infoblox

HOW CAN DNS SECURITY HELP SECOPS?

RICCARDO CANETTA

COUNTRY MANAGER, MED COUNTRIES
RCANETTA@INFOBLOX.COM

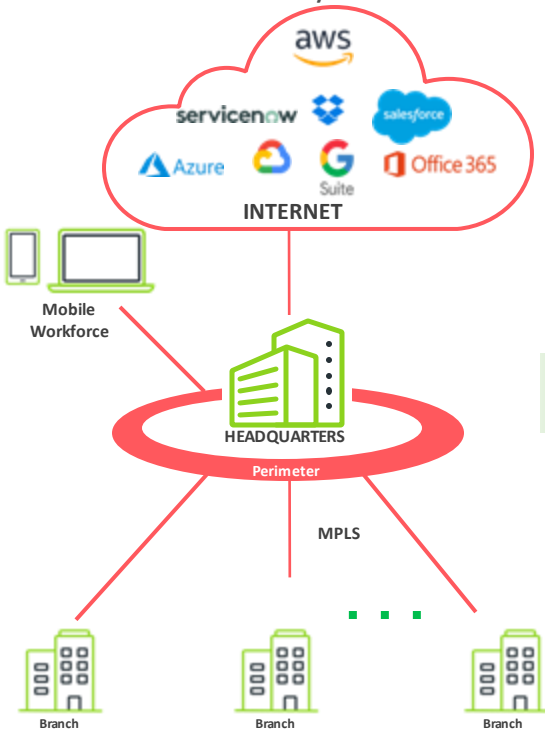
TRENDS: NETWORK AND SECURITY HAVE CHANGED

