Infoblox
NEXT LEVEL NETWORKING

Enabling SOAR and Automated Incident Response Using Comprehensive Ecosystem Integrations

Victor Danevich, CTO, System Engineering

Cybercrime Growing in Complexity and Scale

- $2.7 billion monetary losses in 2018 per FBI[1]
- Breach victims often hire expensive forensic firms, law firms

- Notable public breaches have resulted in millions of records stolen
- Breach victim's future business jeopardized

1. FBI Internet Crime Report 2018

But Security Teams Cannot Respond to Incidents Fast Enough

- 196 days on average between infection and detection
- Not all organizations have necessary tools/automation to correlate data from multiple systems

Customer A

Had a lot of data to analyze and decided to outsource SOC operations because they couldn't analyze it themselves

Customer B

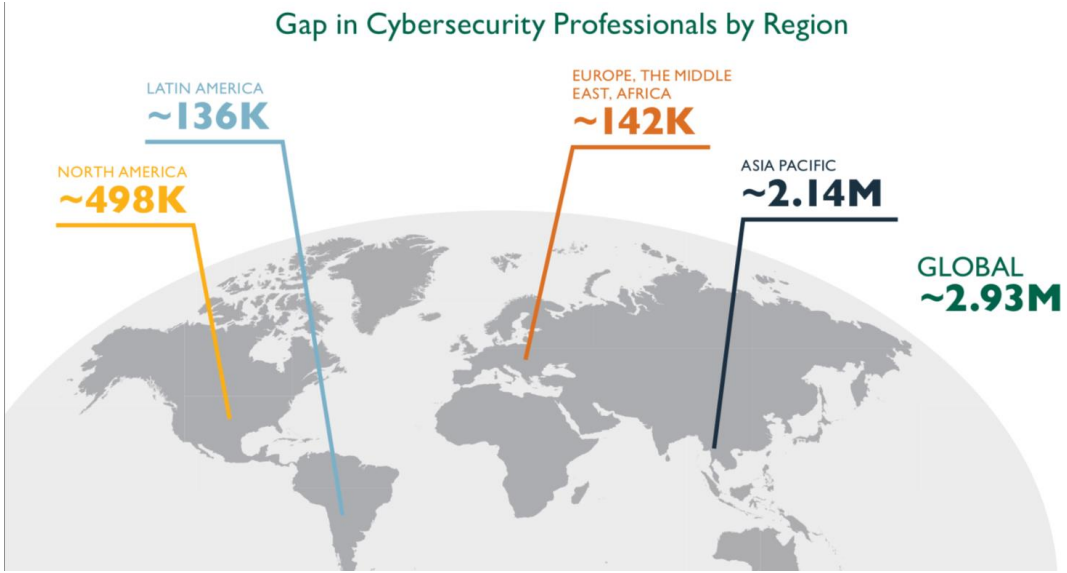
Didn't know all the places in the network where they were using threat intel and failed to operationalize on it

And Throwing More People at the Problem is Not Possible

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

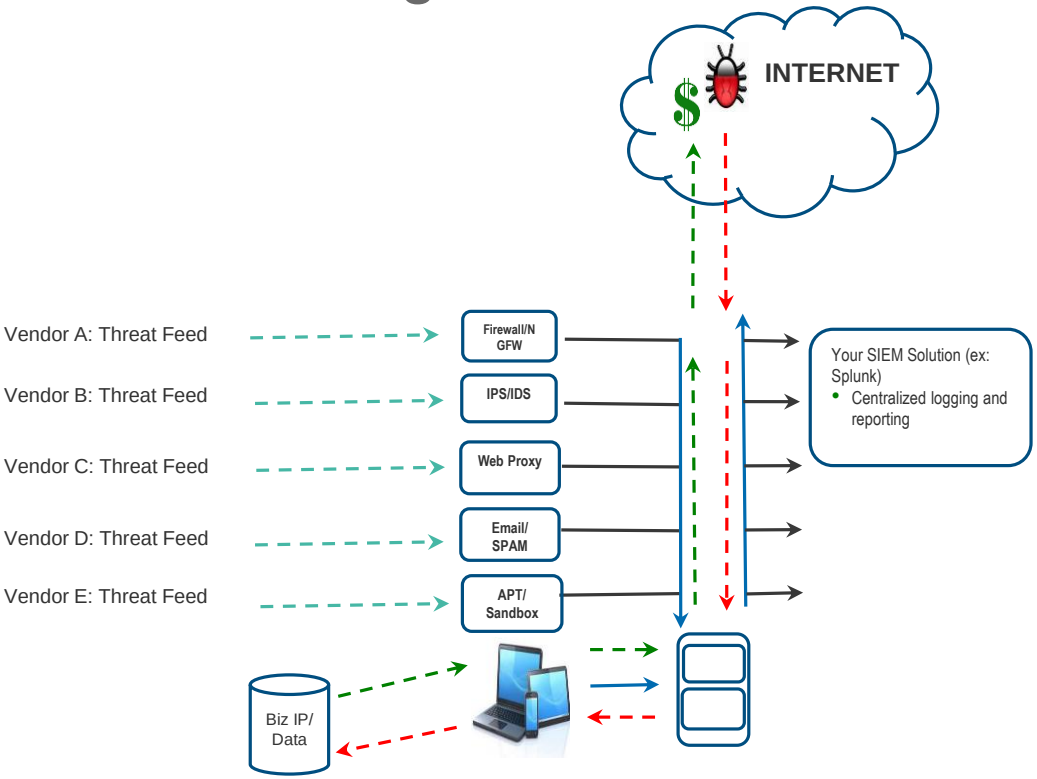
4% of alerts, only, are investigated; not enough humans to keep organizations safe

