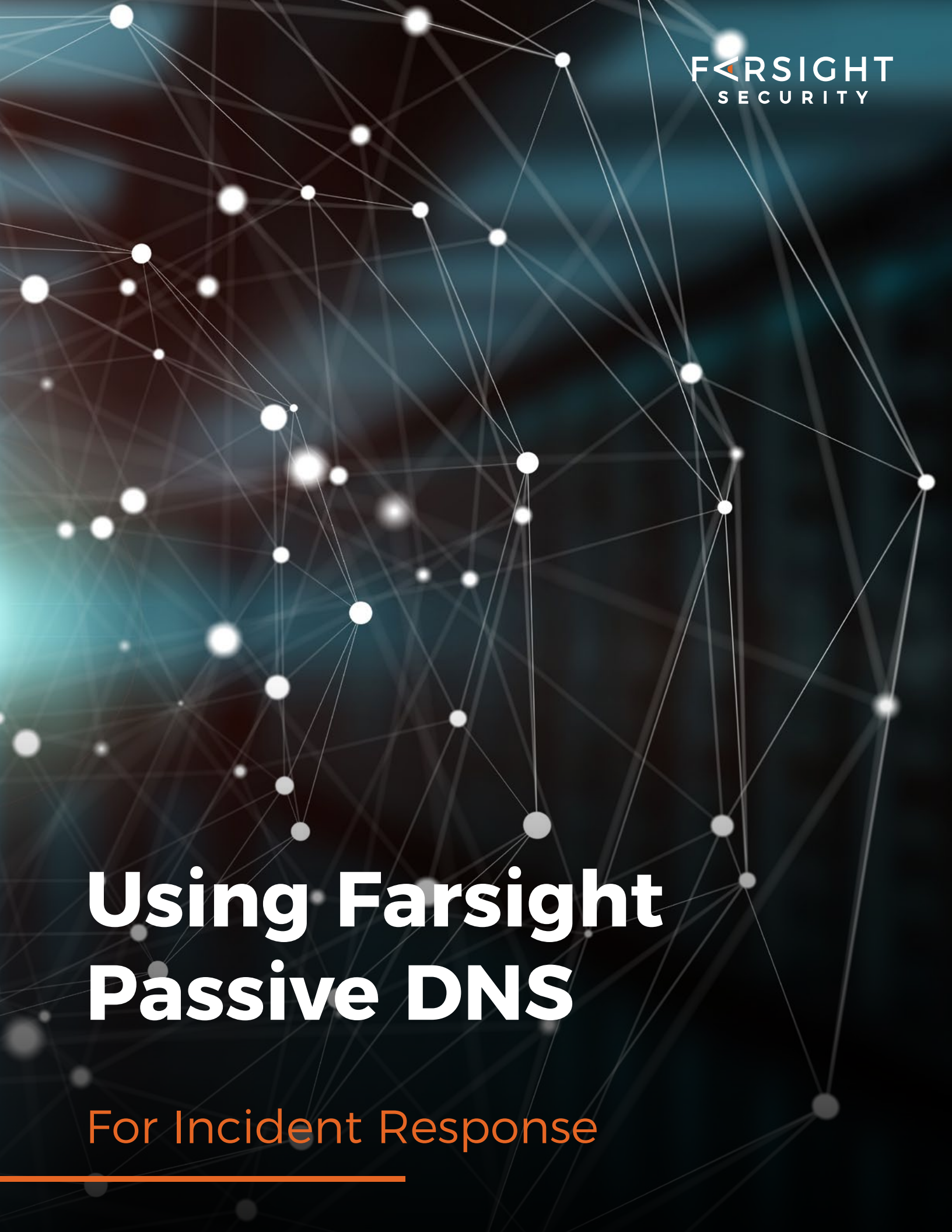


Using Farsight Passive DNS

For Incident Response

FARSIGHT SECURITY

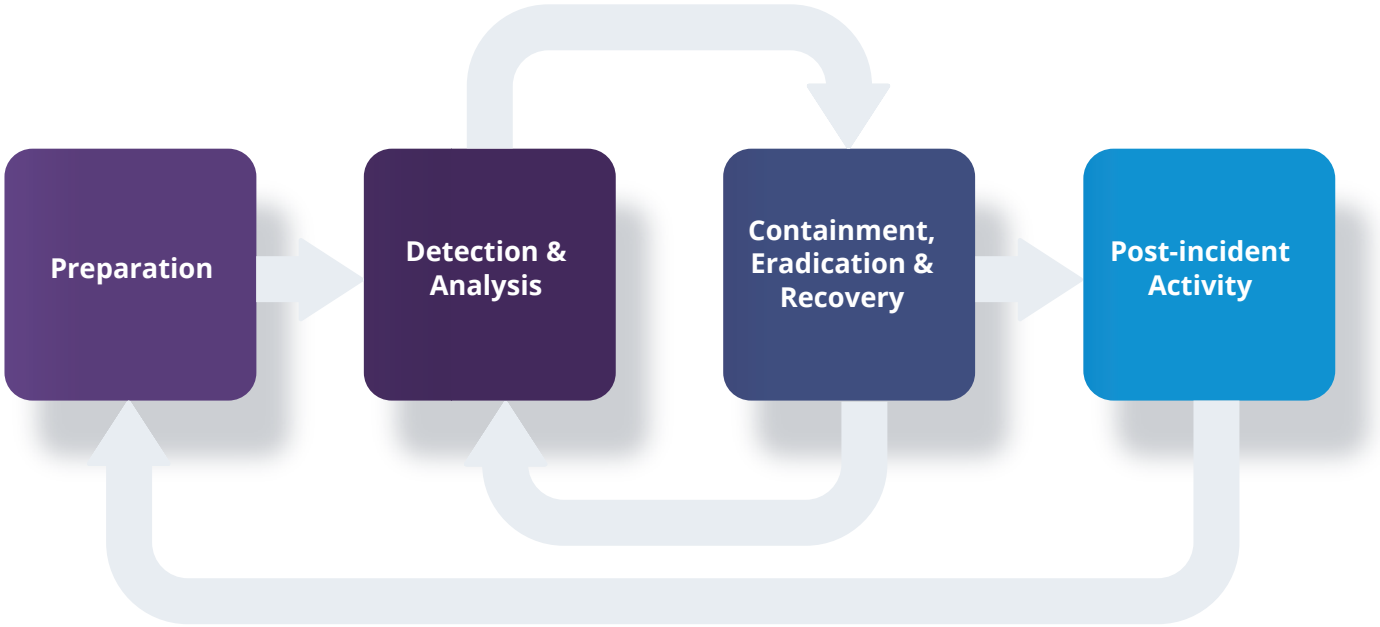
Contents

Introduction

According to the 2019 Verizon Data Breach Investigations Report (DBIR), phishing is the number one cause of data breaches. With a single click on a spoofed domain name, an unsuspecting user can provide attackers entry into a commercial or government network.

Today's threat landscape is fast-moving – cybercriminals provision, exploit and discard newly acquired DNS-related assets as quickly as they can obtain them. For example, domain names targeted for spam or phishing campaigns can be created, used in an attack, and then discarded within a period of a few minutes. Passive DNS, a proven technology used by thousands of security professionals around the world, provides realtime visibility about the DNS assets used in a cyberattack and is a must-have tool for all phases of an organization's incident response program.

In its Computer Security Incident Handling Guide, National Institute of Standards and Technology (NIST) outlines the four phases for the Incident Response Lifecycle (shown below):



Four Phases of Incident Response

FARSIGHT SECURITY

NIST Incident Response Lifecycle

Step 1: **Preparation**

While prevention is optimal, keeping the number of incidents reasonably low is very important for your organization's business continuity. Periodic risk assessments of systems and applications can determine what risks are posed by combinations of threats and vulnerabilities. It is important to have a baseline of "normal" for your network.

Step 2: **Detection & Analysis**

Organizations should be generally prepared to handle any incident, but should focus on being prepared to handle incidents that use common attack vectors such as phishing.

Step 3: **Containment, Eradication & Recovery**

After an incident has been contained, eradication may be necessary to eliminate components of the incident as well as identify and mitigate all vulnerabilities that were exploited.