Shift from centralized to cloud friendly architectures

Dedicated WAN

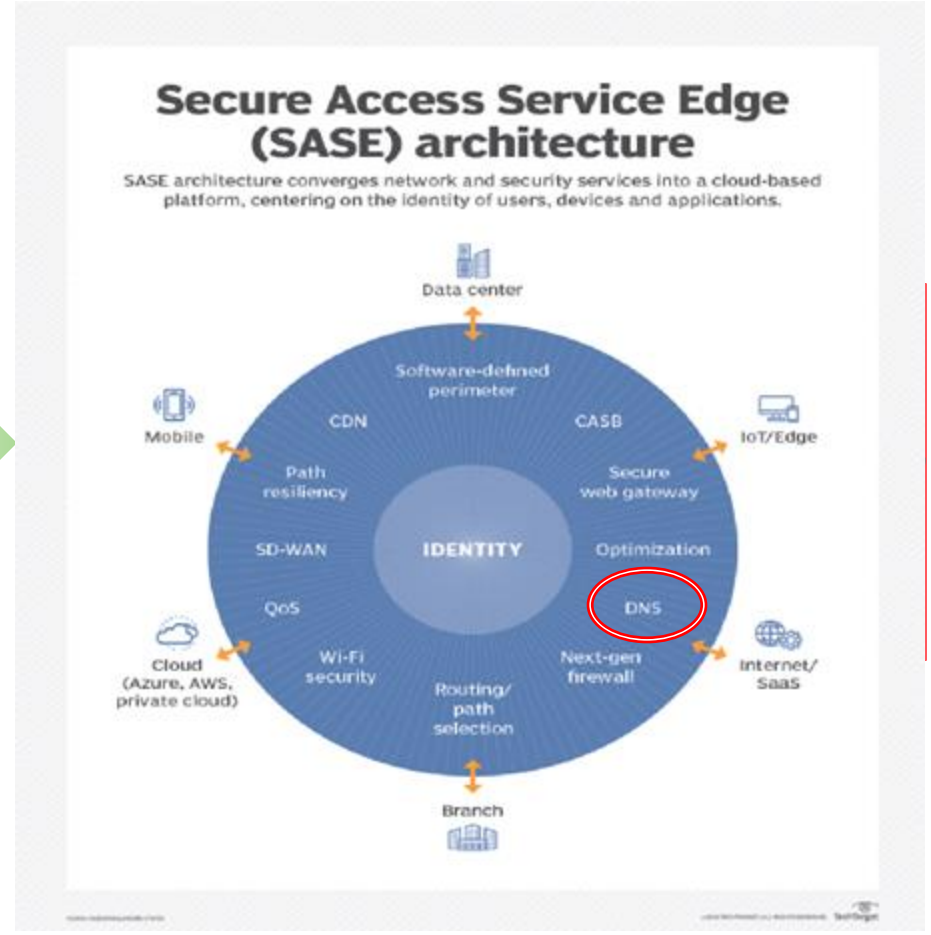
All traffic to HQ

Centralized, perimeter-based security



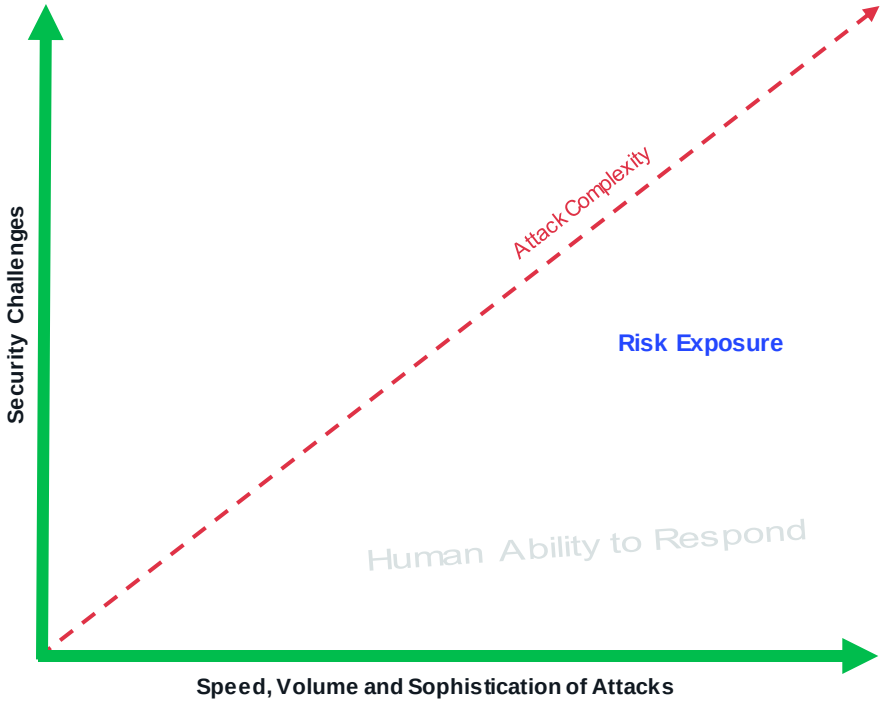
CENTRALISED

All Traffic to HQ/DC



TRENDS: ATTACKS OUTWEIGHS HUMAN ABILITY

Attackers innovate faster than defenders



> Technology complexity exceeds human ability to cope. The human-technology system becomes unstable, and a different approach is required to bring complexity under control.
>
> IDC
>
> Market Analysis Perspective: Worldwide Cybersecurity, 2021

- **800%** Malware increase (focus on Ransomware)
- Adversarial AI
- Zero Day, unknown malware
- Multi-stage, supply chain
- Tons of Alerts…, rise in false positives

Alert Fatigue and Overload, resources to investigate **only about 4% of those alerts**

infoblox.

PUTTING MORE PRESSURE ON SOC AND NOC TEAMS

Lower
Response Times

NOC CHALLENGES

Ensuring **business continuity/SLAs**

Visibility into **all IT assets**

Management of hybrid networks **at scale**

Automation of **IT Service Management (ITSM) workflows**

SOC CHALLENGES

Increased **attack surface**

Nonstandard endpoints

Complex **threat landscape**

Over-burdened short-staffed teams

Data everywhere

Everyday, NOC and SOC teams are challenged to do more with less
Slow Incident Response Still a Problem

infoblox.

WHY DNS BASED SECURITY?

