digital shadows_

DATASHEET

BRAND PROTECTION

## 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 brand risks
- Launch managed takedowns from within SearchLight's playbooks
- Integrate with Cisco Umbrella, Palo Alto, Demisto, or Phantom (among many others) for further remediation options

digital shadows_

# BRAND 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 used by attackers. With more than $26 billion lost to Business Email Compromise since 2016, phishing has a real business impact. By impersonating organizations' brands online, attackers can launch more convincing phishing campaigns.

SearchLight finds for where organizations' brands are exposed online - 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 and safeguard your brand.

**290**

***Annual number of impersonating domains a typical SearchLight customer detects***

**95%**

***Of Enterprise attacks involve successful spear phishing attempts***

# ALERTS

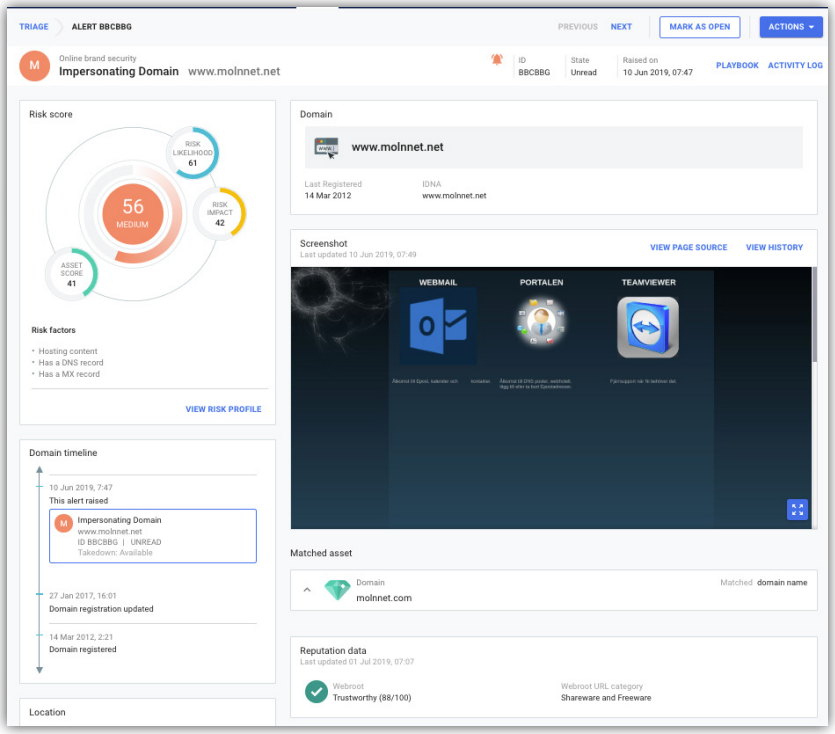
## Domains

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

- Recently registered domains from most major domain registrars
- Malicious domain feeds from third parties

## Spoof Company Social Media Profiles

Cybercriminals impersonate company social media accounts as an alternative way of targeting customers. For example, they act as the customer support representative and try to lure the customer to reveal sensitive data or visit malicious websites. By monitoring for these spoof accounts, clients can remove them before they target customers.




***Example SearchLight Domain Risk Alerts***

## Spoof VIP Social Media Profiles

Executives and VIPs present an attractive target, and impersonating these individuals can help to sow disinformation and advanced phishing campaigns. Therefore, as well as impersonating the company and it's support accounts, SearchLight also detects social media accounts impersonating VIPs in the business.

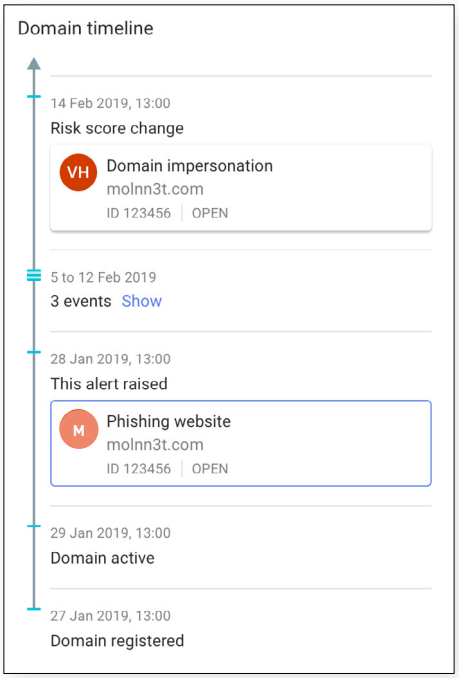
## Malicious Mobile Applications

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.

# 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, as an example.

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.




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

# 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. This methodology is aligned to the Factor Analysis of Information 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 technologies like Cisco Umbrella, ServiceNow, 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

splunk> phantom

servicenow

DEMISTO
A PALO ALTO NETWORKS® COMPANY

**EXPLORE 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_