Infoblox
NEXT LEVEL NETWORKING

Boost the Efficiency of Your Security Operations

Chris Usserman, Principal Security Architect
Infoblox

Agenda

Operational challenges

Accelerating Incident Response

Improving SOC Efficiency

Operational Challenges

Siloed security tools

Too many alerts/ too much noise

Cyber security skills shortage

Manual investigation processes

Business Disruptions are Costly and Impacts Brand

$40M

Initial loss from a recent ransomware attack

$119B

Wiped off from Facebook's market cap after Cambridge Analytica breach

196 DAYS

Average time to identify a breach

Sources: Ponemon Institute, The Guardian

Operational Challenges Continue to Mount

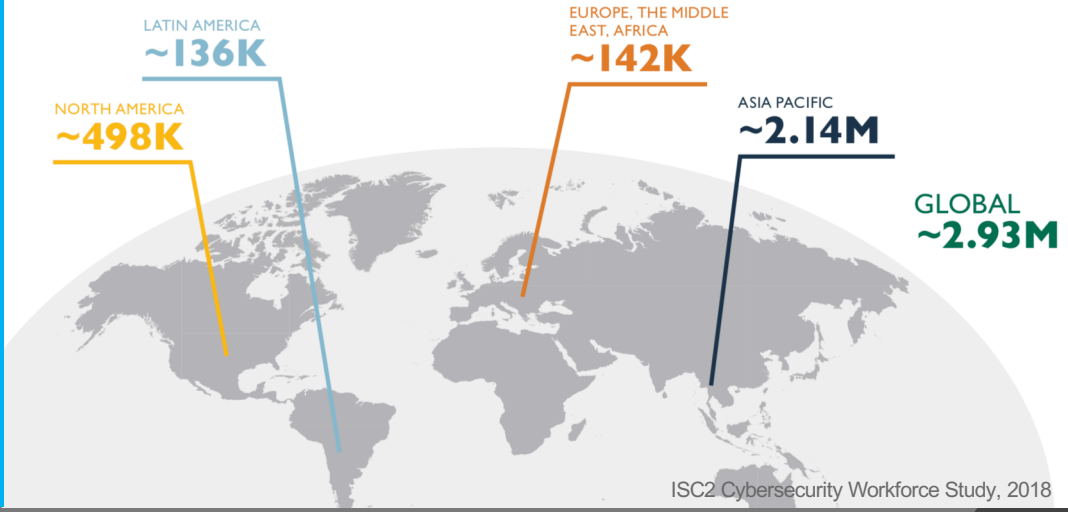
92% of companies get more than 500 alerts per day; a single cyber analyst can handle only 10

8% of alerts are investigated; not enough humans to keep organizations safe

30+ security tools in operation, with staff and expertise to manage 12

And We Can't Throw More People at the Problem

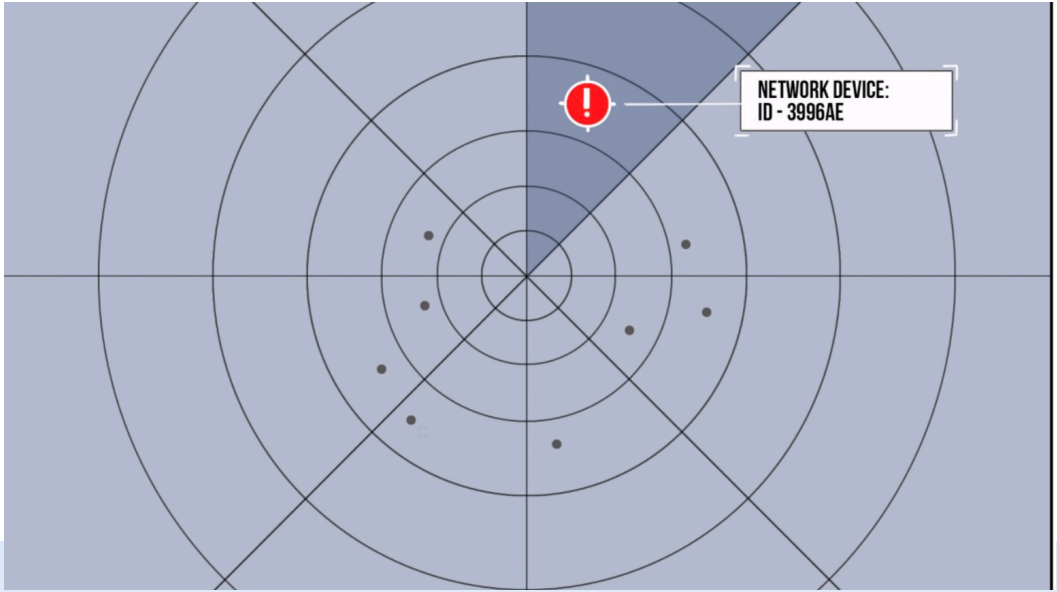
Gap in Cybersecurity Professionals by Region



