

Brought to you by



# Cybersecurity Automation

for  
**dummies**<sup>®</sup>  
A Wiley Brand

Infoblox Special Edition



Automate security  
responses

—  
Optimize your  
security ecosystem

—  
Eliminate  
tool siloes

Robert Nagy

Todd Christensen

Geoff Horne

# About Infoblox

Network landscapes are rapidly evolving, driven by trends in security, virtualization, cloud, and the Internet of Things (IoT). Conventional network management solutions are manual, fragmented, and vulnerable to attack. They're no longer able to keep pace with the exponential growth of devices, IP traffic, and sophisticated security threats.

Through its secure, cloud-managed network services, Infoblox enables organizations the world over to bring next-level security, reliability and automation to traditional networks as well as digital transformations like SD-WAN, IoT and hybrid cloud, all managed through a single pane of glass.

With Infoblox solutions, organizations are able to:

- Fortify and orchestrate security across any infrastructure while making third-party security solutions more effective
- Gain the always-on, rock-solid foundation their networks demand, even as they extend across virtual and hybrid cloud environments
- Use advanced automation to cut manual tasks by 70%, shorten time to remediation by up to two thirds, and make threat analysts up to 3x more productive

Infoblox delivers products and solutions to more than 8,500 enterprises, government agencies, and service providers in more than 25 countries around the world — including 7 of the top 10 aerospace and defense companies, 7 of the top 10 telecommunications providers, 8 of the top 10 retailers, 8 of the top 10 major banks, and 9 of the top 10 automakers.



# Cybersecurity Automation

Infoblox Special Edition

**by Robert Nagy,  
Todd Christensen, and  
Geoff Horne**

FOREWORD BY **Cricket Liu**

for  
**dummies**<sup>®</sup>  
A Wiley Brand

# Cybersecurity Automation For Dummies®, Infoblox Special Edition

Published by

**John Wiley & Sons, Inc.**

111 River St.

Hoboken, NJ 07030-5774

[www.wiley.com](http://www.wiley.com)

Copyright © 2019 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Trademarks:** Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. Infoblox and the Infoblox logo are trademarks or registered trademarks of Infoblox, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

In Chapter 1, the Gartner quote attribution is Gartner, Use a Capability Matrix for a More Effective Threat Intelligence Program, Ruggero Contu, et al, 14 February 2019

In Chapter 5, the Gartner graphic attribution is Gartner, *Make Sure Your Organization is Mature Enough for SOAR*, Pete Shoard and Ryan Benson, 27 March 2019

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact [info@dummies.biz](mailto:info@dummies.biz), or visit [www.wiley.com/go/custompub](http://www.wiley.com/go/custompub). For information about licensing the *For Dummies* brand for products or services, contact [BrandedRights&Licenses@Wiley.com](mailto:BrandedRights&Licenses@Wiley.com).

ISBN 978-1-119-57580-1 (pbk); ISBN 978-1-119-57564-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

## Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

**Development Editor:** Amanda Cross

**Editorial Manager:** Rev Mengle

**Project Editor:** Jennifer Bingham

**Business Development Representative:**  
Ashley Coffey

**Acquisitions Editor:**

Karen Hattan

**Production Editor:** Tamilmani Varadharaj

**Proofreader:** Debbye Butler

# Foreword

“No man is an island,” wrote John Donne. Yes, I thought it might have been Shakespeare, but I looked it up and apparently it was John Donne. Whoever he was.

That lesson, now over 400 years old, applies equally to IT solutions as well as people — which was remarkably prescient of Donne, when you think about it. However critical those of us in the DNS, DHCP, and IPAM (DDI) business think our technologies are, they’re of limited use all by themselves. To wring the most benefit from your DDI infrastructure, it needs to be integrated with other components of your IT infrastructure: Security components, such as your firewall and your SIEM solution. Your security orchestration, automation, and response (SOAR) system. Your authentication service.

On their own, DDI solutions may be able to identify malicious activity through the use of Response Policy Zones, for example, but it’s really your firewall that would implement any policy changes to quarantine an infected device. Conversely, an intrusion detection system might flag traffic from a host as suspicious. However, in order to make an airtight determination, it might need context from your DDI system, including the host’s MAC address and operating system and information about the user who logged in from the host.

And all these interactions and integrations must be automated, because activity on a network runs on machine timescales, not human timescales. By the time a person notices suspect activity and takes action, it’s likely too late.

This book will provide you with tips on how to integrate your DDI solution with the rest of your security ecosystem, including firewalls, SIEMs, and SOARs — using standard protocols such as STIX and TAXII, as well as Infoblox’s own RESTful API. The end result should be a more responsive, more robust security infrastructure and better use of your DDI solution, and who wouldn’t want that?

—Cricket Liu, Chief DNS Architect and Senior Fellow at Infoblox

# Introduction

Companies today know that Internet security is a top priority. Protecting your customers' data, corporate knowledge, and intellectual property are absolute prerequisites to doing any kind of online business.

Unfortunately, while enforcing Internet security is just a part of what your company does, breaking through your Internet security is a full-time job for hackers. Many unethical hackers from around the world work around the clock to develop new ways to harvest your data, extort your company, or just disrupt your business. You can't maintain a battle against such dynamic foes on so many fronts without tools to help you.

That's why we wrote this book: We want you to know about the cybersecurity automation tools that make it possible for just a small team of security experts to successfully deflect the hordes of attackers trying to break through your defenses.

## About This Book

We wrote this book for people who are self-assured enough to admit they don't take full advantage of cybersecurity automation but also savvy enough to seek out more information. We think this book is a great starting point. Though it is slender, it is bulging with introductory information about terminology, technologies, and strategies that will serve you well as you begin your Internet security automation journey.

Like all titles in the *For Dummies* series, this book features easy-access organization. At the beginning of each chapter, you can find a summary of the topics covered, which makes it easy to flip through and find just the information you're looking for.

## Foolish Assumptions

Cybersecurity isn't exactly a general-interest kind of topic; you probably don't chat about it with just any person who happens to be sharing the elevator. Therefore, we assume that readers of

this book have a vested interest in keeping the online aspects of a company functioning and secure. However, we tried to write this book so that all people who pick up a copy can learn something new and interesting that deepens their understanding of Internet security automation.

You can't write a book like this without making a few assumptions, though. For this book, we assume that you're an experienced user of the Internet. We define most of our terms, but we do assume you understand the basics of networking like *server*, *client*, and *API*.

## Icons Used in This Book

Throughout this book, you occasionally see special icons to call your attention to important information. Here's what to expect:



TIP

These paragraphs point you in the right direction to get things done the fast and easy way.



REMEMBER

You want to pause and take note of these paragraphs.



WARNING

These paragraphs offer practical advice to help you avoid making mistakes.

## Beyond the Book

There's only so much that can be covered in 48 pages, so if you find yourself at the end of this book wondering where you can learn more, you can head to the Infoblox website at [www.infoblox.com](http://www.infoblox.com).

## IN THIS CHAPTER

- » The history of network or cybersecurity automation
- » How a rapidly changing environment complicates network security
- » Investing time up front to create a stronger, more efficient network

# Chapter 1

# Cybersecurity Automation: What's the Hype?

**B**efore diving into the tools and methodologies of network security automation, it's probably a good idea to explain what is meant by network or cybersecurity automation and tell you how the technology got to where it is today. The challenges and the tools to meet those challenges keep changing faster and faster, so making sure you understand that is a great way to start.

## Cybersecurity Automation

The term *cybersecurity automation* here means the process of automating configuration, alerting, and other tasks performed by security administrators and the products they manage. This automation is frequently also called *orchestration*. This term offers a good metaphor of what the core advantage is: If you think of the products in your security architecture as instruments, then the security administrator is the conductor of the orchestra. Or should



be at least. Security administrators can easily get too caught up in tuning instruments and flipping pages for the players instead of standing at the front, conducting.



