Infoblox®
NEXT LEVEL NETWORKING

Boost the Efficiency of Your Security Operations

Agenda

Operational challenges

Accelerating Incident Response

Improving SOC Efficiency

Operational Challenges

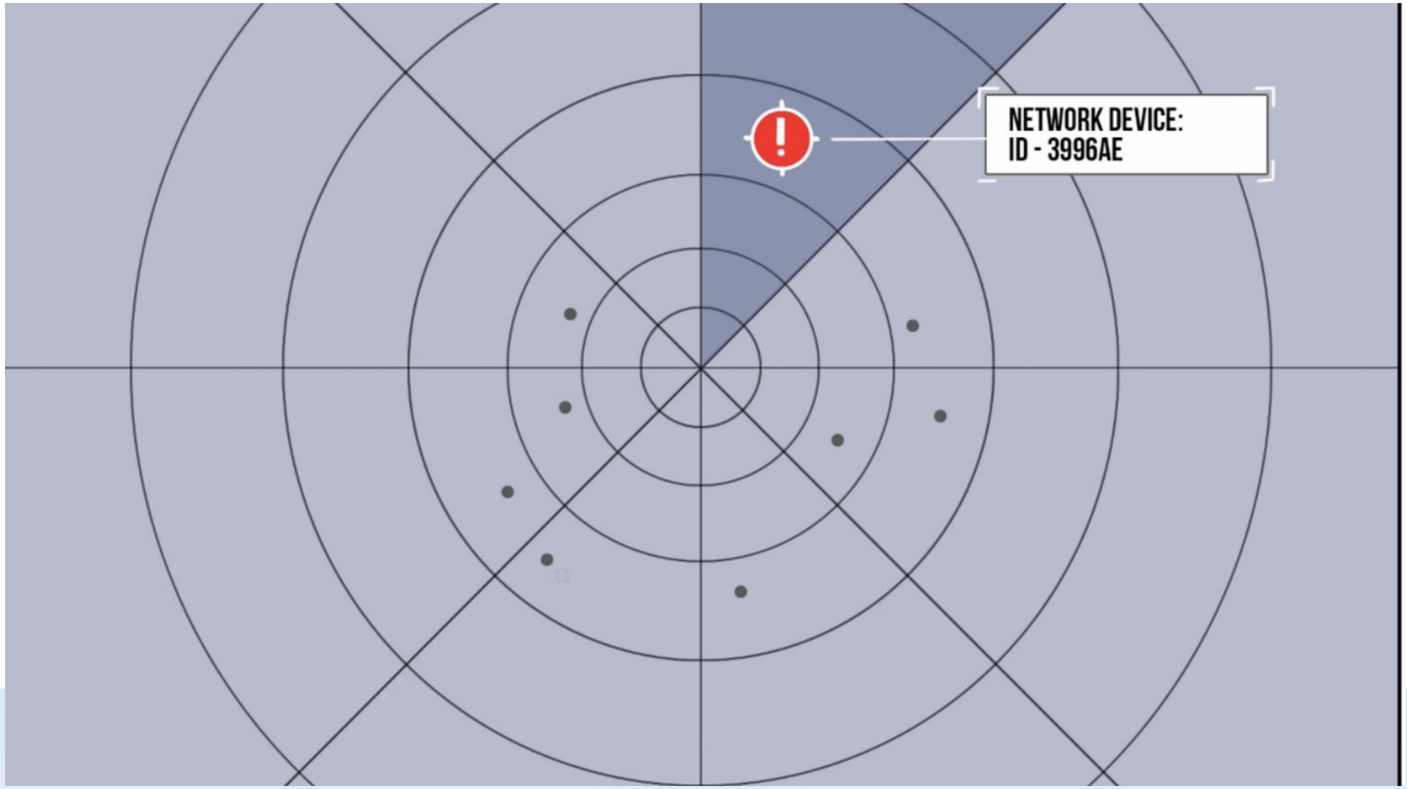
Siloed security tools

Too many alerts/ too much noise

Cyber security skills shortage

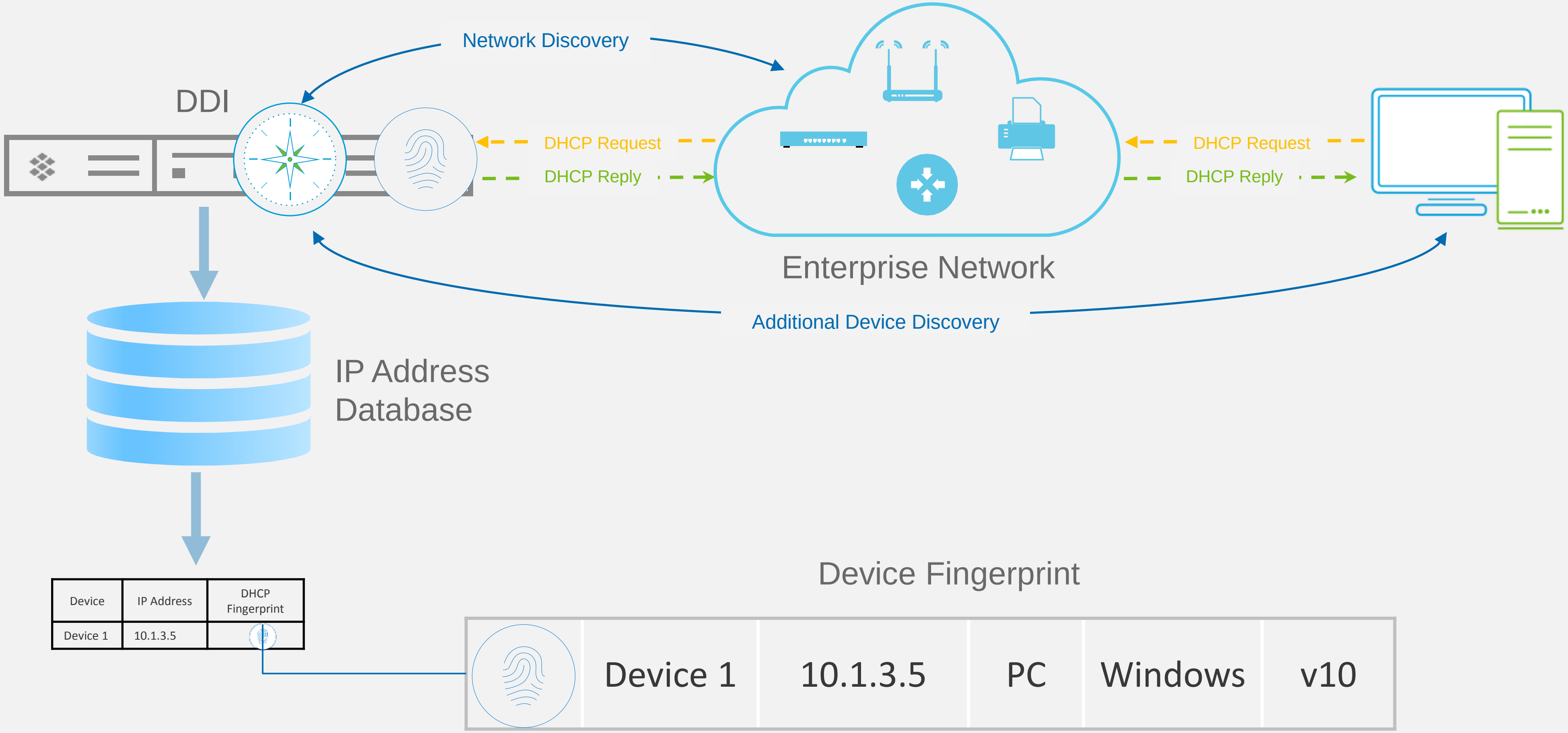
