VERCARA

We can’t live without DNS.

How Vercara protects your DNS and uses your DNS to protect you.

VERCARA

Agenda

1. Intros – Host & Vercara
2. Attack landscape update
3. Vercara Q2 DDoS Trends
4. DNS – can’t live without it!
5. How Can DNS and Vercara Help?
6. Quick demo

Who is Vercara?

Vercara provides a purpose-built, global, cloud-based security platform that provides layers of protection to safeguard businesses' online presence, no matter where attacks originate or where they are aimed.

Securing the Online Experience

The Attack Landscape

UK NCSC: state-aligned groups are often sympathetic to Russia's invasion and are ideologically, rather than financially, motivated. desire to achieve a more disruptive and destructive impact against western critical national infrastructure (CNI), including in the UK.

Freecycle 7million user data breach, likely an exploitation of a web app vulnerability.

Reuters, the US State Department has warned that China was capable of launching cyberattacks against critical infrastructure, including oil and gas pipelines and rail systems, after researchers discovered a Chinese hacking group had been spying on such networks.

Iranian Hackers Breach Defence Orgs in Password Spray Attacks.

Waterfall - public reports of cyberattacks with physical consequences in the Infrastructure Industries have more than doubled annually since 2020. number of attacks and the number of affected sites is increasing at a rate of 10x every 2.5 years.

chatbots, which are commonly used in online banking or online shopping, can be manipulated through "prompt injection" attacks

E-commerce websites utilizing Adobe's Magento 2 software have been under attack since at least January 2023. Attackers taking transaction info from 10 days.

Anonymous Sudan - an onslaught of cyber-attacks against Swedish infrastructure

High-Level Insights

- Largest DDoS Attack (Gbps): 873.85 (May)
- Largest DDoS Attack (pps): 157 Million (May)
- Longest DDoS Attack (duration): 16.4 days (May 7th – May 23rd)

- Average DDoS Attack (Gbps): 10.3 – **69.41% increase from Q1**
- Average DDoS Attack (pps): 2.75 Million – **30.95% increase from Q1**
- Average DDoS Attack (Duration): 89 minutes – **22.93% increase from Q1**

How Can We Help?

- UltraDNS and UltraDNS^2
- UltraDDR (DNS Detection and Response)
- UltraDDoS Protect
- UltraWAF

DNS is the answer and source!

The DNS is so old it is used in ways it was not originally designed for.

Traffic spikes can be positive, just noise, or malicious.

So be resilient, but it’s a thin tightrope between separation and feature compatibility.

UltraDNS[2,] is hosted separately, new Points of Presence, separate NOC, different provisioning, automation and routing, Staged updates, upgrades

DNS is the source and answer!

DNS Enumeration – tools to locate all DNS servers and their resource records for an org. = usernames, computer names, IPs. Finds apps / servers for future attacks.

DNS Abuse – first.org DNS-Abuse-Matrix. 21 x Techniques – domain generation,

DNSSEC – encryption and authentication for traffic – to prove who is there at each end.

For DNS security, Vercara recommends:

- Use Two Factor Authentication on the UltraDNS web portal as well as at their registrar
- Employ registrar locks when available
- Keep track of all contact and recovery emails to make sure they are company controlled, not personal emails
- Review existing accounts with registrars and others
- Ensure that you have notifications in place about expiry dates
- Monitor the issuance of any new SSL Certificates for your domains
- Enabling DNSSEC on your zone could provide an early indication of compromise

Vercara UltraDDR (DNS Detection and Response) offers a secure, scoped protective recursive DNS solution that filters internal DNS responses from users as well as machines using both definedcategories including botnet C&C as well as machine learning to detect previously uncategorized malicious associations and help prevent data exfiltration or malware detonation.

