De l’importance du DNS, DHCP et IPAM pour le SOC

Nicolas Jeanselme – Principal Systems Engineer

Date: March 27th 2019

Operational Challenges

4%

of alerts, are investigated

human resources insufficient to keep organizations safe

92%

of companies get more than 500 alerts per day

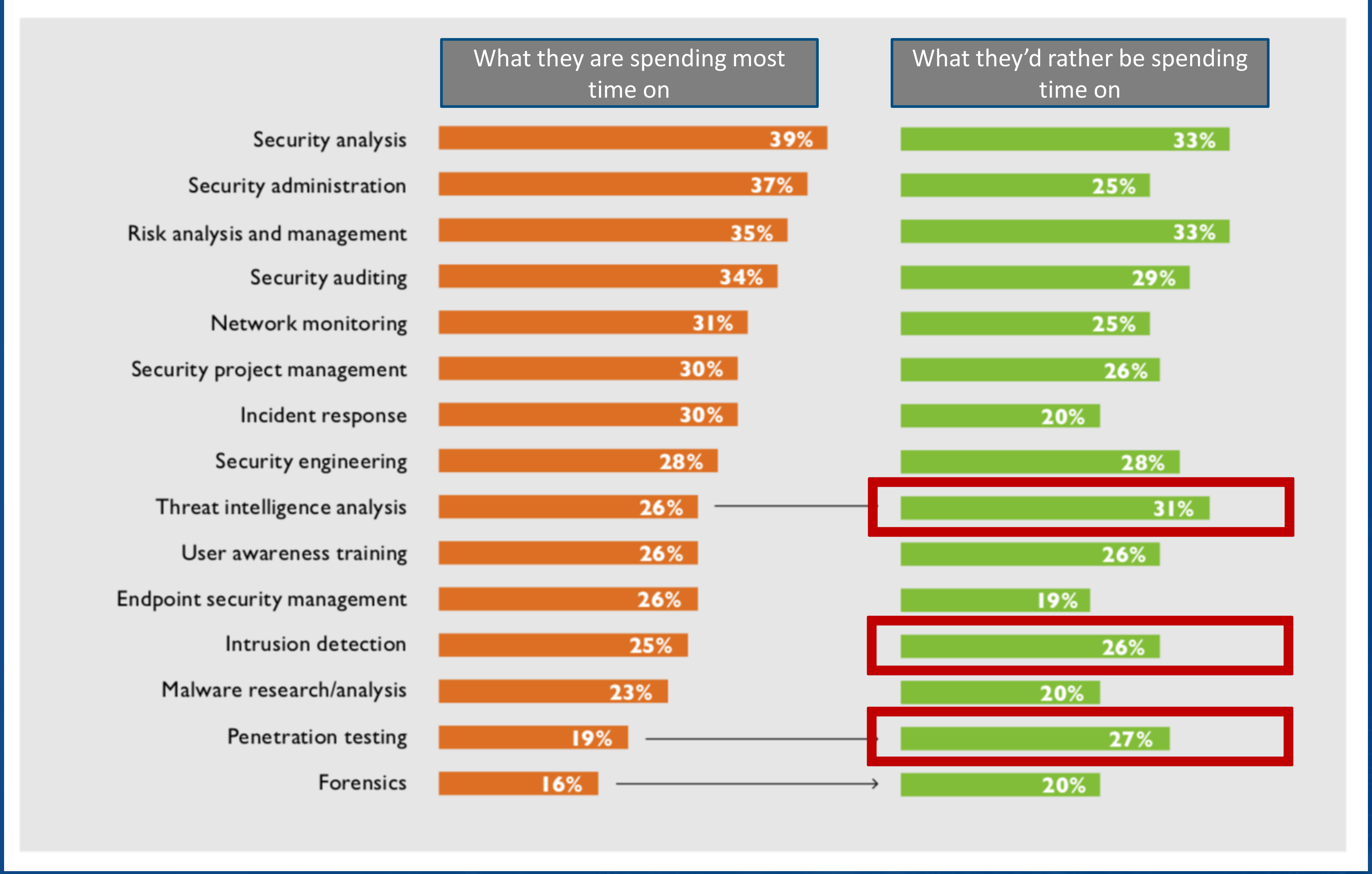
a single cyber analyst can handle only 10 alerts per day

30+

security tools in operation

staff and expertise to operationalize 12 of them

Cybersecurity Professionals’ Perspective



Security professionals would rather spend time on more high value activities like threat intelligence analysis and forensics, and not on the day-to-day tasks

ISC2 Cybersecurity Workforce Study, 2018

No Knowledge of Threat Context

Context – **environmental** information required to take the **right** action

WHO (identity)

WHAT (what network device)

WHERE (where in the network)

WHEN (time of day, how often)

