How to Check Site Activity & Validity with Domain and IP Intelligence Tools

Posted on April 28, 2020

In an industry that increasingly gets more competitive every day, a seller's reputation matters a lot. As personal selling is not possible online, e-commerce sites rely on several factors to establish consumer trust. Among them are reviews, which compensate for the lack of face-to-face transactions. In fact, 90% of consumers stated that positive reviews influence their purchasing decisions. Consistency in terms of the quality of one's product and services also plays a crucial role in fostering trust.

But because digital commerce is cut-throat, online merchants sometimes resort to whatever it takes to maintain their share of the profits—even if they tarnish someone else's reputation in the process. For instance, some sell replicas and pass them off as authentic items. They may also impersonate legitimate businesses on your site or manipulate product search results with blackhat marketing techniques. Finally, with the right exploit tools, some even manage to hijack someone else's brand, starting with products and the target's account.

This tutorial instructs users on performing vendor website assessments with enterprise-grade domain and IP intelligence solutions to prevent rogue sellers from abusing e-commerce platforms. But before we go on, let's first deconstruct the reasons behind website audits.

Why Conduct Website Activity and Validity Checks?

It's widely known that any site operating online faces constant security risks from external threats, such as hackers and criminal networks. Insider threats such as third-party vendors, however, can be just as worrisome.

For e-commerce sites, inactive users and illegitimate sellers hawking counterfeit products on their platforms pose significant threats to their operations. Financial losses attributed to counterfeit products, for example, cost American businesses around $200 billion per year. This amount doesn't even factor in indirect costs, such as lawsuit fees and lost revenue from poor customer experience (CX).

Such problems highlight the need for e-commerce platforms to boost their protection byconducting routine website audits. By looking into a seller's background, you can better protectyour platform's reputation. Below are a few issues you can avoid by ridding your platform ofunscrupulous sellers and third-party affiliates:

- **Advertising fraud:** Advertising fraud comes in many forms. Competitors may send you traffic from fake ads tied to spammy keywords that you did not set up. The resulting traffic could get your site penalized (if you're a third-party seller) and taken offline by search engines or, worse, the Federal Trade Commission (FTC).

- **Scam sites:** Scamming "sellers" often put up links to malicious, broken, or parked domains on their profiles with malicious ends in mind. In turn, unsuspecting users may not be able to tell the difference from legitimate sites and fall for traps.

- **Inactive or unsecured accounts:** Unfortunately, hackers may attempt to take over seller accounts that are left inactive for a long time. Some account details even end up for sale on underground marketplaces.

Domain and IP Intelligence Tools You Can Use to Check a Seller's Website Activity and Validity

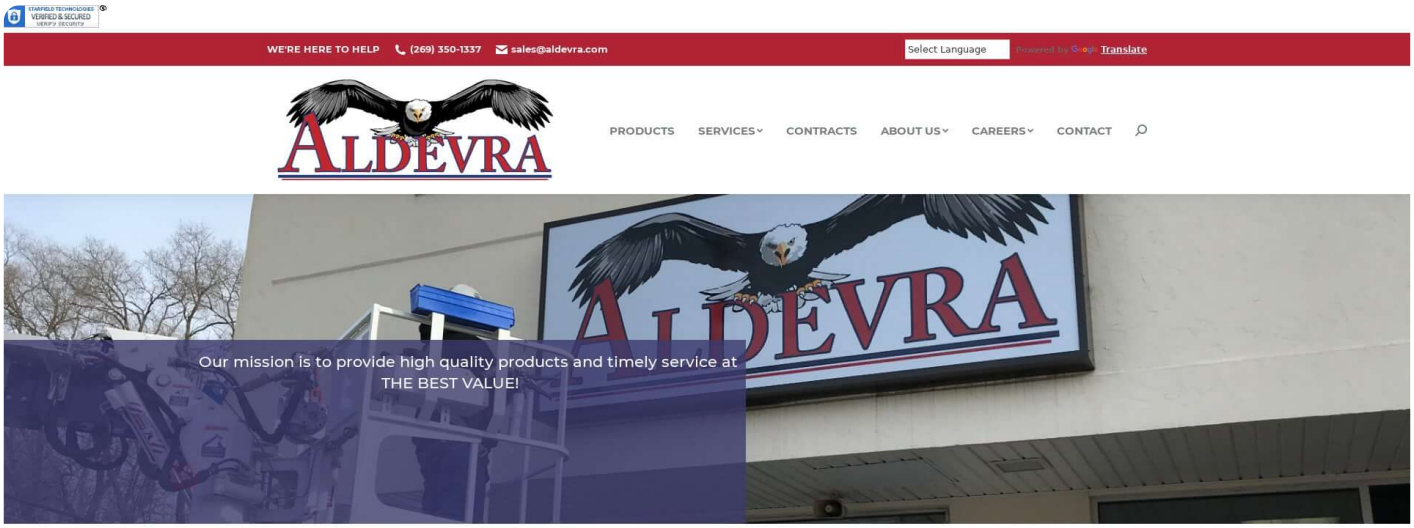
Practicing due diligence on individual sellers may be a tedious job, but the benefits outweigh the inconvenience. Below, we demonstrate how to use some domain and IP intelligence tools to help e-commerce platform owners identify red flags during seller analysis.