ISC2 Cybersecurity Workforce Study, 2018

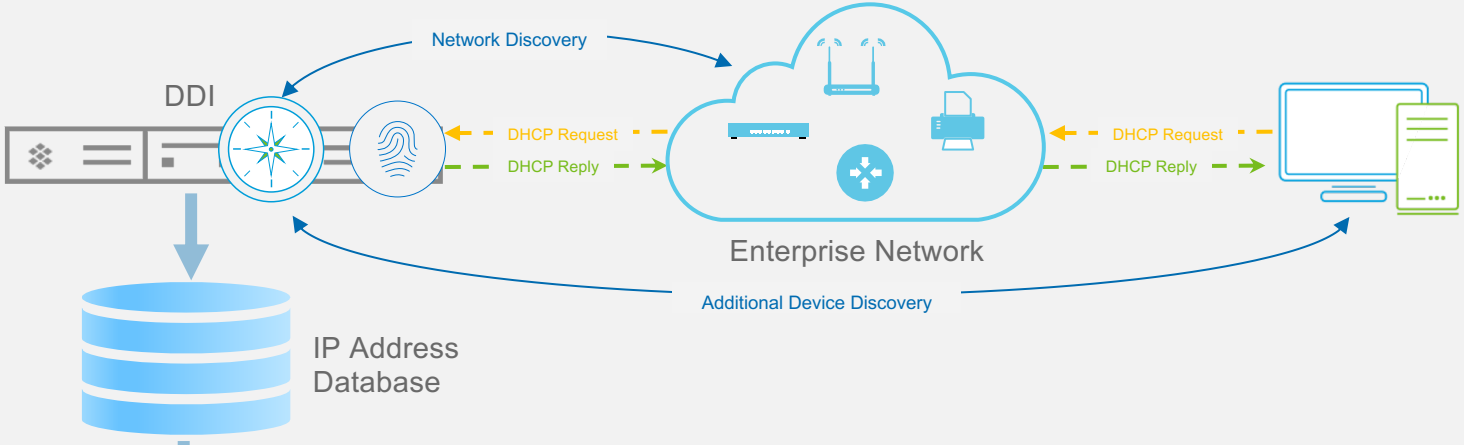
 |

Visibility is Key for Security Operations



- Visibility that extends beyond the campus network (public cloud, IoT, roaming users, branch offices)
- Network context for efficient correlation
- Key datasets for making threat intelligence actionable

