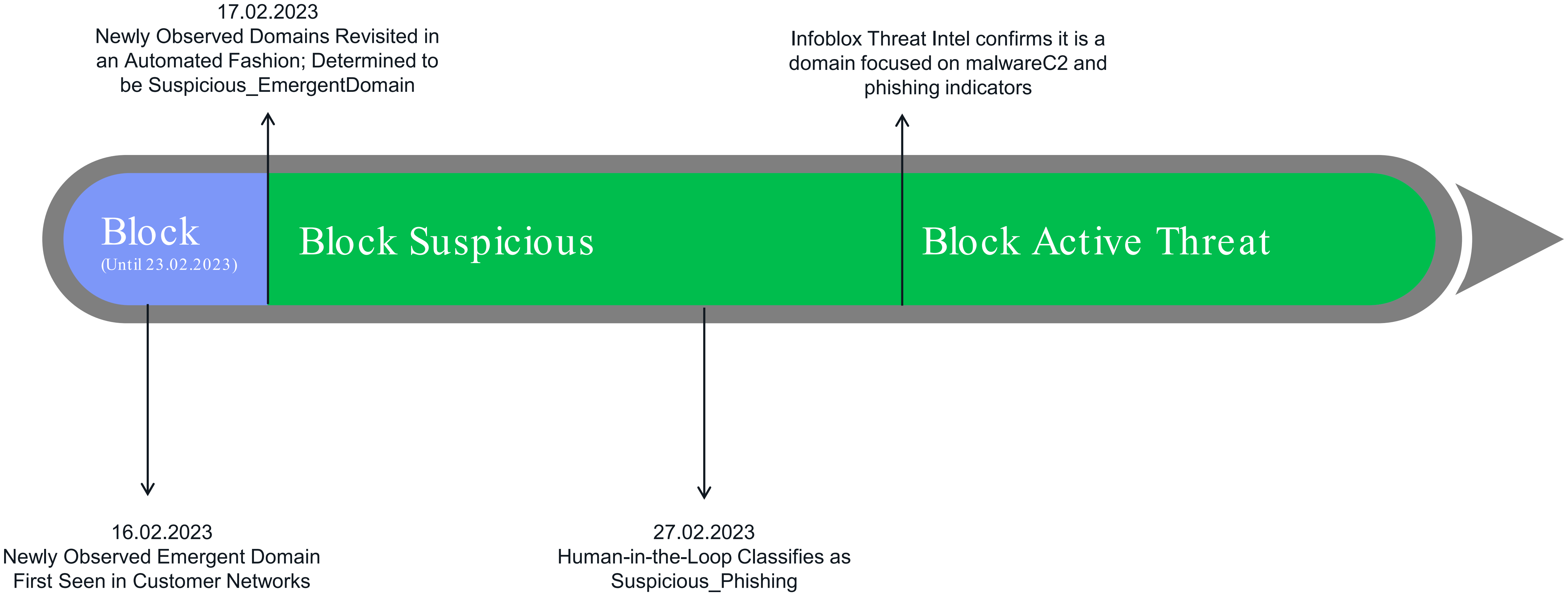
DNS Minutiae Patterns:

- Hosting IP addresses
- Name servers
- Mail servers
- CNAME records
- Registrars
- Registrant organizations
- SOA Records
- TTL Values

EMERGENT DOMAINS

INDICATOR EKISENOS-JP[.]TOP

+10 days average time between domain registration and first malicious query



17.02.2023
Newly Observed Domains Revisited in an Automated Fashion; Determined to be Suspicious_EmergentDomain

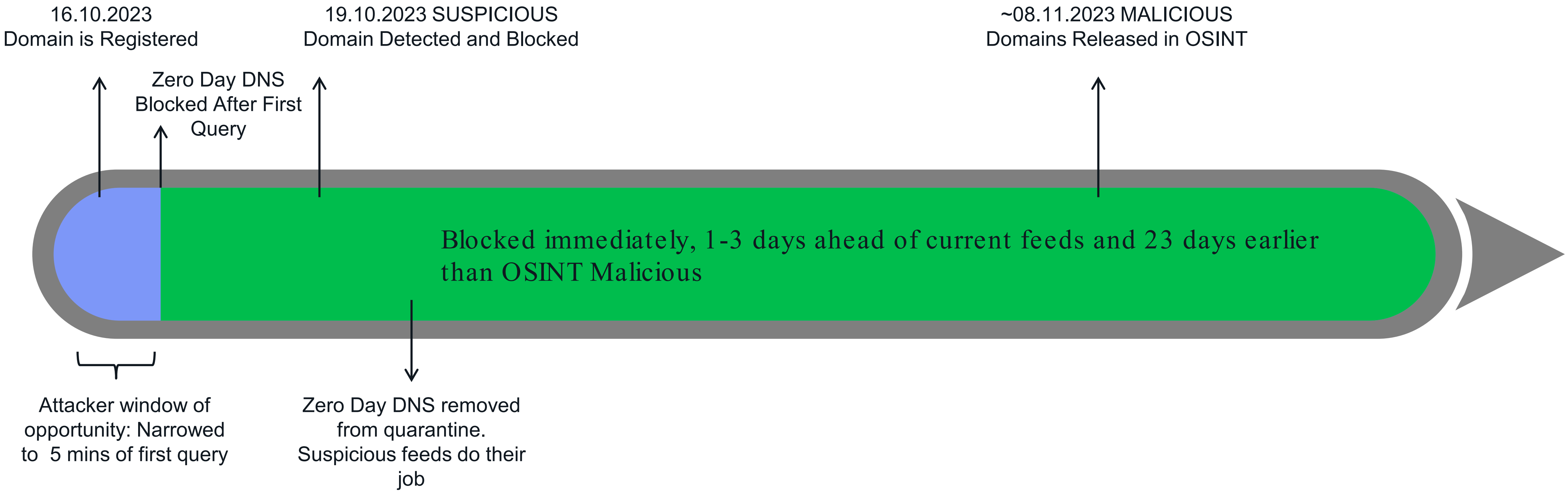
Infoblox Threat Intel confirms it is a domain focused on malwareC2 and phishing indicators

16.02.2023
Newly Observed Emergent Domain First Seen in Customer Networks

27.02.2023
Human-in-the-Loop Classifies as Suspicious_Phishing

ZERO DAY DNS™

- Attackers are registering and using lookalike domains almost immediately as part of targeted spear phishing attacks
- Infoblox's Zero Day DNS™ capability blocks threats from first-seen domains that are registered just minutes to hours before being used in an attack
- Near real-time monitoring/ intercepting targeted attacks like spear phishing



16.10.2023
Domain is Registered

Zero Day DNS
Blocked After First
Query

19.10.2023 SUSPICIOUS
Domain Detected and Blocked

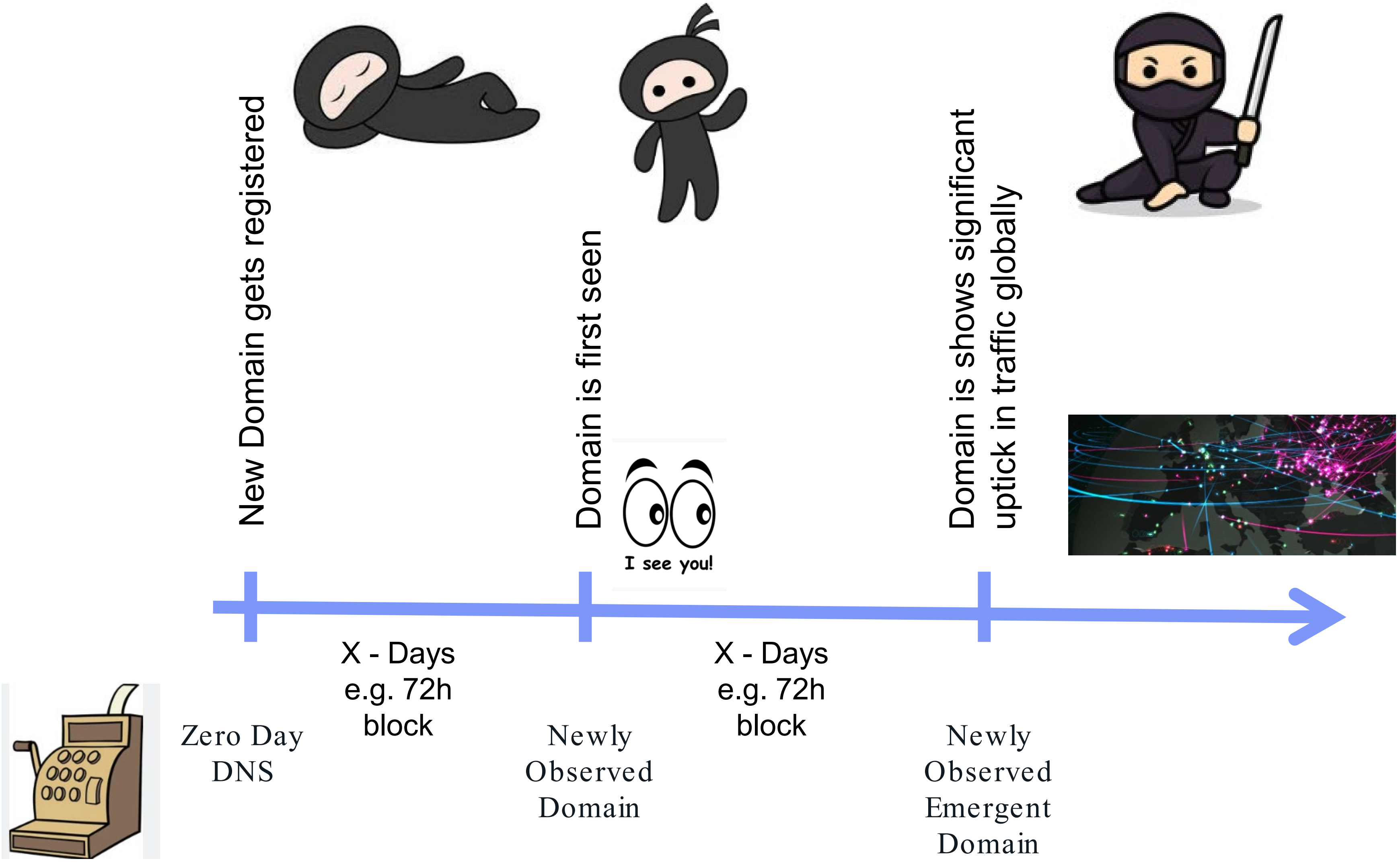
~08.11.2023 MALICIOUS
Domains Released in OSINT

Blocked immediately, 1-3 days ahead of current feeds and 23 days earlier than OSINT Malicious

Attacker window of opportunity: Narrowed to 5 mins of first query

Zero Day DNS removed from quarantine. Suspicious feeds do their job

Newly-Registered, -Observed, -Observed Emergent Domains



New Domain gets registered

Domain is first seen

Domain is shows significant uptick in traffic globally

Zero Day DNS

X - Days e.g. 72h block

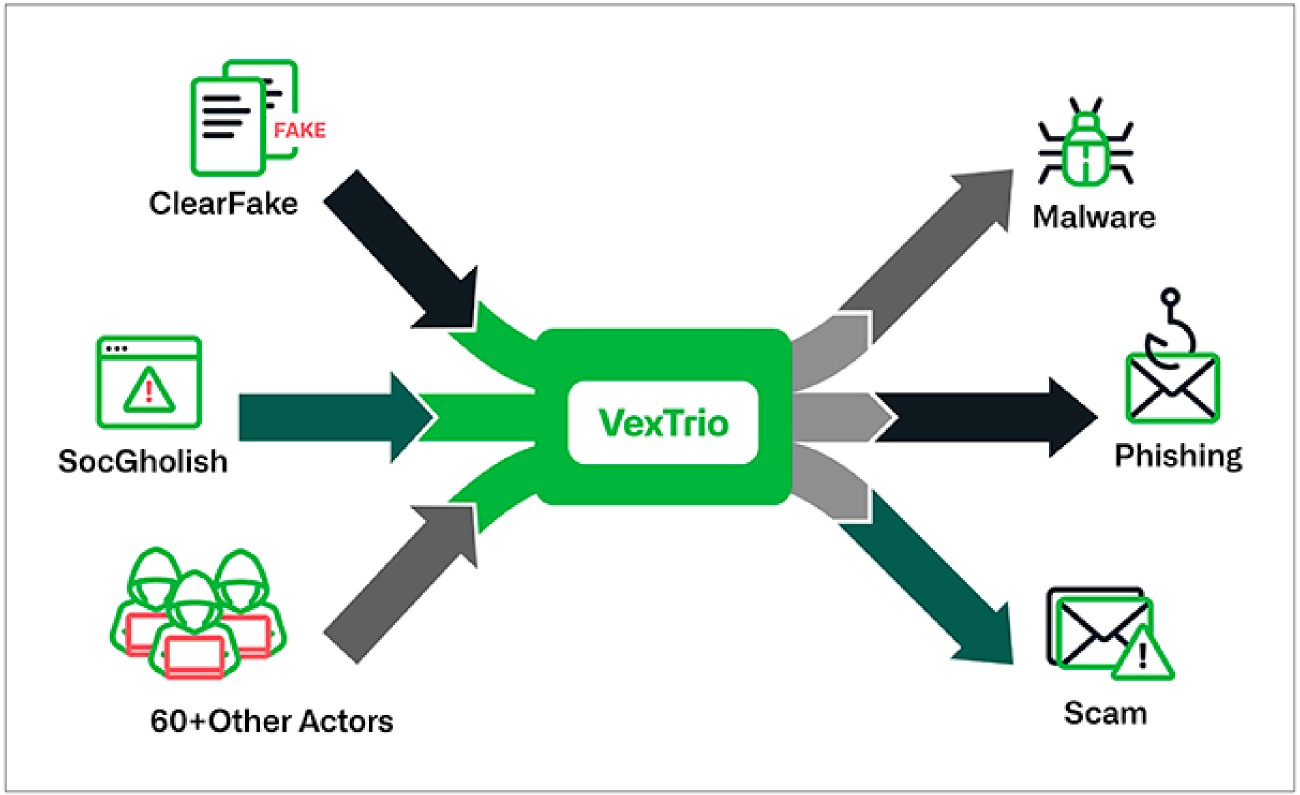
Newly Observed Domain

X - Days e.g. 72h block

Newly Observed Emergent Domain

CYBERCRIME CENTRAL: VEXTRIO OPERATES MASSIVE CRIMINAL AFFILIATE PROGRAM

- ➢ SocGholish and ClearFake are most associated with malware and fake software update pages.
- ➢ VexTrio operates **traffic distribution systems** (TDSs)
- ➢ All are a part of the cybercrime economy.
- ➢ VexTrio is the **single most pervasive** threat in our customers' networks.
- ➢ Of VexTrio more than 70k known domains, **nearly half** have been observed in customer networks.
- ➢ We found Vextrio in **over half** of all customer networks in the last two years.