Screenshot API

If in doubt about the legitimacy of a seller's website, we highly recommend that you safely preview it with Screenshot API first. The program is a handy tool for finding out if a domain featured on a seller's account is parked or if a site's content matches the brand's claims.

For example, Aldevra is among the top sellers on Amazon's Appliances category. It lists aldevra[.]com on its Amazon storefront profile. Using Screenshot API, we generated a preview of

its website to show it’s currently active:



ALDEVRA IS PROUD TO OFFER COMMERCIAL FOOD SERVICE EQUIPMENT, MEDICAL EQUIPMENT, AND HEALTHCARE AND SERVICE STAFFING, SPECIALIZING IN FEDERAL GOVERNMENT PROCUREMENT.

SERVICES

HEALTHCARE

SEARCH FOR HEALTHCARE PRODUCTS HERE!

LEARN MORE ►

FOOD SERVICE

SEARCH FOR FOOD SERVICE PRODUCTS HERE!

LEARN MORE ►

STAFFING SERVICES

FIND ALDEVRA'S STAFFING CAPABILITIES HERE!

LEARN MORE ►

LOGISTICS

FIND ALDEVRA'S LOGISTICS CAPABILITIES HERE!

LEARN MORE ►

ALDEVRA'S RESPONSE TO COVID-19

EQUIPMENT & SUPPLIES ALDEVRA OFFERS TO HELP WITH CORONAVIRUS:

THERMOMETERS

Out of all thermometers except – wall mount – 3656-301 – 20 in stock now

The probe sleeves to go with this is part # 12702

https://www.riester.de/en/products/l/thermometry/

VITAL SIGN MONITORS

https://www.riester.de/en/productdetails/d/patient-monitoring/rvs-100-advanced-vital-signs-monitor/

PULSE OXIMETERS

https://www.riester.de/en/productdetails/d/patient-monitoring/ri-fox-n-pulse-oximeter/

IV STANDS:

https://pedigo-usa.com/products/infusion-pump-iv-stands/i-v-stands/

- LEAD TIME: 4 WEEKS OR LESS
- MADE IN US (WASHINGTON)

STRETCHERS WITH SIDE RAILS MADE FROM CUVERRO® BACTERICIDAL COPPER ALLOY

https://pedigo-usa.com/products/stretchers/7500-series-stretchers/guardian/

- LEAD TIME: 6 WEEKS
- MADE IN US (WASHINGTON)

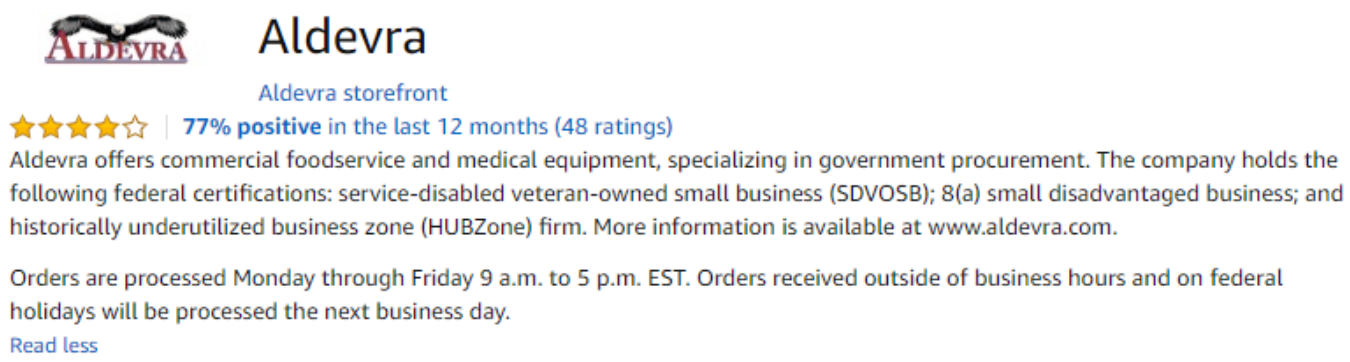
MEDICAL-GRADE REFRIGERATORS TO STORE TEST KITS (FROM 1 TO 45 CUBIC FEET)

