DATASHEET

ATTACK SURFACE MONITORING

HIGHLIGHTS

- 22,000 new vulnerabilities reported in 2018
- Only 29% of organizations believe they sufficiently understand their attack surface
- The average SearchLight customer receives a manageable 360 infrastructure alerts per year
- Continuously identifies exploitable vulnerabilities on external-facing applications
- Identify certificate issues before they create a business problem

digital shadows_

ATTACK SURFACE MONITORING

Gain an attackers-eye-view of online infrastructure

As an organizations' infrastructure grows and becomes more complex, it can be difficult to keep up with expanding attack surfaces. Indeed, only 29% of organizations believe they have sufficient visibility into their attack surface.[1] Attackers are aware of this and frequently look to exploit public-facing applications as part of their campaigns. As many public breaches have demonstrated, when these are not remediated in a timely manner, it can lead to a great deal of brand and financial damage to the organization.

Security teams seeking to identify and asssess weaknesses in their infrastructure may turn to a range of tools. While it's easy to perform a vulnerability scan against known assets, ascertaining what is the highest priority is difficult. Worse still, it's difficult to keep track of the infrastructure you are trying to protect.

SearchLight identifies the most critical risks you need to care about, such as vulnerabilities on your external infrastructure with known exploits. Each comes with clear remediation advice; enabling you to continuously detect and remediate.

71%

Of organizations do not have sufficient understanding of their attack surface[1]

1. Bridging the Digital Transformation Divide, Ponemon Institute, 2018

360

Infrastructure issues detected on average per year, per client

22k

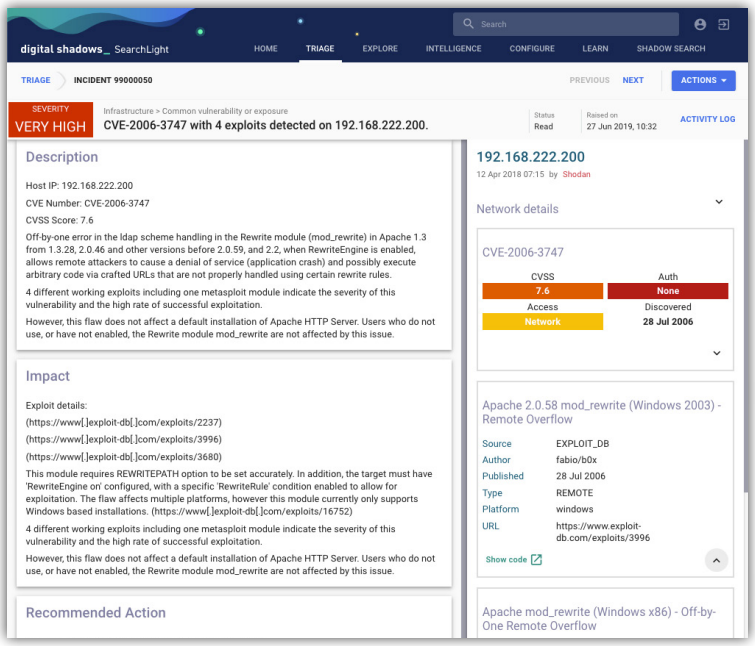
Vulnerabilities disclosed in 2018

ALERTS

Exploitable Vulnerabilities

Major vulnerabilities in your infrastructure that have active exploits and allow for remote code execution are quickly exploited by by threat actors. One of many examples is the 2017 Equifax Breach, where attackers utilized a vulnerability in the Apache Struts software to gain valuable data on millions of customers and employees.

Identifying these exploited vulnerabilities and prioritizing them based on the level of risk can be extremely difficult. SearchLight continually identifies these vulnerabilities, maps them with the severity of exploitation, raises alerts, and provides remediation options to protect your organization.



Example SearchLight Vulnerability Alerts

Certificate Issues

Expiring, revoked, insecure or vulnerable SSL certificates and configurations can have real impacts on your organization. With SearchLight we monitor the exposure of these certificates and help you to identify risks surrounding them that threaten business operations.

Open Ports

Exposed ports offer a route to compromising your network and pose a significant risk. SearchLight helps to identify these ports and reduce your attack surface, thereby helping secure your digital footprint.

This includes the ability to identify open files stores, such as SMB, that are exposing data on your infrastructure. If there are misconfigured, publicly-accessible file services on your infrastructure, we'll detect it and provide you the context you need to remediate it in a timely manner.

