digital shadows_

DATASHEET

PHISHING

HIGHLIGHTS

- Monitor for spoof domains, mobile apps, and social media profiles
- Track changes to domain ownership and hosting over time
- Gain the context you need to remediate phishing risks
- Launch managed takedowns from within SearchLight's phishing playbooks
- Integrate with Cisco Umbrella, Palo Alto, Demisto, or Phantom for further remediation options
- Quantify phishing risk, and demonstrate true business impact

PHISHING PROTECTION

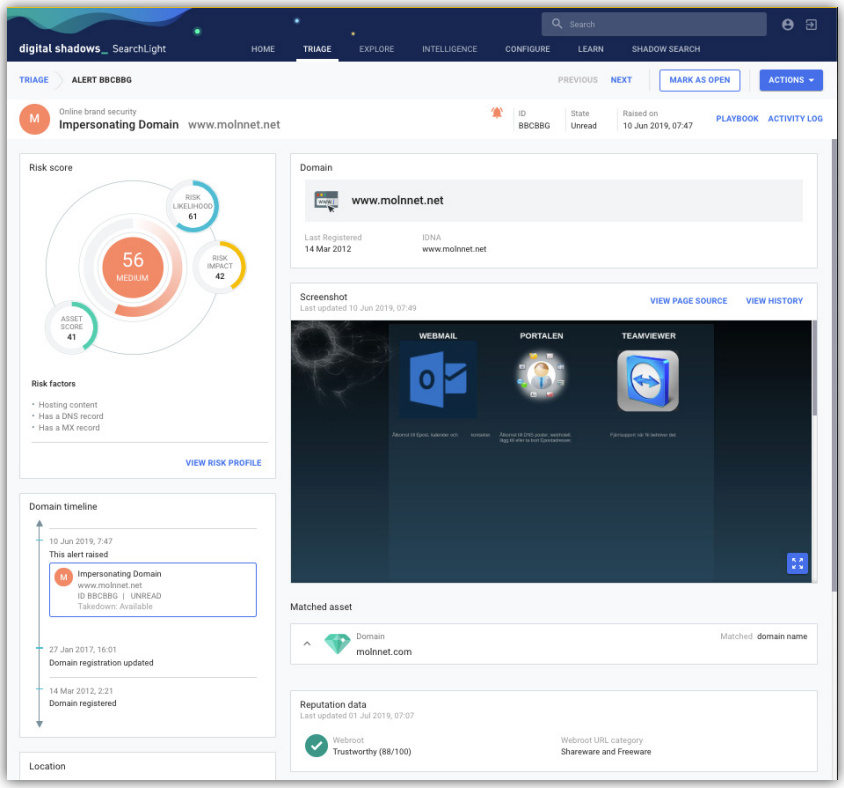
Discover attackers impersonating your domains, social accounts, people, and mobile applications.

From cybercriminals to nation-states, phishing is one of the most popular and trusted tactics. With an estimated $12.5 billion lost to Business Email Compromise, phishing has a real business impact. What's more - email is only one part of the story.

Many technologies exist to identify known malicious phishing emails, detect anomalies, or prevent email spoofing. But they do not provide the full picture - especially as organizations increasingly interact with customers and prospects online.

SearchLight looks beyond the perimeter - looking for impersonating domains, spoof social media accounts, and mobile applications targeting your customers, employees, and suppliers.

With continuous detection, vital context, and quick remediation, you can effectively disrupt their adversaries' attempts to target your employees and customers.