REMEMBER

Cybersecurity automation can take many forms, but it simply means automating tasks that could be handled by the devices without human interaction. You can accomplish this automation either through scripts or automation tools. But the result should be that, for a small amount of effort up front, you relinquish the menial tasks that bog you down as well as have your devices talk to each other proactively, thus allowing you to focus on the bigger picture.

## Cybersecurity Automation History

Automating tasks is nothing new. In the early days of networking, Unix admins loved to automate everything they could. They created scripts that automated common and multi-step tasks such as creating a new host on the network, adding a firewall rule, or enforcing the access-control list. The scheduler `cron` was useful for executing recurring tasks at predetermined times. Tools like `expect` and `autoexpect` scripts came along and made automating command-line functions even easier.

Over time, as single-person shops were replaced by multiple systems and network divisions, all these new players required changes to the network security but were not necessarily expected to have skills in these automation tools. This automation wisdom took its exit along with the Unix Gods of Old.

### The advent of networking silos

As corporate networking needs increased and grew more complex, silos of networking knowledge began to form. This often started when companies split the management of the systems from the management of the networking components. Then came multiple systems teams to manage the Windows environment separately from the non-Windows environment. Then came security to the mix (which could grow large enough to even overshadow the actual network team). It's possible that the storage or database groups were broken into their own teams. The design function of the core networking team may even have been split out into its own architecture/build team.

As these multiple teams developed, specialized products took over as king. The number of products, plus the network vendors' incentive to get companies to do things in proprietary ways, meant that silos of information were created. These silos were not just in the products themselves, but also often in the knowledge of the team members responsible for the network and its security. As the complexity of networks grew and security became a bigger part of running a network, the silos increased.

## NAC and IF-MAP

People tried to introduce new protocols to ease the pain of these silos, or at least find a way to automate some of the more common access problems. These included things like 802.1X and NAC (Network Access Control) and the Trusted Computing Group's (TCG) introduction of IF-MAP (Interface for Metadata Access Points). By using these automated tools, users could give credentials and the network could decide their access. However, vendors again decided that they would add proprietary spin onto these standards and made the technology very difficult to implement in multivendor networks.

The TCG worked to remove these vendor lock-ins by providing a common language and transport protocol layer that all vendors could use to write to and read from a central security database. This effort resulted in the creation of IF-MAP. Infoblox developed the necessary database layer and each vendor provided read- and write-functions. A subsequent IETF working group was formed to make IF-MAP a standard, but the vendors didn't have their hearts in pushing it and most customers to this day don't know it is available. Interoperability is not the hallmark of this industry.

## Orchestrators

The growth of specialist teams continued with the creation of devops models and the demand for more automation, which was invisible to the end developer, continued. Orchestration tools such as Ansible, Chef, and Puppet began to appear. Ansible, in particular, gained a lot of traction after being purchased by Red Hat in 2015.

These tools automated tasks mainly related to end hosts and servers, but with a bit of work also could make changes to network and security devices on your networks. Ironically, this required some basic Unix understanding from the good old days; in many ways, things had come full circle.

Implementing automation tools could reap great long-term benefits, but many organizations remain reluctant to move back to this type of scripting style solution.

## Pace of change

Today, multiple security specialists have their own teams and the trend is to add differentiated cloud and cloud security teams. It can seem to be a never-ending expansion and specialization cycle.

The growth rate of networks is ever-increasing, as is the focus on securing them. Both the number of devices and their bandwidth demand are skyrocketing. And the number of different types of products used to deliver, manage, and secure the networks is also increasing rapidly.

Anyone who has ever sat in a change-control meeting can attest that a seemingly simple change can involve several teams who often have opposing goals and views. Each team gets the tools that work best for their piece of the overall environment. Coworkers using separate silos is bad, but the siloing of the tools is even more dangerous. A network is one large environment that needs to function and be secured as a whole, no matter how many separate teams work on it.



REMEMBER

It just isn't realistic to think any one person, or one team, can possibly keep up with this growth and be an expert on all of it. It is also unrealistic to rely on human communication and processing to identify and mitigate security issues as they arise in enterprise networks. In particular, the amount of effort required to constantly monitor centralized logs exceeds human capacity and is not the most valuable use of your engineering resources. As such, automation can play an integral role in identifying important events proactively.

Using automation, a human can configure simple rules like “if A happens, then alert B,” and the systems should be able to take it from there. This allows security specialists to focus on the events that really deserve human attention and analysis.

You already rely on systems and protocols that automate things: Dynamic Host Configuration Protocol (DHCP) is maybe the oldest and most basic example of such automation technology. The issues we have today arise because the protocols that we already use don't communicate with each other. The protocols don't

typically have built-in mechanisms to alert other protocols or products that might leverage that data. The vendors whose products power the protocol servers haven't historically taken the initiative to add this level of functionality and instead, just deliver the protocol as defined.

Some vendors still believe that it is in their self-interest not to “play nice” with other vendors. This is an archaic concept, but evidence of vendors trying to freeze each other out by offering a suite of products that work only with products from the same suite is all around you.

The value of interoperability becomes apparent when looking at recent PII (personally identifiable information) and the hacks around it, like the very public one at Target. This hack could have been avoided — or at least could have been much less severe — if the system that initially recognized the illegal access could have notified other security systems such as firewalls, IPS (intrusion protection system), and vulnerability management systems instead of just logging the issue to syslog, where it was lost among the noise. Throughout this book, you will see many uses for automating with vulnerability management systems. In the context of this publication, we are referring to security software that can scan and evaluate the presence of known vulnerabilities that can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system.



REMEMBER

The bottom line is this: The complexity of your networks and their security, plus the ever-evolving threats, are always growing at a rate that administrators and engineers can't keep up with. You need tools to automate basic processes like getting a client an IP address or allowing users to authenticate into the wireless network without human intervention. Now more than ever, networks need tools that talk to each other in a logical fashion.

## Incredible Growth and Diversity of Client Devices

The growth of client devices is nothing new to seasoned network administrators. Recent years have seen a large surge in the diversity of these devices, as well as the new ways to access network resources.

## BYOD

Allowing users to BYOD (bring your own device) means that network administrators now have more devices to worry about. Whether mobile phones, IP phones, watches, tablets, laptops, or servers, an ever-growing list of client devices need access to network resources. This creates the need for more network and security products because these unique device types must function with the network and must function securely.

## IoT

While not a huge factor in enterprise networks (yet), IoT (Internet of Things) is becoming more and more of an issue as things administrators never thought of as network devices join the party. Cameras, refrigerators, automobiles, light bulbs, clocks, and everything you can imagine are demanding network connectivity. These devices usually don't have a human behind them in the traditional sense and, as such, create a new paradigm. How these independent devices function on a secured network is an evolving challenge. To make matters worse, many IoT devices are created by companies who are new to the information technology arena, and many early versions are full of bugs and vulnerabilities, and are short on security features but long on bandwidth connectivity demands. Some jokingly say the Internet of Things should be renamed to the insecure distributed internet of things (IDIoT).

## Cloud services

All this talk about clients ignores maybe the single-largest change of the last few years: the movement of network services to cloud environments. Cloud networks add a new silo. Because of this, network administrators have had to add people specializing in cloud technology and cloud security, which often resulted in creating whole new teams. Most companies settled on a hybrid solution with a mix of cloud, on-premises, and third-party solutions. To the network and security administrators, this means even more tools, products, and people to manage these varying environments. It also creates security and logging challenges as each environment can behave very differently.

# The Current State of Cybersecurity Automation

It's safe to say that today's enterprise networks are as complex as ever. The job of a modern-day security administrator involves ensuring smooth access for mission-critical servers, laptops, smartphones, and BYOD devices in the most secure way possible. However, complexity means you must have eyes, ears, and fingers everywhere, all at the same time. Looking for a threat, a breach, or anomalous activity amidst all the other network chatter is worse than finding a needle in a haystack: It's finding a needle in an ever-growing number of haystacks that are constantly growing themselves.