Step 4: **Post-incident Activity**

One of the key activities is to leverage collected incident data. The data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the incident response team. A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends. This data can be put back into the risk assessment process.

Farsight Passive DNS for Incident Response

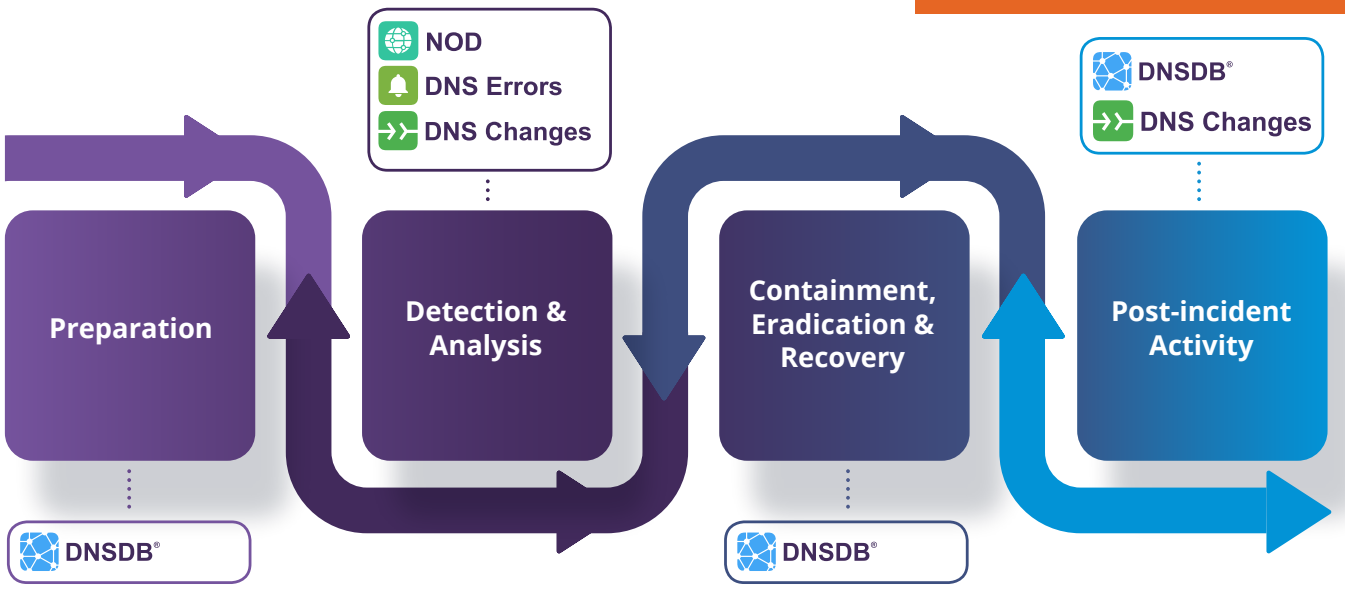
Step 1: **Preparation**

Use Farsight solutions to conduct risk assessment and prevent future attacks.

Farsight DNSDB®, our flagship historical passive DNS solution, can help organizations assess the current state – and the history -- of its infrastructure assets. It can answer questions that other security tools are unable to including:

- Where did this domain name point to in the past?
- What domain names are hosted by a given nameserver?
- What domain names point into a given IP network?
- What subdomains exist below a certain domain name?

Passive DNS or "passive DNS replication" is a technique invented by Florian Weimer in 2004 to opportunistically reconstruct a partial view of the data available in the global DNS into a central database where it can be indexed and queried. Dating back to 2010, Farsight DNSDB is the world's largest historical passive DNS database. It is used by the top Fortune 1000 organizations.



Step 2: **Detection & Analysis**

Farsight solutions can be used to detect and investigate phishing and other types of cyberattacks.

Farsight DNS Changes Organizations use Farsight DNS Changes solution to watch for changes in their IT infrastructure (classic example: substitution of hostile name servers). Whenever a new domain is created or a domain's configuration changes, the DNS Changes channel highlights that change in real-time. This lets organizations easily monitor their DNS worldwide and alert on unauthorized changes due to operational accidents — or an attack.