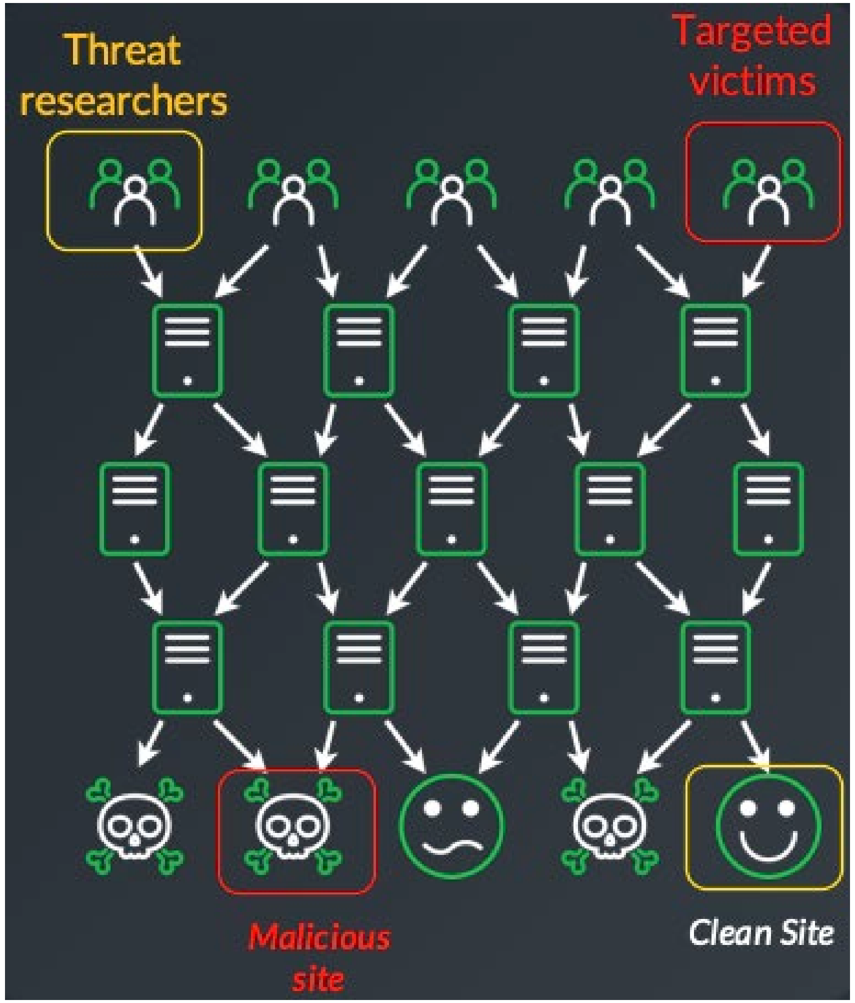


=> block the infrastructure!!

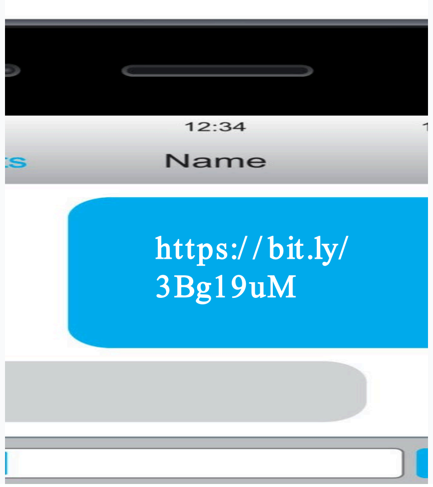
infoblox

Traffic Distribution Systems

- **50%** of customer networks
- **+600,000** Registered domains
- TDSs exist for years and are resilient to take-downs
- **DNS** is the best place to stop cybercrime using a TDS
- TDSs route victims through a maze of domains delivering malicious content and **throw off researchers.**
- Redirection can be done on multiple techniques.

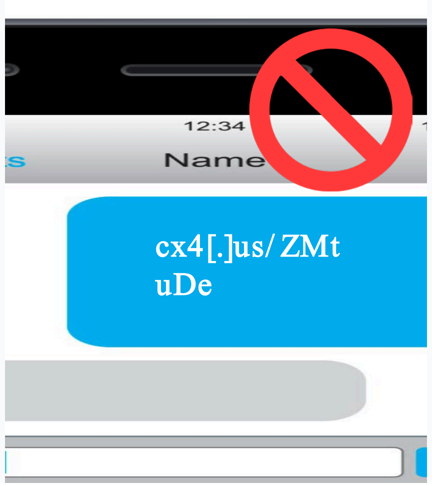


EXAMPLE – PROLIFIC PUMA



https://bit.ly/3Bg19uM

Legitimate Link Shortening Service



cx4[.]us/ZMtuDe

Illegitimate Link Shortening Service – Prolific Puma

Attackers can't use Bitly to shorten their links

So they use Prolific Puma malicious link shortening service

Since April 2022, Prolific Puma has registered up to 75k unique domains

If you know what the attackers are using, you can block their supply chain

Infoblox Actor Naming Convention

Descriptor: Chosen by Threat Researcher

+

Animal: Defined by DNS Technique

Rabbit Registered Domain Generation Algorithm

Lizard Lookalike Domain

Meerkat MX Abuse

Hawk Hijack Domains

Puma TDS Link shortener

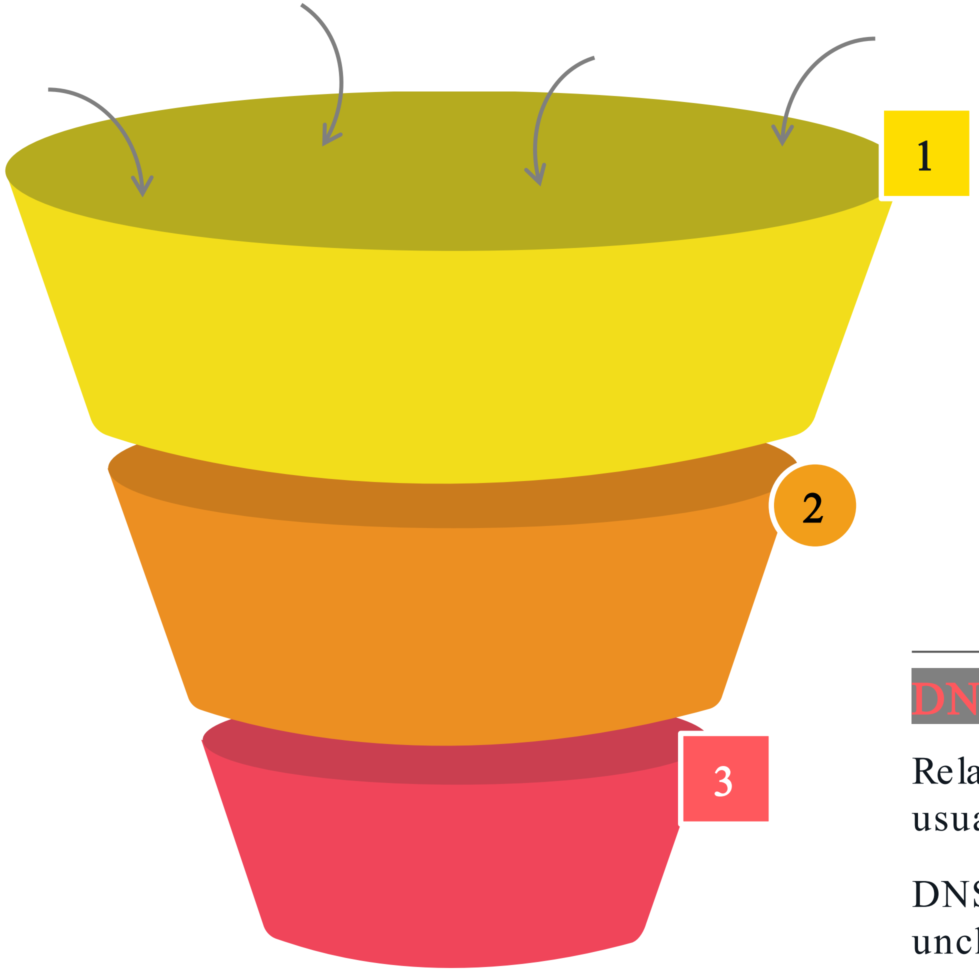
Viper TDS HTTP Based

Seahorse TDS DNS CNAME

Dog DNS C2 Malware

THREAT INTEL

EMERGENT/ SUSPICIOUS, MALICIOUS AND THREAT ACTORS



Suspicious Domains and IP Addresses

Large volume, low regret of blocking, emergent threats

Broad based methods that involves reputation, proximity to existing bad infrastructure, and patterns of registration or queries

Malicious Domains and IP Addresses

Medium volume, very high confidence of malicious intent

Analytics that are tied to specific bad actor techniques and infrastructure

DNS Threat Actor

Relate domains and IP addresses to the same actor, usually persistent

DNS fingerprint driven analysis and review of unclassified domains or previous detections

DISRUPTING THE SECURITY INDUSTRY

Our Differentiated Approach

INFOBLOX

- **DNS-focused**
  - Domain name features
  - Registration features
  - Resource record features
- **Upstream**
  - "Leans Left" – prevention

TYPICAL SECURITY VENDOR

- **Malware-focused**
  - What malware is used?
  - How and where is it deployed?
  - What are the capabilities?
- **Downstream**
  - "Leans Right" – mitigation

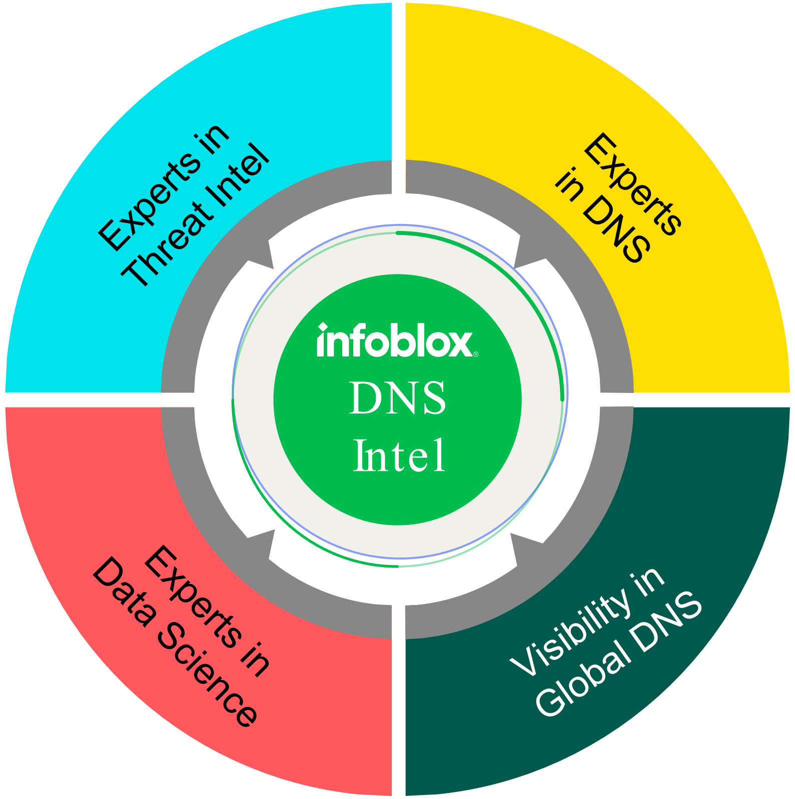
Infoblox Threat Intel

DNS All Day, Every Day

DNS is notoriously tricky to interpret and hunt from, but our deep understanding and unique access give us a high-powered scope to zero in on cyber threats.

- ➢ 75% of threats **detected before the first DNS query!**
- ➢ 63 days of protection on average **before OSINT!**
- ➢ 0.0002% false positive rate (2023)
- ➢ +20 million new suspicious and malicious indicators
- ➢ 4 Million new indicators added **per month**
- ➢ 70 Billion DNS events analyzed **daily**

- ➢ >500 Hours SOC analyst hours saved per month
- ➢ 400K USD SOC Productivity savings per year