To make matters worse, many teams have to use out-of-band communication to coordinate efforts between their silos, further complicating the process to track down and address issues and alerts in a timely manner. Take, for example, the process of adding a new client to the network. This was once a simple case of deploying the device, allowing DHCP to do its magic, and adding a client to the main domain. Nowadays, this process can involve all kinds of other tasks, such as adding the client MAC address to different security devices to grant access, configuring proxy and logging, and client vulnerability scanning. With coordination between independent groups, this can be a complex process that not only includes the time to execute the various tasks but also includes all the time needed to coordinate the varying efforts. Tomorrow this process could include even more.

And maybe the scariest fact about human involvement is that there just aren't enough qualified people available. The 2018 (ISC)<sup>2</sup> Cybersecurity Workforce Study showed a nearly three-million-person gap in the cybersecurity space. This shortfall has been growing and shows no sign of stopping. Now is a good time to figure out how to make any and all basic network administration tasks less human intensive.

The study also showed that 63 percent of respondents report that their organizations have a shortage of IT staff dedicated to cybersecurity. More than half, 59 percent, say their companies are at moderate or extreme risk of cybersecurity attacks due to this shortage.



WARNING

Hackers grow ever more sophisticated and actually rely on you not seeing minor intrusions among the vast amount of data they know you're collecting. If you even get an alert among the millions of items checked, hackers know that one alert on one product probably just causes you to say "Oh, well: If it really is an issue, Product Y will catch it." Just a single slip-up such as this can result in allowing hackers access into your network. They actually play on the complexity of the system. The complexity is ever increasing and yet the number of people expected to manage and secure the network doesn't keep up.

Current tools are, however, growing in awareness and may have the opportunity to bring security automation without the complexity of other open source or homespun solutions. This also introduces some new methodologies and processes that change the way we approach security. The physical security models (barriers, guards, chokepoints) can no longer be applied to a cyberspace environment, much in the same way that people had to redesign castles after the discovery of gunpowder.

## Threat intelligence

According to Gartner, "Threat intelligence is defined as evidence-based knowledge — including context, mechanisms, indicators, implications and action-oriented advice — about an existing or emerging hazard to IT or information assets. It can be used to inform decisions regarding the subject's response to that menace or hazard."



REMEMBER

Gartner's definition gets to the idea that the gathering and curating of threats must be at the core of network administration and security. It's not enough to just act on an attack after the fact; security professionals must be in a constant state of data gathering and learning about the threats as they evolve in the wild. This is a far cry from just blocking ports and looking for hits. Network administrators now must be actively engaged in what is going on

in the world of the bad actors. More and more, the industry can gather this data from various sources and leverage in the corporate policies. For this to happen in real time and with data sets far larger than humans can process, network administrators must engage computing power to help sort through the noise.

## STIX and TAXII

Recent years have seen the adoption of open standard languages and protocols such as the language STIX (Structured Threat Information eXpression) and the transport TAXII (Trusted Automated eXchange of Indicator Information) to better allow the sharing of security information. These open standards allow the secure sharing of cyberthreat information.

Understanding that no one organization has all the knowledge of the bad actors and their current behaviors, the industry recognized the need to share the widest range of information securely. It is interesting to note that these efforts, unlike previous attempts, began outside of typical standards and vendor consortiums like the IETF and was reportedly developed in an offshoot from a cybersecurity mailing list. Since then, this effort has seen the involvement of many of the industry's best people and organizations to help grow and evolve the standard.

## Start Simple If You Must

You are overworked as it is; taking on an additional automation effort might not seem very appealing. But even if you can't leverage fully integrated automation tools or security workflows inside devops recipes, you don't have to be stuck doing everything by hand. A more limited approach might sacrifice the preemptive aspect, but you can still gain cycles back for your team. More and more products offer web-based APIs. Using these APIs to automate common tasks is a step in the right direction.

The following example shows how creating a single task that executes three commonly grouped configuration tasks against multiple systems reduces workload and allows time to focus on more important security tasks like gathering and processing threat intelligence.



When a new host joins, you would execute a script that:

1. Contacts our IPAM server to get the next available IP address for the desired network.
2. Alerts the local vulnerability management system that it will scan a new host on the network using the API provided by that vendor.
3. Notifies the firewall that a new host has joined the network and that host should be added to the monitoring group for the next 24 hours per company policy.

## IN THIS CHAPTER

- » Discussing the different approaches to setting up your security automation
- » Introducing the most common file format you'll encounter
- » Reviewing code samples in each language

# Chapter 2

# Automation Technologies: Tools and Languages

The approaches to and technologies for cybersecurity automation are as varied as the companies that implement them. The skills and capacity of your team, the sophistication of your business systems, the sensitivity of your data, and other factors all contribute to your decision about how to set up your security automation. In this chapter, we talk about the most common approaches people take and the pros and cons of each one.

## Automation Modalities

As the administrator, you can easily leverage API access to control a wide variety of network and security devices (see Chapter 1 for more information). You can use common scripting languages such as Perl, Python, Bash, JavaScript, and others to automate web calls to configure or read from your network security products. Since you control the implementation, you can make this as simple or as complex as you want.

This section covers some possible implementation models.

## Client-device

With this model, you use an external client to configure a security product that runs at certain times. You might set up the external client to run the security product when a product alerts you that a trigger event has occurred, or you might set it up to run based on time of day.

The following example shows a Bash script that, every two hours, grabs the current “bad actors” list from product A and feeds it to product B (the security product) for scanning.

1. Configure crontab with the line `0 */2 * * * /home/bad-actors.sh`
2. Create `bad-actors.sh` based on the API documentations of products A and B.



TIP

Values in <angle brackets> are placeholders for real values that vary depending on your setup.

```
#!/bin/bash

# This Script is run from cron every 2 hours to
# move
# a new bad-actors access list from Product A to
# Product B where it can be scanned
# This script is a SIMPLIFIED EXAMPLE of what a
# script could look like

# Get "bad-actor" access-list from Product A
SEARCH=`curl -k -u rob:password -X GET
'https://<IP-ProductA>/wapi/v3.8/access-list=
'bad-actors`
LIST_REF=`echo $SEARCH `

# Put the list we got from Product A into product B

ADD=`curl -k -u rob:password -X PUT '<IP-ProductA>/
wapi/v1.2/scan-list='new-bad'?data=$LIST_REF`

SCAN_LIST= `echo $ADD`
#Put list into Product B
```

The previous script is just a very simplified example to demonstrate the steps you might use as it would be dependent on the REST API implementations of the products.

The pros of the client-device setup relate to its simplicity:

- » It's easy to implement.
- » You don't need outside tools.
- » It can start in response to a trigger event or be based on a schedule.

The client-device setup approach does have some drawbacks, though:

- » It must be maintained in-house.
- » The person implementing it must have basic scripting skills.
- » It doesn't take advantage of machine learning or artificial intelligence (AI).

## Device-device

If you rank the approaches by their sophistication, the next level of automation is the model where one product can update another product directly. In this model, each vendor decides what events trigger API calls to other vendors or products.



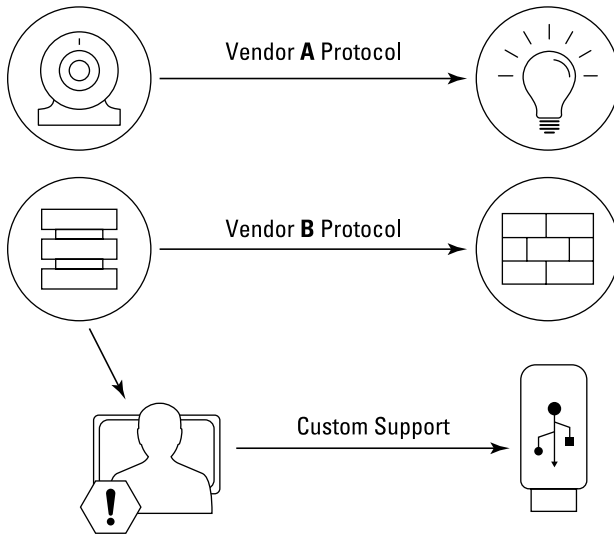
TIP

On supported platforms, this kind of integration may work out-of-the-box, requiring little-to-no work on your part, but it is rare. This kind of automation requires each product to have the capability to send updates to other products when key events occur, and those receiving products must use common APIs and integration capabilities (for example, RESTful) to allow these independent updates to occur. Therefore, picking the right products is critical to this kind of automation.