https://www.follettice.com/healthcare/compact-refrigeration

- LEAD TIME: DEPENDS ON SIZE; STARTS AT ONE WEEK TO SHIP; LARGER SIZES 4-6 WEEKS TO SHIP
- MADE IN US (PENNSYLVANIA)

Product Name	Lead-Time
REF4-##-##-##	< 7 Days
REF5-##-##-##	< 7 Days

The screenshot reveals that the website's branding matches that of its Amazon storefront.



So far, our analysis is going in the right direction. However, we can use other tools to further confirm that Aldevra is indeed the company it claims to be.

Domain Availability API

Another quick way to check if a seller's domain is working is by running it in Domain Availability Check/API. With that tool, you can determine if a domain is still available for registration or not. If it is, the seller may be lying about having a website. The report for Aldevra's domain reveals that it isn't available—which is good news.

```
{
    "DomainInfo": {
        "domainAvailability": "UNAVAILABLE",
        "domainName": "aldevra.com"
    }
}
```


WHOIS API

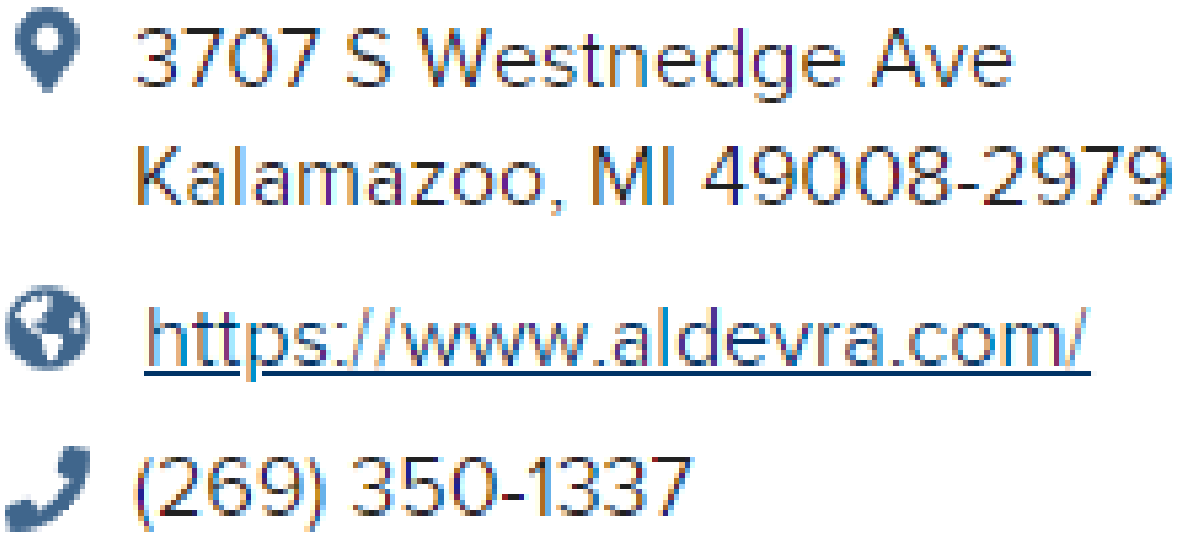
The next step is to check the domain's WHOIS records for further details. You can use WHOIS API to see if the domain's registration records match the seller's information.