Manual investigation processes

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



Network Discovery

DDI

DHCP Request

DHCP Reply

Enterprise Network

DHCP Request

DHCP Reply

Additional Device Discovery

IP Address Database

Device	IP Address	DHCP Fingerprint
Device 1	10.1.3.5	

Device Fingerprint

	Device 1	10.1.3.5	PC	Windows	v10

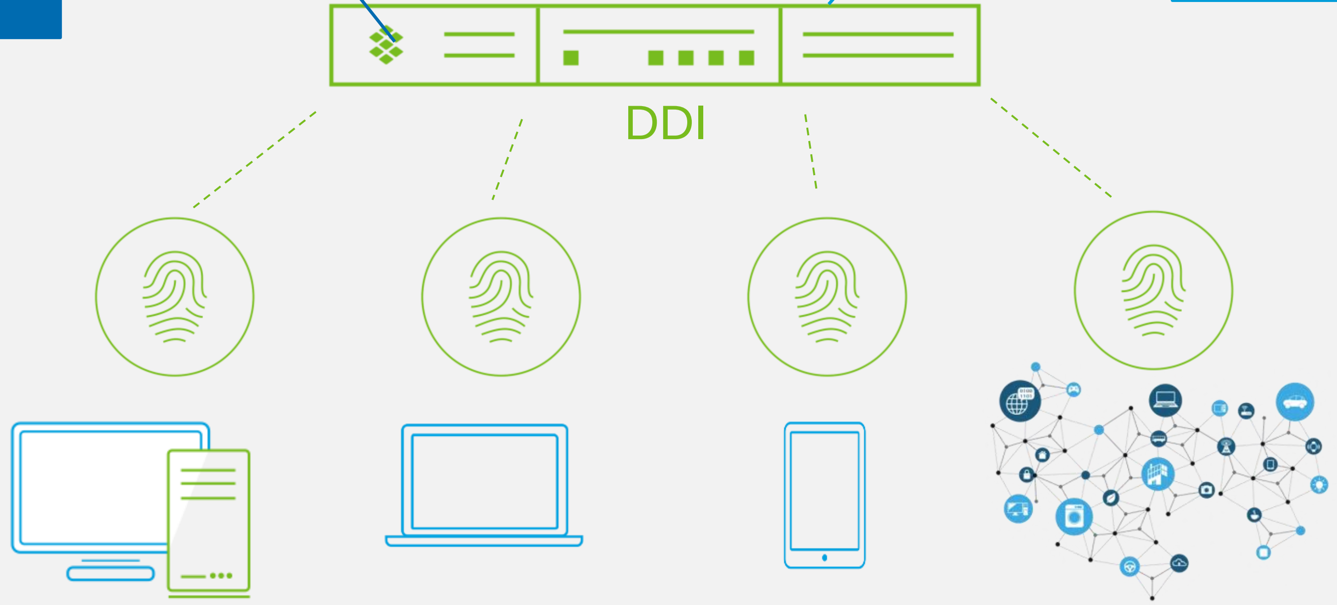
DDI Meta-data for Entire Infrastructure

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



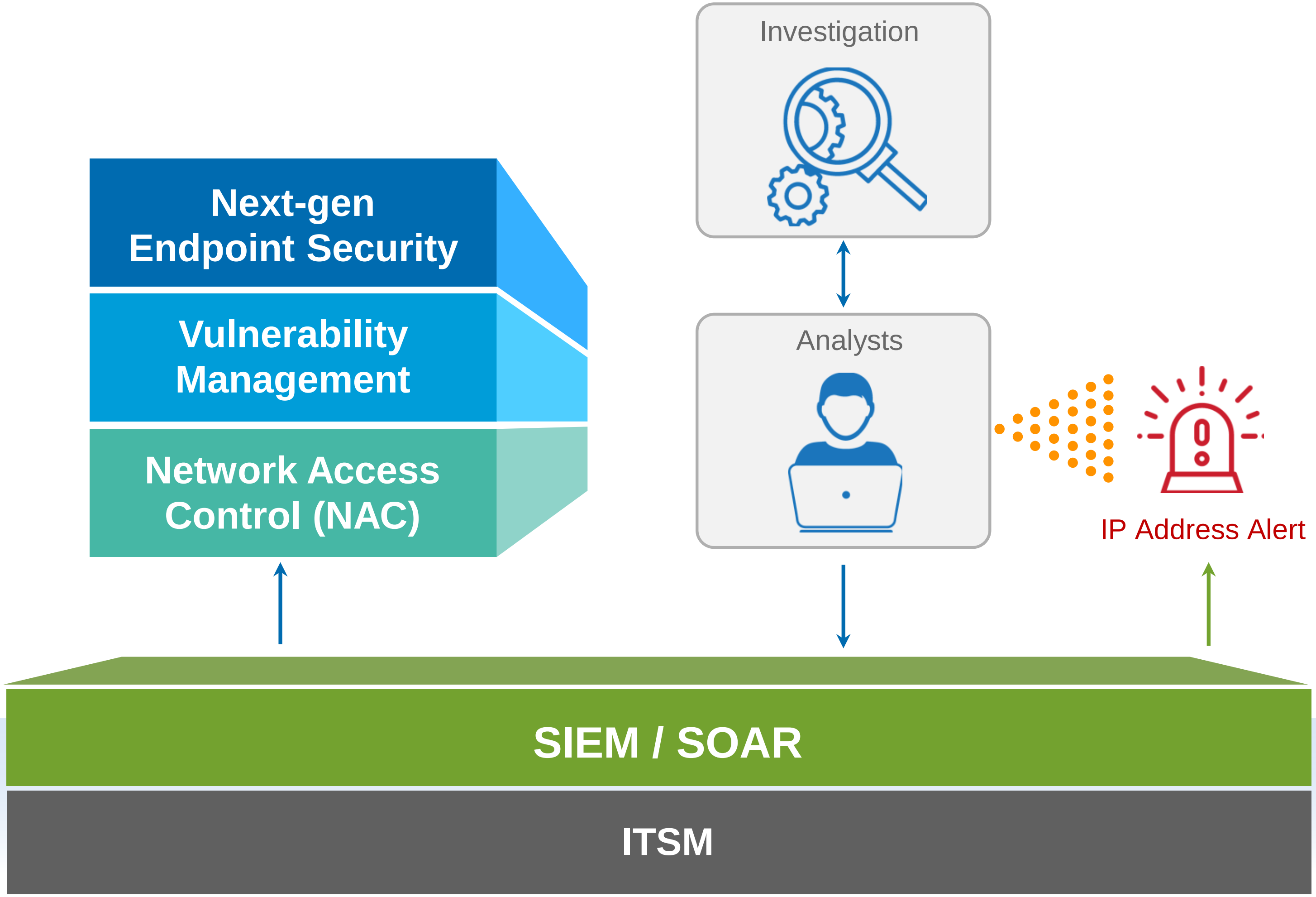
Agenda

Operational challenges

Accelerating Incident Response

Improving SOC Efficiency

Typical Incident Response

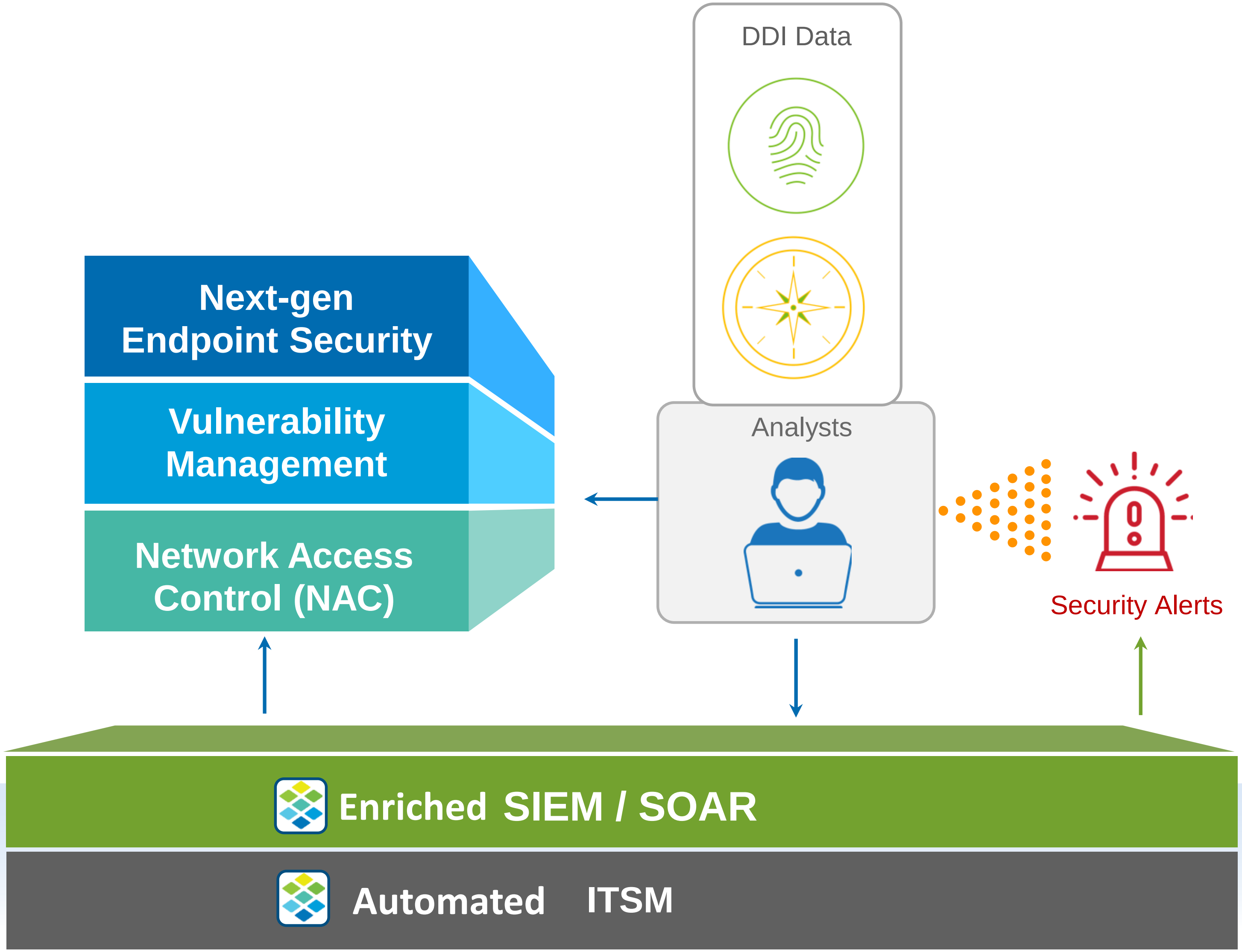


Lengthy
Response Times