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



ISC2 Cybersecurity Workforce Study, 2018

Bolted on Security Architecture Leads to Siloed and Ineffective Threat Intelligence

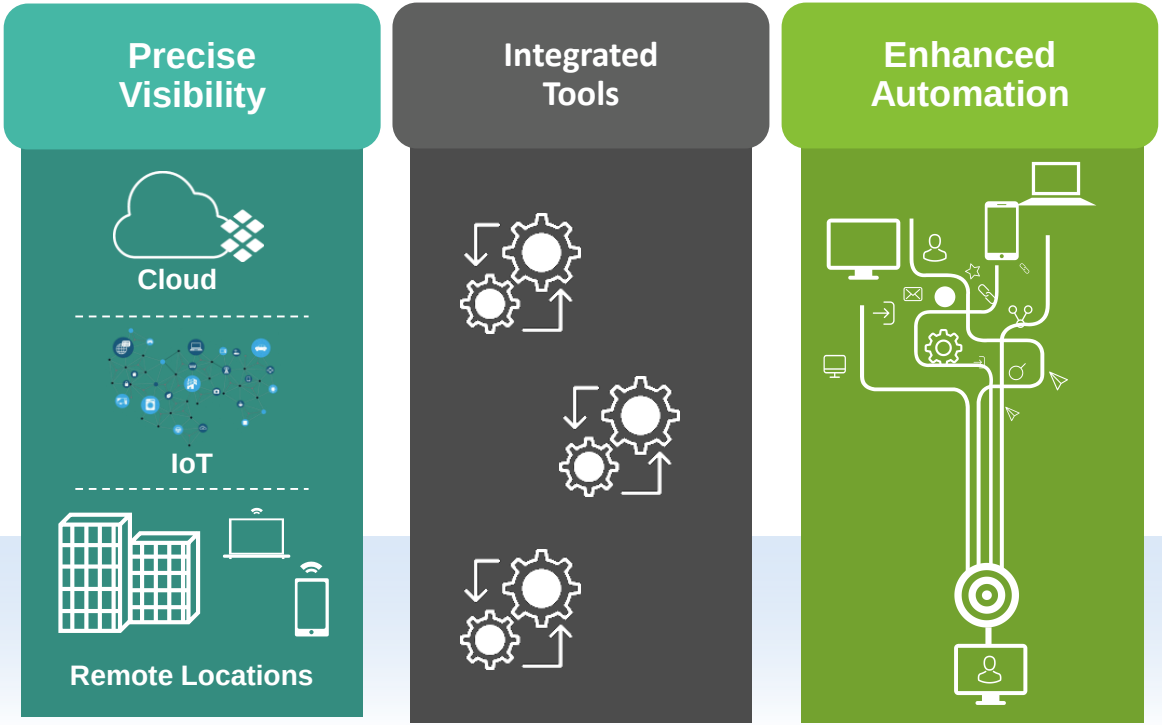


 |

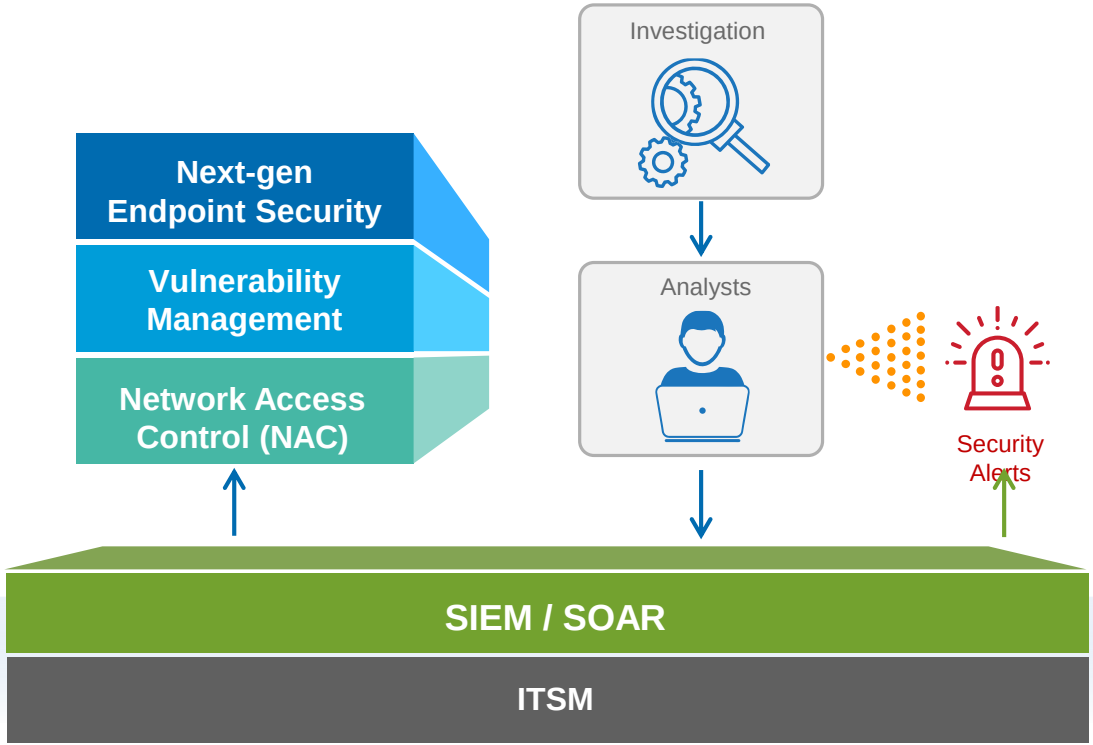
The Bottomline

- Threats growing exponentially