With WHOIS API, we found that the domain is owned by Michigan-based Aldevra, LLC. We also discovered that the domain was set up in March 2009, as the partial report below reveals:

```
<WhoisRecord>
  <createdDate>2009-03-01T15:46:55Z</createdDate>
  <updatedDate>2020-03-02T19:12:34Z</updatedDate>
  <expiresDate>2022-03-01T15:46:55Z</expiresDate>
  <registrant>
    <organization>Aldevra LLC</organization>
    <state>Michigan</state>
    <country>UNITED STATES</country>
    <countryCode>US</countryCode>
    <rawText>Registrant Organization: Aldevra LLC
Registrant State/Province: Michigan
Registrant Country: US
Registrant Email: Select Contact Domain Holder link at https://www.secureserver.net/whois?plid=1387&domain=ALDEVRA.COM</rawText>
  </registrant>
  <administrativeContact>
    <country>UNITED STATES</country>
    <countryCode>US</countryCode>
    <rawText>Admin Email: Select Contact Domain Holder link at https://www.secureserver.net/whois?plid=1387&domain=ALDEVRA.COM</rawText>
  </administrativeContact>
  <technicalContact>
    <country>UNITED STATES</country>
    <countryCode>US</countryCode>
    <rawText>Tech Email: Select Contact Domain Holder link at https://www.secureserver.net/whois?plid=1387&domain=ALDEVRA.COM</rawText>
  </technicalContact>
```


From there, you can cross-check other data against the organization's publicly available corporate records. We consulted a reliable database such as the Better Business Bureau (BBB) to confirm other relevant details for the company.

The contact details and address below reflect that the company is associated with the domain in question. The domain's registration location also matches the address of the organization's headquarters.



As you can also see in the BBB report below, the business was incorporated on March 9, 2009 — around the same time that its domain was reserved.

Location of This Business
3707 S Westnedge Ave, Kalamazoo, MI 49008-2979

BBB File Opened:	10/3/2018
Years in Business:	11
Business Started:	3/9/2009
Business Incorporated:	3/9/2009 in MI, USA
Type of Entity:	Limited Liability Company (LLC)

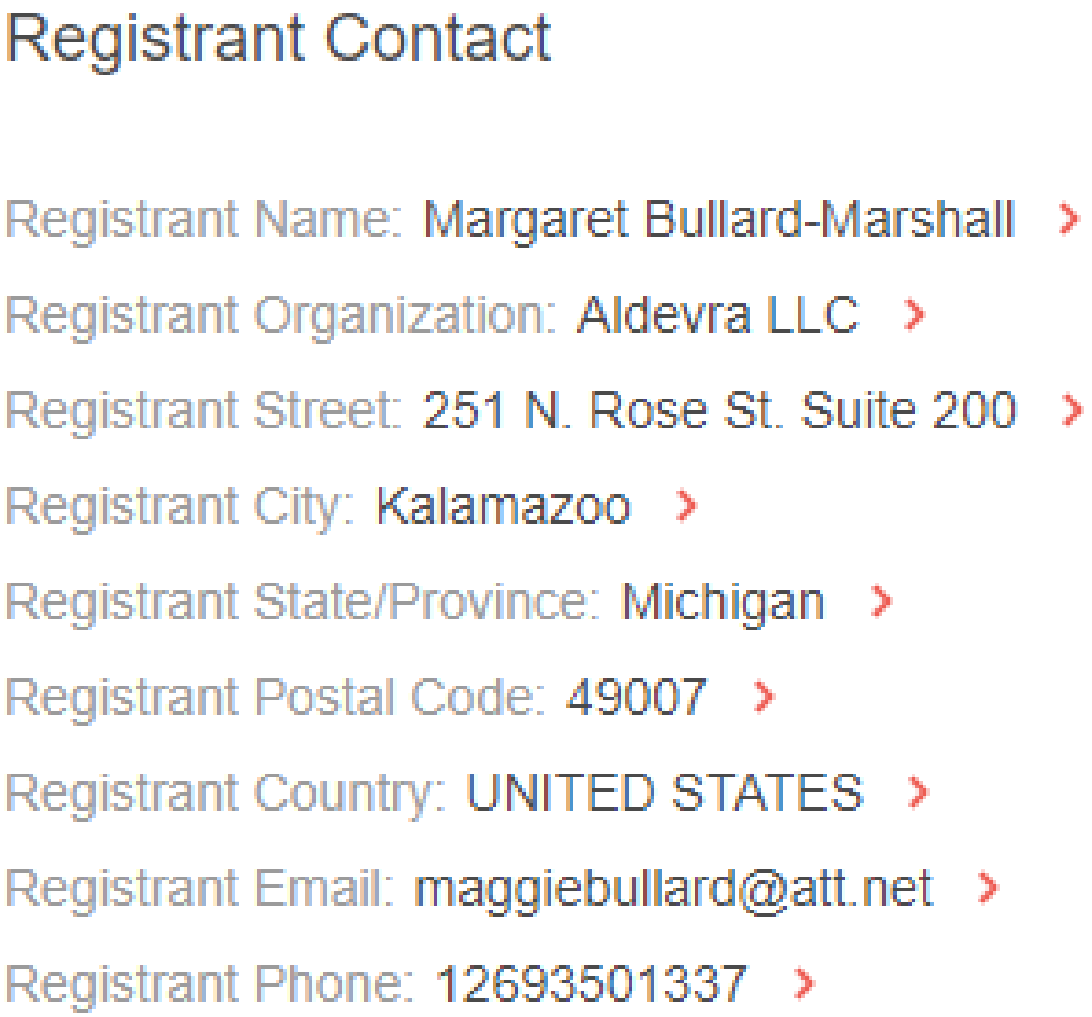
Contact Information
Principal
Josh Vance, Other