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

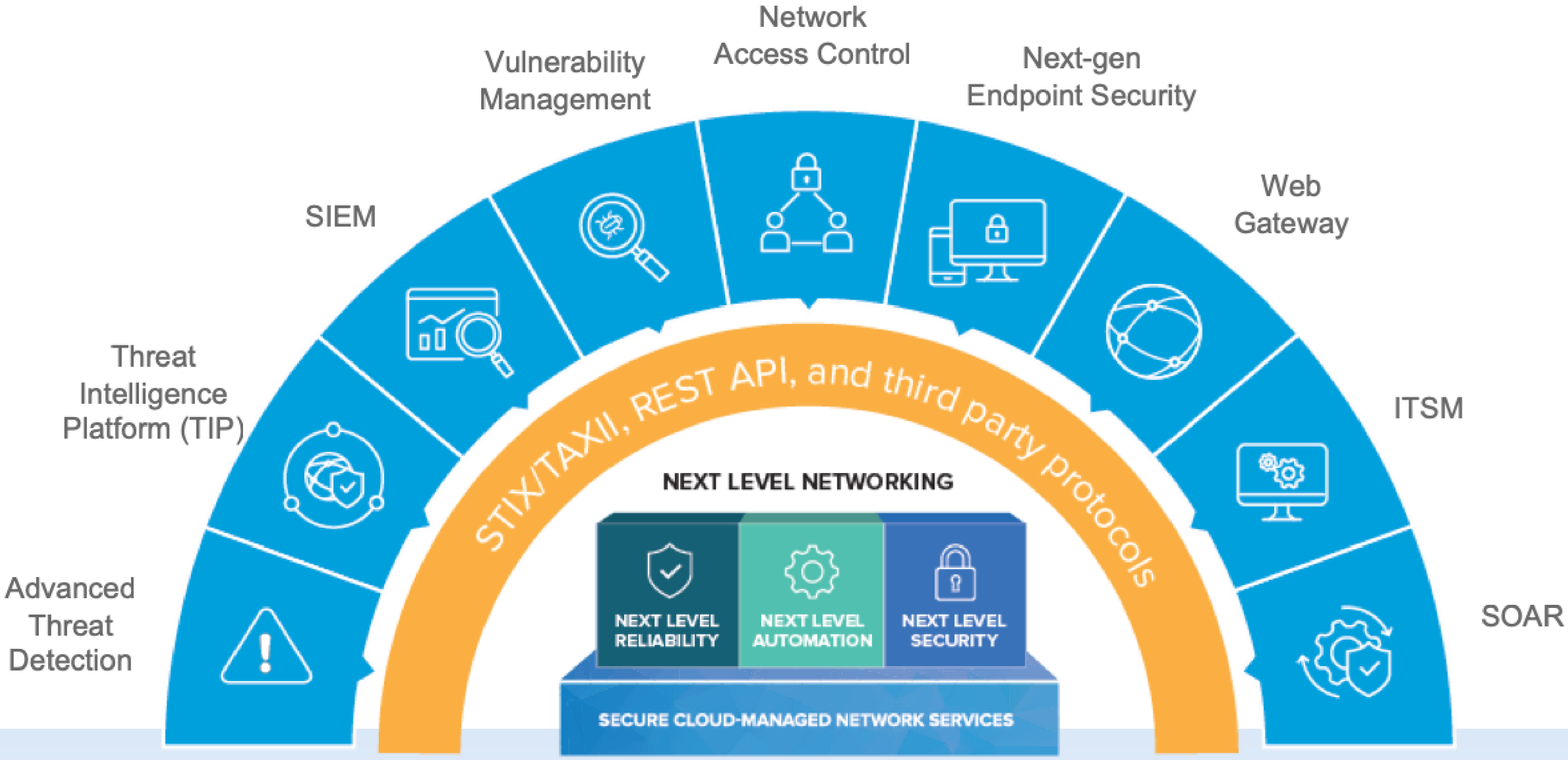
- “Metadata” via Extended Attributes: Owner, app, security level, location, ticket number
- Context for accurate risk assessment and event prioritization

Bridging Silos with Security Orchestration

Network and threat context data to entire ecosystem

Automate network wide remediation

Improve ROI of security stack



Network Access Control
Vulnerability Management
Next-gen Endpoint Security
SIEM
Web Gateway
Threat Intelligence Platform (TIP)
ITSM
Advanced Threat Detection
SOAR
STIX/TAXII, REST API, and third party protocols
NEXT LEVEL NETWORKING
NEXT LEVEL RELIABILITY
NEXT LEVEL AUTOMATION
NEXT LEVEL SECURITY
SECURE CLOUD-MANAGED NETWORK SERVICES

