The Source of Security

5 Data Sources All Analysts Should Consider

MeriTalk
The Government IT Network

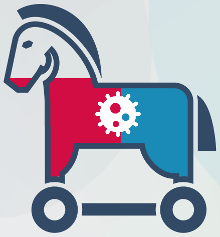
Underwritten by

splunk>

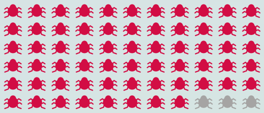
Government cyberattacks are on the rise...

Governments were the **NUMBER ONE** most preferred target for cyber attackers in 2014[1]

Federal agencies reported nearly **70,000** information security incidents in FY 2014 – up 15% from FY 2013[2]

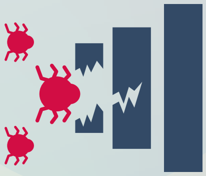


Over **95%** of agencies have at least 10 malicious infections bypass security mechanisms each week –

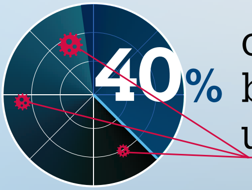


80% experience more than 100 new infections each week[3]

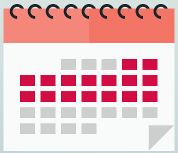
Since 2006, there have been more than **87 million** sensitive or private records exposed by breaches of Federal networks[4]



...but the majority of threats aren't even on the radar...



40% of government breaches go undetected[5]

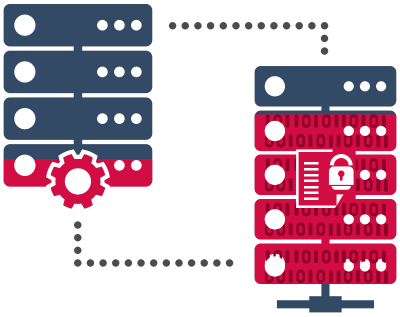


Cyber threats go undetected for an average of **16 days** on government networks[6]

The Worst Part...?

Many of these attacks could be mitigated if the right data was analyzed

Organizations only analyze **12%** of their data[7]



78% say at least some of their security data goes unanalyzed due to a lack of time and or skill[8]

It's time for agencies to uncover the threats hiding in the shadows.

[1] http://hackmageddon.com/category/security/cyber-attacks-statistics/ | [2] https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf | [3] http://www.chippewa.ca/wp-content/uploads/2013/09/Cyber-Attacks-on-Government-White-Paper.pdf | [4] http://www.huffingtonpost.com/2014/11/10/cyberattack-government-computers_n_6131134.html | [5] http://freebeacon.com/national-security/report-4-in-10-government-security-breaches-go-undetected/ | [6] www.meritalk.com/go-big-security | [7] http://go.centurylinktechnology.com/2014ForresterBigDataWhitepaperPage | [8] www.meritalk.com/go-big-security

Data for Defense: The TOP 5 Security Data Sources All Analysts Need to Consider

Security data analysis helps agencies effectively prevent and remediate cyber threats. However, key data sources are often neglected.

1 Proxy Logs

- **Reality:** 73% of browser-based attacks are from anonymizer proxy websites[9]
- **Importance:** See where and how the attacker moved and communicated within an infected host
- **Benefit:** Uncover Web-based attacks, browser attacks, injections, session hijacking, and data exfiltration. Source for pre-compromise and post-compromise analysis

2 Virtual Private Network (VPN) Logs

- **Reality:** Majority of attackers look for remote access to infiltrate a network
- **Importance:** See what deploys, where it comes from, and what IP addresses communicate with networks. View who is remotely logged into an environment on a day-to-day basis
- **Benefit:** Expose Advanced Persistent Threats (APTs)

3 Vulnerability Scan Data

- **Reality:** From 2013-2014, the number of security vulnerabilities rose by **46%**[10]
- **Importance:** Identify which host on your network is the most vulnerable, import data about assets, vulnerabilities, and patches
- **Benefit:** Discover APTs

4 Dynamic Host Configuration Protocol (DHCP) Logs

- **Reality:** Attackers need a DHCP lease to access a Wi-Fi network
- **Importance:** Monitor systems assigned to IP addresses – identify which IP addresses were used, and for how long
- **Benefit:** Reveal network-based attacks. Potential post-compromise analysis

5 Mail Logs

- **Reality:** 69% of all security incidents reported to US-CERT in 2013 were attributed to phishing[11]
- **Importance:** Review inbound/outbound mail for malicious links, unauthorized files, and bad attachments
- **Benefit:** Identify APTs

Situational Awareness: The Full Picture

Threats come from all angles. To see the full picture, start at the source – security data analysis helps provide a comprehensive view of threat risk and activity.

- Detect, mitigate, respond to, and predict cyberattacks
- Correlate threat attacks and malicious activity both internally and externally
- Create situational awareness of advanced threats

Listen To Your Data – Learn More

ALL DATA IS SECURITY RELEVANT

To learn how your agency can use big data to improve security outcomes, visit
http://www.splunk.com/cybersecurity

For more information,
please call **1.866.GET.SPLUNK**,
email fed_sales@splunk.com,
or visit www.splunk.com/publicsector.

[9] http://www.continue.uottawa.ca/uploads/File/Symantec_Cyber_Report_2014.pdf | [10] http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/ | [11] http://archive.federaltimes.com/article/20141024/CYBER/310240013/-Spear-phishing-tactics-becoming-more-sophisticated