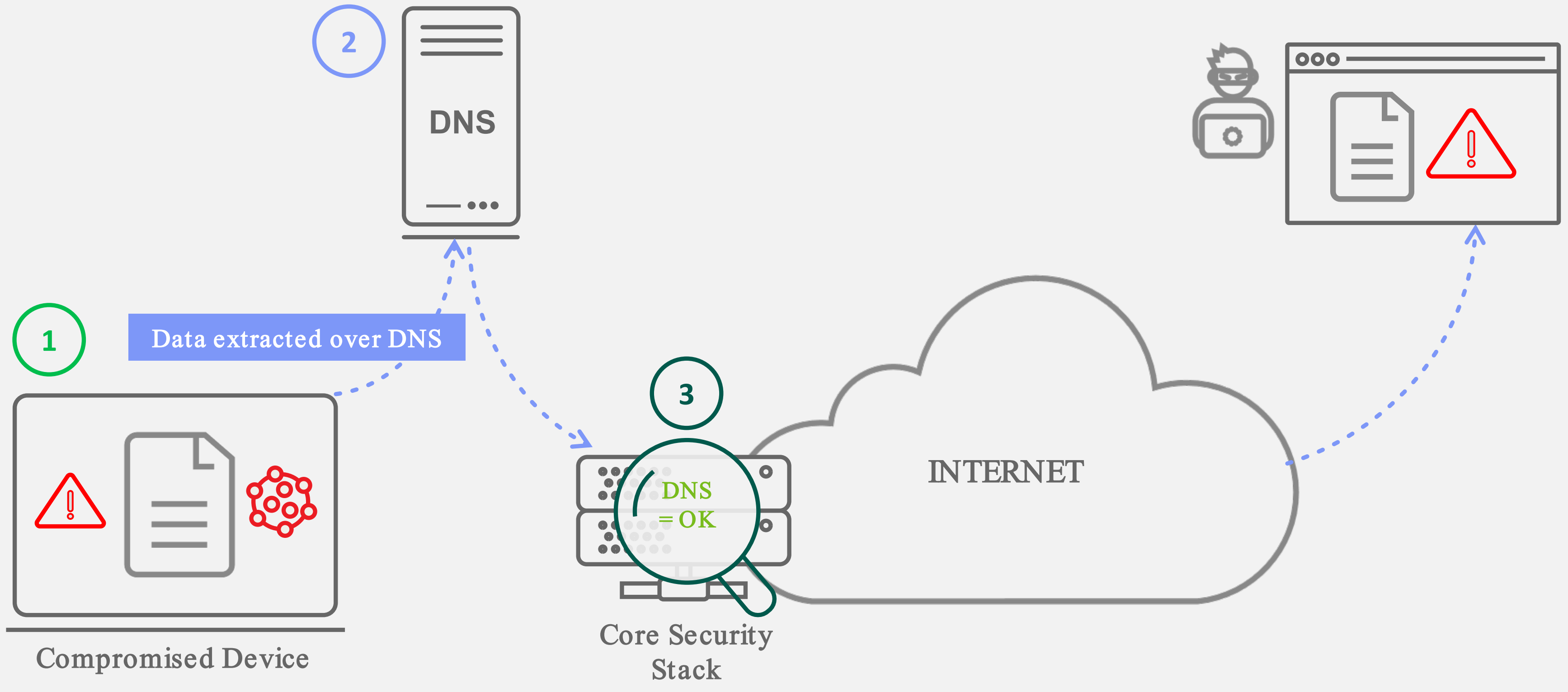


Data Exfiltration over DNS

1 Malware on device seeks sensitive data

2 Malware uses DNS channel to send data

3 Traditional security does not inspect DNS traffic



Sensitive data tunnelled over DNS protocols to avoid detection

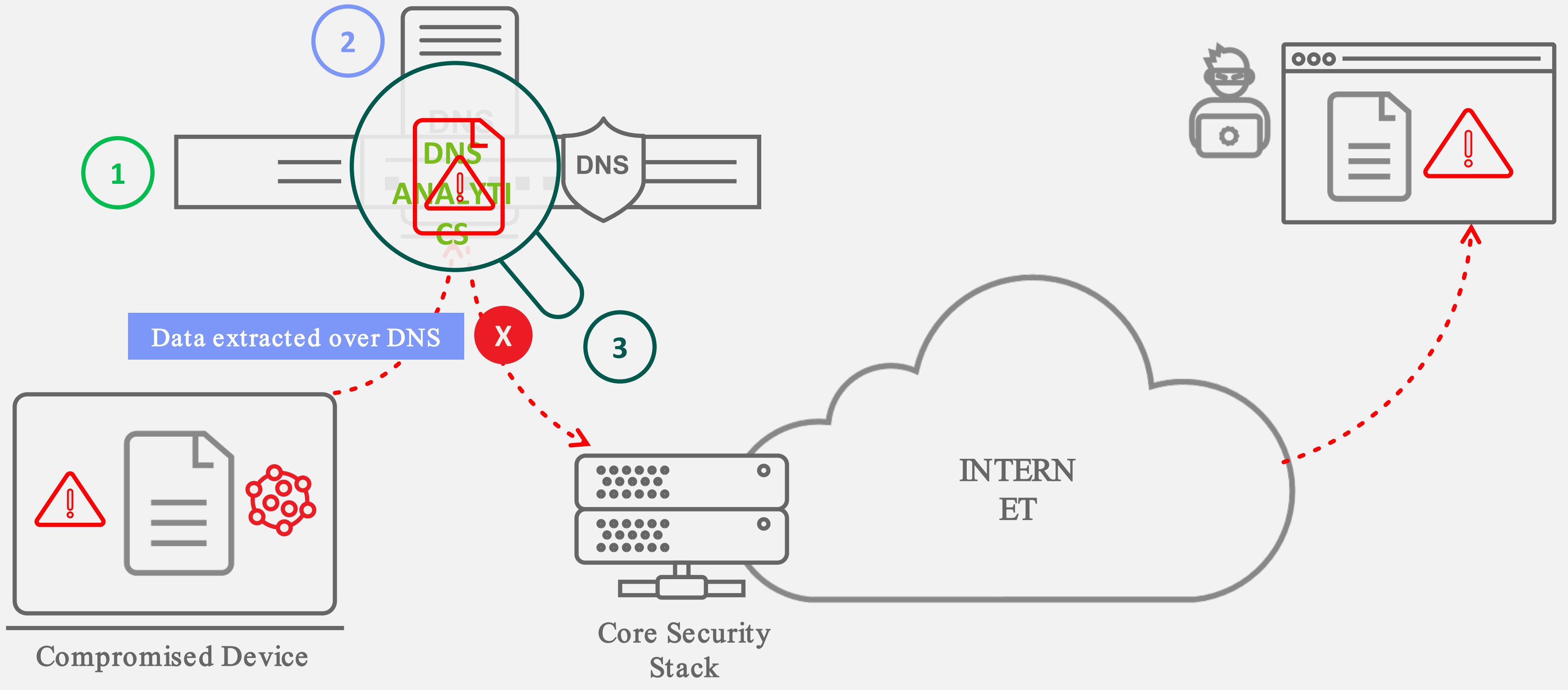
infoblox

Protecting Against Data Exfiltration over DNS

1 DNS with threat intelligence and analytics

2 Machine learning analytics inspects DNS traffic, detects data exfil

3 Data prevented from exiting enterprise by blocking DNS request to destination



Attempted data exfiltration over DNS protocols detected and blocked

Detecting DNS Tunnels & Data Exfiltration

Infoblox approach

Signature

Use **Advanced DNS Protection** to detect and block all known DNS Tunneling tools
(in hardware, at line speed)

Reputation

Use **DNS Firewall** to automatically block known tunnel, C2 and data exfiltration endpoints and newly registered domains

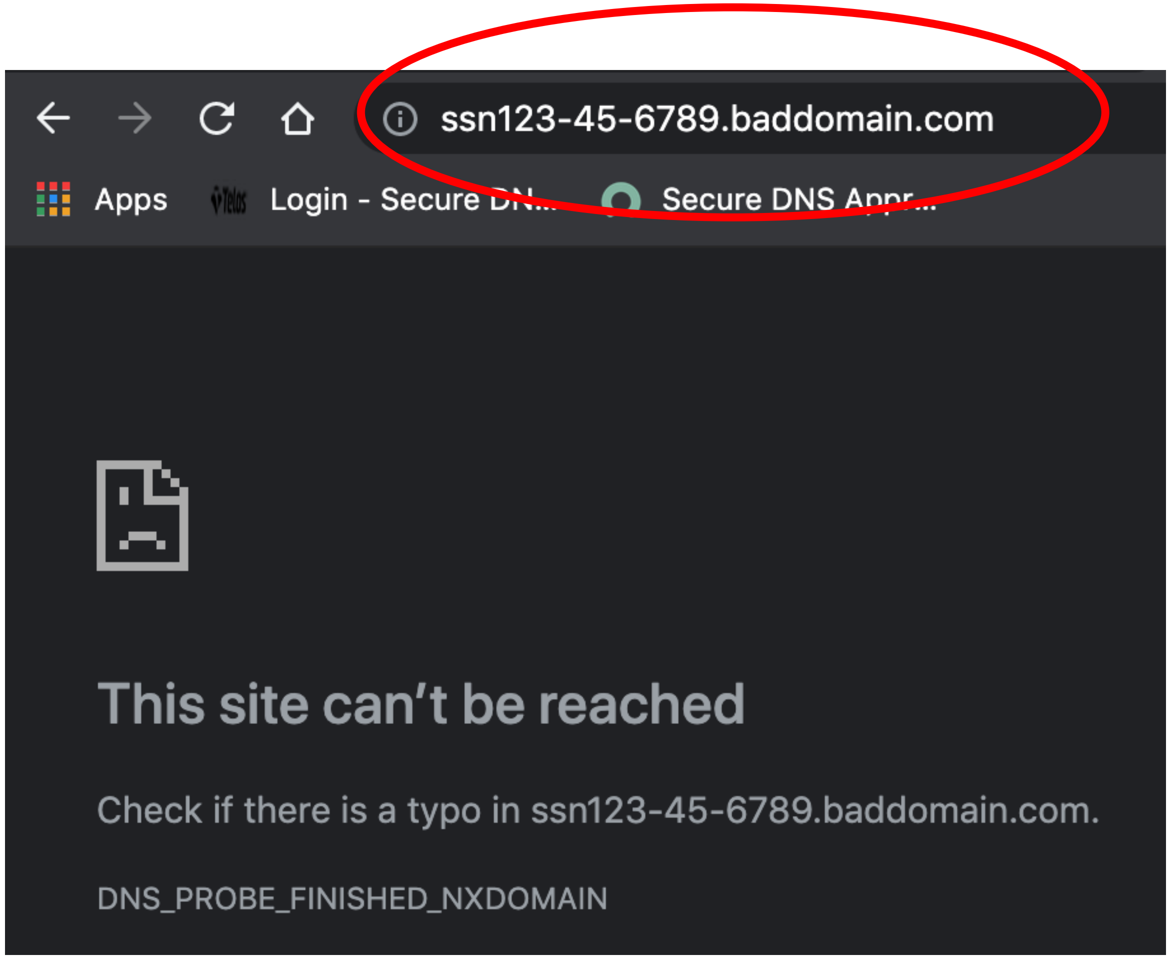
01100
10110

Behavior

Use **Threat Insight** to detect and block zero day data exfiltration, using real-time streaming analytics to mitigate against previously unseen code

PROTECT

DETECTING BAD DOMAINS



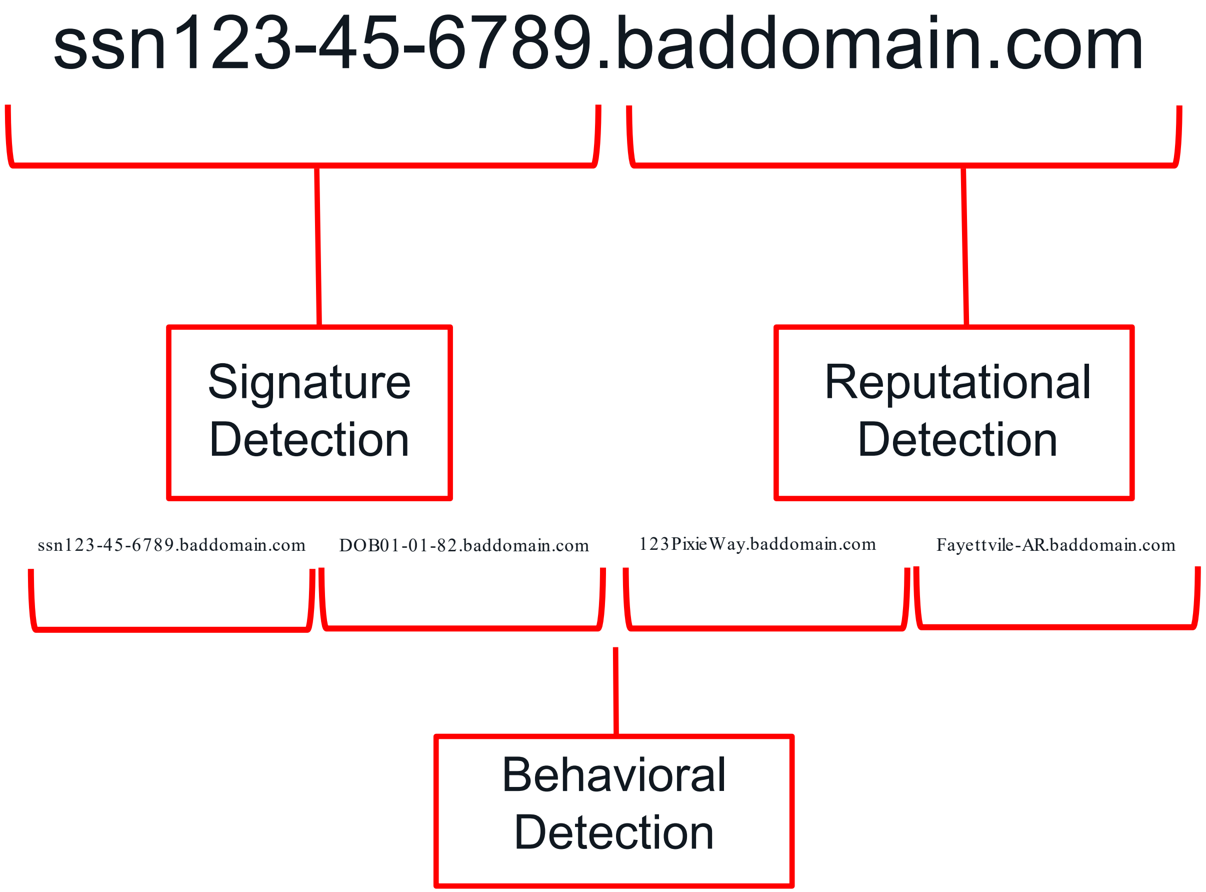
ssn123-45-6789.baddomain.com

Apps Login - Secure DN... Secure DNS Appr...

This site can’t be reached

Check if there is a typo in ssn123-45-6789.baddomain.com.