Gathering Device Data with DDI



Device	IP Address	DHCP Fingerprint
Device 1	10.1.3.5	

Device Fingerprint

Device 1	10.1.3.5	PC	Windows	v10

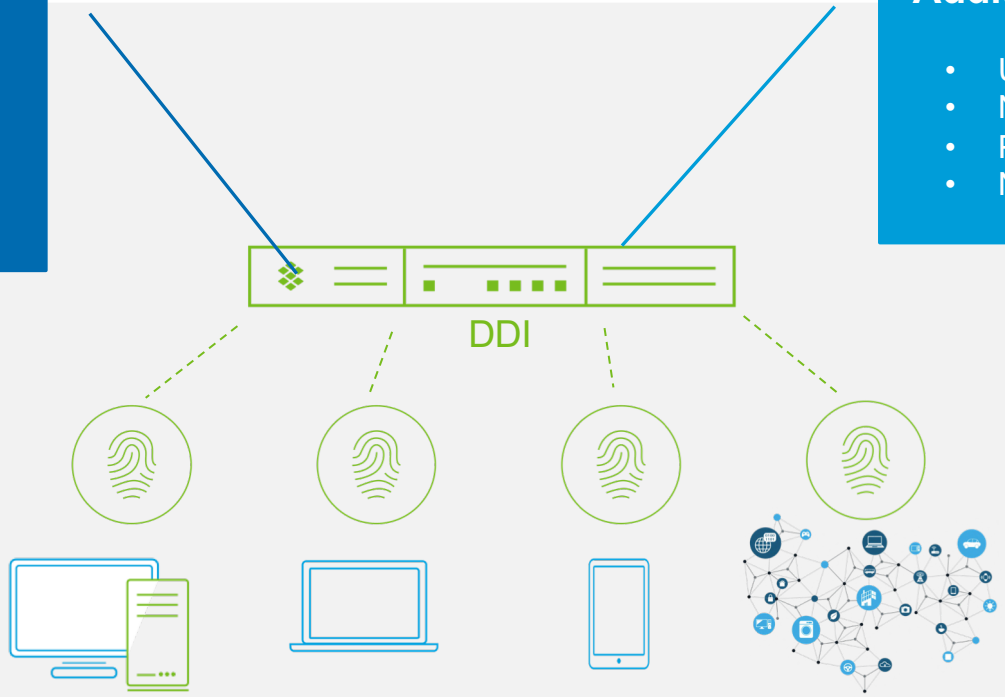
DDI Meta-data for Entire Infrastructure

DHCP Discovery

- MAC Address
- Device type
- OS information
- Current IP
- Historical IP's and locations