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Gartner

How can Organizations use DNS to improve their security posture?[1]

92% of Malware uses DNS as it's security control plane[2]

DNS increasingly used as a threat vector by criminals and nation state actors[3]

DNS is seen as the most scalable approach to malware mitigation in a deperimeterized security world[4 5]

Visibility: DNS, DHCP and IPAM data are essential network context for security operations

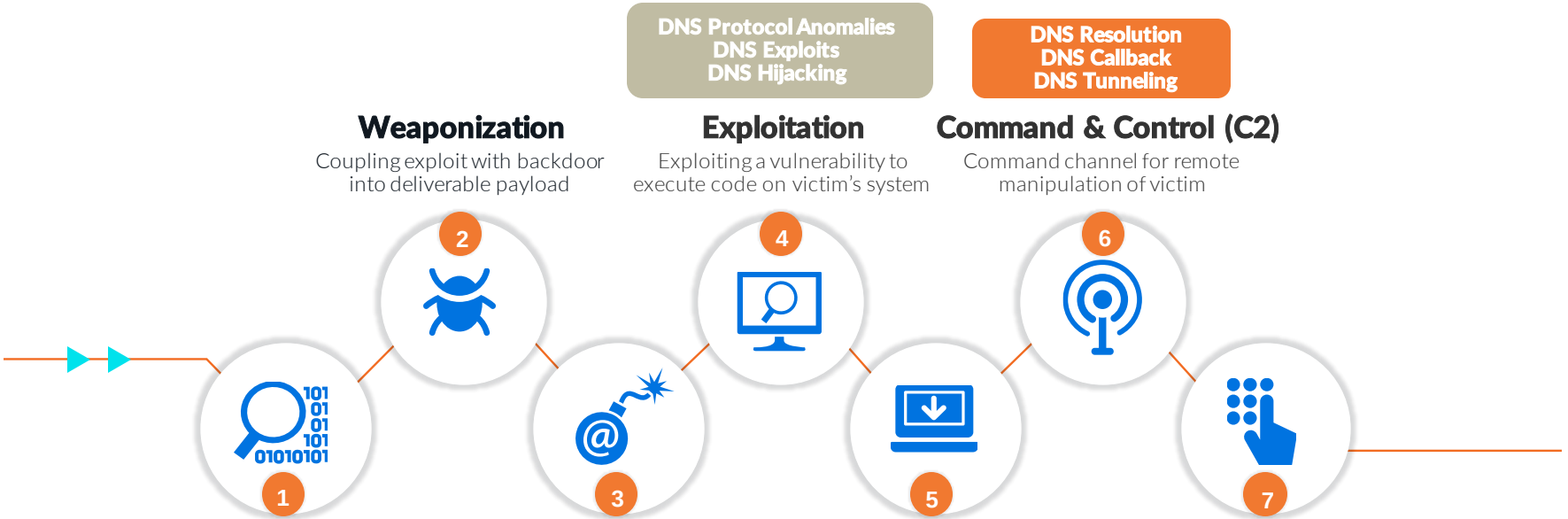
Host Isolation: protect IoT devices by filtering their DNS usage

Ubiquity: Consistent security for any app, on any OS, on any device, anywhere

1. https://info.infoblox.com/EMEA-WAT-FY22-IT-Gartner-DNS-Security-202112.html
2. https://newsworthy-news.com/2021/03/16/nsa-cisa-promote-domain-name-system-incorporating-threat-information/
3. https://us-cert.cisa.gov/ncas/current-activity/2012/02/23/DNSChanger-Malware
4. https://us-cert.cisa.gov/ncas/current-activity/2021/03/04/joint-nsa-and-cisa-guidance-strengthening-cyber-defense-through
5. https://www.ncsc.gov.uk/information/pdns

infoblox.

HOW IS DNS USED BY MALWARE?



infoblox.