- Impossible to match skills of a well trained, distributed, global malware developer
- Malware operators work round the clock and are relentless
- Encryption makes it difficult to separate malicious from normal traffic
- Simple manual review of logs not enough to recognize patterns over time

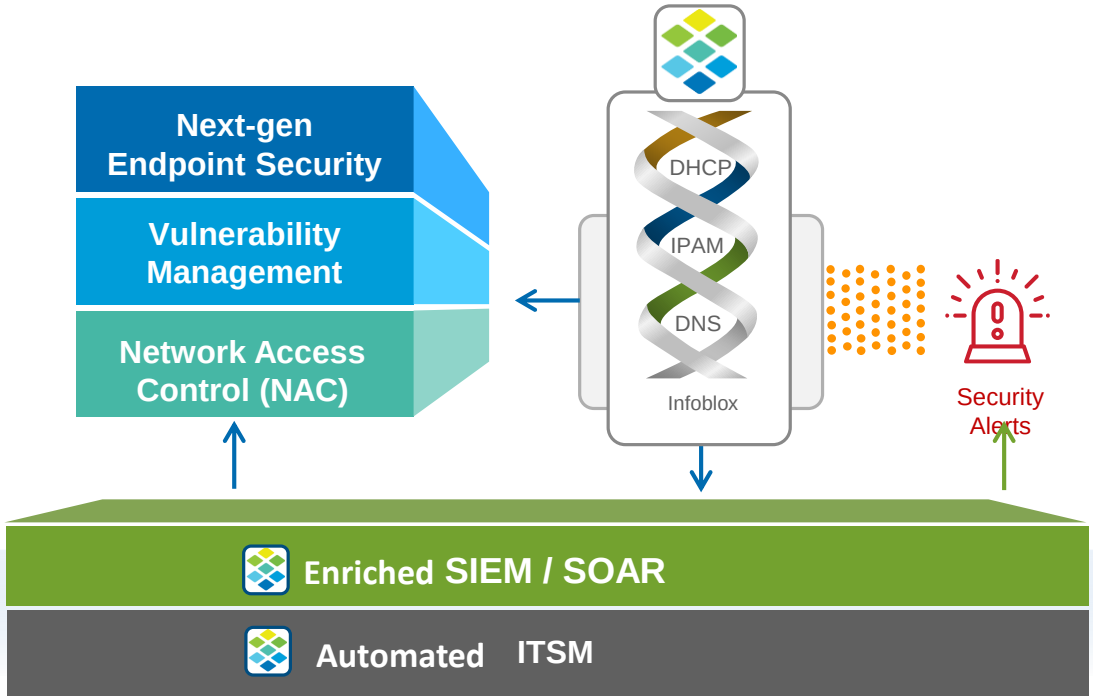
Key Tenets of Efficient Security Operations