Figure 2-1 shows an example of automating events around a worker entering an office:

- » When the webcam recognizes the user's face in the office, turn on the light bulb in the room
- » When the authentication server sees the user logging in to the office network, update the firewall rules to allow the user access from the office network

- » Also, when the authentication server sees the user logging in to the office network, activate enforcement to encrypt USB-connected drives on the user's laptop



Source: Infoblox

**FIGURE 2-1:** The automation you can accomplish with the device-device approach depends on the capabilities of the tools that you choose.

Since the webcam vendor supports the lightbulb, that integration was easily accomplished. The same goes for the authentication server and the firewall. However, the authentication server doesn't support updating encryption policy on the USB devices, so that portion must be manually performed by alerting a human administrator to update security configuration.

The pros of the device-device approach relate to convenience:

- » The vendor controls the triggers and syntax.
- » You have no need to maintain a scripting environment.
- » The vendor deals with updating the required tools.

The cons of this approach relate to limitations in functionality:

- » The only events that can trigger updates are the events the device sees.

- » You become dependent on the vendor for new features and product support.
- » You probably can't customize the notifications that come out of the system.

## Central control: Automation tools-device

Automation tools are growing in popularity. These tools have migrated from open source projects that run on Unix-style (\*nix) operating systems to orchestration tools that each have different languages and methodologies (for more on this, see Chapter 1). What these tools have in common is that they control the devices from a separate, often dedicated, server, which allows the automation server to be maintained separately from the tools being managed.



TIP

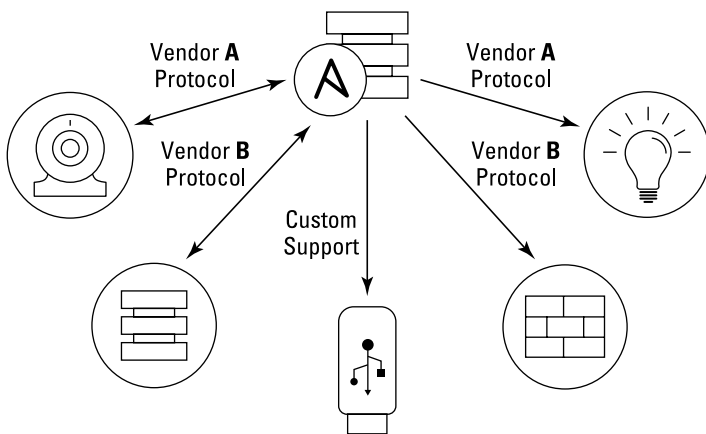
One advantage of having the automation/configuration server separate from the other devices is that it can support very complex flows. It can query and act on responses from multiple devices. Some of these automation tools require a software agent to be installed on the target device; some work without these agents.

While it is possible to make a combination solution using different automation tools, such as by combining Ansible and Puppet, the separate tools may not necessarily integrate well with each other or might require learning even more specialized languages. One of the bigger challenges for many organizations is that each of these orchestration tools chose different configuration languages (we dive into this in the next section), so the orchestrator itself becomes a specialization and a silo.

Solutions that use automation tools to centralize control of devices can range from the incredibly simple and straightforward to the incredibly sophisticated and powerful. However, because the users are responsible for all this functionality and its maintenance, achieving all your desired workflows can become a big undertaking.

Of all the open-source automation tools out there, Ansible has certainly grabbed the most attention and adoptions. Ansible is an agentless solution, and its primary mechanisms for control are the SSH protocol and Python PowerShell. It is configured using “playbooks” written typically in YAML (Yet Another Markup Language). Ansible has over 200 different network modules for vendors such as Cisco, F5, Infoblox, Juniper, Palo Alto, and more.

Figure 2-2 shows automating the same event described in Figure 2-1, this time using an automation system (Ansible) housed on a dedicated automation server. The automation server communicates with the webcam and the authentication server to make desired configuration changes to the light bulb, firewall, and USB encryption policy. The added advantage to this approach is that the automation system can have additional logical checks built in, such as requiring both conditions (webcam detects user AND successful authentication) to be met before making any configuration changes. This level of sophistication wasn't possible with the previous automation approaches.



Source: Infoblox

**FIGURE 2-2:** A centralized automation server offers a wider range of capabilities.

The benefits of using automation tools come from how much you can customize them:

- »» The automation tool can execute a wide variety of functions, including everything from enforcing client-configurations to triggering security tools.
- »» The automation tool may be supportable by vendors, depending on the tool you choose.

Of course, there are also drawbacks to the automation tool approach:

- » Maintenance of the Control System can be time-consuming.
- » If you want any changes made to the managed systems you have to make them yourself.
- » Complex solutions can take a lot of up-front effort.

## Central control: Orchestration tools-device (SOAR)

SOAR (Security Orchestration, Automation, and Remediation) is a very hot topic in 2019. The fact that companies need to make security products interoperate and respond on the company's behalf has become mission-critical. The complexity of networks and network security grows at a rate beyond our ability to keep up with as humans, and the costs associated with failing to secure our enterprise networks is growing just as quickly. For these reasons, SOAR is being discussed everywhere you turn.

SOAR looks to bring more abstract orchestrations, machine learning, and AI into automating or assisting in a response to an event. By using a toolset to analyze and act on your behalf, SOAR is exactly what you need in order to allow your systems to scale beyond the limitations of human operators. Security professionals are still the most important part of your security strategy, but by letting machines keep up with the ever-increasing amount and speed of the data that needs to be sifted through, the security professionals save their own time to focus on the creative problem solving that humans do best.

There are several vendors in this space, and each tool has its own strengths and features. They can leverage various types of AI and machine learning and range from incredibly robust to very simple. The overall intent is that these orchestration tools can collate, organize, and summarize events based on higher level rules (such as business operations) and combine them into a single event or action item.



TIP

Instead of making recommendations on any one product, we recommend you do research on which solution works best for your organization based on the following criteria:

- » Ease of use
- » Security vendor support



- » Interoperability support, and resources
- » Available product education

## Overview of Common File Formats

In order to automate security, your systems need to be able to “speak to” a wide variety of security products. Being able to send and receive complex information and data structures is critical because your system must send and receive information from security products, parse data in and out of human language, and output something the network products can make use of. Structured data and common fields are only the starting point.



REMEMBER

While there are many possible formats (and vendors can even create their own), the following three formats are the most commonly used today:

- » JSON
- » YAML
- » XML

It is important to note that there are converters between these three languages available both online and as modules for most scripting and programming languages. Therefore, if you like one language more than another, translating between them is easy.

### JSON (JavaScript Object Notation)

JSON is a file format (or language) used to express complex objects and make them human-readable. While “JavaScript” is in the title, that is a misnomer: Although JSON was developed for JavaScript applications, it is a format, and not part of the language. JSON’s simple expression of complex structures makes it suitable for almost any programming language. JSON was first used in the 1990s and gained adoption in the 2000s, finally being standardized by the IETF in 2014 with RFC-7159.

An important use of JSON in network security is its use in STIX 2.0 (see Chapter 1) when the standard format was moved from XML in STIX 1.0 to JSON in STIX 2.0.

In the following example, you can see information on a host represented in JSON Format.

```
[
  {
    "ip_address": "10.45.45.45",
    "is_conflict": false,
    "lease_state": "ACTIVE",
    "mac_address": "00:09:de:ad:be:ef",
    "names": "noyb",
    "network": "10.45.45.0/24",
    "usage": [
      "DHCP",
      "DNS"
    ]
  }
]
```

## YAML (YAML Ain't Markup Language)

We want to begin discussing YAML by noting that we consider it one of the best acronyms in the industry. YAML is primarily intended for use in configuration files and, as such, favors being more human-readable. But don't be fooled. YAML is still easy for machines to use and it leverages Python-style indenting to convey much of what other markup languages use punctuation to convey. When using YAML, be very careful with your indenting: While giving meaning to indentation it makes the code very readable, it can also be difficult to debug.