USING DNS TO 'SHIFT LEFT' ON DEFENSE

Initial Request

Internal Device

User or device requests connection to Internet location

DNS Resolve

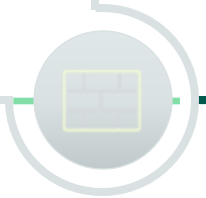
Local DNS Lookup

Requested Internet location lookup with internal DNS server

Network Security

Traffic Processing

Network application traffic processed by internal security devices



Connection

Connection Established

Connection established to requested Internet location

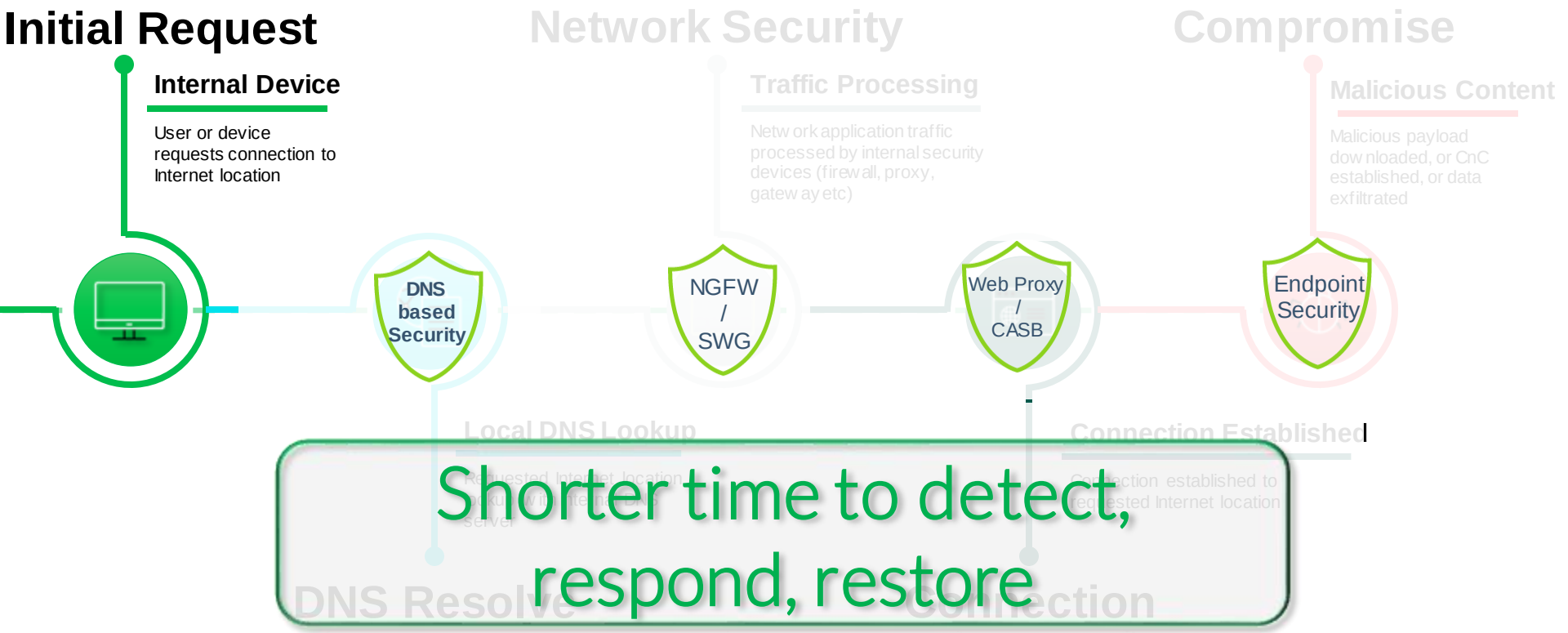
Compromise

Malicious Content

Malicious payload downloaded, or CnC established, or data exfiltrated

infoblox.