Leading to…

Poor Security Posture

- Infected end not isolated
- Risk of lateral infection
- Data at risk

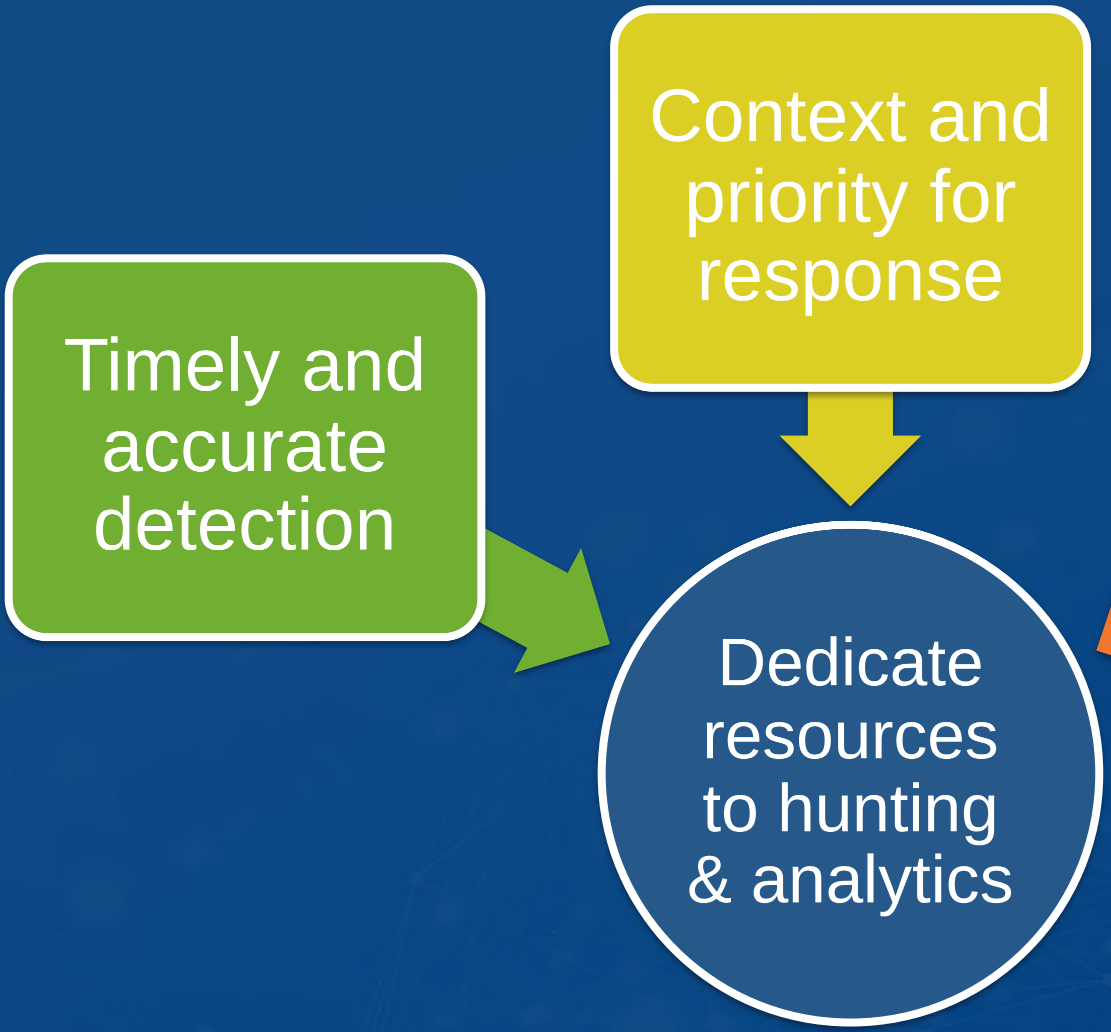
Inefficient Operations

- Manual incident search
- Manual threat intel research
- Slow isolation/disinfection

Lack of Agility

- Manual operations
- Multiple teams handover

Address the Priorities



Timely and accurate detection

Context and priority for response

Faster action or remediation

Dedicate resources to hunting & analytics

DDI (DNS, DHCP, IPAM)

- **Ubiquitous visibility** and enforcement platform for malware detection and threat hunting – 91% of malware relies on DNS as a control plane
- **Rich network data**, device inventory info and audit trail of internal activity
- Domain registration **history** and passive DNS essential for effective threat investigation
- Ideal data source for anomaly based (zero day) threat detection **leveraging machine learning and AI**

Improved SOC Maturity : IPAM

Event Correlation

DHCP servers responsible for allocating IP addresses can be used to track infected devices

DHCP correlates disparate events related to the same device under investigation especially in dynamic environments