UltraDDR Make DNS your unsung hero

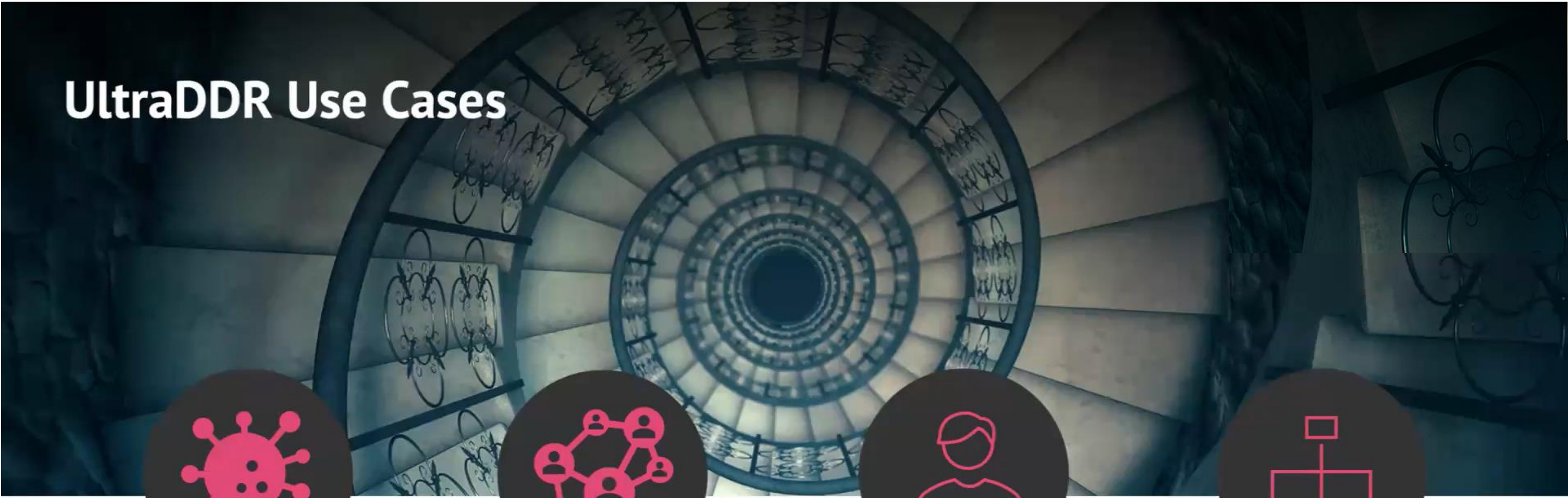
Protective DNS to protect users and devices from ransomware, phishing, supply chain compromise.

Acceptable Use Policy Compliance (Customize and easily enforce company-wide internet use policies)

Add DNS intelligence to augment and correlate with existing security investments (e.g., existing SIEM, firewalls, endpoint solutions, and more)

Secure and reliable recursive DNS

UltraDDR Use Cases



External Threats and Controls
DNS monitoring provides an enterprise-wide view as a key means to detect and expose potential security issues

DNS Anomalies
DNS logging allows the collection and analysis of DNS query and response data, which can help identify various types of DNS anomalies.

Insider Threats
Unusual DNS query behavior, such as excessive queries to suspicious domains or queries related to restricted resources, can indicate insider threats.