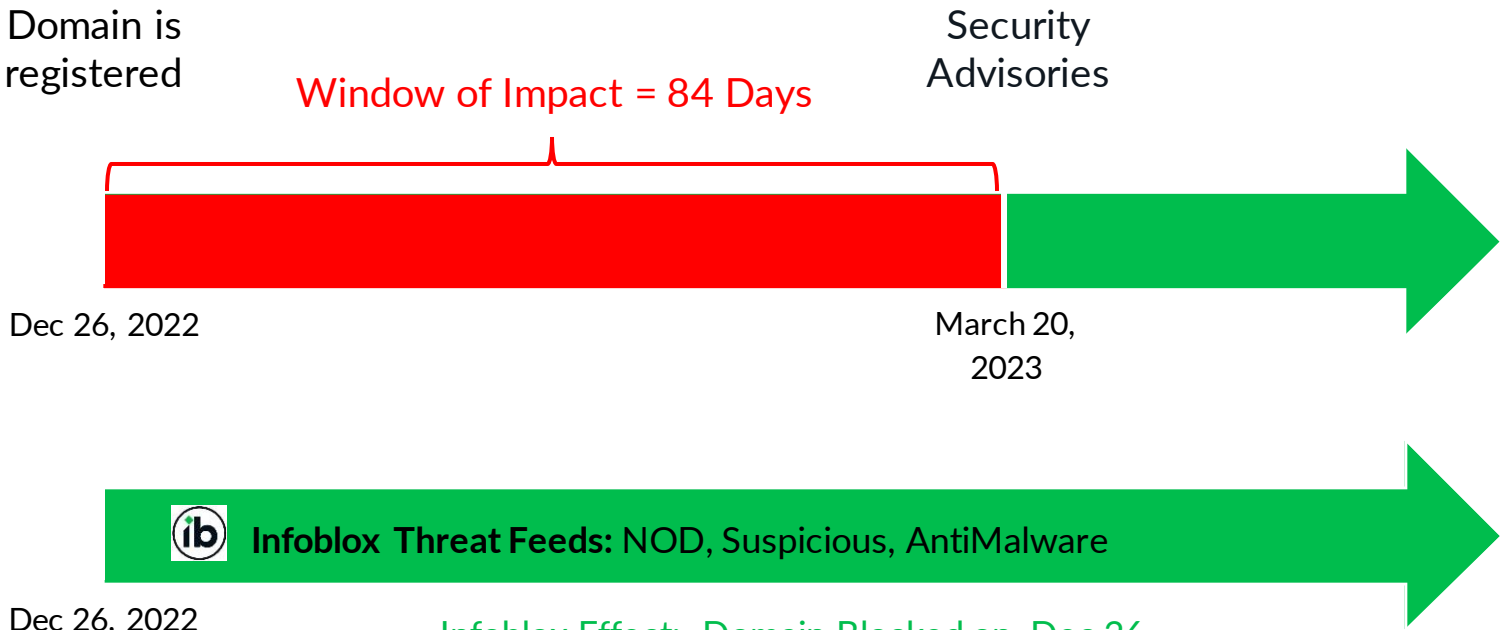
DNS SECURITY – SHIFTING ALL THE WAY TO THE LEFT



infoblox.

ONE STEP MORE TO THE LEFT with Suspicious Domains

Indicator of Compromise: pbxphonenetwork[.]com



infoblox.