Here you see the same structure expressed in YAML.

```
---
root:
  element:
    ip_address: 10.45.45.45
    is_conflict: false
    lease_state: ACTIVE
    mac_address: 00:09:de:ad:be:ef
    names: noyb
    network: 10.45.45.0/24
```

```
usage:
  element:
    - DHCP
    - DNS
```

## XML (eXtensible Markup Language)

The history of XML is long and goes back to the 1970s. XML is documented in many books of its own. For the purposes of this book, though, it is just important to note that XML has seen many other formats come and go. It is, in many ways, the basis of other formats. For people who can read and write other formats such as HTML, XML can be an easy way to get started. However, while the verbosity that comes from XML's extensible nature makes it easily understandable, that same verbosity can be overbearing when creating large and complex objects or processing large amounts of data.

Here you see the final example with the same structure conveyed in XML.

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
  <element>
    <ip_address>10.45.45.45</ip_address>
    <is_conflict>>false</is_conflict>
    <lease_state>ACTIVE</lease_state>
    <mac_address>00:09:de:ad:be:ef</mac_address>
    <names>noyb</names>
    <network>10.45.45.0/24</network>
    <usage>
      <element>DHCP</element>
      <element>DNS</element>
    </usage>
  </element>
</root>
```

## IN THIS CHAPTER

- » Unpacking the components of DDI
- » Using a client-centric approach
- » Sharing information among systems to improve security

# Chapter 3

## The Role of DDI in Security Automation

**D**DI is shorthand for the integration of DNS, DHCP, and IPAM (IP Address Management) into a unified solution. These technologies comprise the foundation of core network services that enable all communications over an IP-based network.

A well-structured DDI solution gives you visibility beyond just the perimeter and network core, and extends it down to the client. DDI also adds the benefit of not just controlling clients' current state (address and name management), but also their history over time (with DHCP leases and DNS queries).

### Benefits of a Client-Centric Solution

Traditional network defense is planned around the perimeter: Firewalls, IDSs (intrusion detection systems), and other devices guard the network like a castle. The castle metaphor seems like a good approach until you realize that the perimeter is always shifting, with users directly accessing cloud applications and branch office Internet breakouts.

# INTRUSION DETECTION SYSTEM (IDS) AND INTRUSION PREVENTION SYSTEM (IPS)

An IDS is typically a perimeter defense that monitors the network for signs of bad behavior. This can be based on characteristics of either the traffic itself or of the contents of the traffic. With an IDS when issues are detected that information is shared with other tools such as SIEM to take action.

An IPS, on the other hand, will take action such as restricting or blocking access of the bad actor to prevent the detected behavior.



REMEMBER

A quick note on IDS and IPS (intrusion protection system) since they can be a large part of a traditional defense approach. We are not saying these devices aren't valuable; we are just stating that they shouldn't be the only solution. For clarification, the nearby sidebar explains how we define IDS and IPS for the purposes of this book.



WARNING

Unfortunately, the real threat may be coming from within the walls. On today's network, any device connecting to the internal network could be harboring an intruder trying to climb over your (fire)walls. Unwitting users who just clicked on a link to a funny video or opened an email while at a local coffee shop can do more damage than they can imagine. Bad people work very hard to trick everyday users, and it's hard, even for information security professionals, to keep up with all the latest hacks to get your laptop or mobile device infected with malware.

User awareness is usually the weakest link in the security armor, but even fully educating everyone in your enterprise and securing all their phones and laptops doesn't guarantee your network is safe. Some devices on your network don't even have a human behind them. With BYOD and IoT, many of these devices roam about your network, run unattended apps in the background, all with little visibility into what they're really doing ("Is the smart lightbulb supposed to be downloading files from abc.xyz.example.com?").

A client-centric approach lets you leverage core services such as DNS and DHCP as early warning signs of issues. If you can examine what is happening on the control plane of these devices, you can get indicators of behavior before a flow is created. Often the simplest core protocols provide the first indications that there is something you need to look at, but these sadly often go unnoticed by security teams, who have only so many resources and are stuck guarding the outer gates. Often the team identifies these patterns only after a breach has played out.



TIP

Core services can give the first signs of trouble and help stop issues before they start. Protocols like DHCP and DNS capture critical events and trigger tasks that you probably batch and run in groups during off-peak hours. If you instead use automation, you could trigger those tasks when they're most needed, at the first contact by a new client or the first sign that a client isn't behaving normally.

For example, you could use automation to begin security protocols when DHCP first sees a client or when a client makes a suspect DNS query. In addition to limiting the damage, stopping malware before it can initiate a network flow can benefit your other security products (for example, deep packet inspection tools) by reducing their workload and enhances the value from your investment in larger defensive tools.



TIP

For these reasons, DDI is your best front line to security, identifying clients as they connect and taking multiple security actions through automation. By using these tools, you can proactively inform the other security tools and trigger multiple security actions to scan or quarantine the host and open a ticket for further investigation.

## DHCP as the Initial Contact

Imagine a normal network user connecting to the corporate network to check her email. She turns on her laptop and connects to the office wireless network. A lot of things happened under the hood when she connected, and one of those many things is that her laptop contacted a DHCP server and obtained an IP address.



Before a host can really do damage to others, it must first obtain an IP address, and it usually gets that address from a DHCP server. DHCP is automation in and of itself that simplifies the previously laborious process of having to manually assign and configure IP addresses for every client that joined your network. However, DHCP doesn't have good mechanisms to authenticate or authorize the client. It just gives an address to any device on the network that asks for one. DHCP can make decisions on who gets an IP address, but imagine if DHCP could alert other security tools to the presence of a new client on the network.

What could your other tools do to protect the security of your network and resources from this new client? The answer is “a lot!” Just a few possibilities include:

- » They could scan the client to make sure it meets the virus-protection requirements of the network using a vulnerability management system.
- » A firewall that tracks client sessions could put the client into a monitor list for a period of time.

Using DHCP this way is a chance to tell your other security products, “Hey, we have a newcomer, check them out or maybe keep a special eye on them.” DHCP makes such a good starting place for cybersecurity automation and is an ideal first line of defense.

Add in DHCP fingerprinting information (so you can classify the kind of device on the network), the time stamps inherent with DHCP, the client-reported identifiers such as operating system type, the DHCP lease history of the device or address, and all the other information DHCP already gathers, and you can see how DHCP has a wealth of knowledge to share with other security products.

## DNS as the Foundation

Following the same example user in the previous section, once she received an IP address, the next part is probably typing in a password or using some new fancy biometrics to log in to the laptop. As part of that process, the laptop likely also logs in to the corporate internal network by way of contacting authentication servers such as LDAP or RADIUS. However, there is any amount

of additional traffic, legitimate or otherwise, that is also now on the network that most configurations aren't really applying any security layers to. Operating systems do all kinds of stuff in the background that we aren't aware of, and lots of them send traffic into the Internet. All of this is done quietly, before even lighting up the display for human users to know the device is ready for interaction. Whatever the configuration, it is safe to assume that the client made some DNS queries.



REMEMBER

Domain Name System, or DNS, is one of the cornerstones of the modern networks. It has been around for over 30 years and is often overlooked as part of client behavior. In the modern era, DNS queries are always among the first outgoing network traffic when a device comes online, long before any human lays a finger on the keyboard or touchscreen.

In order for a client to access network resources, the client sends a DNS query to retrieve the IP address(es) and other information to contact the server. This lookup behavior is the same for both legitimate and malicious activities: Downloading the latest iTunes software and downloading the latest virus both involve DNS as the first step.

If you think of security in layers (like an onion), DNS is the outer first layer. As such, DNS deserves more attention than other technologies, and many people and companies have developed new security capabilities for it over the last decade (more on this in Chapter 4).

Modern DNS servers can identify bad or malicious lookups, and they can stop these lookups from happening. However, just like with DHCP, why stop here? When a host asks the DNS server: "What is the IP address for evil.malware.example.net?" your DNS server can deny that request (either by saying the name doesn't exist at all or returning a false answer such as 10.0.0.1). Your DNS server can then turn around and notify all the other tools, perhaps quarantine the host into a special isolated network to be scanned for malware, or simply increase the logging for that device.

Security layers are now also able to examine traffic that may move inside your internal network without transiting any firewalls. The DNS query may show a device trying to access a payroll server or other sensitive equipment inside the enterprise. The key here is to identify the intent of the traffic before any data is sent to the wrong locations.



# IPAM Ties It All Together

IP address management (IPAM) doesn't sound exciting, or even relevant to security, at least until you get to know it. Both DHCP and DNS servers can notify other tools and products of the presence of a new client and the client's behavior, respectively. They're capable of sending a message like: "Hey, here is a new MAC address that came online, 00:00:C0:FF:EE" or "IP address 10.1.2.3 tried to look up the known malicious domain name get.malware.example.net." With IPAM, they can send additional information like: "MAC address 00:00:C0:FF:EE has connected to the network; it is seen on edge switch X port Eth0/12; department is HR; asset tag #ABC0001; it is leased to user JKUO; assigned to building POST; campus UHM; device category is Field-Laptop." What's important here is not really the address, but the metadata attached to it.

IPAM empowers other protocols and tools, like DNS and DHCP, by bringing metadata into the mix. Metadata is any additional information you want to track, and it can be specific to your organization. Metadata, like model number, owner's name, building, city, or department, can all be tracked. Other tools can make use of this information, either directly by matching rules on the metadata fields, or indirectly by displaying the metadata as part of an investigation process. When the client receives its DHCP address, it can inform the firewall that this MAC address belongs to someone in the HR department, thus custom firewall rules can be implemented.



TIP

By associating this metadata with a specific client, other tools can receive it, and they can send back information about what they find, or what actions they took. It enriches the value of the information stored in IPAM.

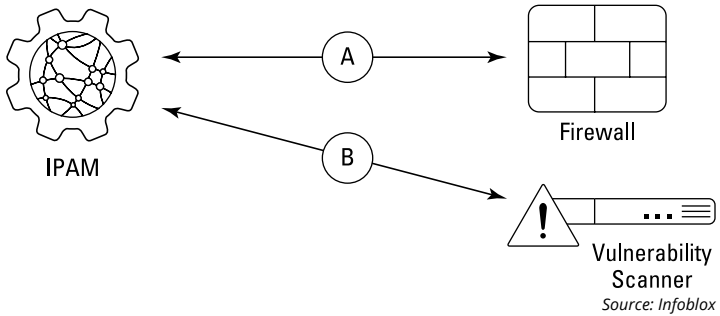
The diagram in Figure 3-1 shows a workflow that is possible when using IPAM client-centric information to enable security products to function more proactively.