Business Categories
Medical Equipment

WHOIS History Search

There are times, however, that a domain's WHOIS records are privacy-protected. Domain intelligence tools such as WHOIS History Search make it possible to find leads by retrieving its registration history.

In Aldevra's case, we found that its domain has always been with Wild West Domains since it set up shop back in 2009. WHOIS History Search also allowed us to obtain the domain's previous registrant contact, who works with the company.



Email Verification API

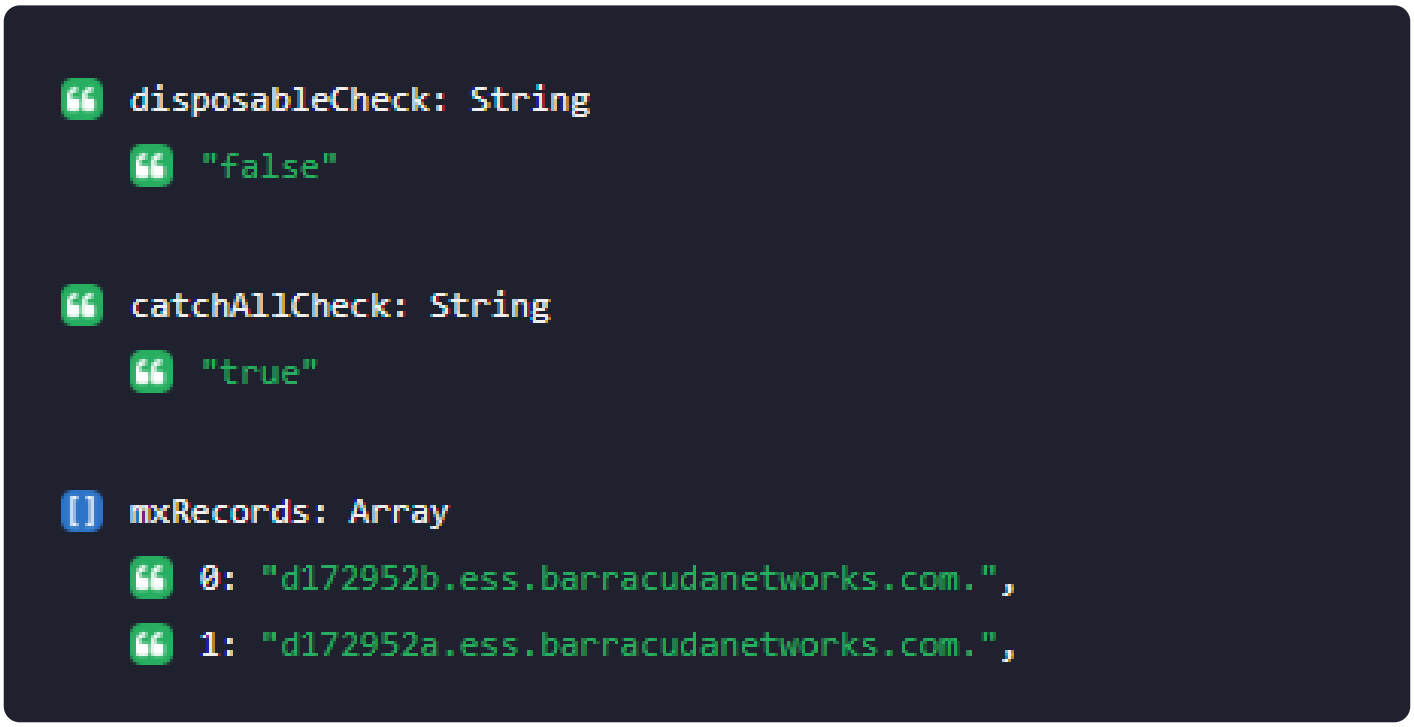
If an email address for the seller is available, you can subject it to a validity check by using Email Verification API. Any irregularities in the API's report, such as missing inboxes or mismatched name servers, could mean that the domain is inactive or has some security flaws.