DNS_PROBE_FINISHED_NXDOMAIN



ssn123-45-6789.baddomain.com

Signature Detection

Reputational Detection

ssn123-45-6789.baddomain.com

DOB01-01-82.baddomain.com

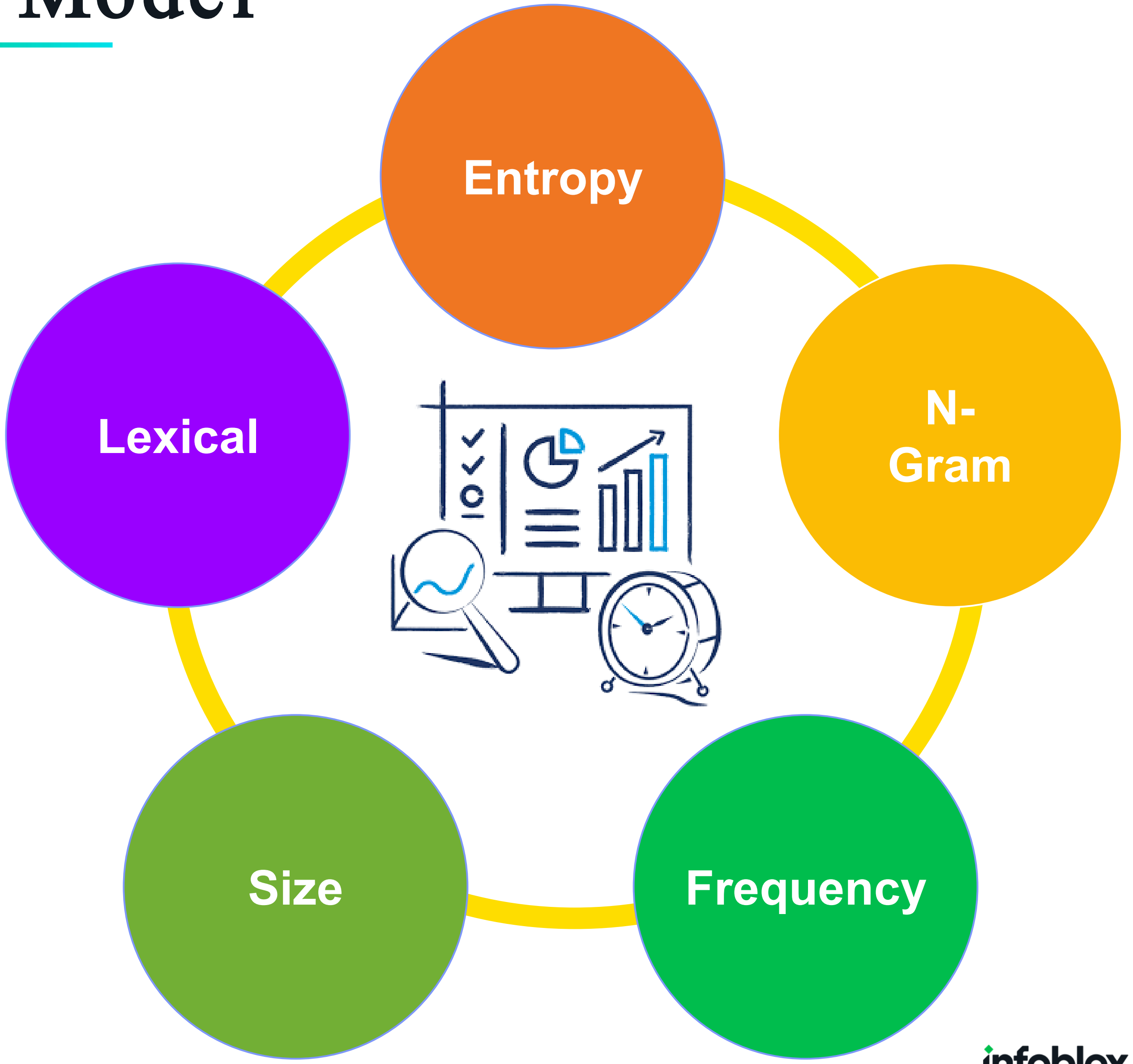
123PixieWay.baddomain.com

Fayettvile-AR.baddomain.com

Behavioral Detection

DNS-Layer Threat Analysis Model

- ➢ Detects transmission of data in DNS queries using behavioral analysis
- ➢ Examines all DNS records (e.g.: A, AAAA, MX, TXT, CNAME, SVR, SOA, ...)
- ➢ Machine Learning / AI

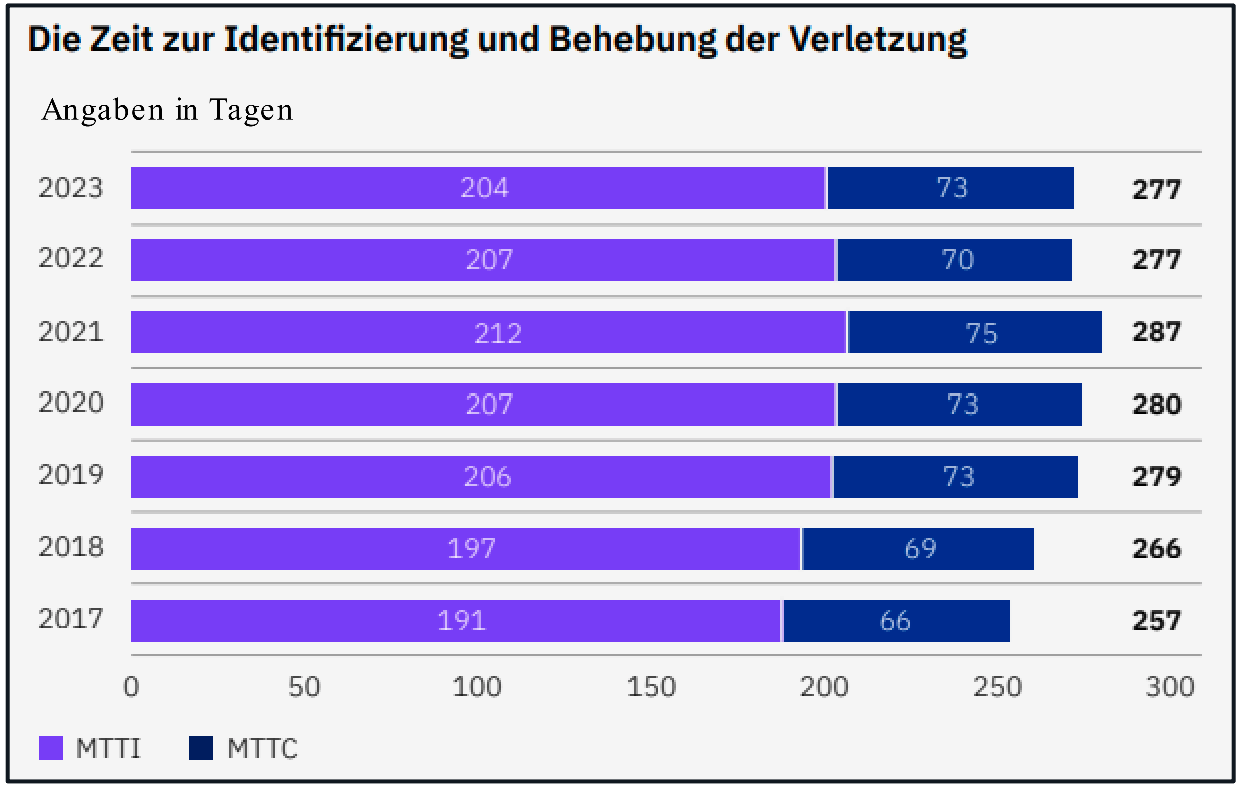


infoblox

Average time to identify and contain a data breach

- ➢ Think like an attacker!!
- ➢ I don't want to get caught.
- ➢ Does it matter to me how long it takes to download a file?
- ➢ Can I tackle several things in parallel?

IBM Security
Cost of a Data Breach Report 2023



DoT & DOH

- Two evolving improvements to DNS privacy have recently made the news:
  - DNS over TLS (Transport Layer Security) or "DoT”
  - DNS over HTTPS or "DoH”
- Mechanisms promote consumer privacy but allow users to circumvent established enterprise DNS controls.
  - Exposure to data exfiltration and malware proliferation

Privacy

≠

Security

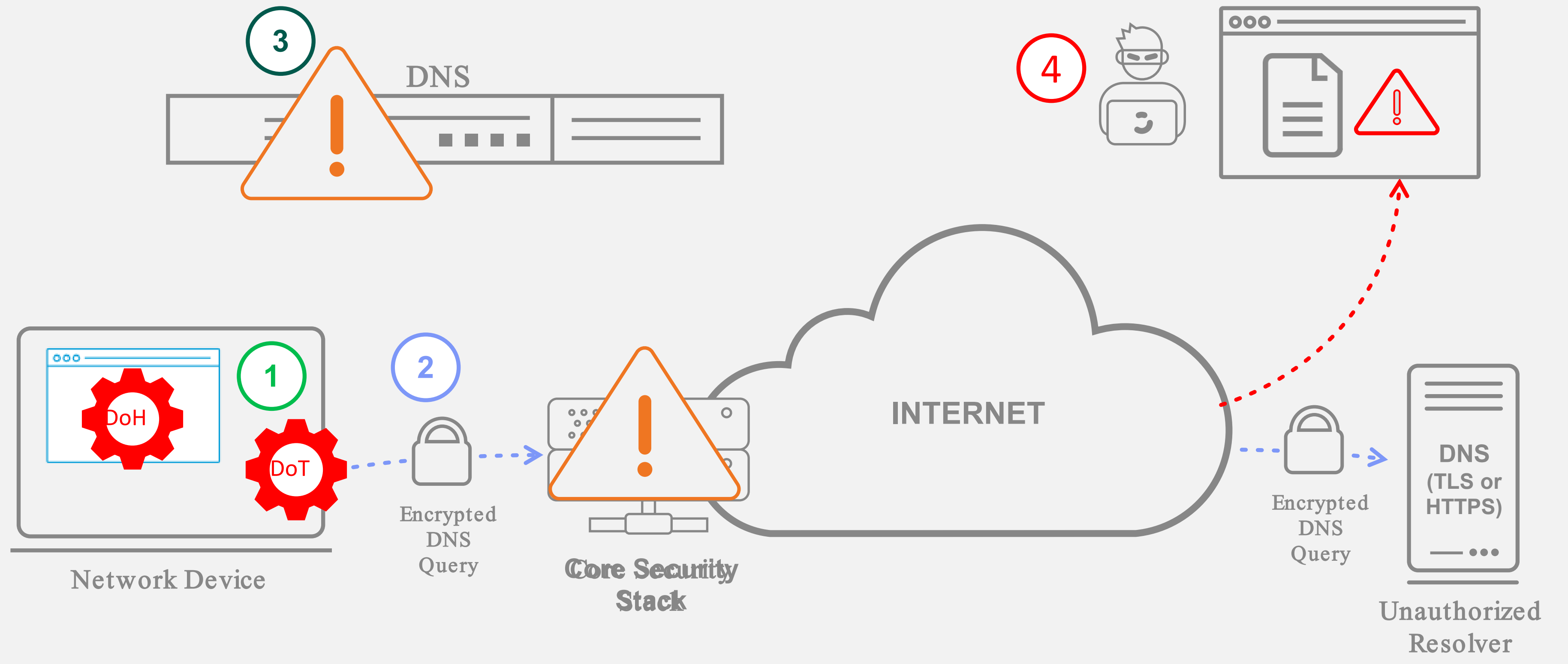
DoT/ DoH: Bypass of Enterprise DNS is a Challenge

1 Device (TLS) or browser (HTTPS) is configured with unauthorized DNS Resolver

2 Encrypted DNS queries sent to external resolver

3 Internal DNS Resolver bypassed, and DNS traffic not inspected

4 Attackers can exploit DoT for their own purpose



DoT/ DoH "HIDES" DNS traffic from your security tools

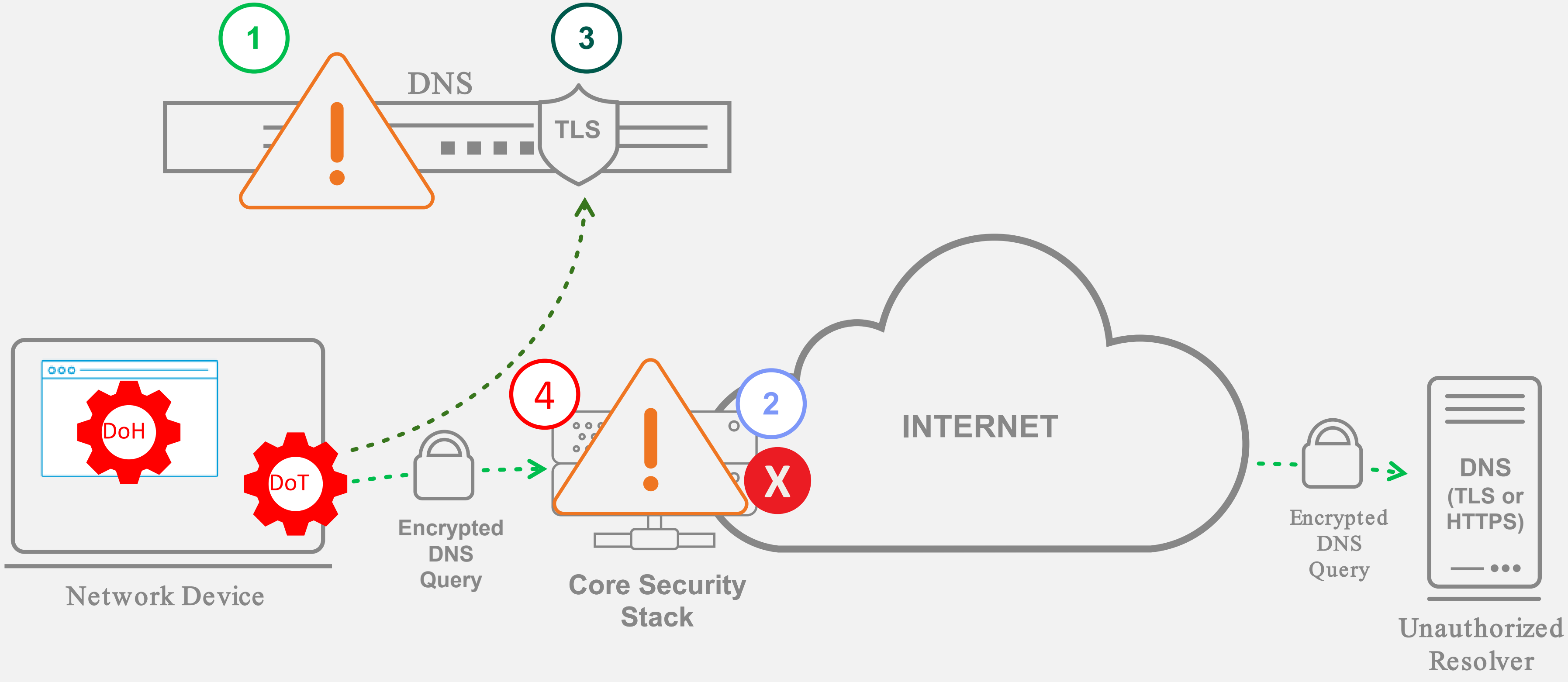
DoT/ DoH Best Practices

1 Circumventing internal DNS is a bad idea

2 Block Access to unauthorized DNS servers

3 Use internal DNS vendor that supports DoT to retain control and security

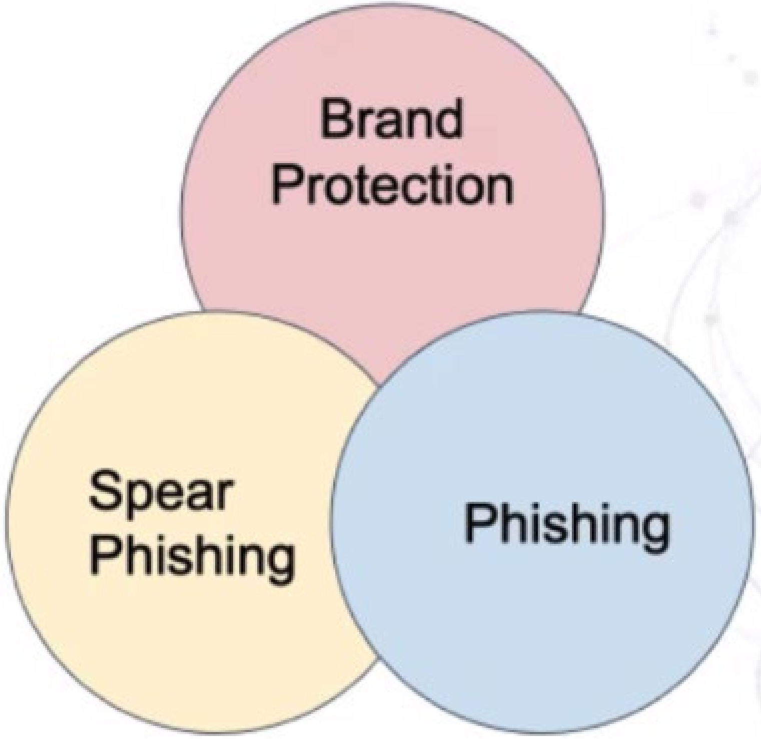
4 Block DoH using Threat Intel List of Canary and unauthorized resolvers



