HVORFOR BRUGE TID PÅ IPAM?

.. OG HVAD POKKER ER DET ALLIGEVEL?

ckrogh@infoblox.com

infoblox.

HVEM ER JEG?

Solution Architect hos **Infoblox**, tidligere Juniper Networks og Trend Micro

Været i IT-industrien i over 18 år.

Min første IPAM løsning var en Lotus Notes database .....

Hvor skal vi hen?

IPAM – En fortælling

…(eller to)

Hvordan IPAM gør dine sikkerhedsinvesteringer bedre

Hvordan IPAM forbedrer dine sikkerhedskontroller

Q&A

infoblox

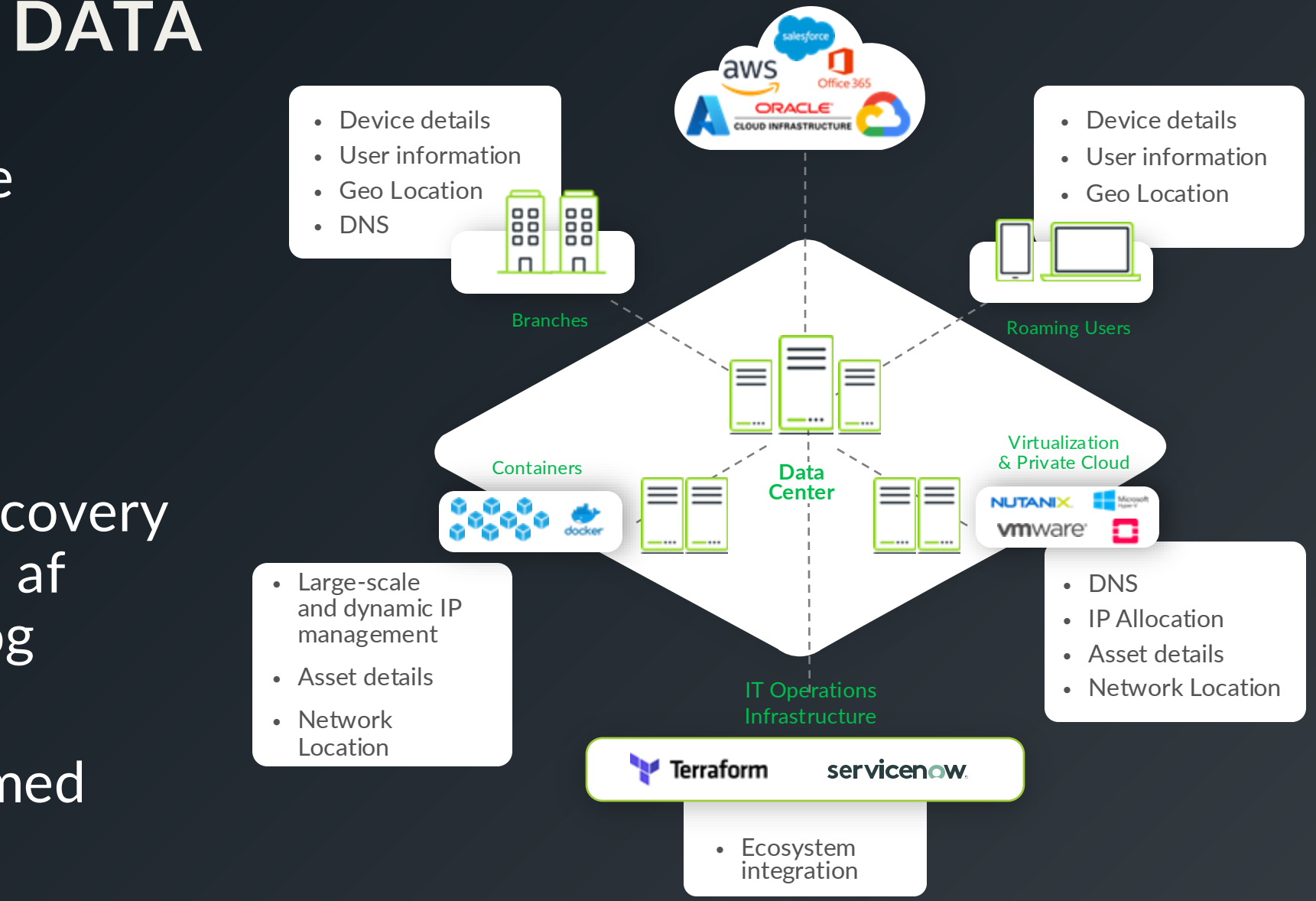
Vores SOC anvender IPAM data i søgen efter de reelle 'ejere' af udstyr/domæner når der opstår et incident. Tidsforbruget er gået fra ***timer/dage til minutter.***