For our analysis, we scanned sales@aldevra[.]com, a commonly cited email address on the

company’s online profiles, with Email Verification API. The program generated the following results:


emailAddress: String
"sales@aldevra.com"
formatCheck: String
"true"
smtpCheck: String
"true"
dnsCheck: String
"true"
freeCheck: String

The API output tells us that the email address follows the correct syntax and has no spelling errors. It also doesn't rely on a disposable email service provider.



However, the current mail server uses a catch-all email address, which accepts messages on behalf of other accounts. That isn't necessarily bad, but sending messages to catch-all email addresses could impact a mail sender's deliverability and reputation score in some instances.

What Else Can Domain and IP Intelligence Tools Tell You About a Website?

In addition to checking site activity and validity, domain and IP intelligence solutions can help to find out a great deal more about who is behind a site and what other ventures that person or organization might be involved in. It can as well point to security vulnerabilities or even ongoing

criminal activities. Let’s use our earlier example to illustrate.

Reverse WHOIS Search

Reverse WHOIS Search is a handy tool that lets users see if a domain’s owner operates other sites. For instance, it appears that Aldevra’s registrant also owns another domain, experienceeastafrica[.]info. While unavailable for registration, the domain isn’t pointing to any live sites yet, which means the owner is probably reserving it for future use.