DoT/DoH Best Practices protects your users and devices

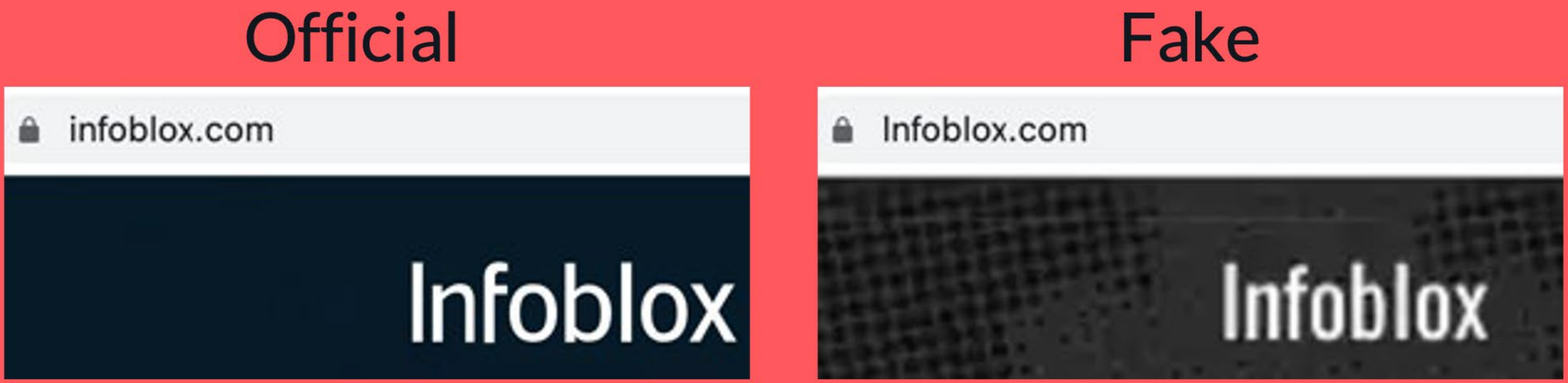
Use Cases: Brand Reputation, Phishing / Spear Phishing

- **Brand Protection:** Protecting customer's own domain from harm via impersonation (Example: using infoblocks.com to harm our customers). Alerts on creation or discovery of domain.
- **Spear Phishing:** User visiting lookalike of company's own domain (Example: user visits Infobloxbenifits[.]com) Alerts when domain is visited.
- **Phishing:** Local users visiting global lookalikes (Example: user going to g00gle.com) Alerts when domain is visited.



LOOKALIKE DOMAINS

EVERYONE IS A TARGET – EVEN US!



Official

infoblox.com

Fake

Infoblox.com

A comparison of logos between the official Infoblox.com website (L) and the fraudulent Infoblox.com (R)

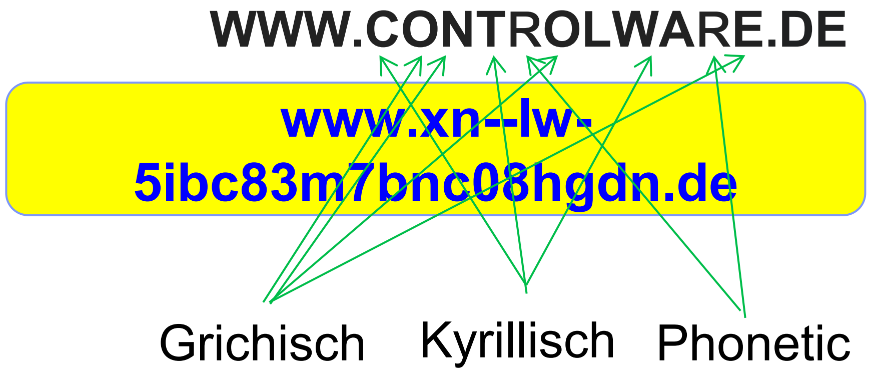
Infoblox.com and Infoblox.com Arial– Infoblox.com and lnfoblox.com Aptos

Lookalike Domain Detection

paypal.com	pąypąl.com	paypal.com	Text
xn--pypl-53dc.com	xn--pypl-btac.com	paypal.com	Punycode

google.com	google.com	google.com	Text
google.com	xn--ggle-0nda.com	xn--ggle-55da.com	Punycode

Lookalike Domain Detection



WWW.CONTROLWARE.DE

www.xn--lw-5ibc83m7bnc08hgdn.de

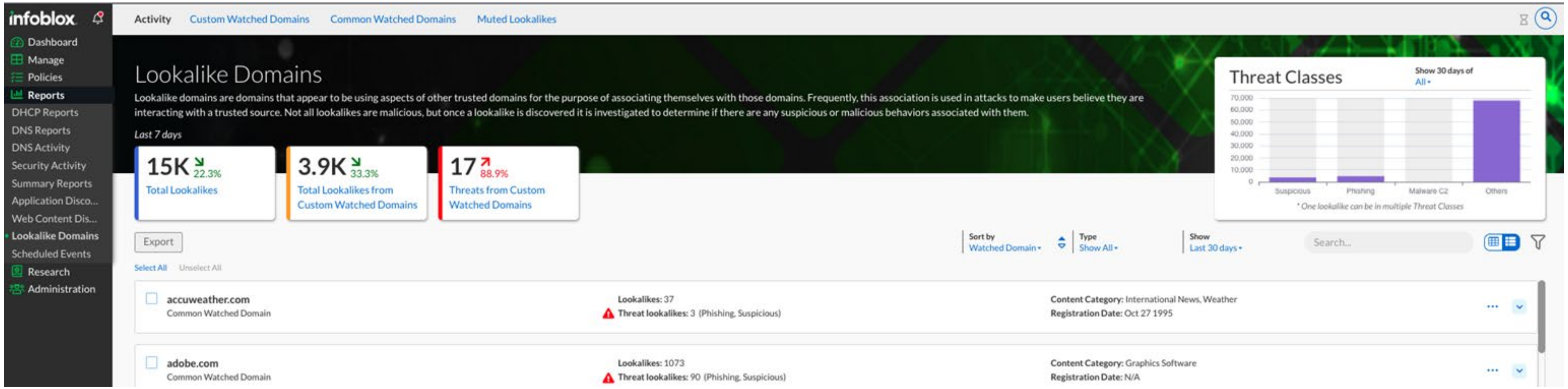
Grichisch

Kyrillisch

Phonetic

www.controlware.de	www.controlware.de	www.controlware.de	Text
www.xn--controlwae-tue.de	www.controlware.de	www.xn--controlwre-nge.de	Punycode

Lookalike Domain Detection



Lookalike Domains

Lookalike domains are domains that appear to be using aspects of other trusted domains for the purpose of associating themselves with those domains. Frequently, this association is used in attacks to make users believe they are interacting with a trusted source. Not all lookalikes are malicious, but once a lookalike is discovered it is investigated to determine if there are any suspicious or malicious behaviors associated with them.

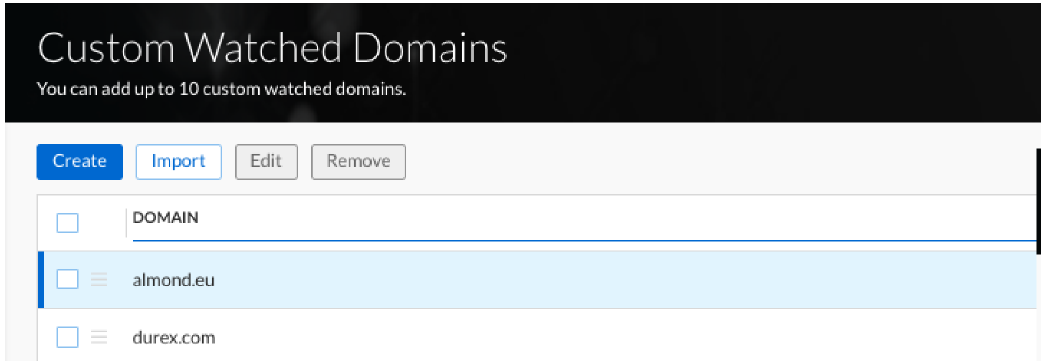
Last 7 days

- 15K ↘ 22.3% Total Lookalikes
- 3.9K ↘ 33.3% Total Lookalikes from Custom Watched Domains
- 17 ↗ 88.9% Threats from Custom Watched Domains

*One lookalike can be in multiple Threat Classes

□ accuweather.com
Common Watched Domain
Lookalikes: 37
Threat lookalikes: 3 (Phishing, Suspicious)
Content Category: International News, Weather
Registration Date: Oct 27 1995

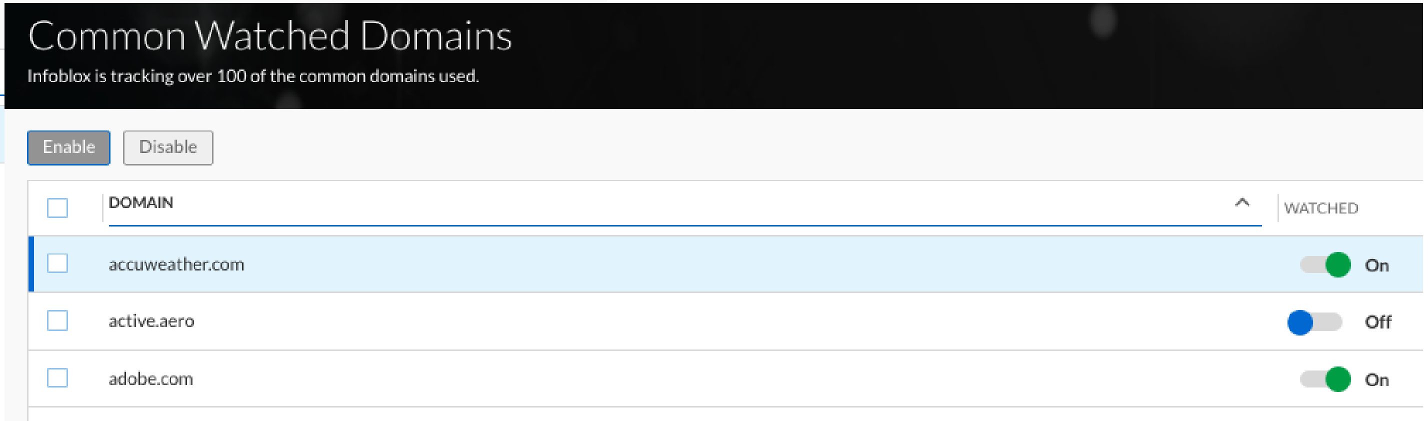
□ adobe.com
Common Watched Domain
Lookalikes: 1073
Threat lookalikes: 90 (Phishing, Suspicious)
Content Category: Graphics Software
Registration Date: N/A



Custom Watched Domains

You can add up to 10 custom watched domains.

□	DOMAIN
□	almond.eu
□	durex.com



Common Watched Domains

Infoblox is tracking over 100 of the common domains used.

□	DOMAIN	WATCHED
□	accuweather.com	On
□	active.aero	Off
□	adobe.com	On

Infoblox Domain Mitigation Services Optimized to Combat Emerging Internet Fraud Incidents

- ➢ Validation:
  - ○ human-driven review of potential internet fraud
  - ○ providing a detailed summary of our in-depth review.
  - ○ Response times of five minutes or less during regular business hours.
  - ○ Once our review is underway, we can typically remove domestic internet fraud within 24 hours.
- ➢ Mitigation:
  - ○ Continuous removal effort to each case, with multiple escalations for cases that cannot be resolved within 24 hours.
  - ○ We leverage our established relationships with ISPs and communication service providers to prioritize your case in abuse queues and ensure the issue is resolved quickly.
  - ○ We also offer registered trademark enforcement to protect your brand reputation.
- ➢ Monitoring and reporting
  - ○ IWe keep track of potential threats.
  - ○ We monitor mitigated threats to address potential reactivation.
  - ○ Our mitigation services remain in effect for up to 30 days.