Incident Response

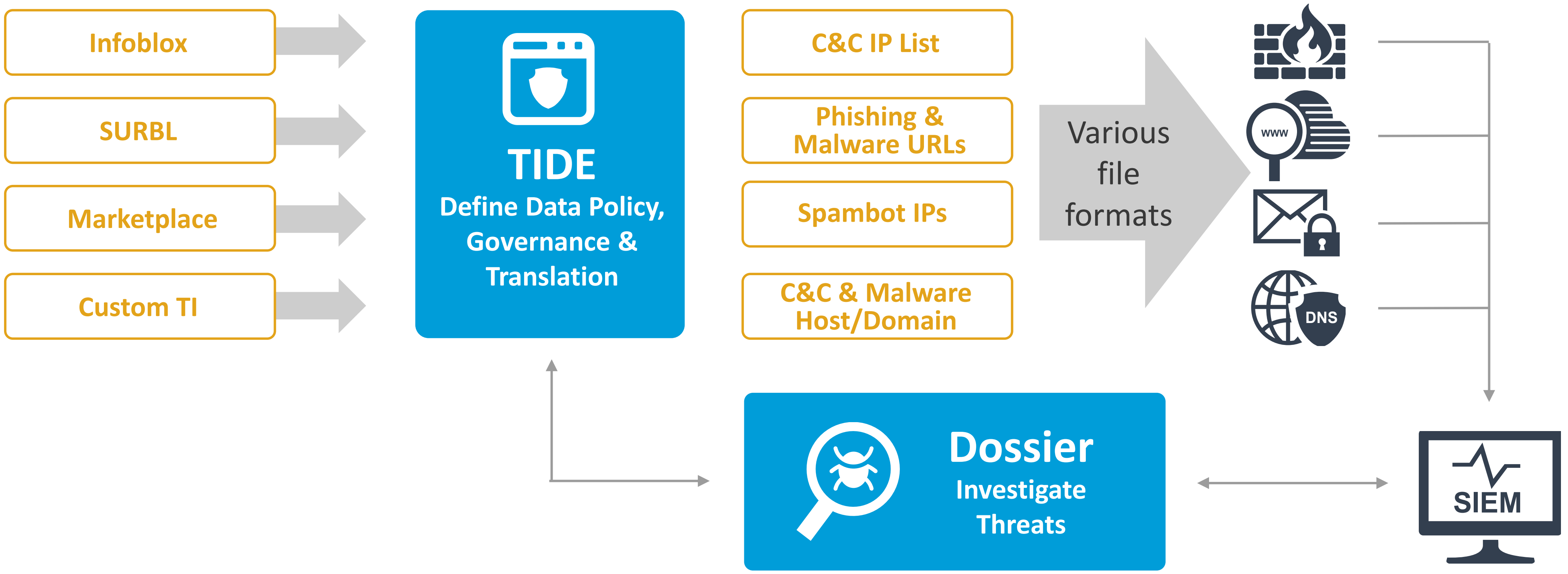
Discovery and Config Management enable operations teams to accurately identify compromised machines and gain visibility into what resources that client has been accessing

Threat Actor Investigation

Public pDNS (passive DNS) and domain registration data help to fully understand scope of adversaries' malicious infrastructure and link events

DNS query logs and history provide detail around activity inside the security perimeter. Visibility into BYOD and IOT devices

Leveraging Threat Intel Across Entire Security Infrastructure



Infoblox

SURBL

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

Dossier

Investigate Threats

RESULT: Single-source of TI management | Faster triage | Threat Prioritization

High Quality Threat Intelligence

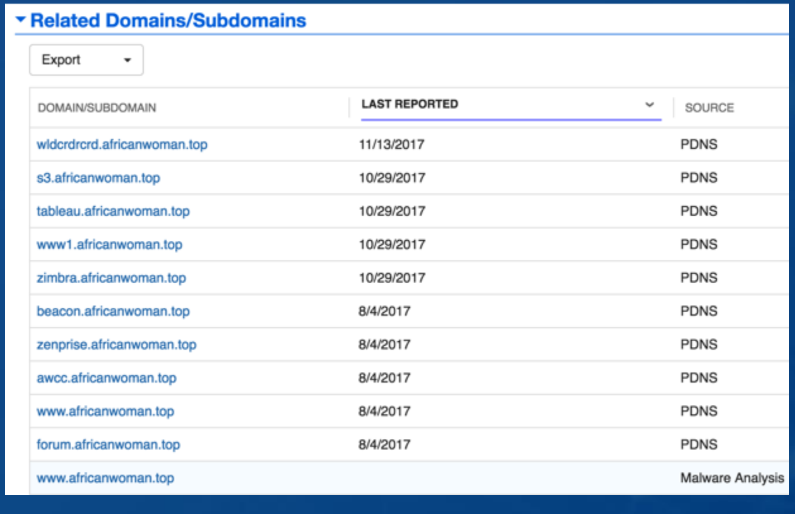
Timely	Every data entry includes an appropriate expiration, so it doesn’t get stale
Reliable	Over 10 years in the business. We publish hundreds of thousands of valuable indicators daily
Accurate	Verified data sets with less than .01% false positives
Contextual	Data include why it’s a threat, and what other indicators are related to it
Easy-to-Use	Available in many forms and many channels