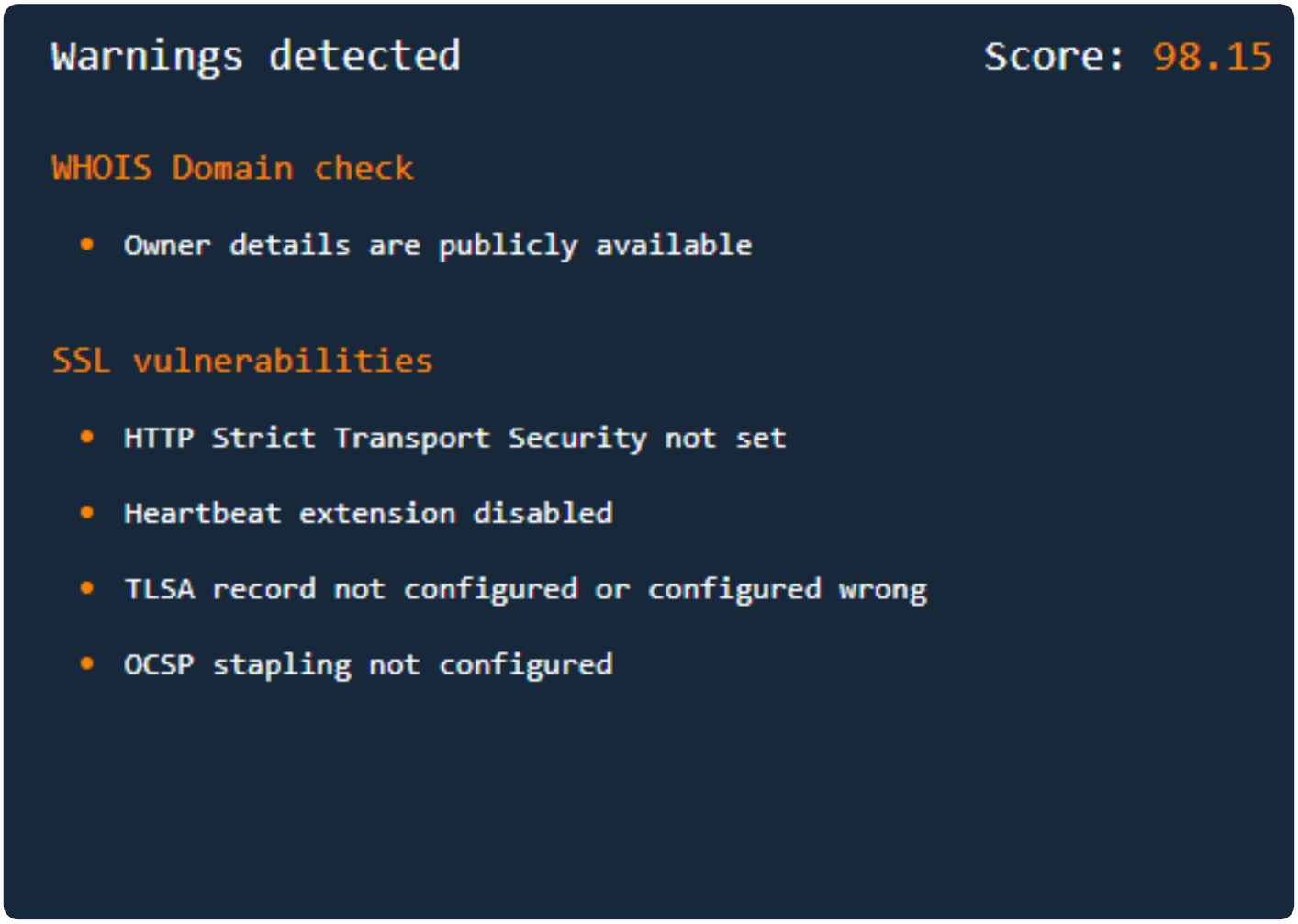
Website Contacts API

Website Contacts API is a supplementary tool that enables users to find out if the contacts indicated on a website match those found in the public domain. The report below includes the official sales@aldevra[.]com email address. We also saw an email address for a person named Maggie, which we first encountered through the domain’s historical WHOIS records.

```
<companyNames/>
<countryCode>US</countryCode>
<domainName>www.aldevra.com</domainName>
<emails>
  <email>
    <description/>
    <email>sales@aldevra.com</email>
  </email>
  <email>
    <description/>
    <email>alex@aldevra.com</email>
  </email>
  <email>
    <description/>
    <email>maggie@aldevra.com</email>
  </email>
  <email>
    <description/>
    <email>tyjon@aldevra.com</email>
  </email>
  <email>
    <description/>
    <email>rodney@aldevra.com</email>
```

Domain Reputation API

Another straightforward program that can reveal a lot about a domain's trustworthiness is Domain Reputation API. The API scans known blacklists and malware databases to determine whether or not a domain has been used in phishing or malware attacks in the past.



Aldevra's domain garnered a high score and therefore passed the API's validation. However, the tool displayed some security certificate vulnerabilities that the site's web developers may consider

looking into.

Threat Intelligence Platform (TIP)

TIP is an all-encompassing platform that enables users to conduct host configuration analysis and validate connected IP addresses and name servers from one place. It reveals other weaknesses in a website that are easily overlooked as well.

For instance, with TIP, we discovered that some of Aldevra's Domain Name System (DNS) records are not up to par with industry standards. TIP revealed the following findings, among others:

- The site has a page that redirects to another destination, which could be caused by invalid links or JavaScript codes.
- Secure Sockets Layer (SSL) settings fail to conform to Internet best practices.
- Its email address servers don't have AAAA records that specifically enable IPv6 resolution.
- The mail exchange (MX) servers don't allow Domain-Based Message Authentication, Reporting, and Conformance (DMARC) that helps prevent spoofing and phishing attacks.

You can view the full TIP report here.

Final Thoughts

Overall, Aldevra has proven that it's a legitimate brand based on its website's contents and WHOIS records. However, its records presented some minor security issues that its IT team should certainly look into.

For its part, Amazon can warn Aldevra of the latter's hosting vulnerabilities. The e-commerce giant can also observe the same risk assessment protocol that we carried out when screening future sellers.

As we've seen in highly publicized attacks, overlooked security loopholes could inflict devastating

damages on a business. However, e-commerce platforms that remain vigilant can focus more on gaining new partners and increasing their customer satisfaction. By integrating domain and IP intelligence tools into your security infrastructure, your organization can fend off dubious third-party sellers and partners.