Lead sikkerheds arkitekt, større globaliseret dansk virksomhed

infoblox.

GULDMINE AF DATA

- Bruger-, og device information til at triagere sikkerhedsevents hurtigere
- Automatiseret discovery af assets på tværs af fysiske, virtuelle og cloud miljøer
- Integreret IPAM med DNS og DHCP



infoblox.

INCIDENT RESPONSE FOR DE FLESTE

1

Security Alert

Security event
Source IP address: 198.18.197.61

"What is this address 198.18.197.61?"

"This address range is on AWS. Check with Cloud team"

Network Team

checks

Excel Spreadsheet "IPAM"

198.18.0.0 /16: AWS

2

Investigation

"What is this address 198.18.197.61?"

"This is a VM running on DevOps_UAT. Check with Apps team for details"

Cloud Team

Log in

192.18.197.0/24: AWS Acc #123
VPC: DevOps_UAT
MAC: aa.bb.cc.dd.ee.ff
Hostname: WebServer01

"Who created this VM WebServer01?"

"This test server is owned by Robert Lim"

DevOps Team

3

Containment and Remediation

infoblox

INCIDENT RESPONSE MED IPAM

1

Security Alert

Security event
Source IP address: 198.18.197.61

IPAM integrated with DNS + DHCP

Location: AWS Account #123
VPC: DevOps_UAT
Hostname: WebServer01
MAC: aa.bb.cc.dd.ee.ff
System Owner: Robert Lim
First Discovered: 2 Jan 2024 14:25:33
Last Detected: 1 May 2024 11:30:32

DNS Query Logs:
- Spike in the number of DNS queries from 1 May 2024
- RPZ blocked queries to *badguy.com*

2

Investigation

"What is this address 198.18.197.61?"

"Lookup badguy.com"

DOMAIN INVESTIGATION TOOL

Threat Property: APT_malwareC2
Threat Level: High
Impacted Devices:
- 198.18.190.26
- 198.18.190.50
- 198.18.190.53
- 198.18.197.61

Plus: Detection Time, Related Domains, Related IPs, WHOIS, MITRE ATT&CK mapping etc

3

Containment and Remediation

infoblox.

På compliance og audit har IPAM hjulpet gevaldigt, hvor vi reelt kan sige hvad/hvor/hvem har og bruger hvad.
Det var umuligt før.

Lead sikkerheds arkitekt, større globaliseret dansk virksomhed

infoblox.


CONTROL 01
Inventory and Control of Enterprise Assets
5 Safeguards
IG1 2/5
IG2 4/5
IG3 5/5
CONTROL 02
Inventory and Control of Software Assets
7 Safeguards
IG1 3/7
IG2 6/7
IG3 7/7
CONTROL 03
Data Protection
14 Safeguards
IG1 6/14
IG2 12/14
IG3 14/14
CONTROL 04
Secure Configuration of Enterprise Assets and Software
12 Safeguards
IG1 7/12
IG2 11/12
IG3 12/12
CONTROL 05
Account Management
6 Safeguards
IG1 4/6
IG2 6/6
IG3 6/6
CONTROL 06
Access Control Management
8 Safeguards
IG1 5/8
IG2 7/8
IG3 8/8
CONTROL 07
Continuous Vulnerability Management
7 Safeguards
IG1 4/7
IG2 7/7
IG3 7/7
CONTROL 08
Audit Log Management
12 Safeguards
IG1 3/12
IG2 11/12
IG3 12/12
CONTROL 09
Email and Web Browser Protections
7 Safeguards
IG1 2/7
IG2 6/7
IG3 7/7
CONTROL 10
Malware Defenses
7 Safeguards
IG1 3/7
IG2 7/7
IG3 7/7
CONTROL 11
Data Recovery
5 Safeguards
IG1 4/5
IG2 5/5
IG3 5/5
CONTROL 12
Network Infrastructure Management
8 Safeguards
IG1 1/8
IG2 7/8
IG3 8/8
CONTROL 13
Network Monitoring and Defense
11 Safeguards
IG1 0/11
IG2 6/11
IG3 11/11
CONTROL 14
Security Awareness and Skills Training
9 Safeguards
IG1 8/9
IG2 9/9
IG3 9/9
CONTROL 15
Service Provider Management
7 Safeguards
IG1 1/7
IG2 4/7
IG3 7/7
CONTROL 16
Applications Software Security
14 Safeguards
IG1 0/14
IG2 11/14
IG3 14/14
CONTROL 17
Incident Response Management
9 Safeguards
IG1 3/9
IG2 8/9
IG3 9/9
CONTROL 18
Penetration Testing
5 Safeguards
IG1 0/5
IG2 3/5
IG3 5/5