Rapid Threat Investigation and Triage with Dossier

Single central view for multiple sources saves time and resources

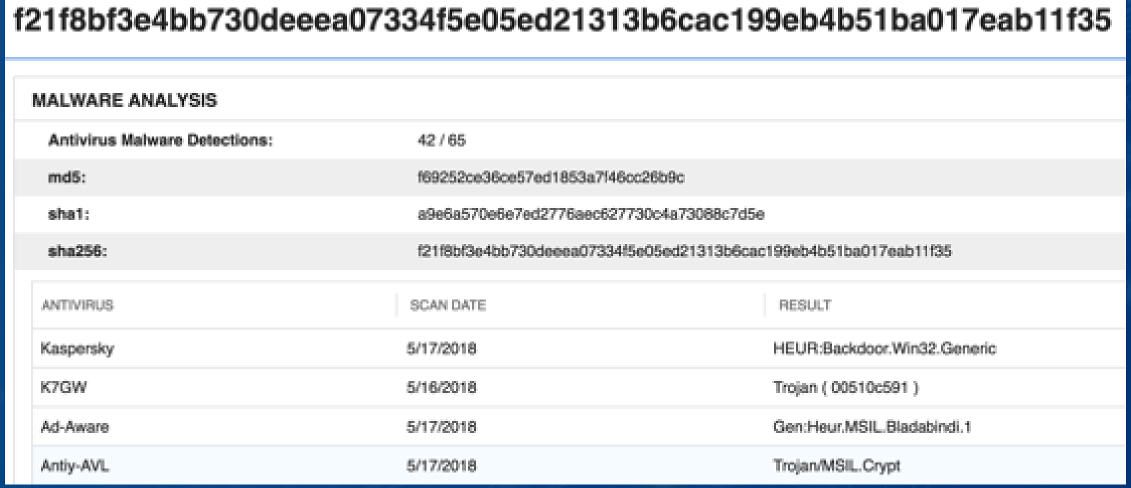
Timely access to contextual information on threat actor, threat campaign, and associated breaches for easier prioritization

Alignment with real world workflows for faster investigation and hunting



Related Domains/Subdomains

DOMAIN/SUBDOMAIN	LAST REPORTED	SOURCE
wldcrdrcrd.africanwoman.top	11/13/2017	PDNS
s3.africanwoman.top	10/29/2017	PDNS
tableau.africanwoman.top	10/29/2017	PDNS
www1.africanwoman.top	10/29/2017	PDNS
zimbra.africanwoman.top	10/29/2017	PDNS
beacon.africanwoman.top	8/4/2017	PDNS
zenprise.africanwoman.top	8/4/2017	PDNS
awcc.africanwoman.top	8/4/2017	PDNS
www.africanwoman.top	8/4/2017	PDNS
forum.africanwoman.top	8/4/2017	PDNS
www.africanwoman.top		Malware Analysis