```
A: Notify Firewall that a new client has accessed
to the network and should go into a category and
that its DHCP fingerprint reports it is an
iPhone.
```

Firewall returns that client has been added to the list for new phones and this is added to the "Firewall Category" attribute in IPAM

B: Alert the Host Scanner device that a new client has joined the network and that it should be scanned immediately.

Scanner returns values to be added to IPAM;  
timestamp for when it initiated the scan  
timestamp for when it completed the latest scan  
results of the latest scan



**FIGURE 3-1:** Sharing information among IPAM, firewalls, and other tools enhances the data set that all the systems use.

Source: Infoblox

## IN THIS CHAPTER

- » How your cybersecurity automation systems create their own ecosystem
- » Setting the scene for implementing a simple example
- » Extending the example to apply to more scenarios

# Chapter 4

# Example Automation with Ecosystem

In the context of biology, an *ecosystem* is a community of interacting organisms and their physical environment. In the context of cybersecurity automation, *ecosystem* also refers to interconnection, but in this case, it's the interconnection of systems.

## Interconnected Security Systems

Starting with a strong foundation in DNS, DHCP, and IPAM (see Chapter 3 for more info), now you also need a robotic ecosystem that enables automated interaction with other security systems in your environment. These interactions occur over industry-standard communication protocols such as syslog, SNMP, STIX/TAXII, and other third-party protocols and RESTful APIs.

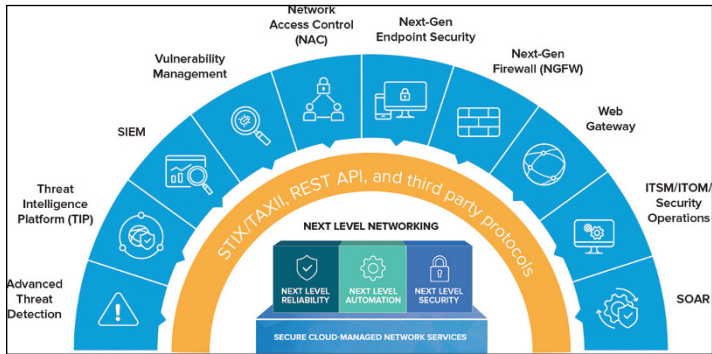


REMEMBER

This focus on intercommunication allows systems not just to notify each other, but also to provide additional contextual information and threat intelligence. Furthermore, these tightly interconnected interactions can initiate action in other parts of the infrastructure. This functionality increases the value of existing security platform investments, eliminates security silos, and

shortens the response time for common repetitive tasks by reducing or even eliminating the need for human involvement.

Figure 4-1 illustrates the different kinds of systems that can work together in a system like this.



Source: Infoblox

**FIGURE 4-1:** Multiple systems, tightly integrated, truly automate your network security.

## Setting a Good Example

In this section, we set up an example scenario of an automation task with Infoblox Ecosystem and a vulnerability management system.

### Scenario

In order to take a proactive approach to security, ACME has implemented a new policy: Going forward, the vulnerability management system must assess all new clients on its network.



TIP

One of the challenges in executing this security objective is the ever-changing inventory of clients on the network. Entry points to the network include:

- » DHCP
- » Remote VPN
- » Public and private cloud

Clients can enter onto and be removed from the network before a scheduled vulnerability scan of the entire network can be completed. The addition of new subnets into a network can require manual entry into the vulnerability management system. Such manual steps leave room for error.

## Solution

A more efficient approach than trying to scan the entire network on a recurring schedule is to use the IPAM data and events to trigger a system of automated actions.

You can accomplish this by using Infoblox's position in the network. Direct interaction with network hosts and infrastructure allows it to be the "single source of truth" for your network inventory. It also provides you with the additional capability to be able to track the last-scanned date information in IPAM. This approach gives you:

- » The capability to see when host devices enter and leave the network
- » DHCP visibility, including operating system fingerprinting data
- » Network discovery, including direct interaction with switches, access points, and firewalls
- » Interaction with cloud orchestration, including public, private, and hybrid
- » Knowledge of newly configured DNS records and DHCP reservations

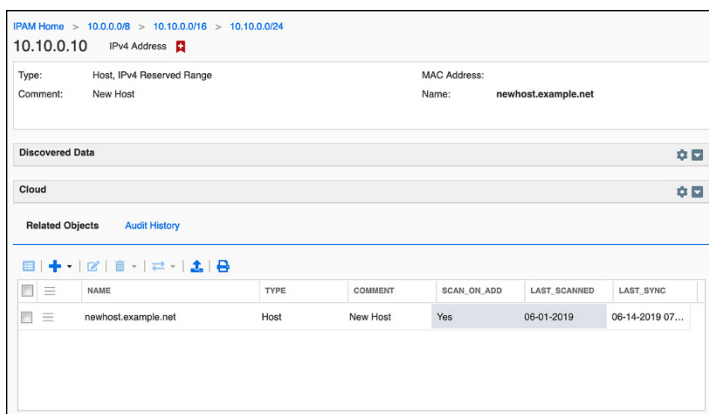
When a new host enters the network, Infoblox can proactively send a notification to a vulnerability management system to scan the new host. When this is complete, Infoblox can tag the host record with a "last scanned date" entry in the IPAM interface. You can view this information inside of Infoblox, report on it with Infoblox reporting, or share it with other systems such as a SIEM (security information and event management), which gathers and analyzes security information and event logs. The "last scanned date" then triggers subsequent scans upon a designated expiration period.

## How it works

Adding the DNS record for a new host in Infoblox automates the addition of the new host into the vulnerability management system and triggers a vulnerability scan on the new host. Once the scan is complete, Infoblox receives the confirmation of the scan and adds to the IPAM data for the host record.

1. A new host joins the DNS. Any one of many alternative inputs might have initiated this addition, such as:
  - DHCP lease
  - Network discovery
  - Cloud discovery
  - Cloud orchestration
  - API
2. The addition of the new host event triggers a *notification*. A notification sends information to an *endpoint* (in this case, the vulnerability management system) in the format of a *template*, which contains code to interact with the vulnerability management administrative interface.
3. These components being utilized result in the outbound API call to the vulnerability management system.
4. The outbound API call provides instructions to add the new host into the vulnerability management system and to run a scan of the new host.
5. The vulnerability management system scans the new host.
6. Once the scan is complete, the vulnerability management system shares this information back to Infoblox. As you can see in Figure 4-2, Infoblox tracks the last scanned date as an extensible attribute, which you can view, report on, and use to trigger future scans.

The preceding example highlights one simple use of the automation technologies to streamline and simplify a process. Using events and IPAM data can improve efficiency and reliability. By using automation, you eliminate manual intervention.



Source: Infoblox

**FIGURE 4-2:** You can see the entry for the new host directly in the Infoblox interface.



REMEMBER