BloxOne® Threat Defense Advanced

Unified Reporting

Cloud Services Portal

Ecosystem I/O APIs

Data Connector

Threat Insight Behavioral

Reputational Threat Intel

DNS Firewall

Cloud/On-Prem/Hybrid

Dossier Threat Research

TIDE Intel Sharing

SIEM

Vuln Scanner

Firewall

TIP

Etc……

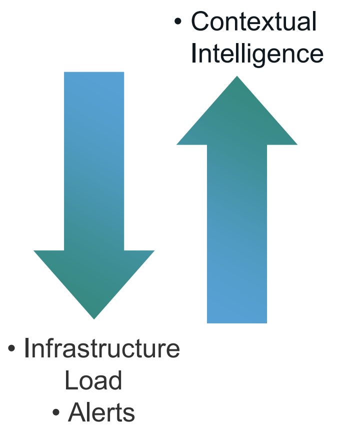
Globally available recursive DNS and web filtering

OnPrem
Infoblox Grid

Cloud
Public, private

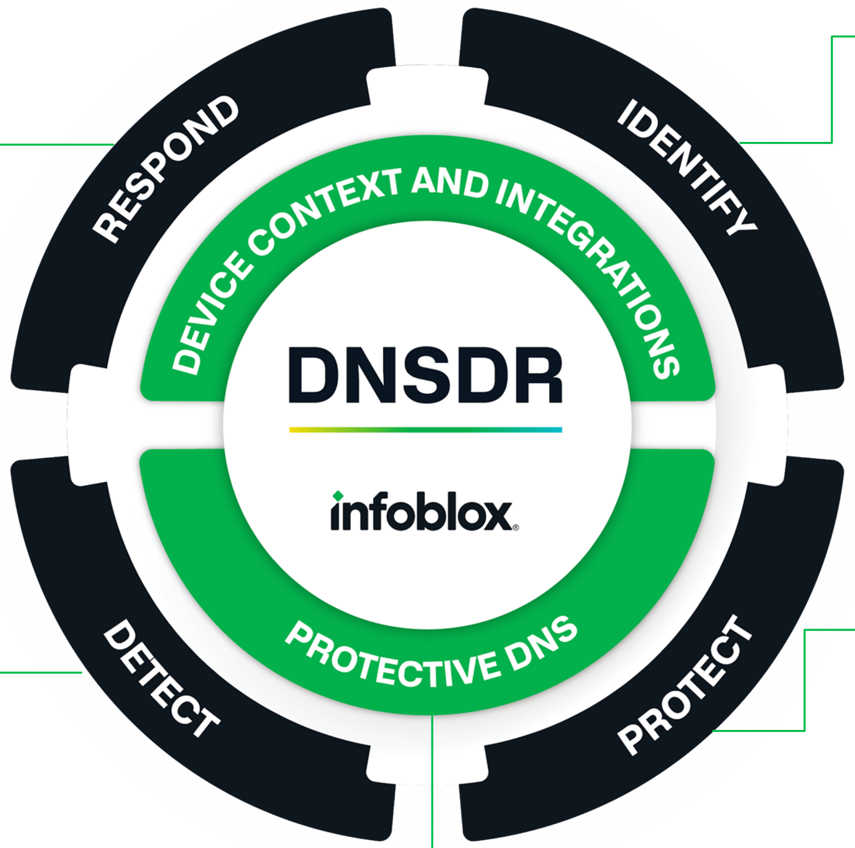
Endpoint
Client

Remote Office
DNS Forwarding Proxy



- Contextual Intelligence
- Infrastructure Load
- Alerts

THE INDUSTRIES ONLY COMPREHENSIVE DNS DETECTION AND RESPONSE SOLUTION : BLOXONE® THREAT DEFENSE



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

PROTECT

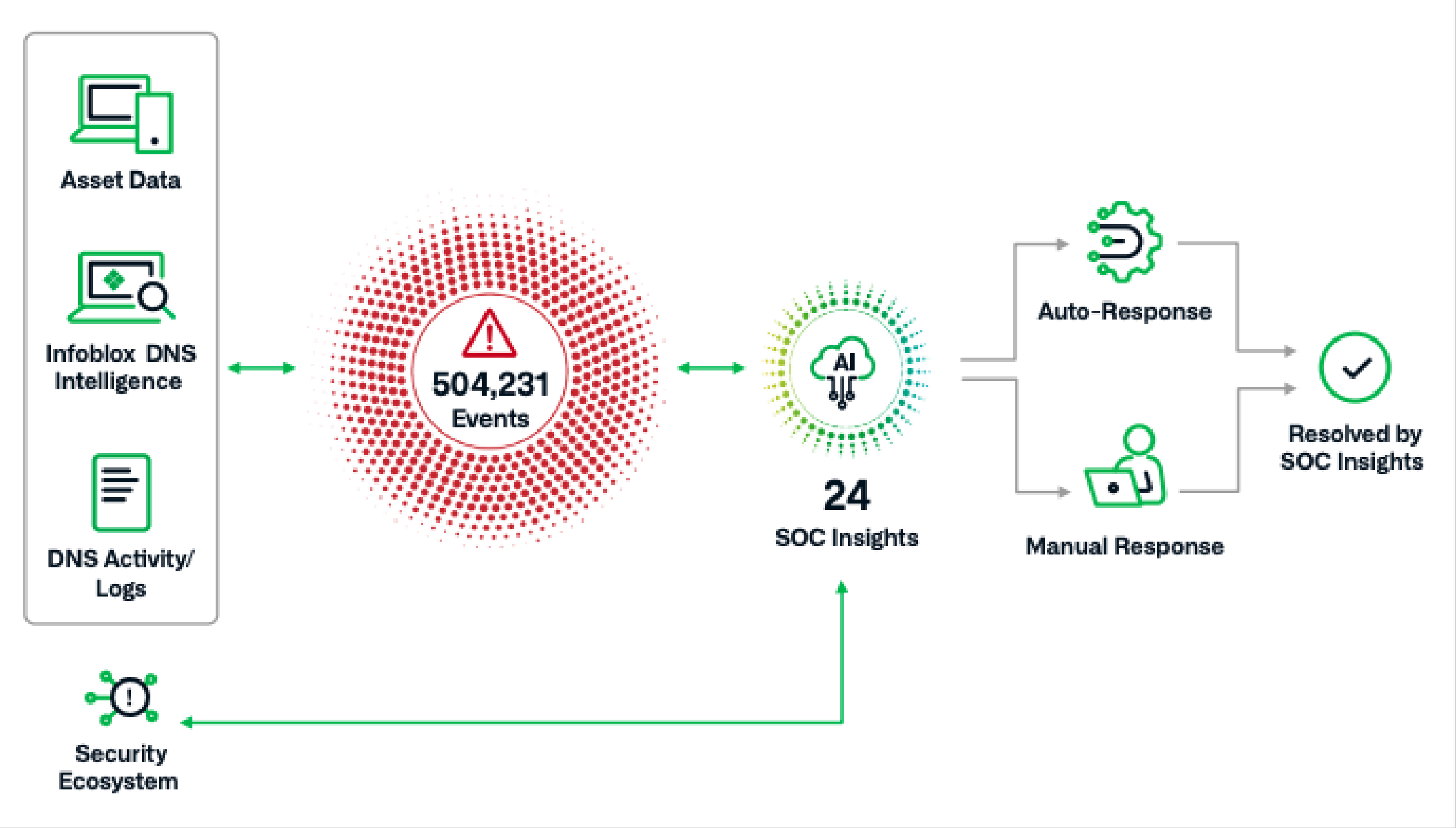
Blocks phishing, DGA, C2, Malware, Ransomware, Exfiltration and Suspicious Domains

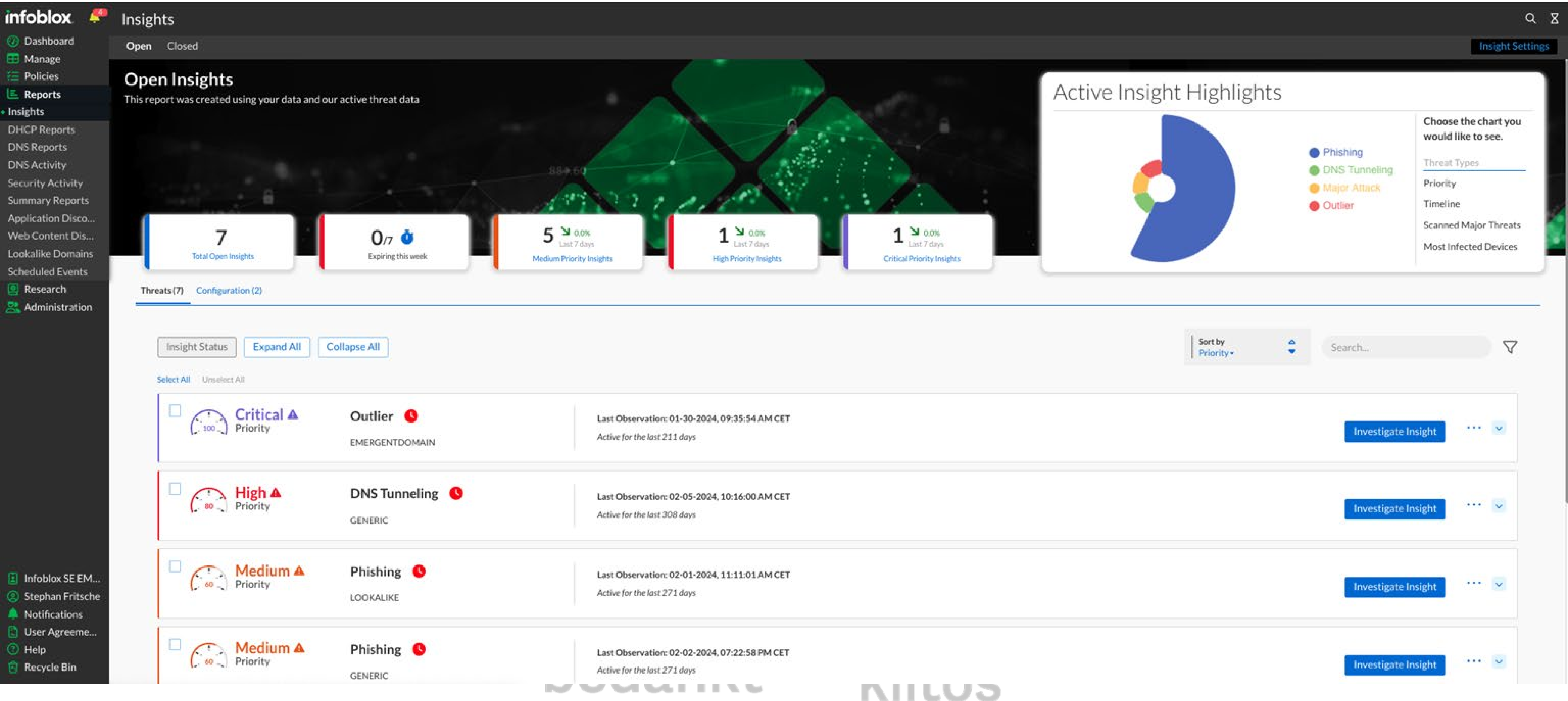
Blocks at the intent to communicate

REDUCE INVESTIGATION AND RESPONSE TIMES

Make the SOC More efficient

- ➢Know which events matter most and reduce
  - ○ Missed True Positives
  - ○ Alert Fatigue
  - ○ Burnout &Turnover
- ➢Eliminate wasted time to:
  - ○ Make critical decisions faster, with confidence
  - ○ Reduce MTTR





infoblox Insights

- Dashboard
- Manage
- Policies
- Reports
- Insights
- DHCP Reports
- DNS Reports
- DNS Activity
- Security Activity
- Summary Reports
- Application Disco...
- Web Content Dis...
- Lookalike Domains
- Scheduled Events
- Research
- Administration
- Infoblox SE EM...
- Stephan Fritsche
- Notifications
- User Agreeme...
- Help
- Recycle Bin

Open Closed Insight Settings

Open Insights

This report was created using your data and our active threat data

7	0/7	5 ↘ 0.0% Last 7 days	1 ↘ 0.0% Last 7 days	1 ↘ 0.0% Last 7 days
Total Open Insights	Expiring this week	Medium Priority Insights	High Priority Insights	Critical Priority Insights

Active Insight Highlights

- ● Phishing
- ● DNS Tunneling
- ● Major Attack
- ● Outlier

Choose the chart you would like to see.

- Threat Types
- Priority
- Timeline
- Scanned Major Threats
- Most Infected Devices

Threats (7) Configuration (2)

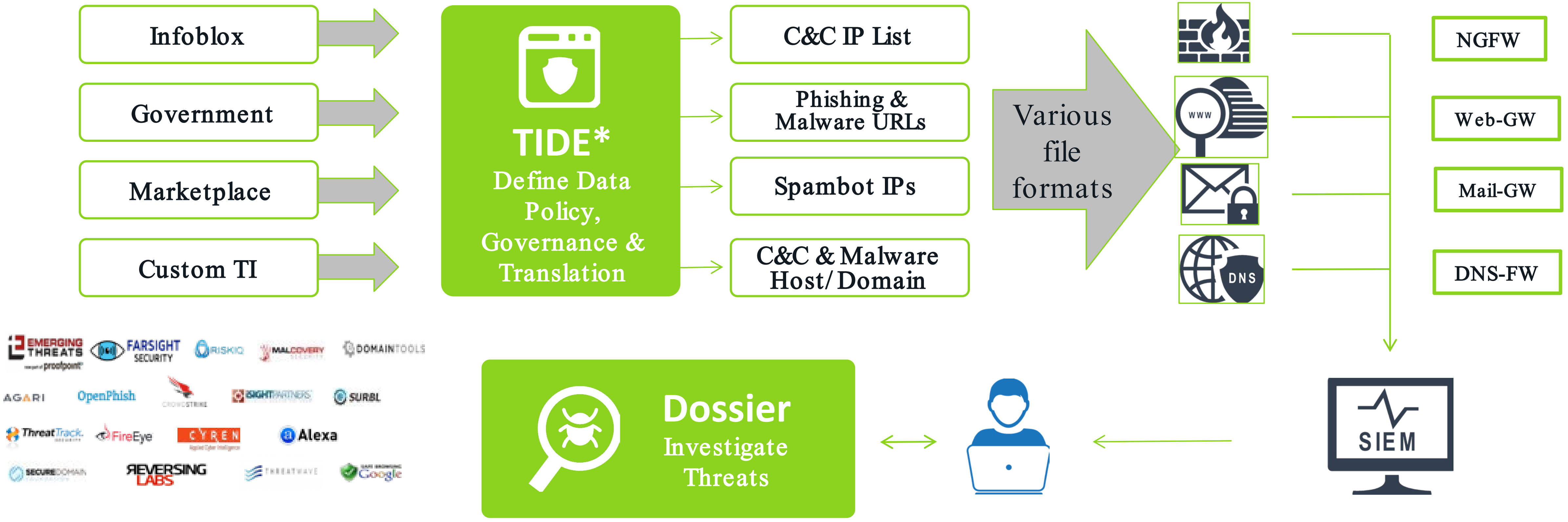
Insight Status | Expand All | Collapse All | Sort by Priority | Search...