Improve Productivity and Enhance Automation



Improve Productivity and Enhance Automation



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

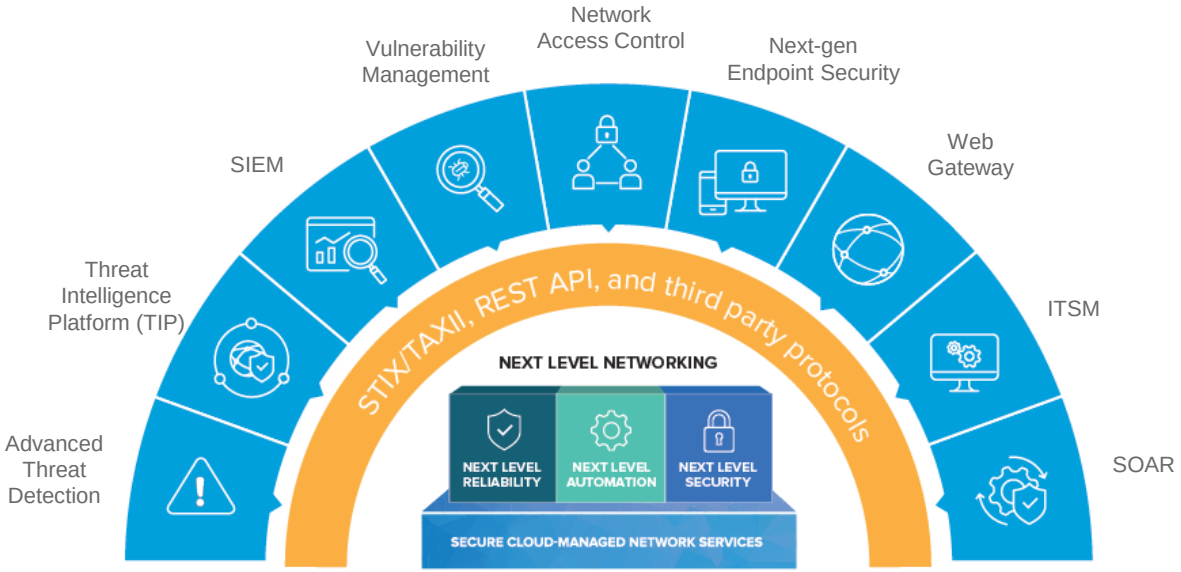
IPAM

Application and Business Context

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

Combined DDI, Threat Intel and Context to Power SOAR Platforms

Enriched data and integrations that can be relied upon to build automation



Prioritize 100s of alerts | Automate incident response | Reduce cost of human touch/error