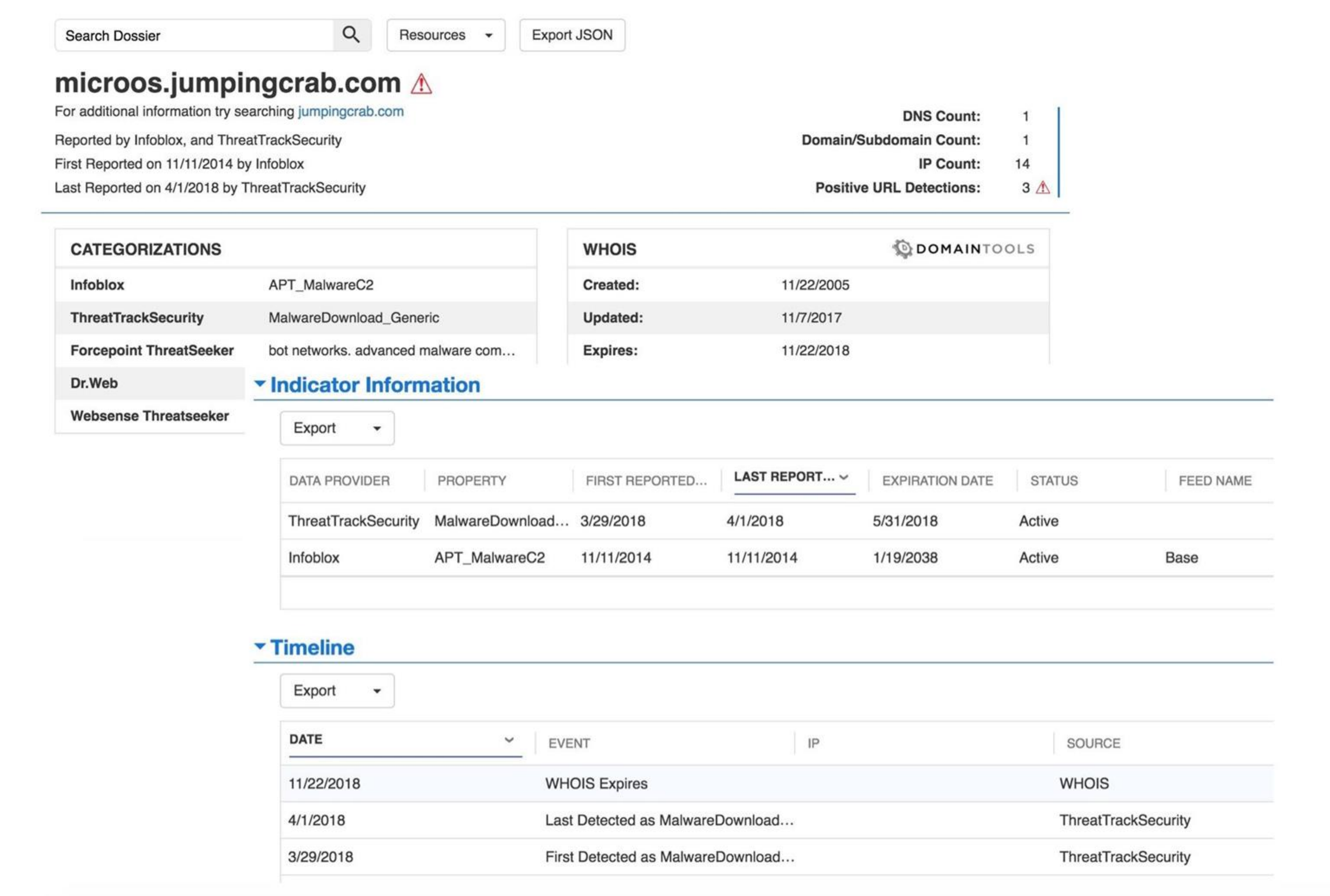


f21f8bf3e4bb730deeea07334f5e05ed21313b6cac199eb4b51ba017eab11f35

MALWARE ANALYSIS

Antivirus Malware Detections:	42 / 65
md5:	f69252ce36ce57ed1853a7f46cc26b9c
sha1:	a9e6a570e6e7ed2776aec627730c4a73088c7d5e
sha256:	f21f8bf3e4bb730deeea07334f5e05ed21313b6cac199eb4b51ba017eab11f35

ANTIVIRUS	SCAN DATE	RESULT
Kaspersky	5/17/2018	HEUR:Backdoor.Win32.Generic
K7GW	5/16/2018	Trojan (00510c591)
Ad-Aware	5/17/2018	Gen:Heur.MSIL.Bladabindi.1
Antiy-AVL	5/17/2018	Trojan/MSIL.Crypt



microoos.jumpingcrab.com ⚠

For additional information try searching jumpingcrab.com

Reported by Infoblox, and ThreatTrackSecurity
First Reported on 11/11/2014 by Infoblox
Last Reported on 4/1/2018 by ThreatTrackSecurity

DNS Count:	1
Domain/Subdomain Count:	1
IP Count:	14
Positive URL Detections:	3 ⚠

CATEGORIZATIONS	
Infoblox	APT_MalwareC2
ThreatTrackSecurity	MalwareDownload_Generic
Forcepoint ThreatSeeker	bot networks. advanced malware com…
Dr.Web	
Websense Threatseeker	

WHOIS	DOMAINTOOLS
Created:	11/22/2005
Updated:	11/7/2017
Expires:	11/22/2018

Indicator Information

DATA PROVIDER	PROPERTY	FIRST REPORTED…	LAST REPORT…	EXPIRATION DATE	STATUS	FEED NAME
ThreatTrackSecurity	MalwareDownload…	3/29/2018	4/1/2018	5/31/2018	Active	
Infoblox	APT_MalwareC2	11/11/2014	11/11/2014	1/19/2038	Active	Base

Timeline

DATE	EVENT	IP	SOURCE
11/22/2018	WHOIS Expires		WHOIS
4/1/2018	Last Detected as MalwareDownload…		ThreatTrackSecurity
3/29/2018	First Detected as MalwareDownload…		ThreatTrackSecurity

Use Cases

Customer Story: EMEA Bank #1

Customer Use Case:

- Difficulty in scaling existing security operations staff to manage risk
- Lack of qualified cybersecurity analysts to hire

Solution: Infoblox Threat Intelligence, Data Connector, ActiveTrust

Outcomes:

- Accelerated incident evaluation and response using Infoblox threat intelligence data and investigation tool
- Easy access to DNS data that provided context

Customer Story: EMEA Bank #2

Customer Use Case:

- Looking to maximize threat intelligence investment
- Existing threat intelligence was tied to appliances they had bought

Solution: Infoblox TIDE, ActiveTrust, Cybersecurity ecosystem

Outcomes:

- Infoblox threat intelligence easily applied to existing Palo Alto Networks, Cisco and ArcSight platforms
- Improved ROI of existing security platforms

Customer Story: US Technology Company

Customer Use Case:

- Analysts typically spent 1 hour evaluating incidents
- 40 minutes spent gathering data from multiple sources

Solution: Infoblox Dossier

Outcomes:

- Eliminated wasted resources and reduced threat investigation time to minutes
- Improved operational efficiency

Summary

- ✓ DDI infrastructure and data are critical for efficient threat detection, event correlation and incident response

- ✓ DNS is an important and common data source that can be used to expand threat detection in dynamic and new IT infrastructure models

- ✓ All organizations have DNS and just need to tap into the gold mine of data.

eb-Qual

CYBER SECURITY

USE CASE
IMPLEMENTATION INFOBLOX AT ISP

CHRISTOPHE ANDRES | *CHRISTOPHE.ANDRES@EB-QUAL.CH*

Common Event, Geneva 27.03.2019

Keep IT secure

Use case - Implementation Infoblox at ISP

- **Situation before implementation**

  Weaknesses (visibility, control, security, availability / performance)