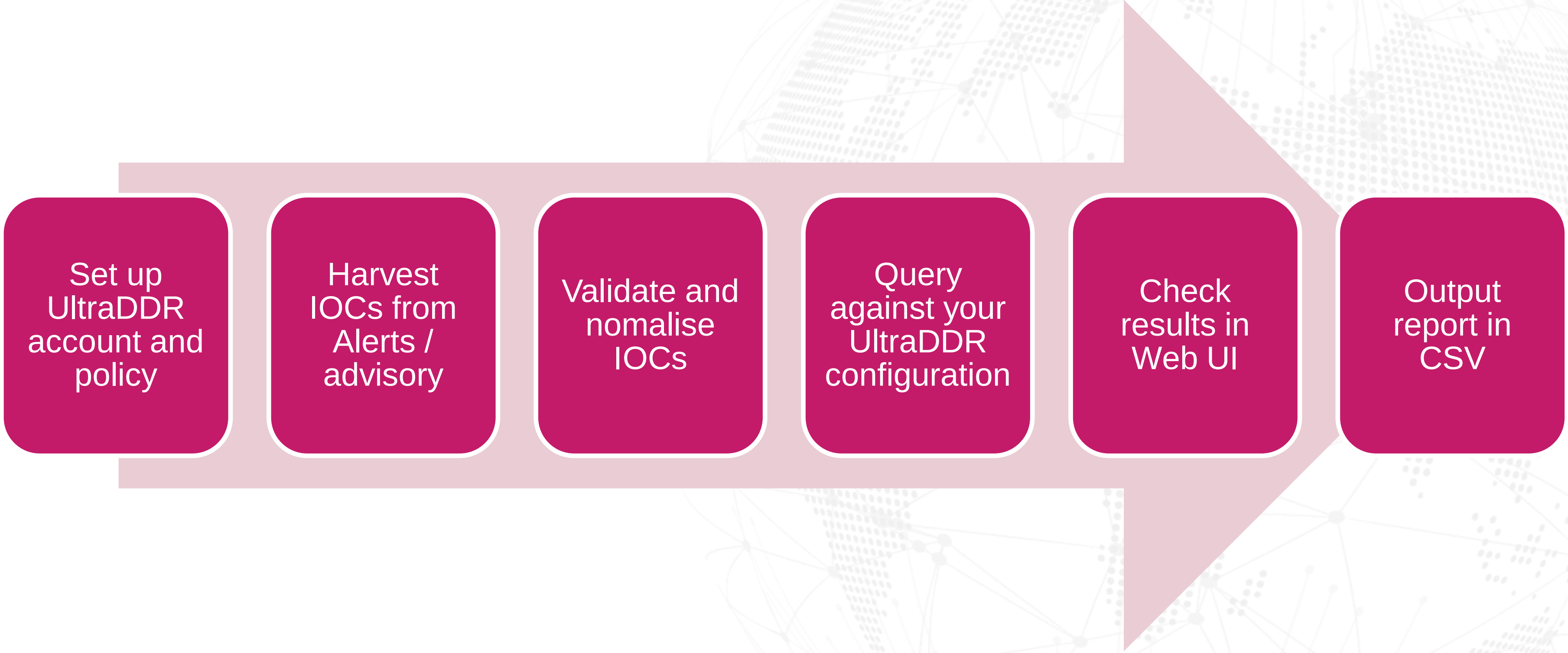
Framework and Standards Compliance
Protective DNS as a fundamental security control. Recommend its implementation as part of a comprehensive security strategy.

Threat Hunting

- Protective DNS is powered by massive amounts of historical and recent DNS Data
  - Domain Age
  - Registrar credibility
  - IP Address Reawakening

- Long Tail Domains – Filter out popular domains to identify malicious traffic
- Watch Engine - These things are under investigation and might be blocked in the future. This typically will be the brand-new FQDNs and domains.
- Known Malicious Domains – Block and identify if previously visited by users
- Categories - an engine that uses feeds of domains outside of the watch engine.

Using DNS for Analysing Indicators of Compromise



Set up UltraDDR account and policy

Harvest IOCs from Alerts / advisory

Validate and nomalise IOCs

Query against your UltraDDR configuration

Check results in Web UI

Output report in CSV

Security Operations Centre – The SOC (2.0)

Endpoint / Server protection

DLP

SWG

CASB

Firewall

SIEM

Threat Intel

Pen testing

Identity Management

CSIRT

IR – Playbooks,
Investigation Tools,
Patient Zero,
Attack reconstruction,
Hygiene,
Clean up

DNS

Secure and reliable recursive DNS
Visibility
Searchability
Enrichment
Correlation

(M)XDR

SOC Maturity =
Bring everything together
Faster TTR
Data Lakes
Proactive Security
= Lower risk
= Lower cost
= Shareholder Value