VISIBILITY – A SINGLE PANE OF GLASS

What is in your network?
Details of every connected device

Who makes DNS queries?
From inside and outside the netw ork

Manage network space
i.e. after mergers & acquisitions

Help during de-centralization process

On-prem, in cloud and cloud-managed
Local survivability & Local cloud access

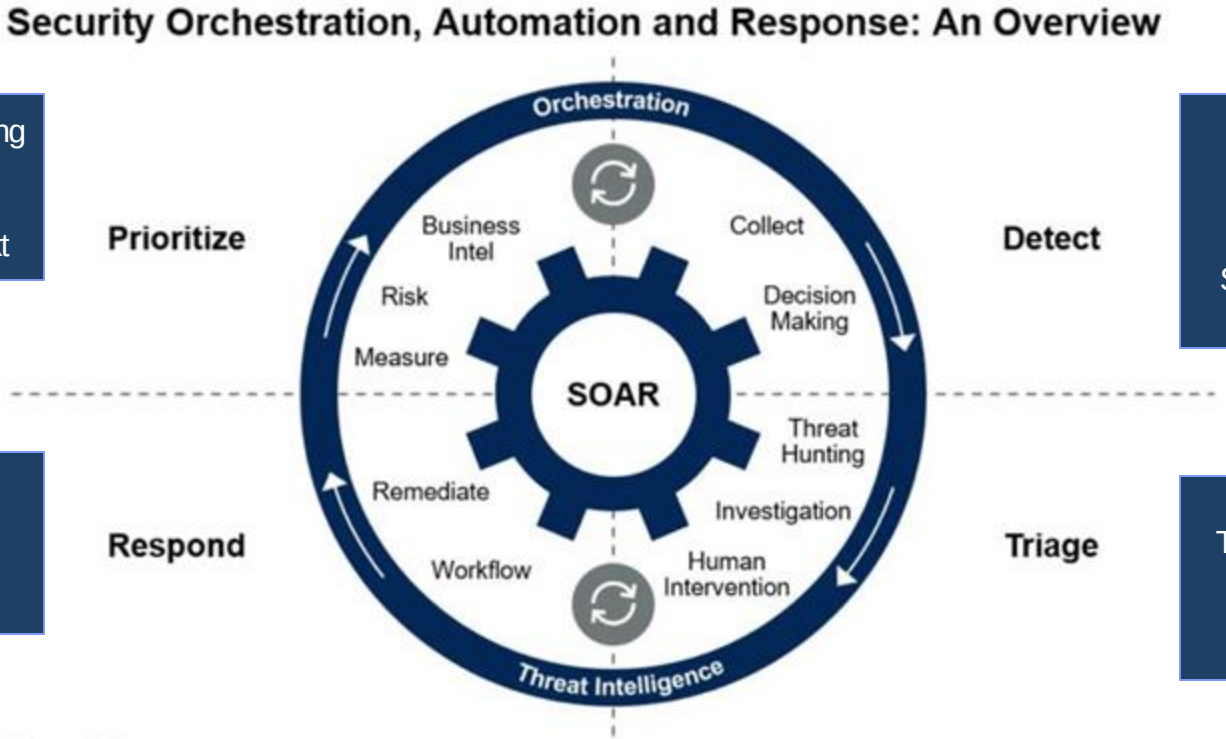
infoblox.

SOAR Model by Gartner and Infoblox Integration

"Intelligence-centric" Security

Threat Risk – Scoring
Threat Context or Attribution
IP Network Context

DNS Firewall
Infoblox Security Ecosystem



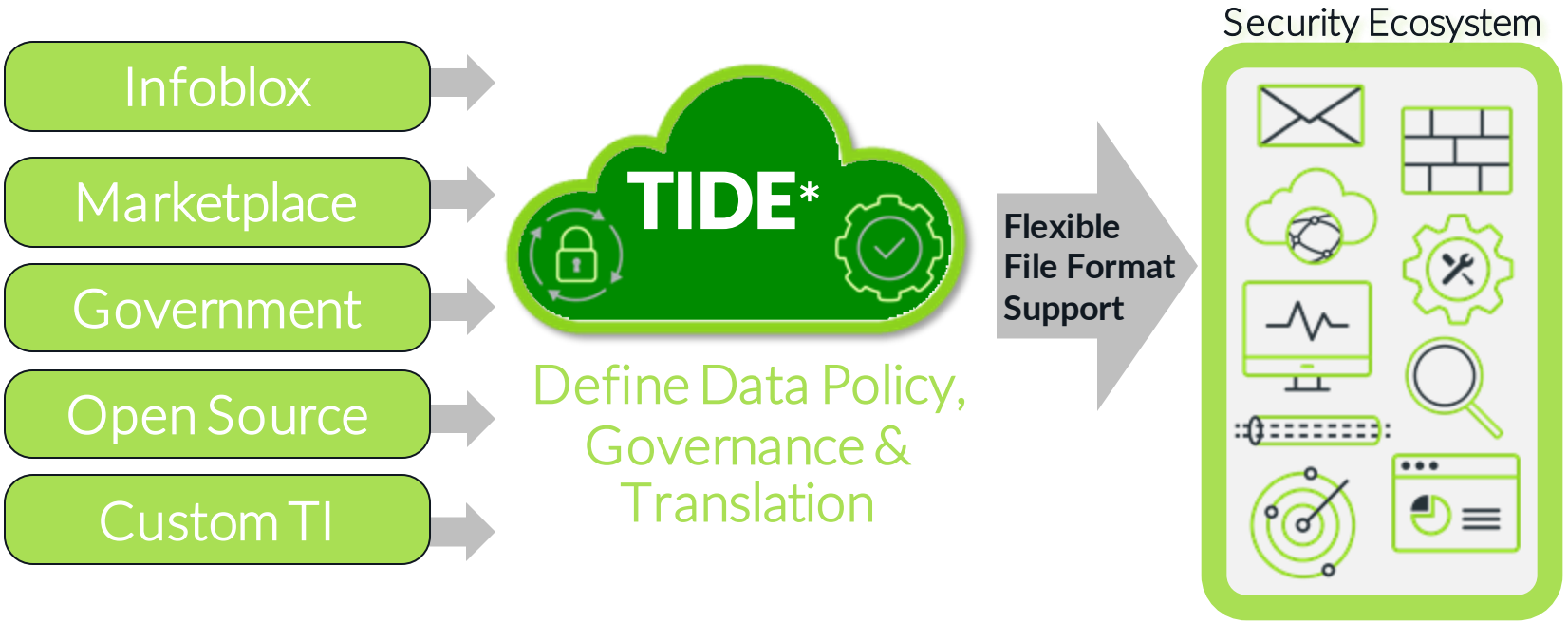
Threat feeds
Behaviour
New Observed
Suspicious Domains