Farsight DNS Errors Organizations use Farsight DNS Errors for operational monitoring. For example, it can provide visibility into global SERVFAIL and REFUSED messages that are otherwise difficult to obtain for monitoring name servers. (i.e. why is my nameserver returning SERVFAIL?) DNS Errors can help network managers determine when the name servers under their responsibility are causing problems in real-time.

The Domain Name System (DNS) is one of the Internet's core protocols. DNS maps domain names (such as www.cnn.com) to numeric IP addresses (such as 151.101.20.73), and vice versa. We use the Domain Name System all the time without even thinking about it, in part because DNS seems to "just magically work" and symbolic domain names are much easier to remember than all numeric IP addresses.

Farsight NXDomains Organizations use Farsight NXDomains to reveal hostile probes (pre-attack reconnaissance). The NXDomains channel provides the ability to empirically characterize user mistakes and identify potentially valuable brand protection opportunities with similar domain names.

Farsight Newly Observed Domains (NOD) This real-time stream of domain names first observed on the Internet can be used to monitor for brand infractions or block connections to new domains often used in malware, phishing, and spam.

Step 3: **Containment, Eradication & Recovery**

Farsight DNSDB can be used for:

- Gathering evidence – While Farsight DNSDB does not collect Personally Identifiable Information (PII), it can provide visibility of an organization's public Internet infrastructure and can help identify the attacker's infrastructure (i.e. hostnames, IP addresses, etc.)
- Gain new intelligence about other attacks against your network - Cybercriminals often will share infrastructure. Chasing one bad guy, you may bump into others.
- Mapping an adversary infrastructure - Bad guys almost always use more than one IP address/domain name to:

  Protect against attack interruptions due to...
  - systems being seized/hosting services getting disabled
  - domain names being seized/put on hold
  - network connectivity getting cut, etc.

  Using multiple domains and multiple IPs can also help...
  - to "fly under the radar"/avoid looking "too prominent"
  - load balancing (some of these guys operate at *scale*)

"Whether the starting point of a customer's investigation is a suspicious domain name in an email address, an IP address or another Indicator of Compromise (IOC), Farsight DNSDB provides actionable information about these artifacts that measurably improves the time to detect and respond to the threat. We selected Farsight DSNDB over other passive DNS vendors because it offers the largest, most diverse DNS records, with the broadest geographical coverage, and its' API is easy to use. We pride ourselves for offering the best-in-breed data sources to our customers. Farsight DNSDB sets the industry standard for Passive DNS." – Ofer Padan,
VP Product, CyberInt

Step 4: **Post-incident Activity**

Once the incident data is collected, it can be used for ongoing risk assessment.

Farsight DNSDB Since Farsight DNSDB is updated in real-time, you can use existing incident indicators to continually identify potential new malicious campaigns against your organization.

Farsight DNS Changes Once the breach recovery is complete, organizations use Farsight DNS Changes solution to monitor changes in their IT infrastructure (classic example: substitution of hostile name servers). Whenever a new domain is created or a domain's configuration changes, the DNS Changes channel highlights that change in real-time. This lets organizations easily monitor their DNS worldwide and alert on unauthorized changes due to operational accidents — or an attack.

FARSIGHT SECURITY

> Farsight Security is committed to helping security professionals detect and respond to today's data breaches quickly to ensure business continuity. Farsight DNS Intelligence solutions can be used throughout the incident response lifecycle.

About Farsight Security, Inc.

Farsight Security®, Inc. is the world's largest provider of historical and realtime DNS intelligence solutions. We enable security teams to qualify, enrich and correlate all sources of threat data and ultimately save time when it is most critical - during an attack or investigation. Our solutions provide enterprise, government and security industry personnel and platforms with unmatched global visibility, context and response. Farsight Security is headquartered in San Mateo, California, USA.

Learn more about how we can empower your threat platform and security team with Farsight Security passive DNS solutions at

www.farsightsecurity.com

or follow us on

Twitter: @FarsightSecInc