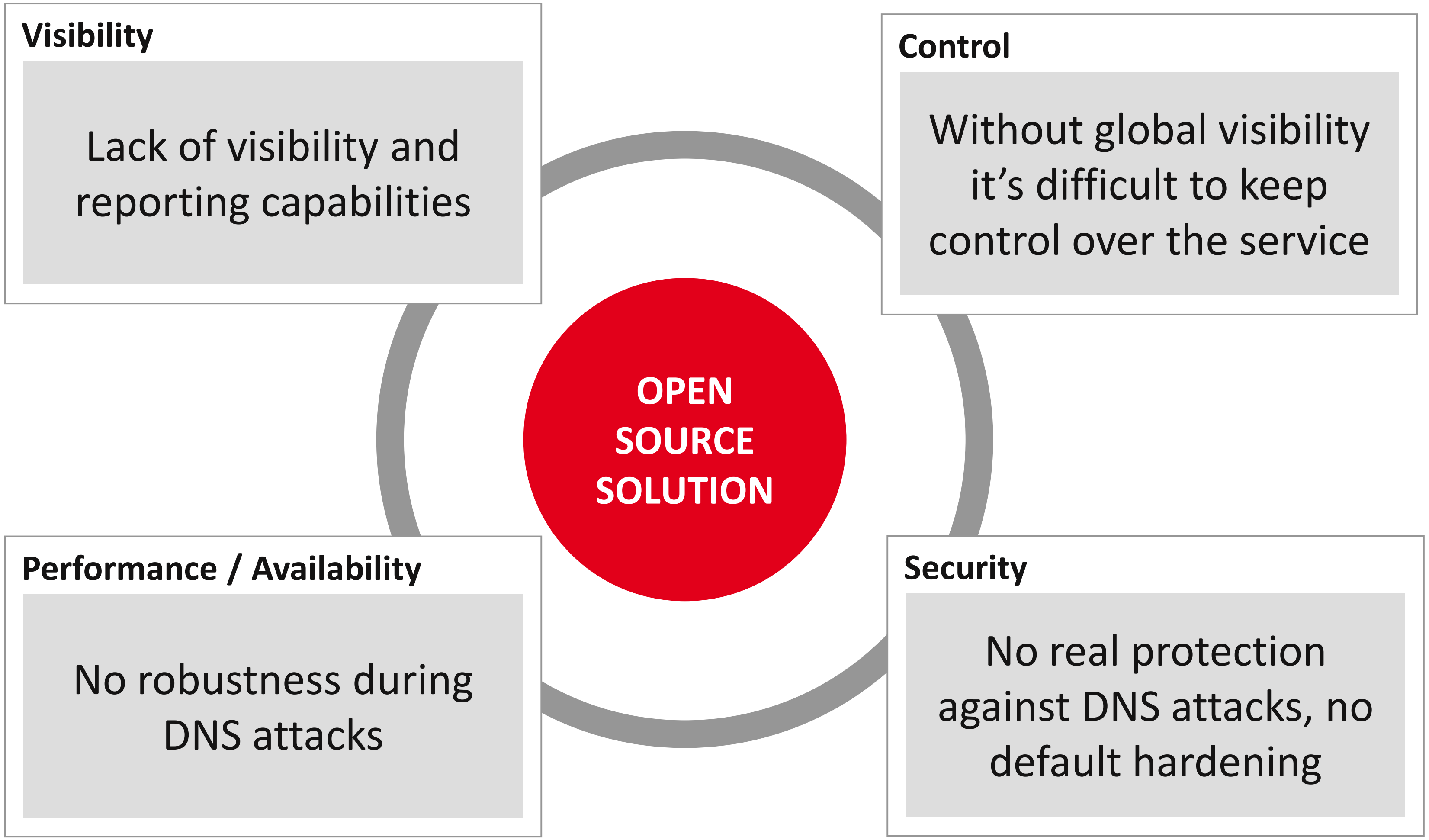
- **Implementation at customer**

  Analyses and planning, design, implementation, testing, production

- **Customer benefits and customer feedback**

  “Better security (Threat Protection Rules), visibility, reporting”