Agenda

Operational challenges

Accelerating Incident Response

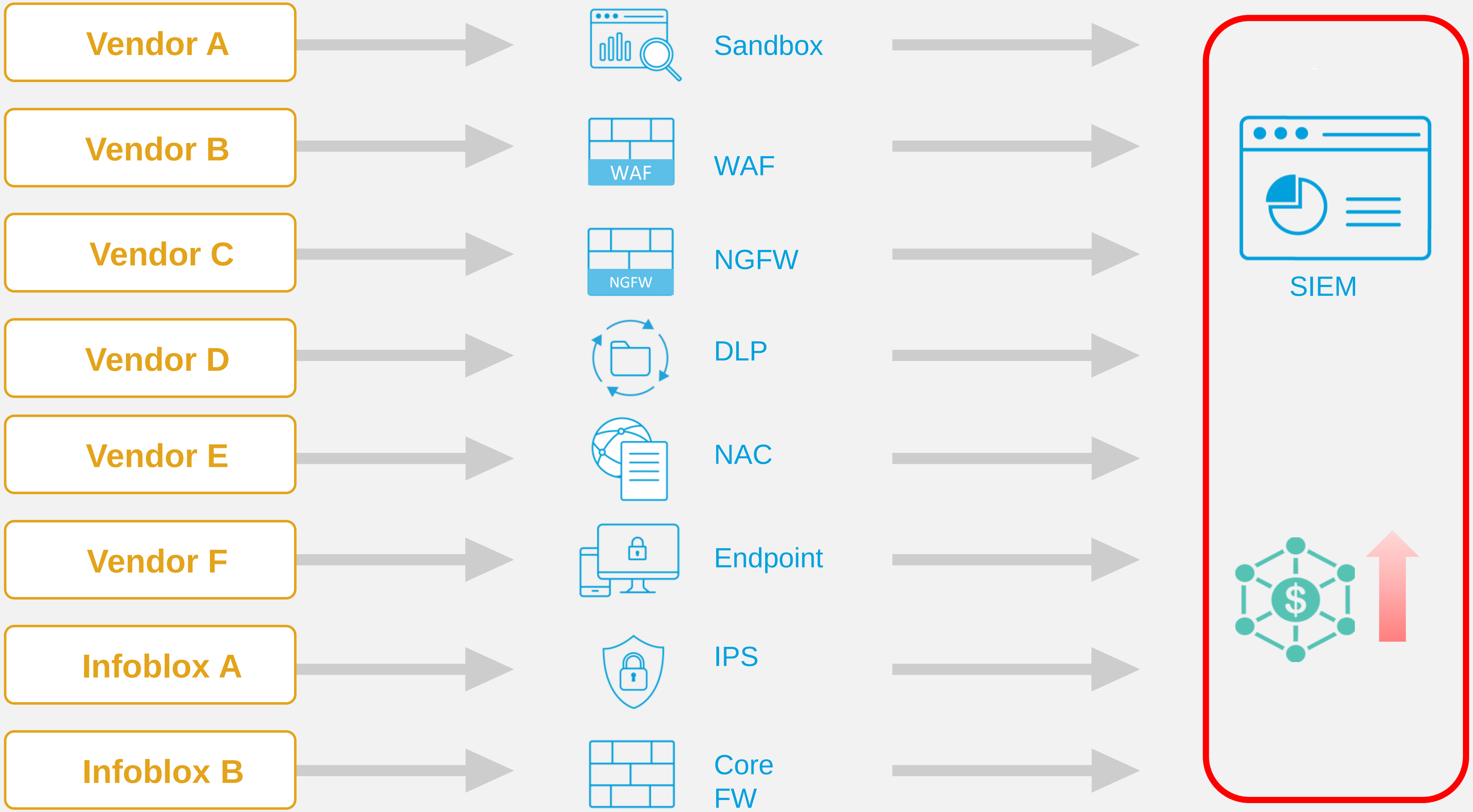
Improving SOC Efficiency

SOC Inefficiencies

Siloed threat intelligence and security architecture

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

Inefficient use of SIEM

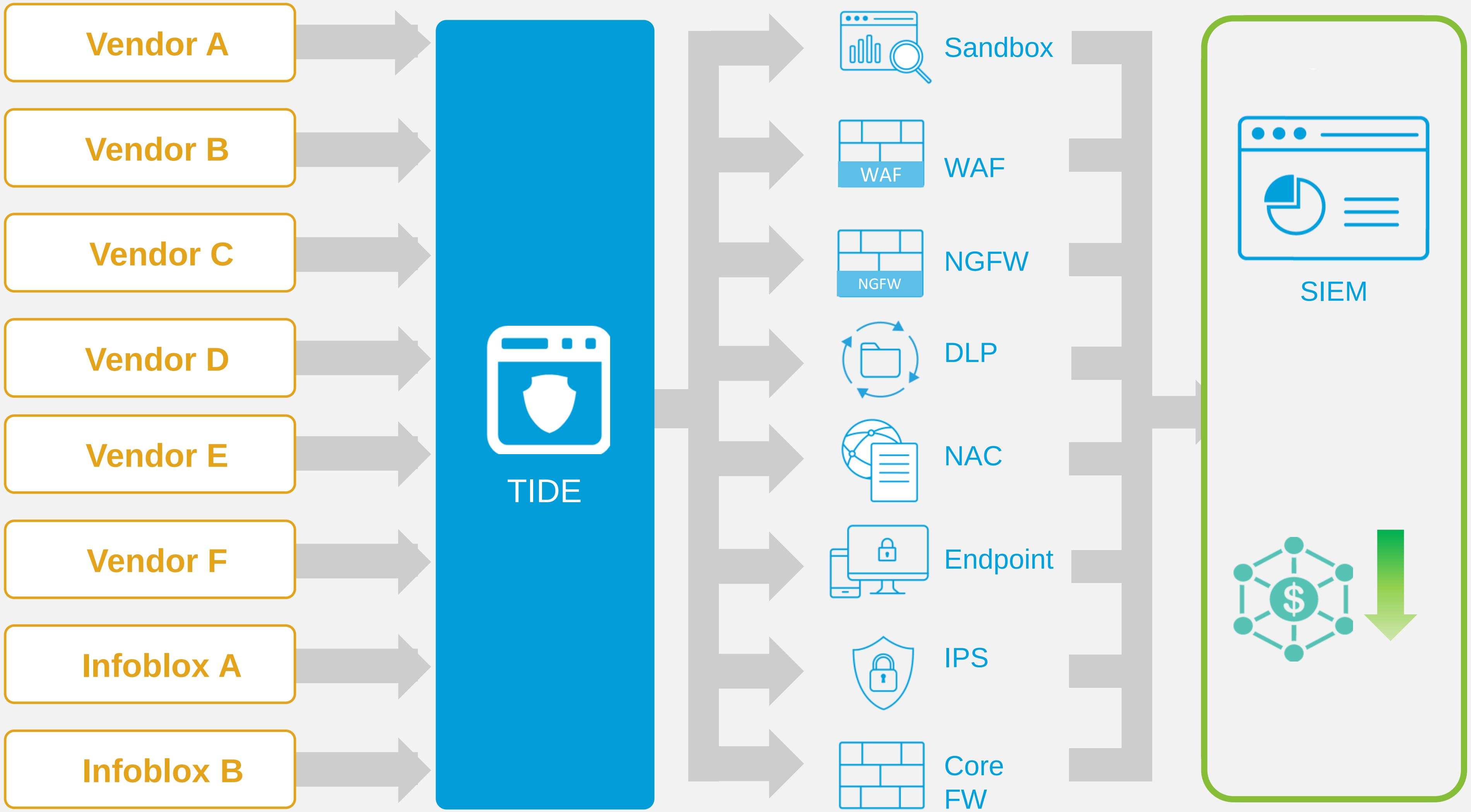


SIEM Optimization and SOC Efficiency Using TIDE*

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