Additional Discovery

- User details
- Network Location
- Physical location
- Network devices



Agenda

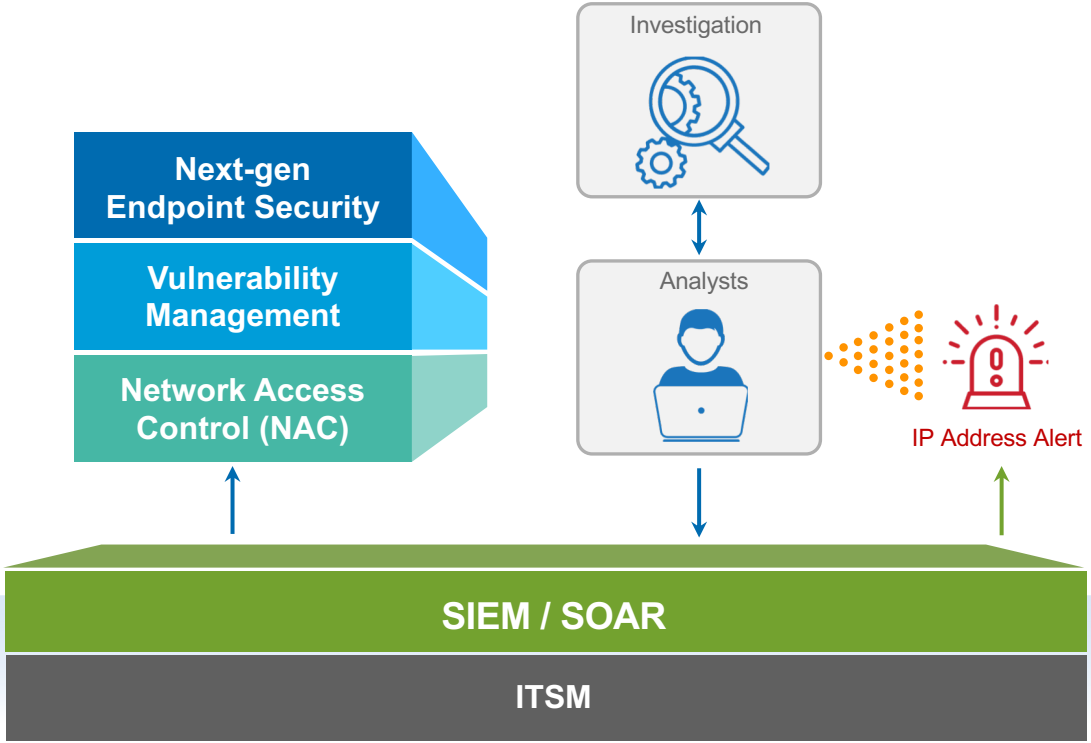
Operational challenges

Accelerating Incident Response

Improving SOC Efficiency

Typical Incident Response

Lengthy
Response Times

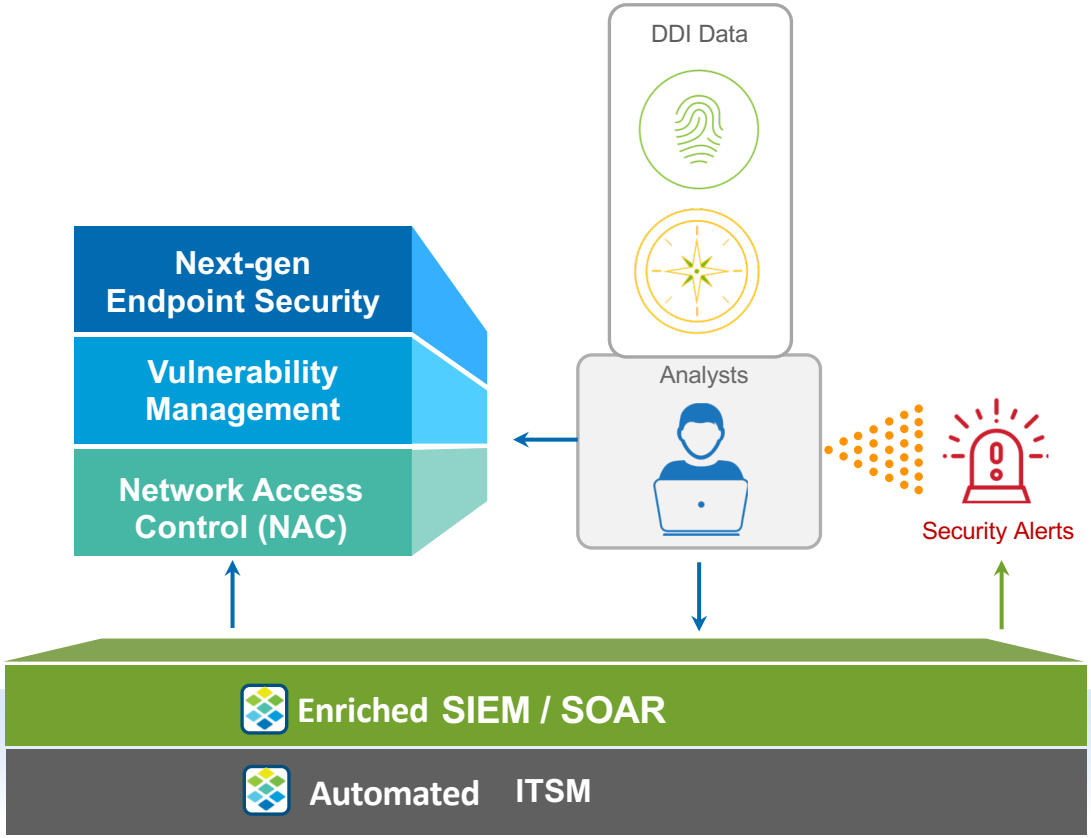


Manual Investigation

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

 |

DDI Data Accelerates Incident Response



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

 |

Agenda

Operational challenges

Accelerating Incident Response

Improving SOC Efficiency

Value of DNS Data to a SIEM

- DDI data enriches events in a SIEM
- DNS query and response info provides insights into device activity
- However, sending all DNS query, response data could quickly overburden the SIEM

 |

Cloud Managed Data Connector for SIEM Optimization

Data Connector gathers DDI data, filters out legitimate activity and sends suspicious event info to SIEM

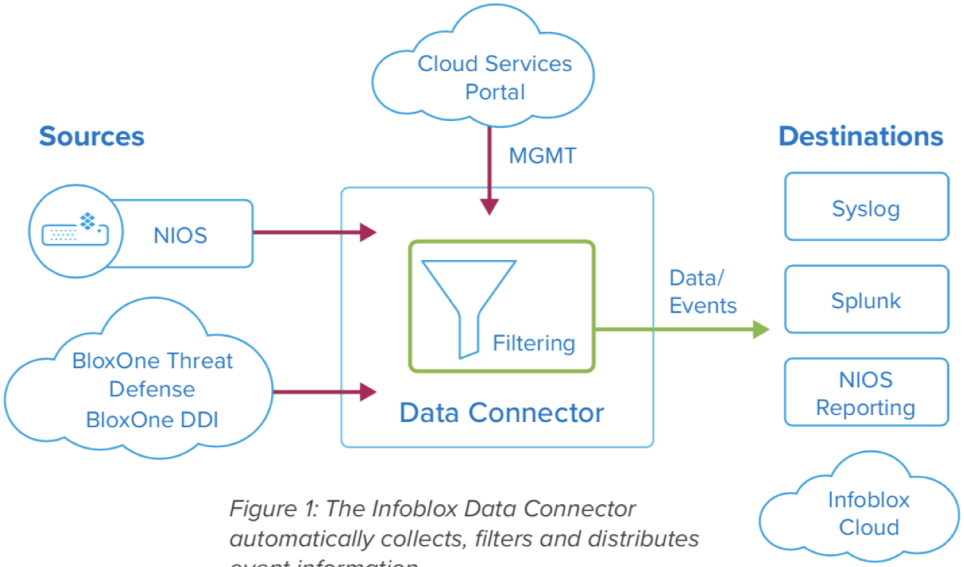


Figure 1: The Infoblox Data Connector automatically collects, filters and distributes event information