Cyber Resilience

Protective DNS

- Protecting users and devices from data exfiltration, ransomware, phishing, supply chain compromise…
- Add DNS intelligence to Threat Hunting and IR to augment and correlate with existing security investments – SIEM, firewalls, endpoint solutions, etc…
- Reliable and Secure Recursive DNS or Leverage native MDE logging

UltraDDR

DDR = DNS Detection and Response

Detection

Protect against adversary infrastructure before it's used

Continuous observability to map attacker assets, understand physical locations of attacks, and prepare proactively for new threats

Response

Prevent attackers from initiating new attacks

Mitigate in real-time to render existing intrusions inert

Watch and analyze suspicious communications to move to block or greenlight

UltraDDR demo

https://vercara.com/resources/ultraddr-demo

https://vercara.com/resources/threat-intelligence-advisory-how-to-protect-against-indicators-of-compromise

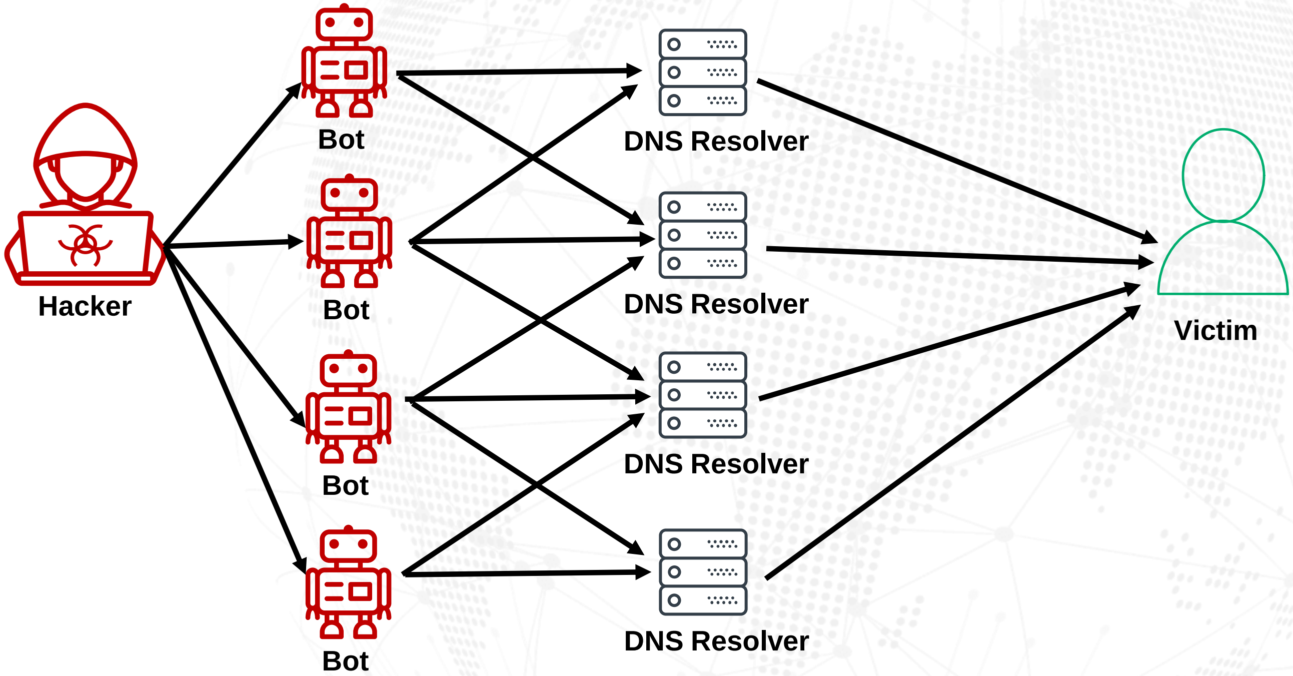
VERCARA

Thank You

What are DNS Amplification DDoS Attacks?