Threat Research tool
DNS threat Hunting
IP Network Context

We can help: Trigger, Enforce, Enrich…

infoblox.

OPTIMIZE THREAT INTELLIGENCE USE



* Threat Intelligence Data Exchange

Lookalikes: An Evolving Threat

81% of organizations experienced one or more email/phishing attacks in past 12 months (Infoblox 2023 Global State of Cybersecurity Report)

Phishing

Cybercriminals use lookalikes in phishing, spam, and compromised websites to support large-volume, **broad-spectrum attacks** for maximum ROI.

Spear phishing & Brand Compromise

Threat Actors use lookalikes in phishing, spam, and compromised websites to support large-volume, **broad-spectrum attacks** for maximum ROI.

Multi-Factor Authentication (MFA) Credential Theft

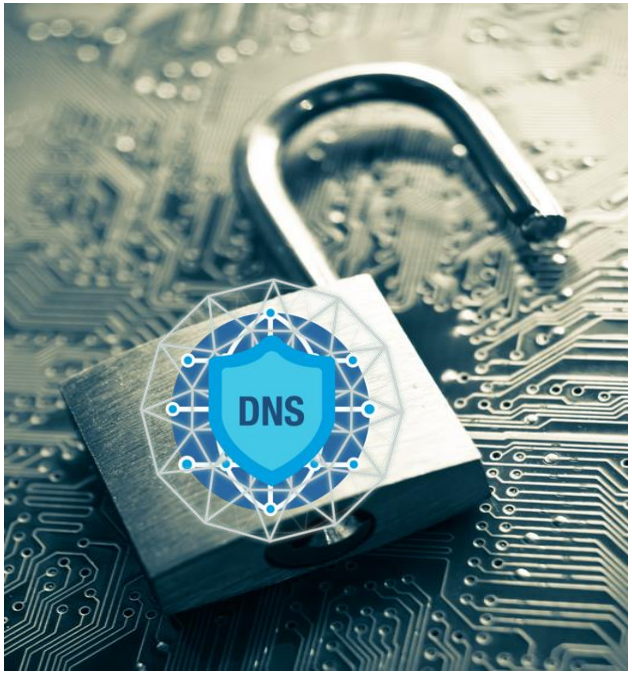
Adversaries use lookalike domains based on corporate internal networks and their MFA provider to actively **steal MFA credentials.**

SUMMARY

Improve SecOps efficiency
Visibility, context, speed and automation

Audit Logging
Who had this IP at that time?

Antimalware and Antiransomware
More than 92% of malware uses DNS



Block exfiltration & infiltration
Including Lateral movements

Host isolation
Automatically restrict queries based on device

Outside the perimeter
Home workers and mobile devices

infoblox.

infoblox.