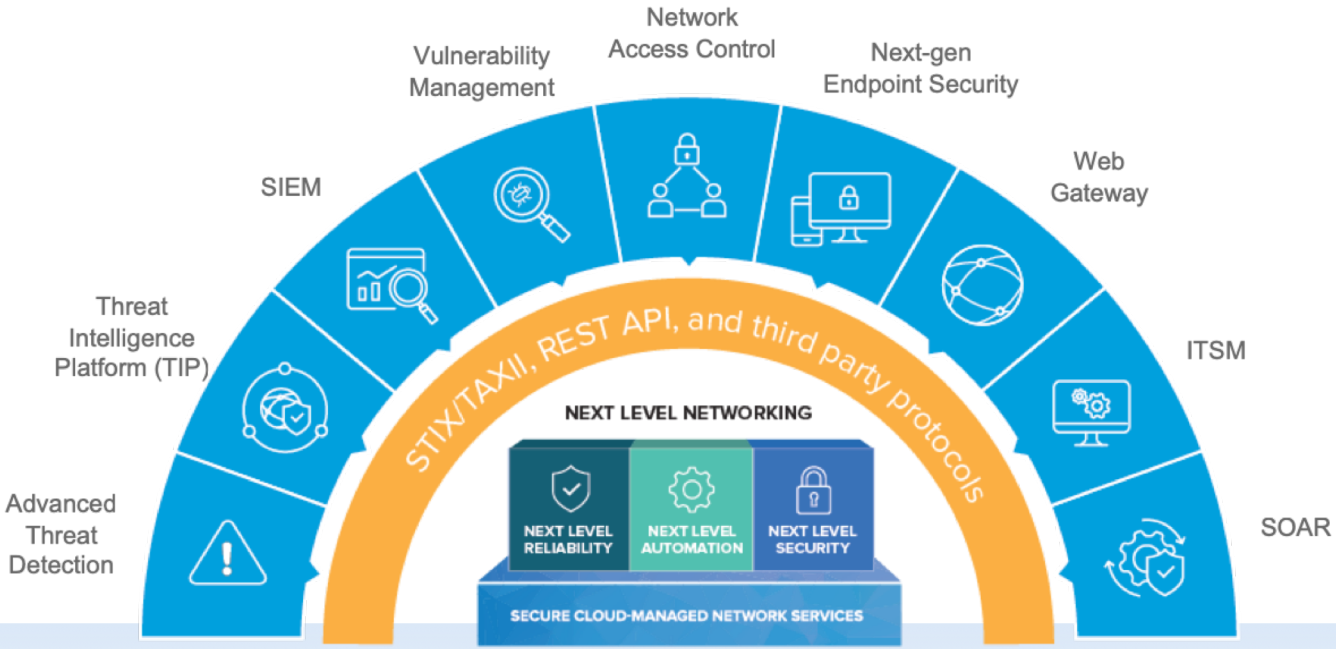
SOC teams can easily connect the dots when investigating incidents, while keeping costs low