infoblox.


CONTROL 01
Inventory and Control of Enterprise Assets
5 Safeguards
IG1 2/5
IG2 4/5
IG3 5/5
CONTROL 02
Inventory and Control of Software Assets
7 Safeguards
IG1 3/7
IG2 6/7
IG3 7/7
CONTROL 03
Data Protection
14 Safeguards
IG1 6/14
IG2 12/14
IG3 14/14
CONTROL 04
Secure Configuration of Enterprise Assets and Software
12 Safeguards
IG1 7/12
IG2 11/12
IG3 12/12
CONTROL 05
Account Management
6 Safeguards
IG1 4/6
IG2 6/6
IG3 6/6
CONTROL 06
Access Control Management
8 Safeguards
IG1 5/8
IG2 7/8
IG3 8/8
CONTROL 07
Continuous Vulnerability Management
7 Safeguards
IG1 4/7
IG2 7/7
IG3 7/7
CONTROL 08
Audit Log Management
12 Safeguards
IG1 3/12
IG2 11/12
IG3 12/12
CONTROL 09
Email and Web Browser Protections
7 Safeguards
IG1 2/7
IG2 6/7
IG3 7/7
CONTROL 10
Malware Defenses
7 Safeguards
IG1 3/7
IG2 7/7
IG3 7/7
CONTROL 11
Data Recovery
5 Safeguards
IG1 4/5
IG2 5/5
IG3 5/5
CONTROL 12
Network Infrastructure Management
8 Safeguards
IG1 1/8
IG2 7/8
IG3 8/8
CONTROL 13
Network Monitoring and Defense
11 Safeguards
IG1 0/11
IG2 6/11
IG3 11/11
CONTROL 14
Security Awareness and Skills Training
9 Safeguards
IG1 8/9
IG2 9/9
IG3 9/9
CONTROL 15
Service Provider Management
7 Safeguards
IG1 1/7
IG2 4/7
IG3 7/7
CONTROL 16
Applications Software Security
14 Safeguards
IG1 0/14
IG2 11/14
IG3 14/14
CONTROL 17
Incident Response Management
9 Safeguards
IG1 3/9
IG2 8/9
IG3 9/9
CONTROL 18
Penetration Testing
5 Safeguards
IG1 0/5
IG2 3/5
IG3 5/5

infoblox.

NIS2

Risk Management Measures (Article 21)

Regulated Entities must take specified measures to manage risks:

- (a) policies on risk analysis and information system security;
- (b) **incident handling**;
- (c) business continuity, such as backup management and disaster recovery, and crisis mgmt;
- (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- (f) **policies and procedures to assess the effectiveness of cybersec risk-management measures**;
- (g) basic cyber hygiene practices and cybersec training;
- (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- (i) human resources security, **access control policies** and **asset management**;
- (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

NIS2

Risk Management Measures (Article 21)

Regulated Entities must take specified measures to manage risks:

- (b) **incident handling**;

- (i) human resources security, access control policies and **asset management**;

Q&A

infoblox

TAK FOR JERES TID

infoblox.