Sharing this information via outbound API to other security platforms reduces duplicate efforts and eliminates security silos. One system processing a new host is now automating the required processing for another system or systems.

Many templates exist for ecosystems developed by Infoblox, partners, and clients that interact with a large profile of security platforms. You can view and download many of them on the Infoblox community website at <https://community.infoblox.com>.

## IN THIS CHAPTER

- » The evolution of the SOAR approach
- » Walking through how SOAR responds to a threat
- » Imagining how a non-SOAR approach responds to threats

# Chapter 5

## Infoblox and SOAR

In this chapter, we go with another acronym: SOAR! Not *sore* like my back, not *soar* like an eagle, but rather, SOAR the acronym meaning security orchestration, automation, and response. While there is work required to set it up, as with other systems, the idea behind SOAR is to save work by automating aspects of security operations.

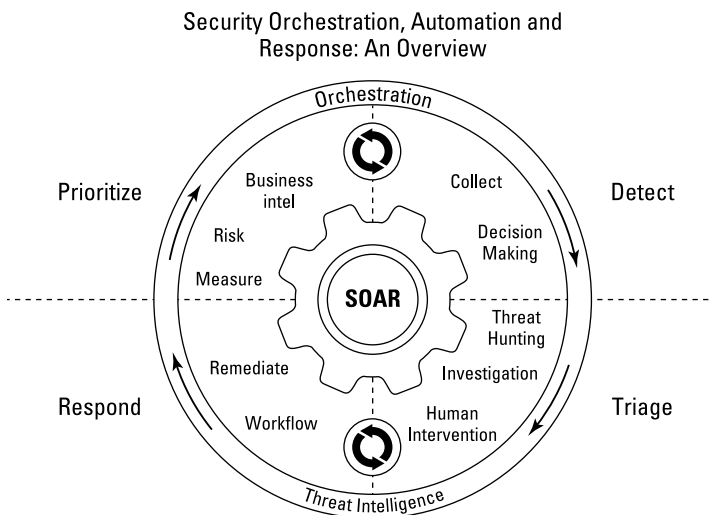
### The SOAR Origin Story

If you take a short trip back in IT history, you will see the development of the SIEM platform. This consolidated platform could organize, compare, and trigger alerts on data. Many systems would feed into the platform, but outputs were typically limited to alerts and reports.

Wouldn't it be great if it were possible to not only ingest this information, but also take action on it? In Chapter 1, we mention that this was attempted many years ago with IF-MAP, but never gained momentum. Today, RESTful APIs are a standard on most infrastructure, networking, and security platforms. These APIs allow for inter-platform communications. Now, add together the “send it all to a SIEM” and the capability to automatically act on that information. The capability to use APIs to contact the



corresponding security platforms for research, prioritization, and remediation of the issues gives us security orchestration, automation, and response (SOAR). See Figure 5-1 for a depiction of SOAR from Gartner.



Source: Gartner

**FIGURE 5-1:** Gartner SOAR components.

## Infoblox and SOAR

The Infoblox technology contributes to SOAR functionality. Infoblox offers a rich IPAM data set, including the DNS and DHCP configurations of most of the hosts on the network. These host objects in Infoblox can also contain metadata tags, or extensible attributes that provide further information on the hosts as well as the networks on which they sit.

Infoblox also provides a discovery engine, which surfaces information on hosts that are added to the network without any corresponding DNS and DHCP configuration. This feature gives a complete and single source of truth for your network inventory. The rich detail that comes with discovery provides connectivity information, such as:

- »» Network device the host is connected to
- »» Switch-port details
- »» VLAN
- »» Connection speeds
- »» Operating system information

From a forensic standpoint, this data can help you reconstruct who had what address and when. This IPAM data provides contextual enrichment for SOAR research and operations.

Infoblox has visibility into when hosts come onto the network, as well as when a host was last seen on a network. As the DNS service provider, it can observe the critical DNS traffic patterns of clients on the network, including potential misconfiguration or DNS security-related events. This allows Infoblox to be a great trigger for alerting and resulting remediation as well as an in-depth source of history data for forensics.

Threat data is another key benefit to SOAR. Many security platforms can utilize threat feeds to enhance their detection and performance capabilities. A threat feed is evidence-based knowledge, including context, mechanisms, indicators, implications, and action-oriented advice about an existing or emerging menace or hazard to assets.

You can use this data on security enforcement systems such as SIEM. By using this threat information, you can investigate alerts arriving in the SIEM from any sources, whether it be on-premise data or from cloud environments. All these alerts and messages can then be analyzed against known threat information and actions initiated based on the threat information.

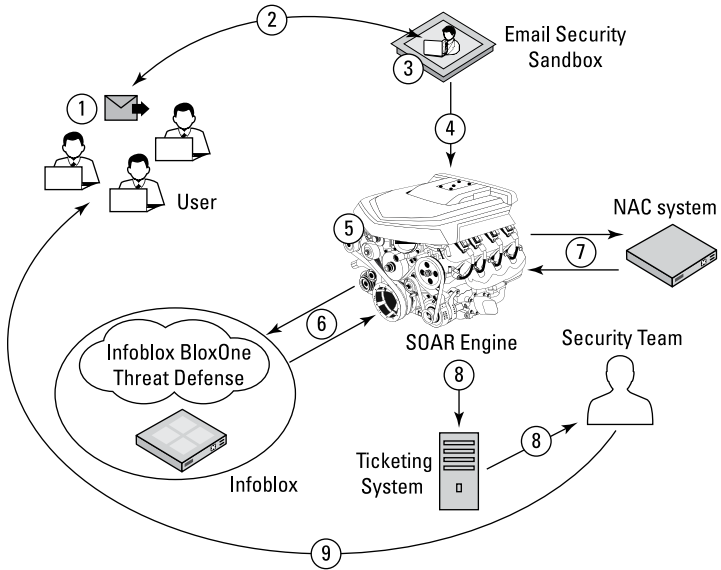


TIP

On top of participating in security enforcement, the data can be useful for threat research. Threat lookup and services (such as Dossier) provide detailed threat data on host, URL, and IP addresses. The capability to identify threat classes from many different threat providers as well as what threat level they pose is key to assisting with prioritizing responses to an event.

# Example of SOAR in Action

Figure 5-2 shows an example of how SOAR can power your cybersecurity automation. It's broken in to nine steps to draw your attention to the most important aspects.

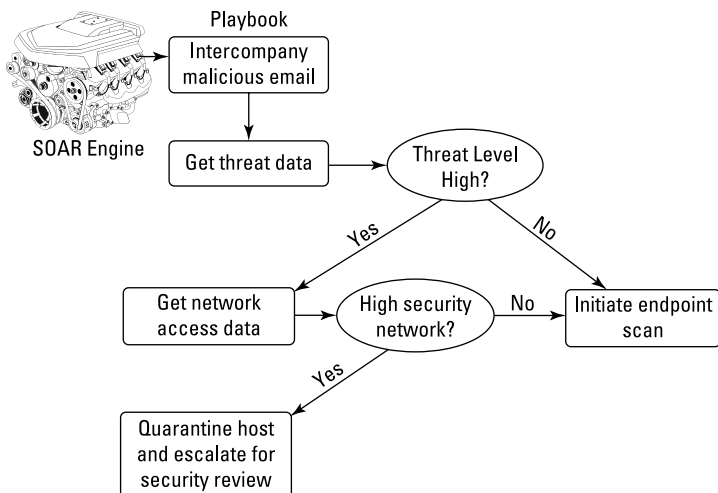


Source: Infoblox

**FIGURE 5-2:** SOAR and Infoblox in the flow of your network security.

1. To kick off this scenario, on Monday, multiple users at ACME Corp receive an email with a link, "This game is awesome, try it here!"
2. The email security system sees the embedded link and initiates analysis.
3. The security system determines the link target to be some form of malware. The system automatically deletes the emails from the users' inboxes. The system determines that the sender of the email is an employee, John Smith, so it does not block the sender.
4. SOAR receives an alert (via SIEM) saying that John Smith sent the email with the link to a malicious file. This alert contains the URL data from the email.

5. SOAR utilizes a “playbook” for malicious emails, which is outlined in Figure 5-3. The playbook contains the steps that SOAR follows to respond to malicious emails.



Source: Infoblox

FIGURE 5-3: Example playbook for malicious emails.

6. SOAR makes an API call to Infoblox for data on John Smith. Infoblox shows that John Smith is currently on the network via a DHCP lease in the financial department network and that he is using a Windows 7 laptop.
- SOAR makes an additional API call to Infoblox’s Dossier application on the cloud for analysis of the URL provided by the email security alert. Dossier responds with the history of the threat and additional metadata, such as who registered the domain, related IP addresses, and the geolocation of the site.
7. Based on the severity of the threat and John Smith’s location on the financial system’s network, SOAR decides to isolate John Smith’s laptop from the production network. It calls the NAC system, putting it into a quarantined VLAN.