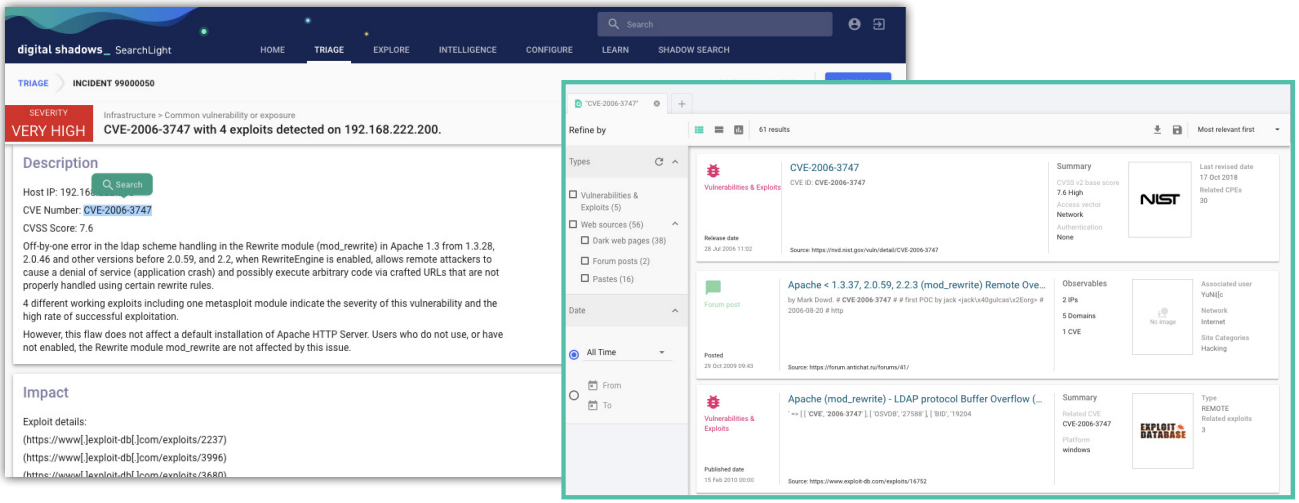
UNDERSTANDING THE THREAT LANDSCAPE

One of the most popular tactics of threat actors is the exploitation of publicly-facing applications. Many vulnerability databases focus on a score that outlines how technically exploitable it is – not if it has been exploited by threat actors. Unfortunately, this means that organizations are challenged with prioritizing thousands of vulnerability patches every year. SearchLight focuses on those vulnerabilities which a) have been exploited by threat actors and b) are remote code execution (RCE) vulnerabilities. This enables you to prioritize which ones pose the biggest threat to your organization so you can proactively mitigate those threats.

We provide the most important context within alerts, but also enable pivoting in to Shadow Search to provide further enrichment and access our finished intelligence reporting.

CVE Enrichment and Prioritization

Get high priority alerts that related to genuine threats to your network infrastructure - not a deluge of CVEs (Common Vulnerability and Exposures). Furthermore, users can pivot off those CVE numbers into Shadow Search and identify where they are discussed across criminal locations, paste sites, and more. Accessing the dark web is difficult – we make it easy.



Analysis of Latest Attacks

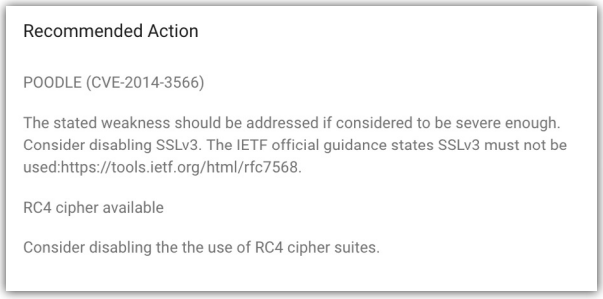
Our team of analysts look at and assess the latest within the threat intelligence world. From new proof of concepts and vulnerabilities, to the threat actors exploiting them - you can access this all from within the Intelligence section of the portal. For example, with breaking vulnerabilities like BlueKeep or EternalBlue we'll look for the latest proof of concepts and developments so you can be up to speed.

REMEDIATION

With your internet-facing applications understood and prioritized, the next step is to remediate the issue. Our alerts provide clear remediation advice, and alert details can be integrated into a range of technology solutions.

Mitigation Advice

Each alert comes with clear, actionable advice into remediating the risk. As an extension of your team - we provide the context you need to make security decisions. With the threat landscape evolving constantly, we stay on top of the latest with threat actors, tactics, techniques, procedures, and motives - and then couple that knowledge with the vulnerability to provide you relevant mitigation advice.



API Integrations

All of our intelligence and alerts is easily consumable within the SearchLight platform, but also through our rich integration ecosystem. Whether you're using a SIEM, Ticketing, or Threat Intelligence Platform, you can consume our information in a way that best suits your needs.

Learn more about our integrations here: https://resources.digitalshadows.com/digital-shadows-integrations.

VIEW 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.