Select All Unselect All

	Priority	Threat	Last Observation	
□	100 Critical Priority	Outlier EMERGENTDOMAIN	Last Observation: 01-30-2024, 09:35:54 AM CET *Active for the last 211 days*	Investigate Insight
□	80 High Priority	DNS Tunneling GENERIC	Last Observation: 02-05-2024, 10:16:00 AM CET *Active for the last 308 days*	Investigate Insight
□	60 Medium Priority	Phishing LOOKALIKE	Last Observation: 02-01-2024, 11:11:01 AM CET *Active for the last 271 days*	Investigate Insight
□	60 Medium Priority	Phishing GENERIC	Last Observation: 02-02-2024, 07:22:58 PM CET *Active for the last 271 days*	Investigate Insight

Threat Intel Data Sharing

TIDE - Threat Intelligence Data Exchange



Infoblox

Government

Marketplace

Custom TI

TIDE*

Define Data Policy, Governance & Translation

C&C IP List

Phishing & Malware URLs

Spambot IPs

C&C & Malware Host/Domain

Various file formats

NGFW

Web-GW

Mail-GW

DNS-FW

SIEM

Dossier

Investigate Threats

Single-source of TI management

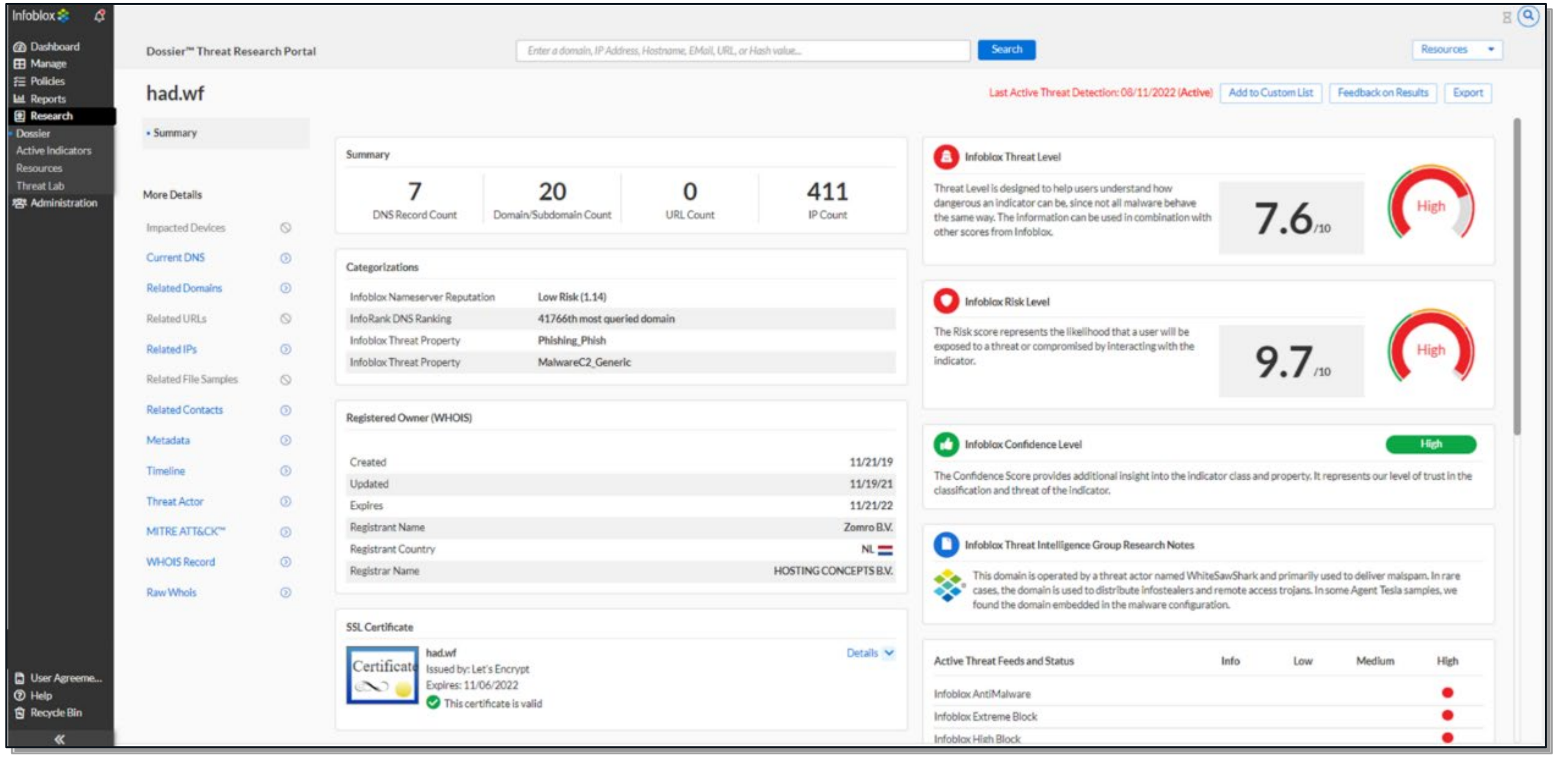
Automate investigation & triage

Orchestrate common security policy across multi-vendor infrastructure

➢ Reduce cost of threat feeds while improving effectiveness across entire security portfolio

Infoblox Dossier for Threat Research

- ➢ Contextual information from multiple data sources in a single view
- ➢ Leverages open source, proprietary and commercial data sources
- ➢ Access historical registration, risk level, MITRE information, related enterprise activity, and more



Dossier™ Threat Research Portal

Enter a domain, IP Address, Hostname, EMail, URL, or Hash value...

had.wf

Last Active Threat Detection: 08/11/2022 (Active)

Summary

7	20	0	411
DNS Record Count	Domain/Subdomain Count	URL Count	IP Count

Categorizations

Infoblox Nameserver Reputation	Low Risk (1.14)
InfoRank DNS Ranking	41766th most queried domain
Infoblox Threat Property	Phishing_Phish
Infoblox Threat Property	MalwareC2_Generic

Registered Owner (WHOIS)

Created	11/21/19
Updated	11/19/21
Expires	11/21/22
Registrant Name	Zomro B.V.
Registrant Country	NL
Registrar Name	HOSTING CONCEPTS B.V.

SSL Certificate

Certificate

had.wf
Issued by: Let's Encrypt
Expires: 11/06/2022
✓ This certificate is valid

Details

Infoblox Threat Level

Threat Level is designed to help users understand how dangerous an indicator can be, since not all malware behave the same way. The information can be used in combination with other scores from Infoblox.

7.6/10

Infoblox Risk Level

The Risk score represents the likelihood that a user will be exposed to a threat or compromised by interacting with the indicator.

9.7/10

Infoblox Confidence Level

The Confidence Score provides additional insight into the indicator class and property. It represents our level of trust in the classification and threat of the indicator.

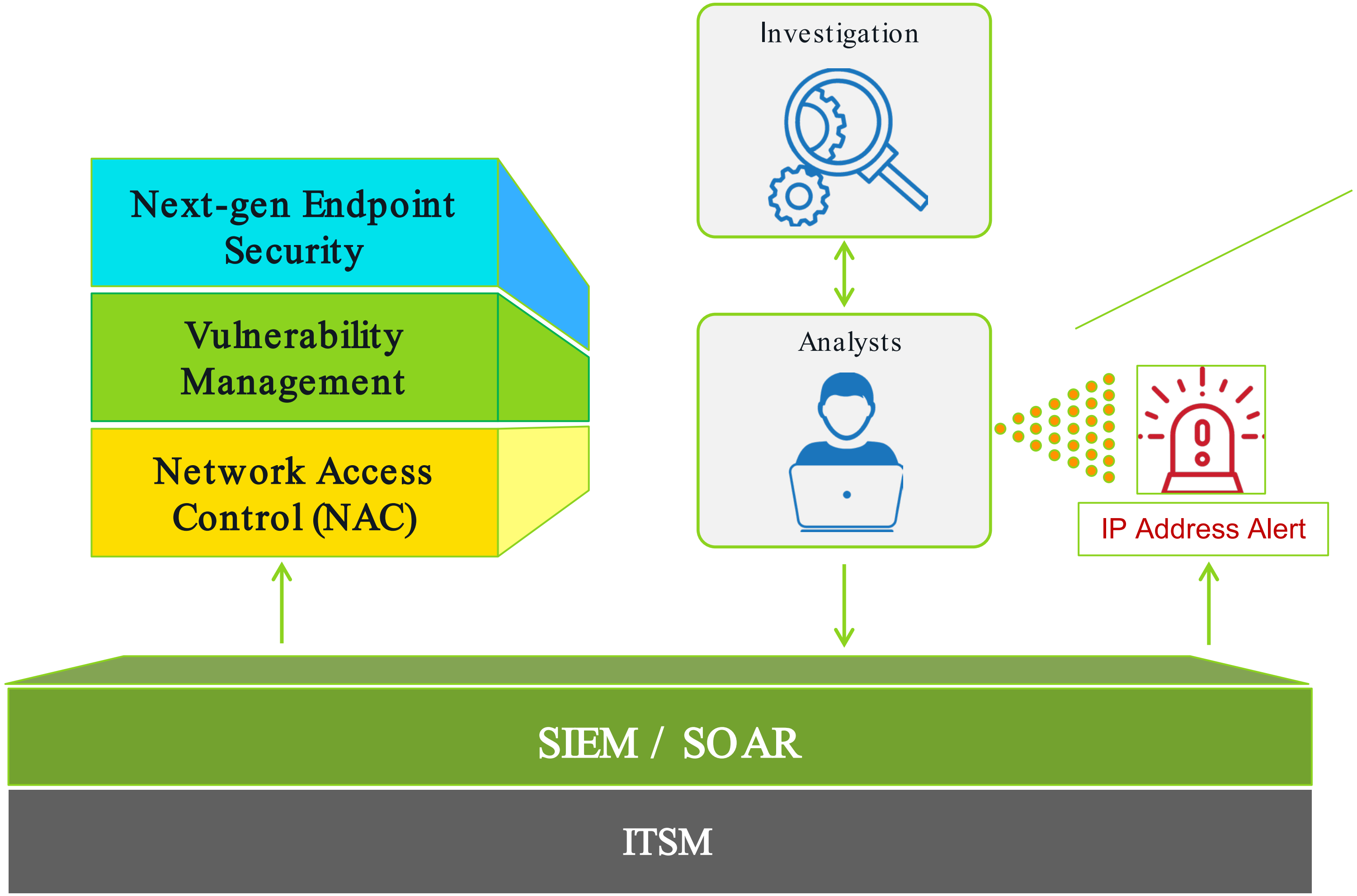
Infoblox Threat Intelligence Group Research Notes

This domain is operated by a threat actor named WhiteSawShark and primarily used to deliver malspam. In rare cases, the domain is used to distribute infostealers and remote access trojans. In some Agent Tesla samples, we found the domain embedded in the malware configuration.

Active Threat Feeds and Status	Info	Low	Medium	High
Infoblox AntiMalware				●
Infoblox Extreme Block				●
Infoblox High Block				●

Reduce threat investigation and response time by 2/3rds

Typical Incident Response

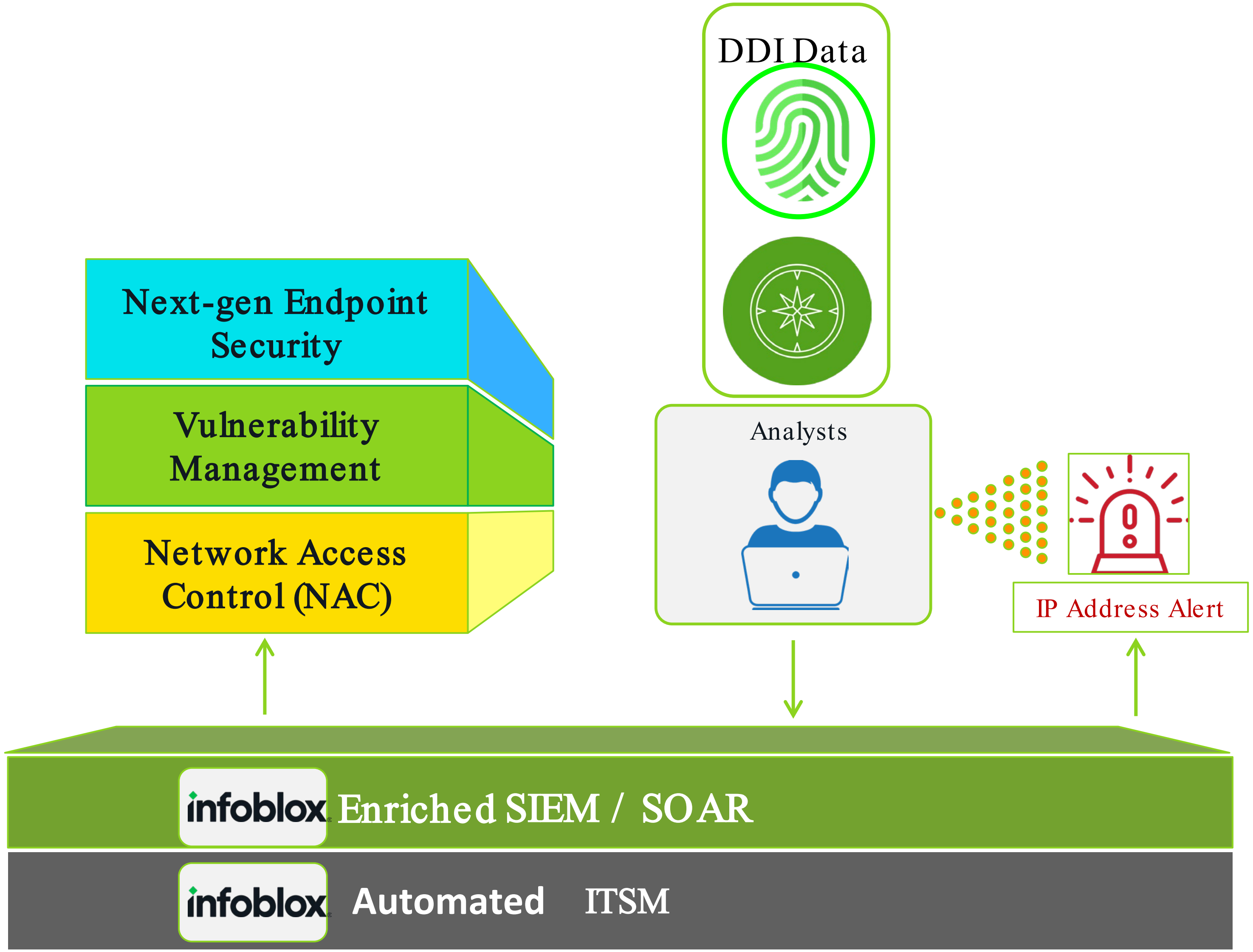


Lengthy Response Times

Manual Investigation

- MAC Address
- User details
- Network Location
- Physical location
- Network devices
- Device type
- OS information
- Current IP
- Historical IP's and locations

Typical Incident Response



DDI Data

Next-gen Endpoint Security

Vulnerability Management

Network Access Control (NAC)

Analysts

IP Address Alert

infoblox Enriched SIEM / SOAR

infoblox Automated ITSM

Lower
Response Times

DNS

- Malicious activity inside the security perimeter
- Includes BYOD and IoT device
- Profile device & user activity