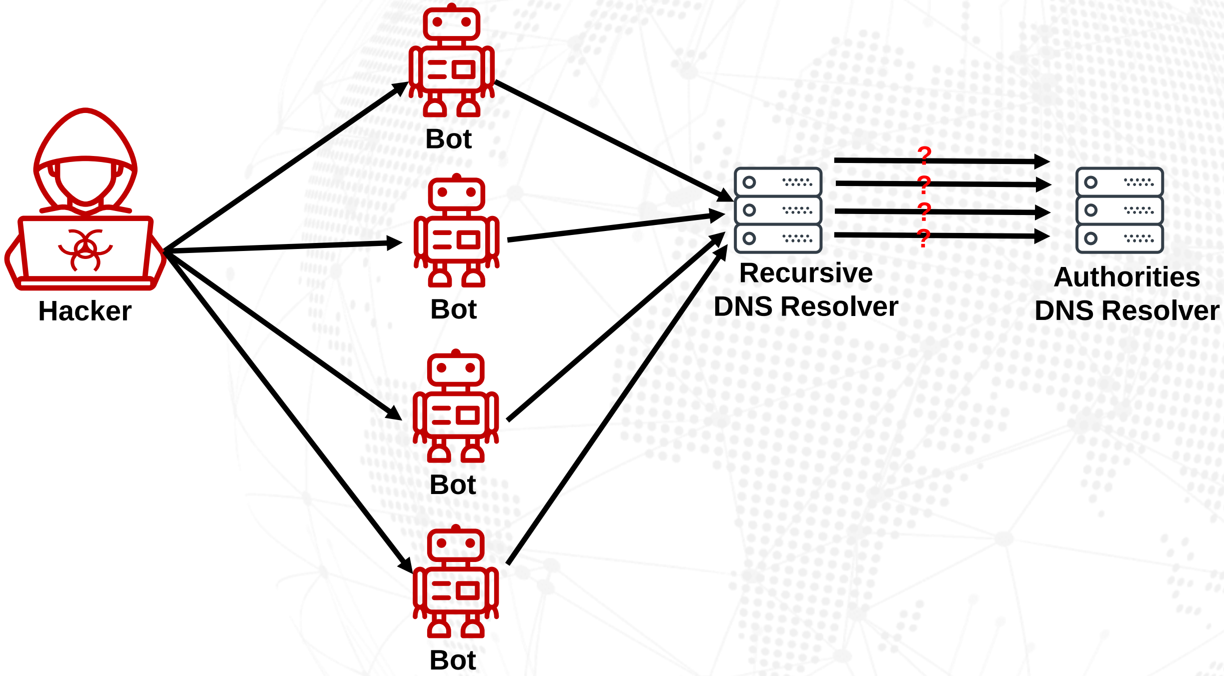
- Attacker sends large volume DNS request with spoofed source IP of the victim

- Victim receives all the responses/return traffic (DDoS)



What are DNS DDoS Attacks?

- Attacker sends significant DNS request with non-existent DNS records (ie: foo.vercara.com, xyz.vercara.com) causing resolvers to be overloaded and resources exhausted



Vercara Observed DDoS Attacks for Q2

13,567

Total DDoS Attacks

6063
April

4357
May

3147
June

4491
July

3973
August (1-27)

What Does Vercara Do?

VERCARA HAS DDOS & DNS IN ITS DNA

- 20+ year market leader in managed authoritative DNS
- 12+ year delivery of cloud-based DDoS services
- Award winning services
- 1473 years experience supporting service delivery
- Service highlights:
  - 3 of the top 5 US and 4 of the top 20 global financials
  - 4 of the top 5 streaming companies
  - Protecting multiple World Cups, Olympics, sports leagues, elections, product launches, and many other global events