Data simplified into a single, optimized feed

Fewer conflicting events into SIEM



Vendor A

Vendor B

Vendor C

Vendor D

Vendor E

Vendor F

Infoblox A

Infoblox B

TIDE

Sandbox

WAF

NGFW

DLP

NAC

Endpoint

IPS

Core FW

SIEM

TIDE – Threat Intelligence Data Exchange

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

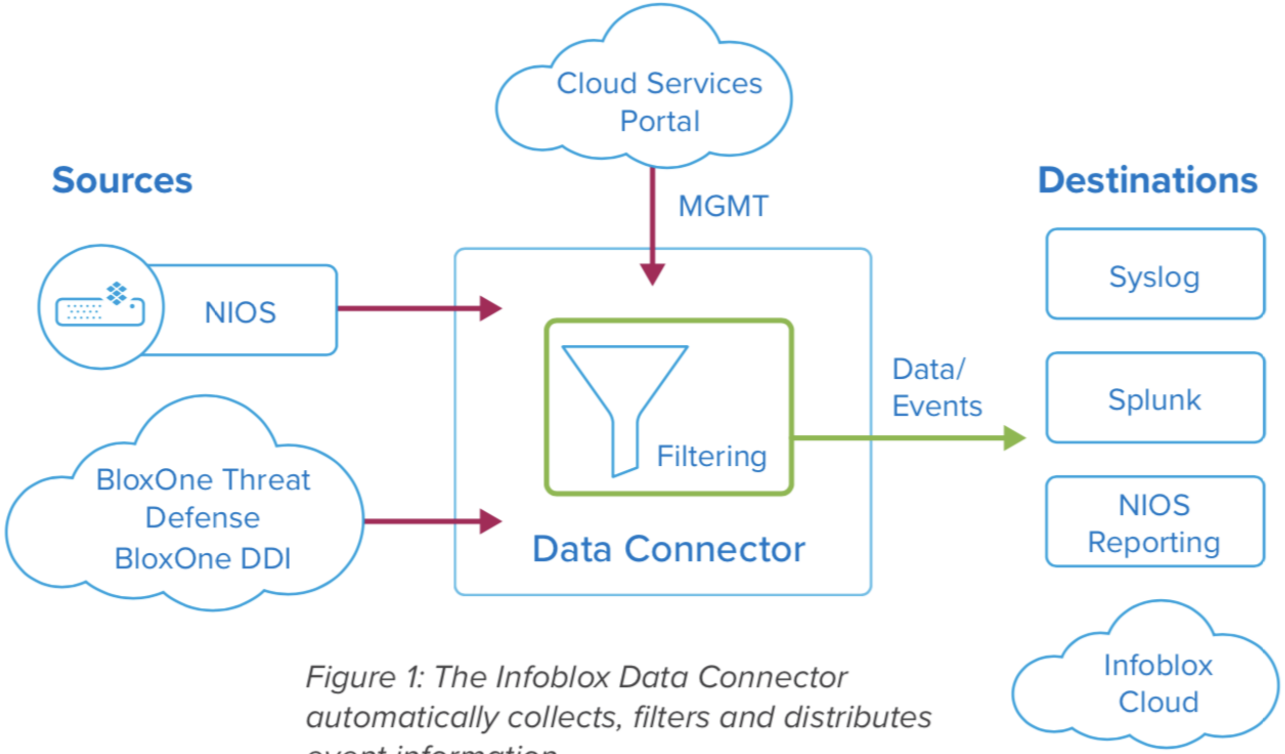
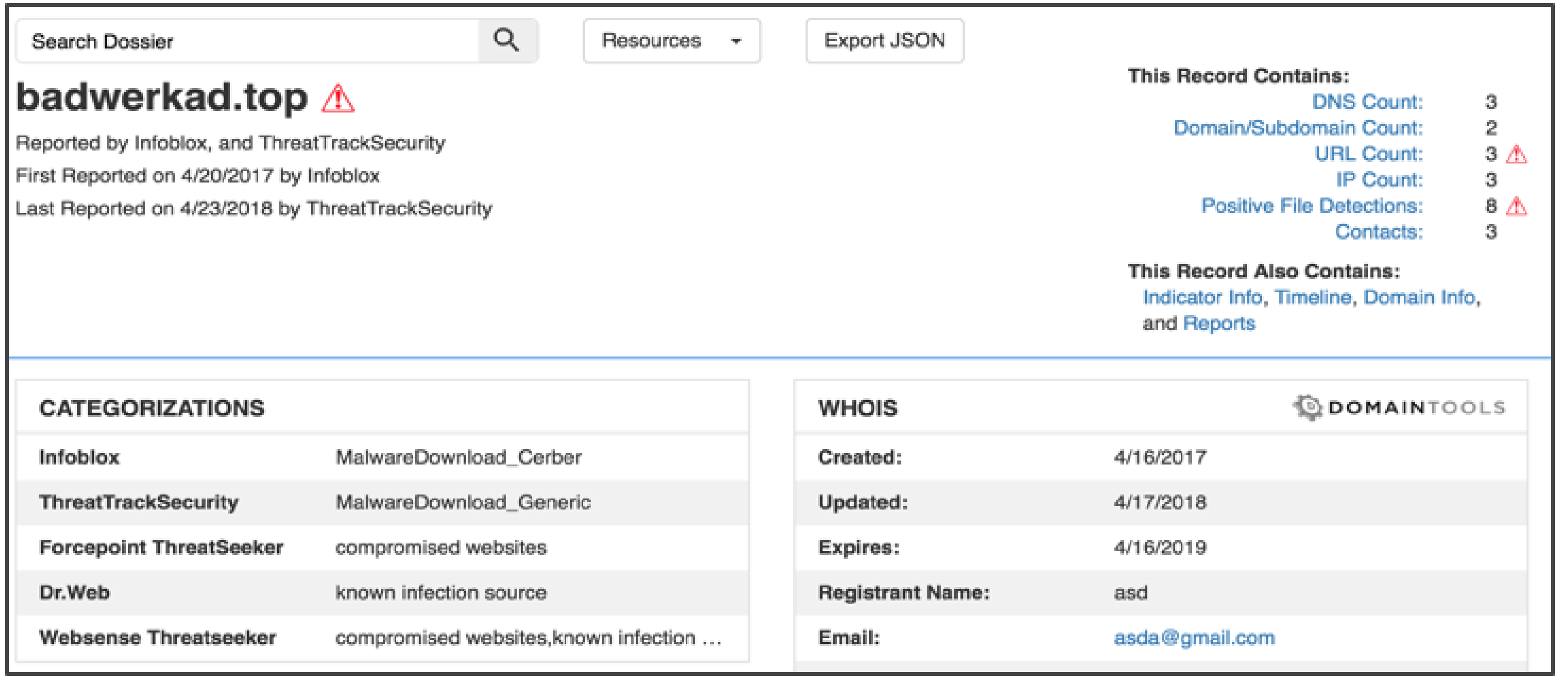


Figure 1: The Infoblox Data Connector automatically collects, filters and distributes event information

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

Dossier for Faster Threat Investigation



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	
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)

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

Boost Efficiency of Security Operations

- 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