8. SOAR also opens a ticket and assigns it to the team responsible for workstation security.

9. The security team contacts John Smith to bring his laptop in for analysis. John Smith says that he received the link to the game on his personal email account over the weekend and had enjoyed the game, but didn't intentionally send any emails to other employees in the company about the game.

Without a SOAR approach, this story could have taken a lot longer to play out and might have had a much less happy ending. Many environments today might just have sent an alert to a large distribution list stating, "User John Smith sent an email with a malicious link." There might be confusion on who owns responsibility for this.

For example, the email team may investigate and find that email had been automatically deleted, so that was the end of concern for them. However, simply deleting the email contents doesn't remove the malicious malware from Smith's laptop.

Would the endpoint team have paid attention to this alert at all? How long would it take to even be looked at; how much employee time would the investigation take; and how much sensitive data could the malware/spyware extract in that amount of time?

Fortunately, the email security platform did an excellent job of detecting the malicious email. Adding the SOAR functionality provided additional security by utilizing the resources available to mitigate the threat automatically. A quick decision to isolate the infected laptop prevented further damage. In addition to this, it assigned a ticket to the correct response team, avoiding the ambiguity of sending alerts to general distribution lists. Even if the security team took time to respond, the laptop was secured to prevent potential data loss, and the system was able to identify additional work to provide a complete cure.

# Chapter 6

## Ten Best Practices for Cybersecurity Automation

Now that we've talked through the basics and you're ready to put your ideas in to action, we want to introduce some best practices. Keep these ten things in mind as you prepare to implement your security automation.

- » **Leverage network context:** IPAM and asset metadata help easily identify compromised devices and provide valuable information on the criticality of the compromised assets.
- » **Automate incident response:** Integrate your DDI security solution with the rest of the security ecosystem through two-way data sharing to enable automated incident response. Automating network-wide remediation stops threats faster and more efficiently than responding manually.
- » **Enrich SOAR with DDI data:** Use ubiquitous network data from DNS, DHCP, and IPAM to empower SOAR platforms and easily extend integration to other security tools.

- » **Unify policy enforcement:** Improve your overall security posture by making aggregated, accurate threat intelligence data available in real time to devices across your entire security stack.
- » **Automate threat investigation:** Look for state-of-the-art threat-investigation technologies that can automatically search threat data from dozens of sources, empowering you to investigate faster and increase analyst effectiveness.
- » **Improve ROI:** Get more value from your existing investments and make your security stack more effective and efficient by leveraging integrated DNS security.
- » **Start with what you have:** Secure your existing network and your digital transformations, such as the cloud, IoT, and SD-WAN, by leveraging the foundational security infrastructure you already have — DNS.
- » **Combine intelligence analysis:** Detect and block known threats as well as zero-day attacks by combining highly accurate threat intelligence with analytics based on machine learning.
- » **Deploy hybrid security:** Use a hybrid architecture that extends protection wherever you're deployed, provides resiliency, and tightly integrates with your on-premises ecosystem.
- » **Lighten the load:** Reduce the burden on your stretched perimeter defenses and give them back processing power by using the DNS control point as your first line for defense to block a wide range of known threats.



# BloxOne™

## THREAT DEFENSE

Unleash the Full Power of Your Security Stack

Turn the core network services you rely on to run your business into your most valuable security assets. These services, which include DNS, DHCP and IP address management (DDI), play a central role in all IP-based communications. With Infoblox, they become the foundational common denominator that enables your entire security stack to work in unison and at Internet scale to detect and anticipate threats sooner and stop them faster.

BloxOne™ Threat Defense maximizes brand protection by securing your existing networks as well as digital imperatives like SD-WAN, IoT and the cloud. It powers security orchestration, automation and response (SOAR) solutions, slashes the time to investigate and remediate cyberthreats, optimizes the performance of the entire security ecosystem and reduces the total cost of enterprise threat defense.



Learn more at:

[www.infoblox.com/products/bloxone-threat-defense/](http://www.infoblox.com/products/bloxone-threat-defense/)



# The what, why, and how of cybersecurity automation

Network security teams are struggling to stay ahead of today's pervasive, fast-moving cyberthreats. They must contend with hundreds of daily alerts, dozens of fragmented security tools, manual processes, and staff shortages — all of which slow response times and increase risk. Cybersecurity automation holds the key to stopping attacks fast. This book provides an overview of cybersecurity automation tools and strategies and how your organization can use them to defend your network more efficiently with less effort.

## Inside...

- Key trends driving cybersecurity automation
- Automation languages and tools
- The essential enablers of automation
- The benefits of ecosystem integration
- Optimizing automation solutions
- Cybersecurity automation best practices


Infoblox 

**Robert Nagy** is the Founder and CTO at DeepDive Networking.  
**Todd Christensen** is a Senior Systems Engineer at Infoblox.  
**Geoff Horne** is the Senior Manager of Subject Matter Experts at Infoblox.

Go to **Dummies.com**<sup>®</sup>  
for videos, step-by-step photos,  
how-to articles, or to shop!

ISBN: 978-1-119-57580-1  
Not For Resale

for  
**dummies**<sup>®</sup>  
A Wiley Brand

 Also available  
as an e-book



# **WILEY END USER LICENSE AGREEMENT**

Go to [www.wiley.com/go/eula](http://www.wiley.com/go/eula) to access Wiley's ebook EULA.