Example SearchLight Domain Risk Alerts

290

Annual number of impersonating domains a typical SearchLight customer detects

CONTINUOUS DETECTION

Domains

SearchLight detects typo and combo-squats across a broad range of Top Level Domains (TLDs), including internationalized domains and subdomain. On a daily basis, SearchLight analyzes millions of domains across:

- Recently registered domains from most major domain registrars
- Forward DNS feed suppliers and DNS Zone Files
- Malicious domain feeds from third parties

4M

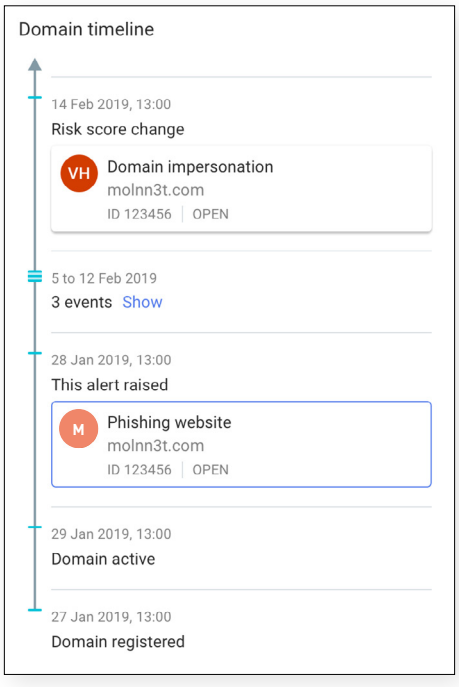
Domains Analyzed Per Day

Spoof Social Media Profiles

Unfortunately, it's not only domains that adversaries impersonate to target customers and employees. Impersonating brands and social media support accounts are popular techniques. SearchLight detects new social media handles across Twitter, Facebook and Instagram that look to imitate your brand or VIPs.

Malicious Mobile Applications

Digital Shadows discovers mobile apps that pose a risk to your organization, from out of-date apps using old branding to mobile apps that have been modified or produced by a threat actor. When possible, SearchLight automatically downloads and performs an analysis of the APK code.



The domain timeline available within SearchLight's impersonating domain risk alert

Continually Monitor and Track Over Time

By immediately detecting when new domains, social media profiles, or mobile apps appear, it can enable you to perform takedowns before the targeting of customers or employees begins.

However, it's not always possible to understand the true intent of a domain until it hosts content, creates MX records, or has a DNS record. We track all of this for you. With SearchLight's domain timeline, the domain's risk score will change - and you'll be alerted when these key risk factors change.