Bridging Silos with Security Orchestration

Network and threat context data to entire ecosystem

Automate network wide remediation

Improve ROI of security stack



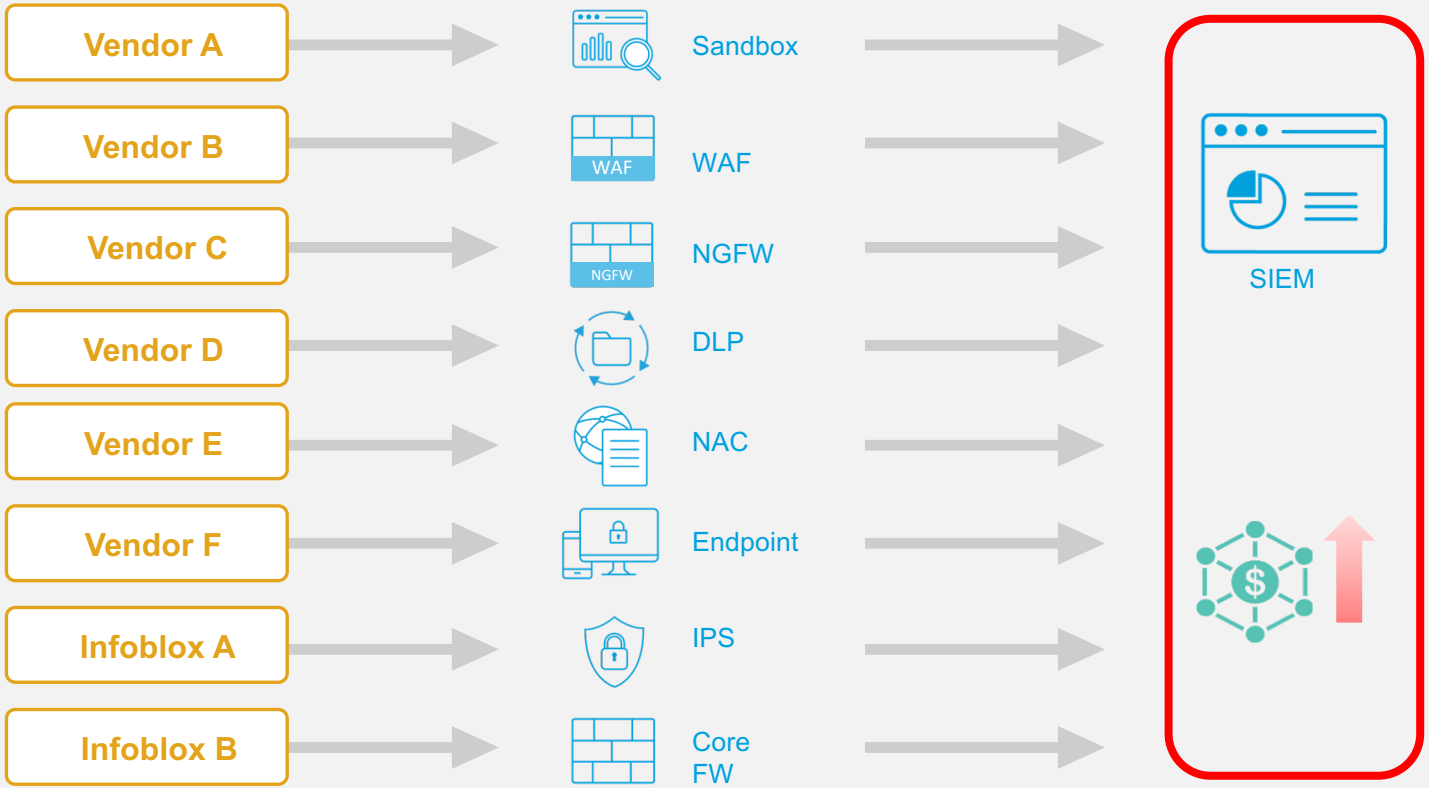
 |

SOC Inefficiencies

Siloed threat intelligence and security architecture

Each tool pushes events into SIEM based on separate uncorrelated vendor feeds

Inefficient use of SIEM



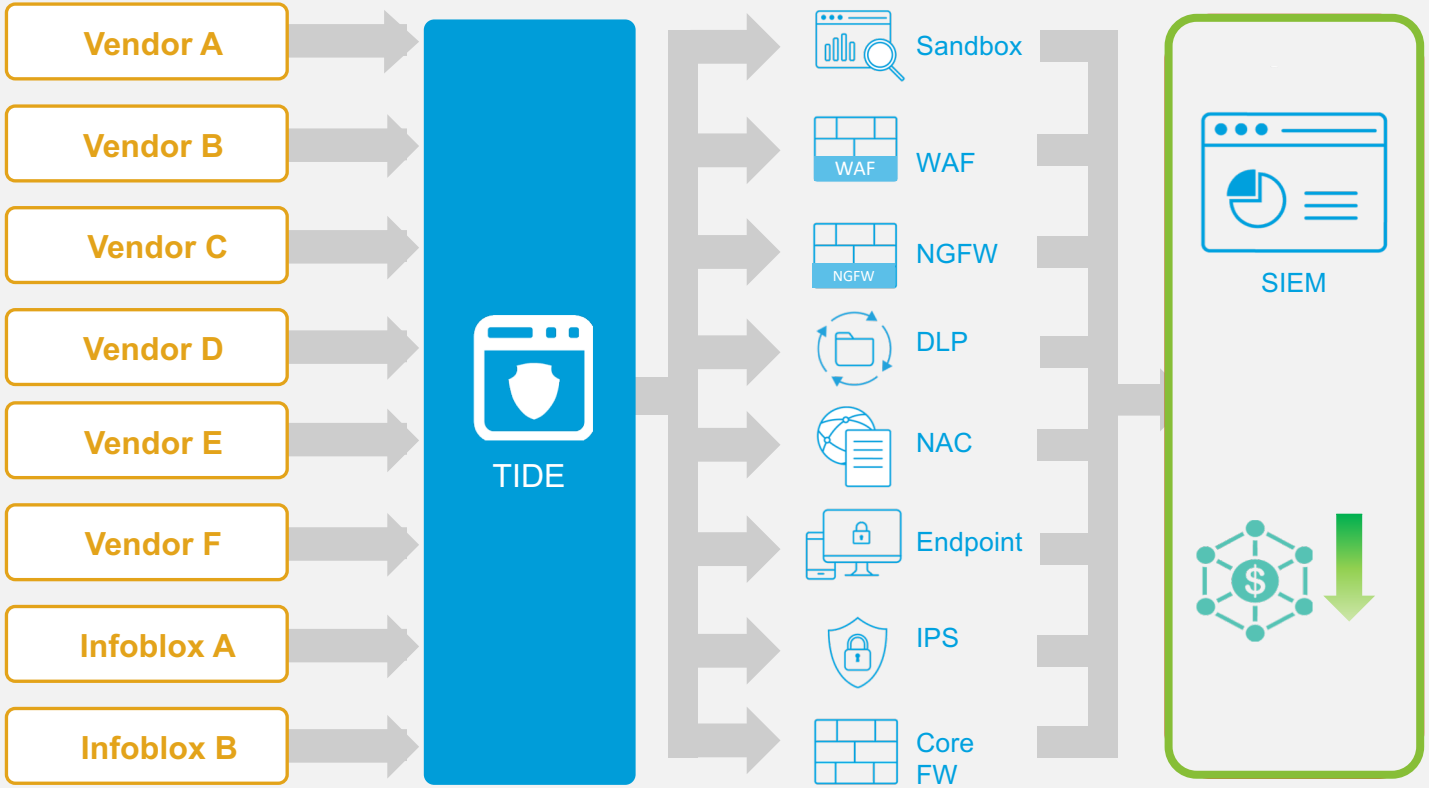
 |

SIEM Optimization and SOC Efficiency Using TIDE*

Disparate threat intelligence is consolidated & curated into one platform, and normalized

Data simplified into a single, optimized "super feed"

Fewer conflicting events into SIEM



TIDE – Threat Intelligence Data Exchange

 |

Dossier for Faster Threat Investigation

Search Dossier | Resources | Export JSON

badwerkad.top

Reported by Infoblox, and ThreatTrackSecurity
First Reported on 4/20/2017 by Infoblox
Last Reported on 4/23/2018 by ThreatTrackSecurity

This Record Contains:

DNS Count:	3
Domain/Subdomain Count:	2
URL Count:	3
IP Count:	3
Positive File Detections:	8
Contacts:	3

This Record Also Contains:
Indicator Info, Timeline, Domain Info, and Reports

CATEGORIZATIONS

Infoblox	MalwareDownload_Cerber
ThreatTrackSecurity	MalwareDownload_Generic
Forcepoint ThreatSeeker	compromised websites
Dr.Web	known infection source