Situation before implementation



Visibility

Lack of visibility and reporting capabilities

Control

Without global visibility it’s difficult to keep control over the service

OPEN SOURCE SOLUTION

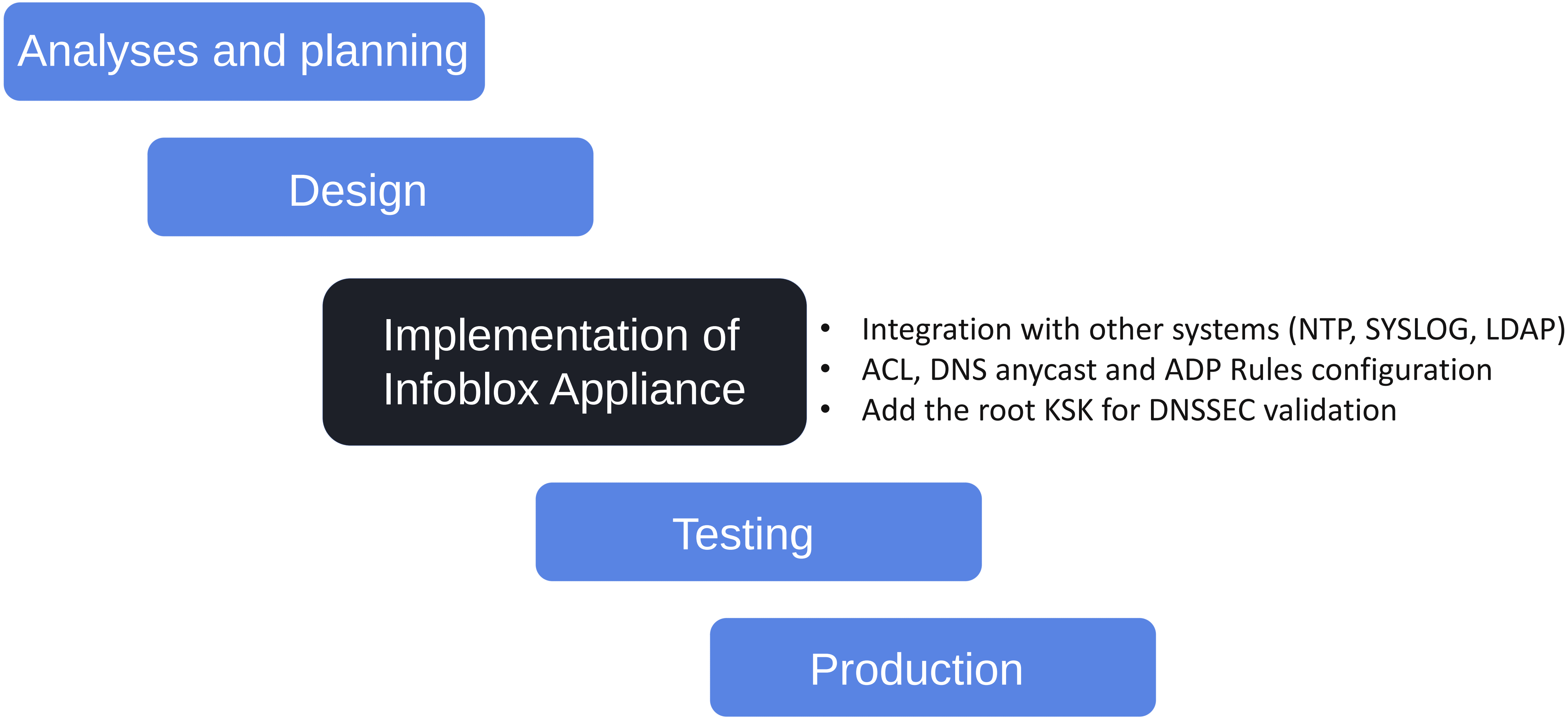
Performance / Availability

No robustness during DNS attacks

Security

No real protection against DNS attacks, no default hardening

Implementation at customer



Analyses and planning

Design

Implementation of Infoblox Appliance

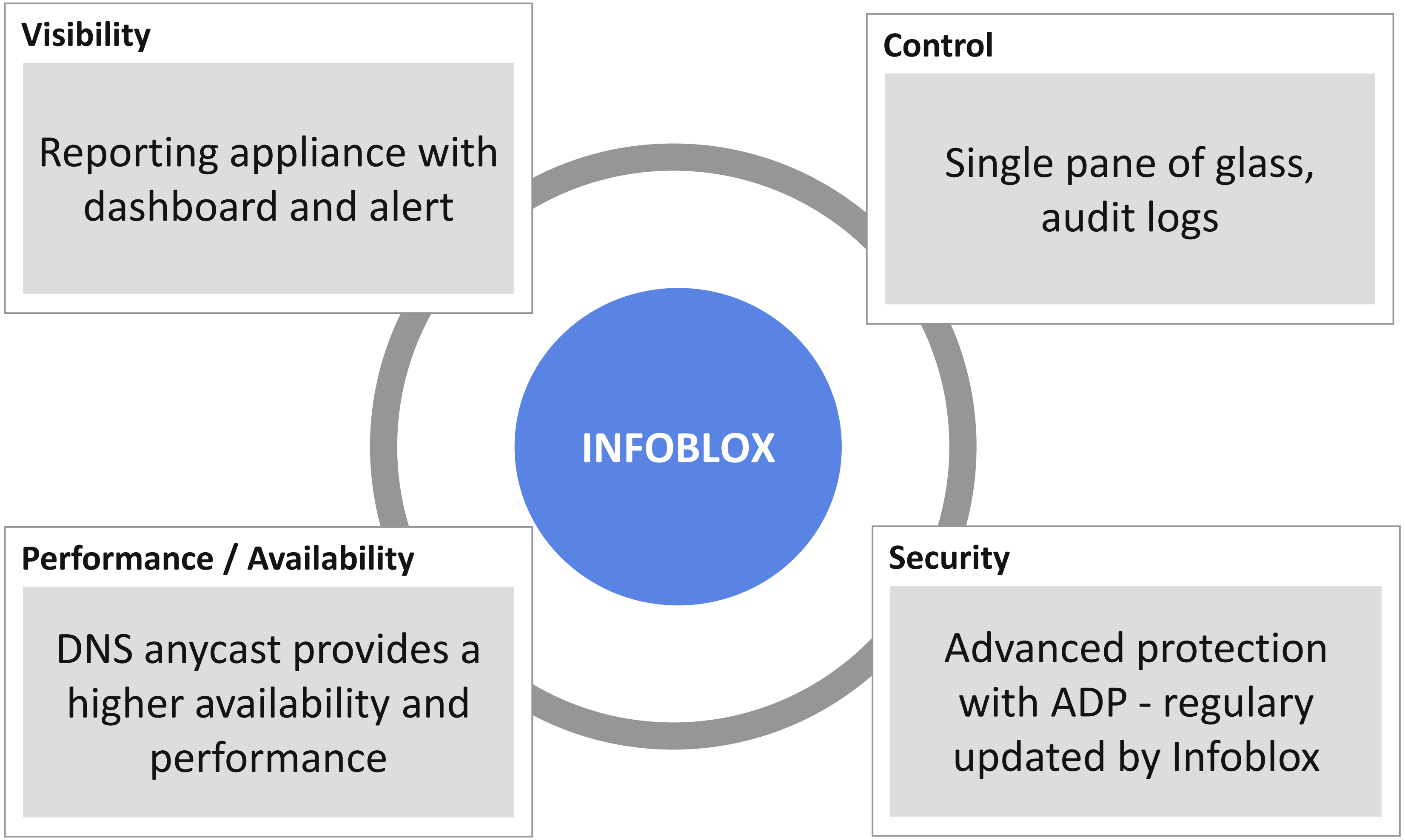
- Integration with other systems (NTP, SYSLOG, LDAP)
- ACL, DNS anycast and ADP Rules configuration
- Add the root KSK for DNSSEC validation

Testing

Production

After implementation

Customer benefits



Visibility

Reporting appliance with dashboard and alert

Control

Single pane of glass, audit logs

INFOBLOX

Performance / Availability

DNS anycast provides a higher availability and performance

Security

Advanced protection with ADP - regulary updated by Infoblox

Feedback of the Service Owner:

- *“Lower operations cost (less incidents)”*
- *“Software upgrades are done faster”*
- *“Better availability and robustness during DNS attacks”*
- *“Better security (Threat Protection Rules), visibility, reporting”*

Questions on

- *Use case implementation Infoblox at ISP*
- *De l’importance du DNS, DHCP et IPAM pour le SOC et retour sur une implémentation Infoblox*