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

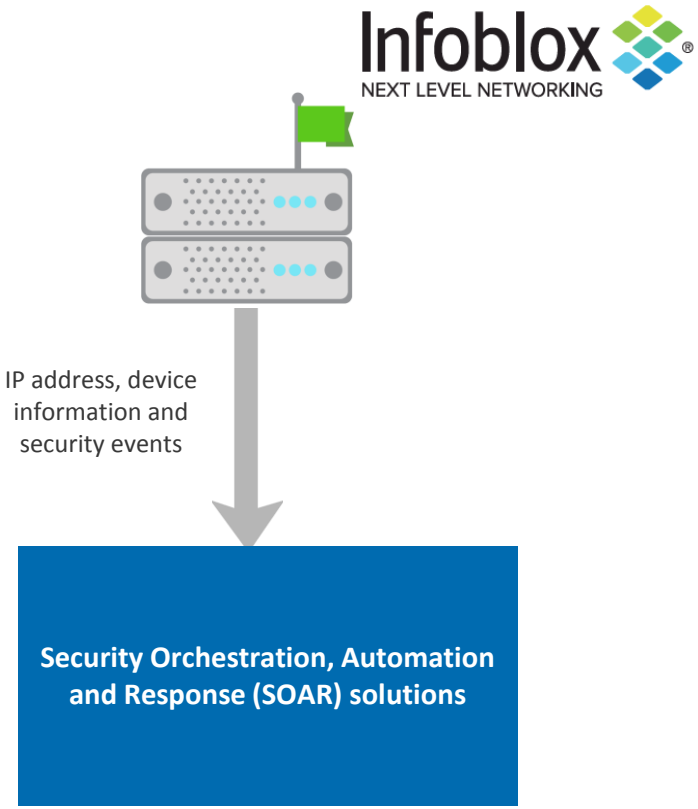
IPAM

Application and Business Context

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

 |

SOAR Integration



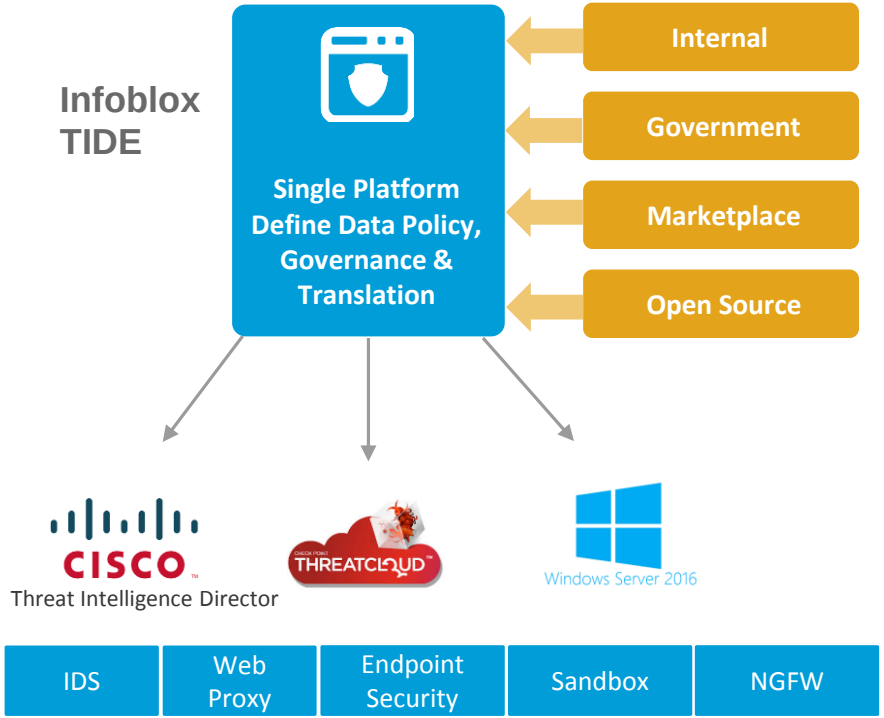
- SOAR solution receives information on IP address, network devices and malicious events from Infoblox
- SOAR uses that information to block/unblock/check domain, check information about IP/host/network/domain
- IPAM information enrichment from events/tools

Benefits:

- Integrate disparate security tools and provide vendor-neutral threat intelligence for all devices
- Faster response with full set of threat intelligence APIs
- Enhance and improve incident response with better threat intelligence
- Improve security processes by integrating with other systems via SOAR

Security Policy Unification

- 3rd party platform receives malicious host names, IP addresses and URLs from TIDE
- 3rd party platform can now block/ monitor more threats
- Improves effectiveness and delivers better ROI for your security stack



 |

Customer Story: Major Insurance Company

Customer Use Case:

- Customer says: “I’m not interested in your DNS firewall. I have a Palo Alto Network Firewall, it can do all the things Infoblox can.”
- But they did have security operations challenges
  - Inefficient and ineffective vulnerability scanning for compliance; hours of wasted time and resources
  - Sandbox solution does not scale for mitigation; expensive and can’t block in remote offices
  - Query logging (for feeding into their SIEM) on Microsoft DNS can’t be enabled

Solution: ActiveTrust with cybersecurity ecosystem

Outcomes:

- Infoblox tells vulnerability scanner when a new device is on the network, making it more effective
- Enable sandbox to add domains to RPZ – block across entire DNS infrastructure
- Enables DNS Query data to be sent to their SIEM

Customer Story: EMEA Bank

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