Websense Threatseeker	compromised websites,known infection ...

WHOIS DOMAINTOOLS

Created:	4/16/2017
Updated:	4/17/2018
Expires:	4/16/2019
Registrant Name:	asd
Email:	asda@gmail.com

- Adds more context for correlation
  - Multiple data sources in a single view
- Accelerates threat investigation (making linkages) and helps prioritize events (based on threat class or the scope of attack)

 |

Security Landscape

Infrastructure Security

Network Firewall

Network Monitoring

Intrusion Prevention Systems

Unified Threat Management

Endpoint Security

Endpoint Protection & Anti-Virus

Endpoint Detection & Response

Application Security

WAF & Application Security

Vulnerability Assessment

Messaging Security

Web Security

IoT Security

Security Operations & Incident Response

SIEM

Security Incident Response

Threat Intelligence

Mobile Security

Data Security

Transaction Security

Risk & Compliance

Specialized Threat Analysis & Protection

Identity & Access Management

Cloud Security

Source: Momentum Partners.

For the second year, Lucky Strike B·A·R Honda brings you its 005 Formula One car stripped bare. From recognisable components such as the front and rear wings and the wheels right down to the electrical assembly systems and engine management controls, B·A·R presents you with the picture you want to see. For more information on the B·A·R Honda 005 visit:

BARf1.com

key components

1 Front wing/nose assembly
2 Monocoque
3 Mirror assembly
4 Honda V10 engine
5 Exhaust system
6 Hydraulic plate assembly
7 Clutch actuator assembly
8 Gearbox assembly
9 Rear impact structure
10 Rear wing assembly
11 Fuel tank
12 Headrest
13 Steering wheel
14 Radiator duct assembly
15 Engine coverside pods
16 Drivers seat
17 Bargeboard
18 Lower front wishbone
19 Top front wishbone
20 Front brake ducts
21 Steering rack assembly
22 Front suspension damper
23 Front pushrod
24 Lower rear wishbone
25 Top rear wishbone
26 Rear pushrod
27 Rear toeirod
28 Driveshaft
29 Brake disc assembly
30 Brake calliper
31 BBS wheels with Bridgestone tyres
32 Water radiator
33 Oil tank assembly
34 Main electrical harness
35 Airbox and air filter
36 Left-hand electrical assembly
37 Fire extinguisher
38 Oil cooler
39 Plank
40 Main floor assembly with diffuser
41 Splitter assembly
42 Engine management controller
43 Battery
44 Steering column
45 Throttle and brake pedal assembly
46 Rear brake ducts
47 Wheel nut
48 Damper cover
49 Engine heatshields
50 Seat belt
51 Camera
52 Airspring
53 Front anti roll bar

Components of Mature Cyber Security Program

Actionable Network Intelligence (IT)

+

Actionable Threat Intelligence (Security)

+

Informed Ecosystem

=

Holistic and Mature Cyber Security Program

"WE'VE NARROWED OUR SECURITY RISKS DOWN to THESE TWO GROUPS."

photo: HondaRacingF1.com

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:

- Infoblox reduced time it took to investigate incidents / eliminated wasted time
- Improved operational efficiency

 |

Summary

- DDI can provide ubiquitous visibility across your entire network
- DDI data can help accelerate incident response
- Threat intelligence optimization can help make your SOC more efficient

 |

Infoblox
NEXT LEVEL NETWORKING

Q & A

Infoblox
NEXT LEVEL NETWORKING

Demo: Aproveche la Infraestructura de Seguridad Existente para Automatizar y Mejorar la Detección de Amenazas y Acelerar la Remediación

Francisco Osornio, Senior Systems Engineer
Infoblox

Infoblox
NEXT LEVEL NETWORKING

Q & A

Customer Panel

Heber Camarillo
Banregio
Chief Cybersecurity Architect

Victor Mejia
Bestel
Director of Sales & Security Operations

Hugo Suarez
Grupo Salinas
Manager DNS Services

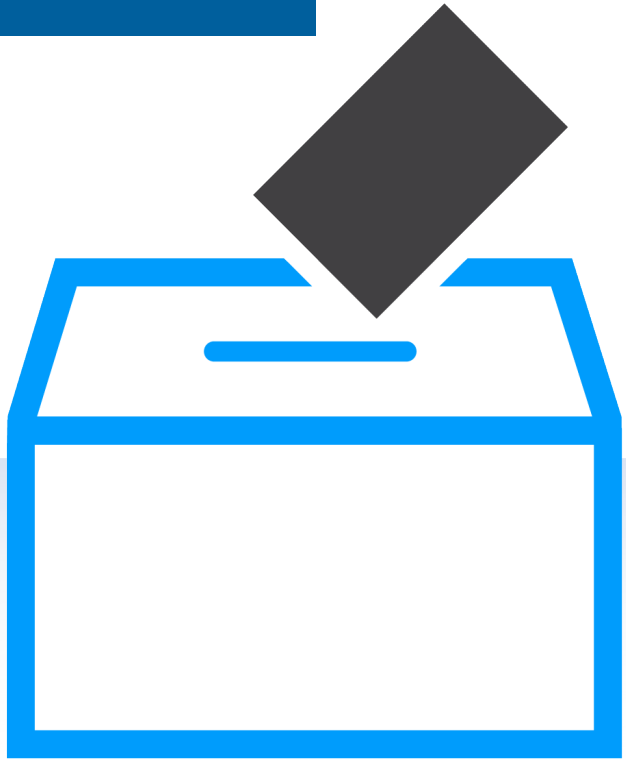
Jorge Lozoya Arandia
Services Operations Coordinator
University of Guadalajara

 |

Infoblox
NEXT LEVEL NETWORKING

CLAUSURA Y CONCLUSIONES

Infoblox Exchange
SECURITY ROADSHOW



Por favor complete su formulario de comentarios para tener la oportunidad de ganar un casco de realidad virtual Oculus Go

Infoblox
NEXT LEVEL NETWORKING

Infoblox Exchange
SECURITY ROADSHOW

23 ROAD SHOW LOCATIONS

North America | Europe | Middle East/Africa | Asia-Pacific

Infoblox
NEXT LEVEL NETWORKING

Infoblox
NEXT LEVEL NETWORKING

MUCHAS GRACIAS!