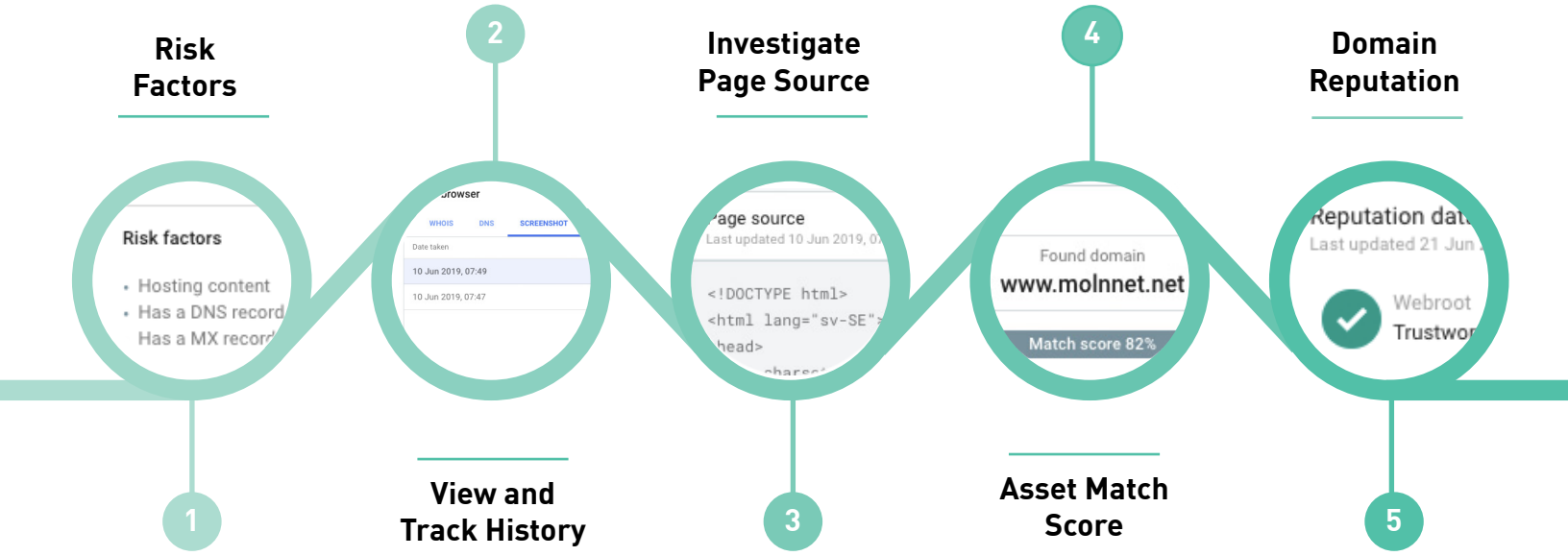
95%

Of Enterprise attacks involve successful spear phishing attempts

INSTANT CONTEXT

For every alert, SearchLight provides rich context that enables you to make better decisions, faster. Here are the top five pieces of context we draw out for impersonating domains.

1. **Identify Risk Factors**. Ascertain if the domain is hosting content, has a DNS record, or has an MX record. These risk factors combine with other observables to form a risk score and help to quickly prioritize the response to the alert.
2. **View and Track History**. Toggle through our history of website screenshots, DNS records, and WHOIS information. With this information at your fingertips, you can spend less time opening new portals, and more time responding to the alert in question. The addition of screenshot history is particularly useful; giving you a view of the content on the page, and saving you the time to visit the domain itself.
3. **Investigate Page Source**. Occasionally websites will redirect traffic, making a screenshot difficult. That's why we also provide the page source code - enabling you to investigate attributes of the site and understand if it is redirecting traffic.
4. **Asset Match Score**. Understand how similar the detecting domain is to the domain you've registered as an asset with SearchLight. Of course, assets are not limited to your domains: adding brand names and other identifiers help to increase the confidence.
5. **Domain Reputation**. View the reputation score of the impersonating domain on Webroot, and identify if the domain has previously been identified as suspicious.



QUICK REMEDIATION

Prioritize Based on Risk Score

Each alert has a risk score, derived from the threat, impact, and risk attributes to provide a risk score. These are all aligned to the Factor Analysis of Informatio Risk (FAIR) framework, enabling you to prioritize your efforts and respond more effectively.

FAIR-Aligned Risk Scores for Alerts

Playbooks for Remediating Risk

Within each alert, response playbooks guide you to the actions you should take. These playbooks are mapped to the following NIST Incident Response Plan stages:

- Detection and Analysis
- Containment, Eradication and Recovery
- Post-Incident Activity

Managed and Templated Takedown Options

Within our playbooks, we provide options to launch templated and managed takedowns. Managed takedowns provide end-to-end management of submitting, chasing, and confirming takedown requests. This empowers security teams to take action without adding cycles to their teams. Learn more about Managed Takedowns here.

Integration Options

Through our turnkey integrations with Cisco Umbrella, Palo Alto Networks, Demisto, and Splunk, organizations can automate their response blocking impersonating domains. Furthermore, we provide full access to our RESTful API - enabling you to further integrate into your technology stack. Learn about our integrations here.

Cisco Umbrella

paloalto NETWORKS

DEMISTO
A PALO ALTO NETWORKS® COMPANY

splunk> phantom

EXPLORE PHISHING WITHIN SEARCHLIGHT

About Digital Shadows

Digital Shadows minimizes digital risk by identifying unwanted exposure and protecting against external threats. Organizations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimize these risks by detecting data loss, securing your online brand, and reducing your attack surface. To learn more and get free access to SearchLight, visit www.digitalshadows.com.

digital shadows_