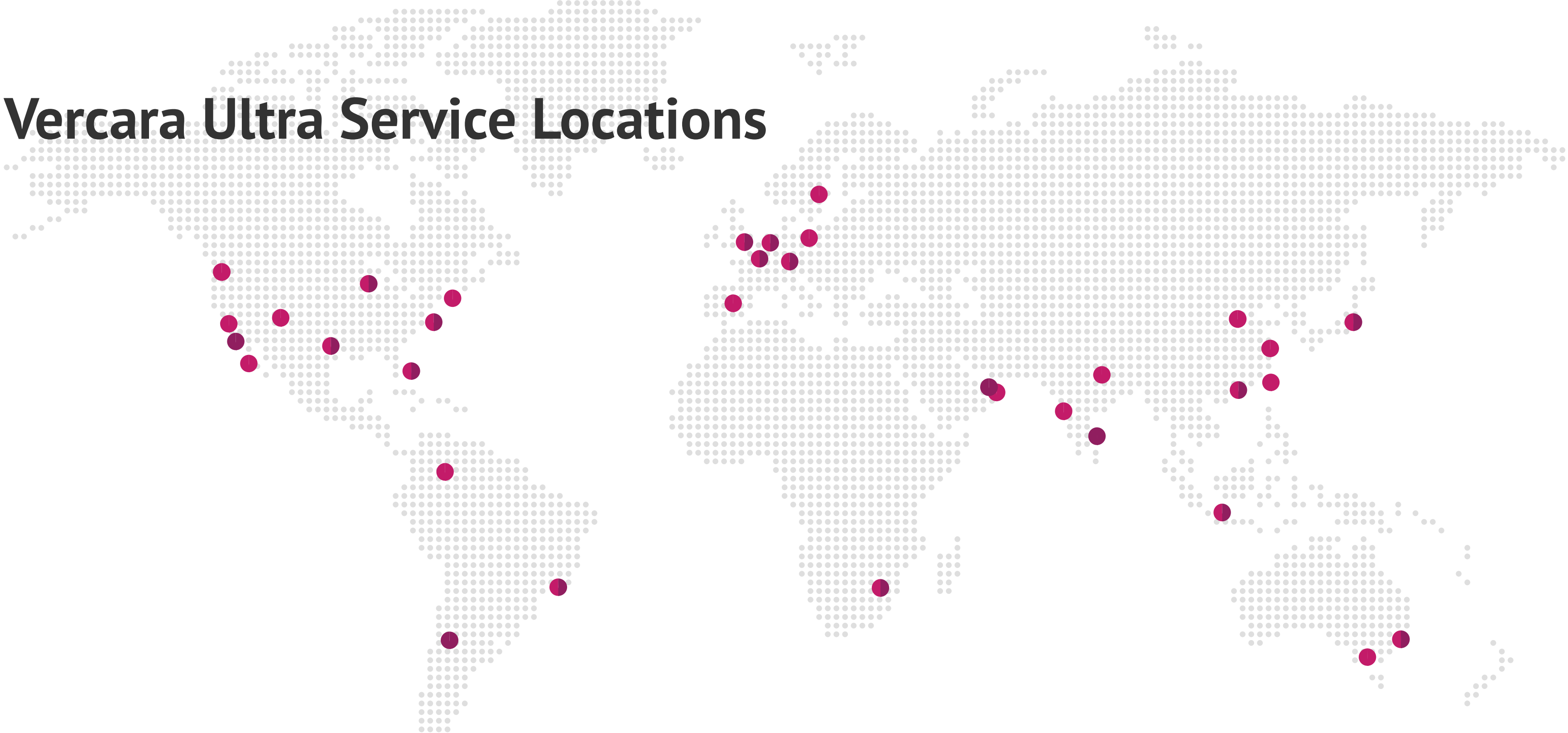
GLOBAL INFOSEC AWARDS WINNER
CYBER DEFENSE MAGAZINE
2023

- **Gold winner: Incident Response**
- **Gold winner: Managed Detection and Response (MDR)**

CYBER SECURITY EXCELLENCE AWARDS
★ WINNER ★
2023

- **Best Solution: Managed Detection and Response (MDR) Service Provider**

Vercara Ultra Service Locations



Operates a **15+ Tbps** globally distributed DDoS mitigation network.

Capable of handling **9 trillion+** Authoritative DNS queries a day.

47 DNS nodes across two distinct, discrete networks.

Presence in **20 countries**, so we operate where you are.