DHCP

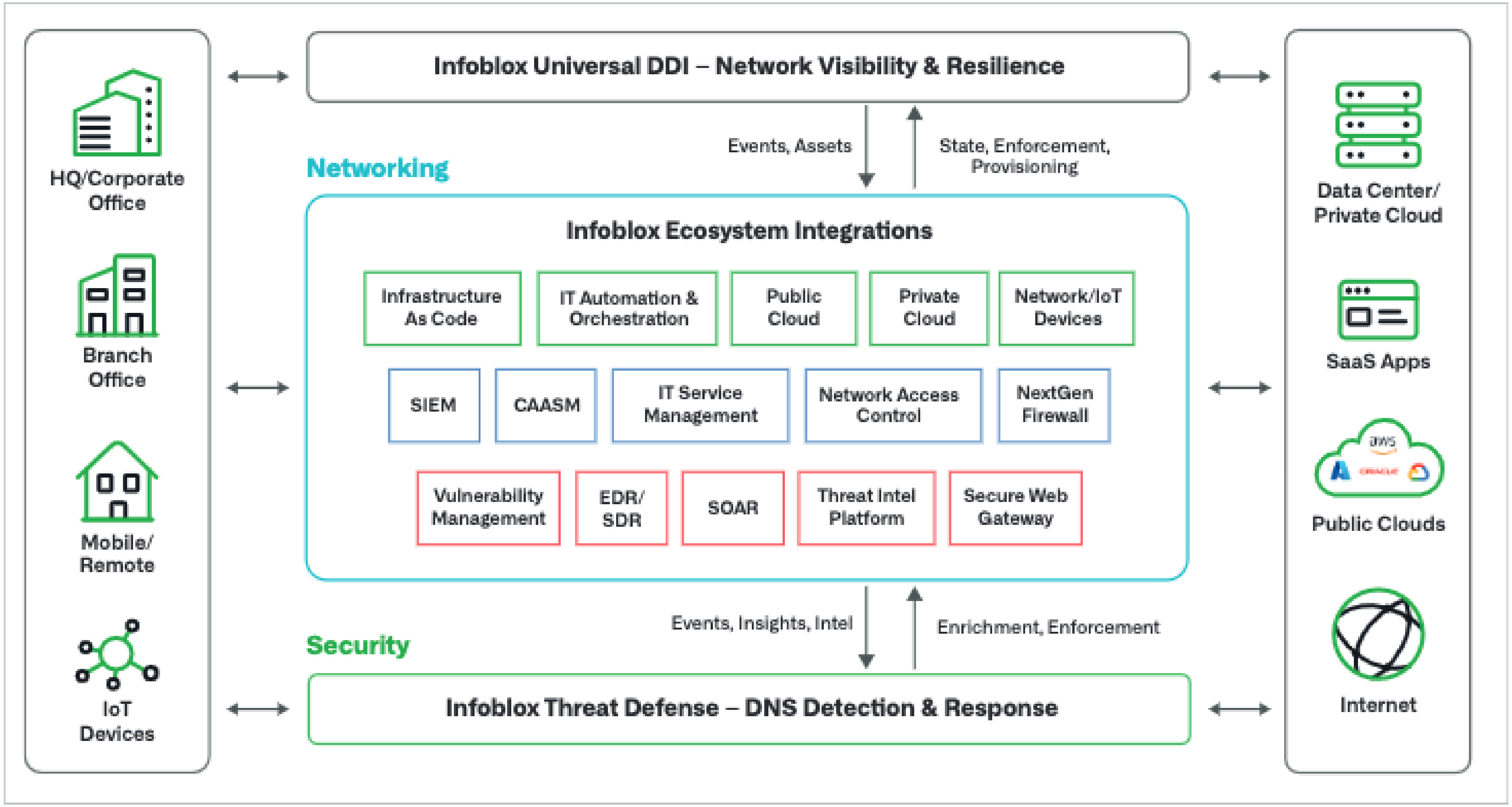
- Device Audit Trail and Fingerprinting
- Device info, MAC, lease history

IPAM

Application and Business Context

- “Metadata” via Extended Attributes: Owner, app, security level, location, ticket number
- Context for accurate risk assessment and event prioritization

INFOBLOX ECOSYSTEM ARCHITECTURE



HQ/Corporate Office

Branch Office

Mobile/ Remote

IoT Devices

Infoblox Universal DDI – Network Visibility & Resilience

Events, Assets

State, Enforcement, Provisioning

Networking

Infoblox Ecosystem Integrations

Infrastructure As Code

IT Automation & Orchestration

Public Cloud

Private Cloud

Network/IoT Devices

SIEM

CAASM

IT Service Management

Network Access Control

NextGen Firewall

Vulnerability Management

EDR/ SDR

SOAR

Threat Intel Platform

Secure Web Gateway

Events, Insights, Intel

Enrichment, Enforcement

Security

Infoblox Threat Defense – DNS Detection & Response

Data Center/ Private Cloud

SaaS Apps

Public Clouds

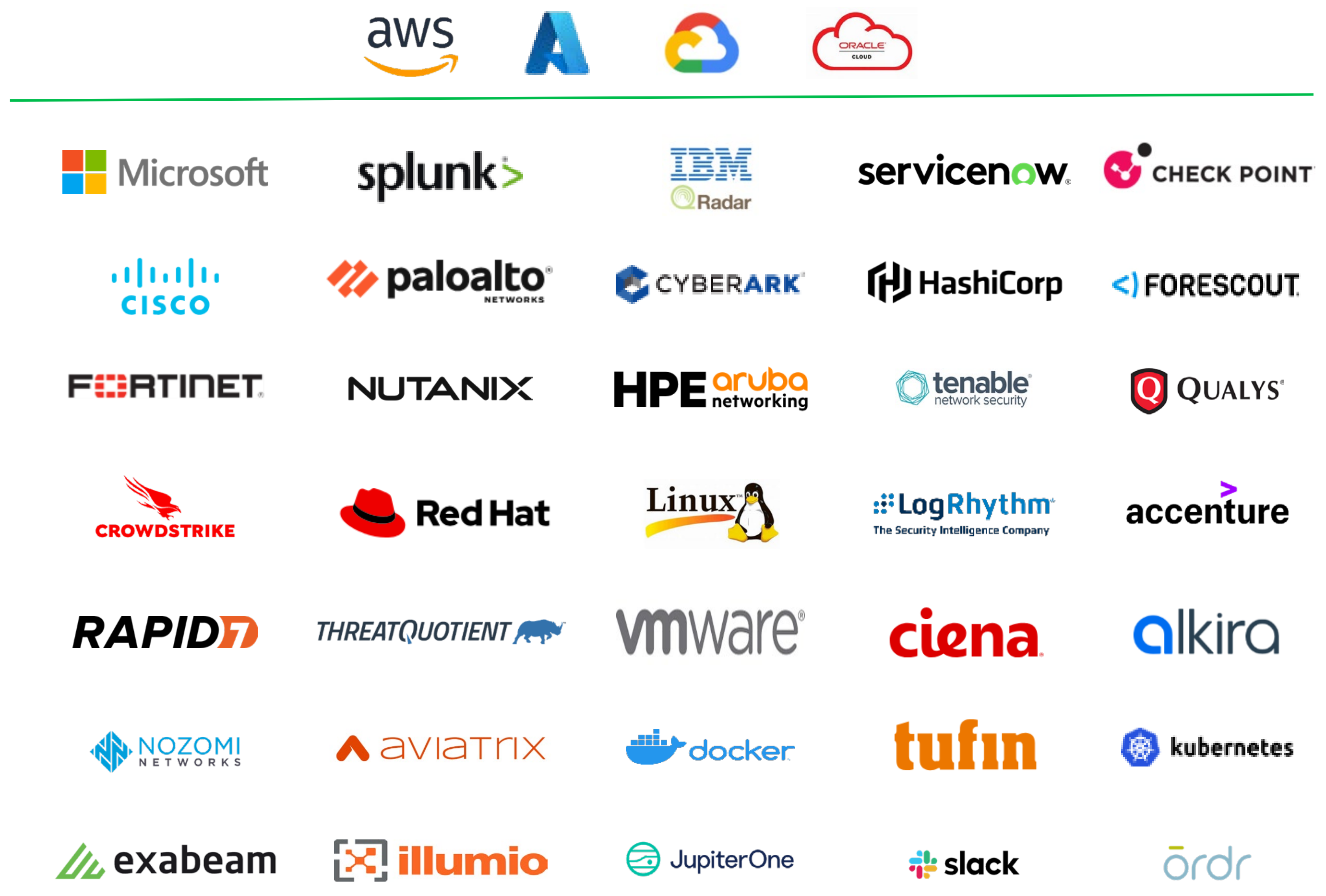
Internet

ECOSYSTEM PARTNERS

ecosystem.infoblox.com

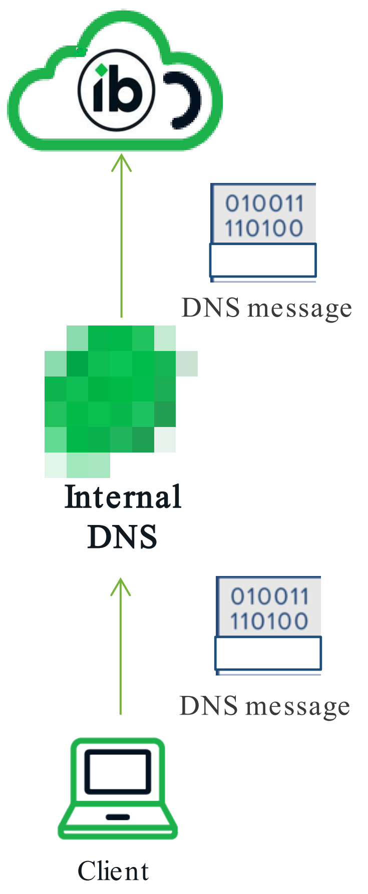
Extensive ecosystem integrations enable us to close visibility gaps, share context across silos, and automate responses to security events.

INFOBLOX ECOSYSTEM PARTNERS



B1TD Deployment Options

1. Direct Forward



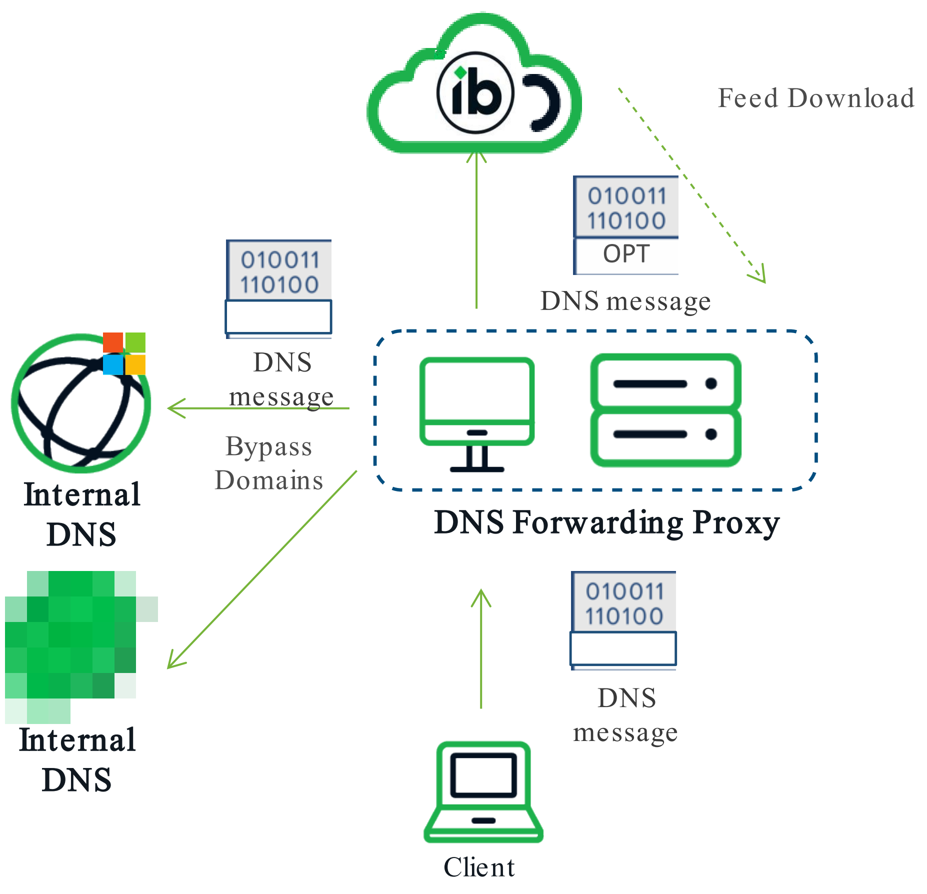
DNS message

Internal DNS

DNS message

Client

2. DNS Forwarding Proxy



Feed Download

DNS message

DNS message

Bypass Domains

Internal DNS

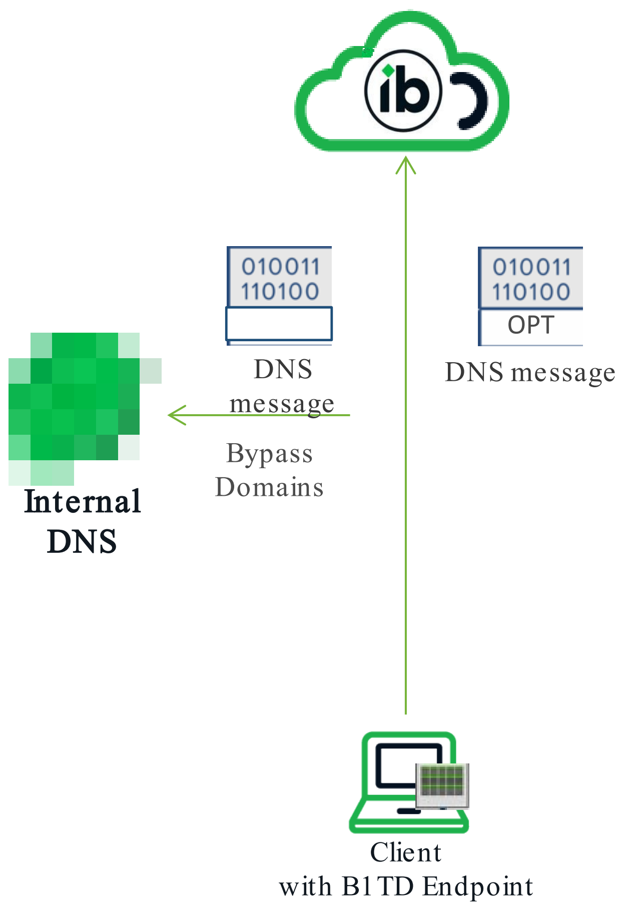
DNS Forwarding Proxy

Internal DNS

DNS message

Client

3. Endpoint Agent



DNS message

DNS message

Bypass Domains

Internal DNS

Client with B1TD Endpoint

Infoblox Security Sales Tools

Infoblox DNS security Initiatives / Activities

- DNS SECURITY WORKSHOP; Customer enablement initiative 2-4 hours, to teach customers how the DNS are used by malware, understand the role of DNS in modern cyber threats & effectiveness
- DNS SECURITY ASSESTMENT; Real Time customer traffic analyst (captured data), to detect insights into potential malicious DNS activity like attacks, threats, content and brand reputation
- DNS SECURITY AUDIT: **Quick review by using simple DNS queries to assess a company DNS security posture and identify potential gaps.**

Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.