splunk>

Government Cybersecurity Pros are Lost in an Ocean of Data

Big Data Analytics Helps You Navigate the Waves of Security Threats

Government organizations are facing a tidal wave of cybersecurity threats

The ones they can see

The most common cyber breaches among government agencies in the last **12 months**

- **62%** phishing
- **42%** inadvertent misuse by insider
- **26%** loss/theft of asset
- **17%** malicious abuse by insider
- **13%** misuse by business partner or third-party supplier
- **10%** SQL injection

And the ones they can't

The average cyberthreat exists on government networks **16 days** before cybersecurity teams identify it

40% of government breaches go undetected*

While cybersecurity is a priority, agencies are still missing the opportunity of big data analytics

92% are working to improve cybersecurity

65% are investing in security technologies

51% are deploying network analysis and visibility solutions

50% are investing in training for personnel

Agencies can use big data analytics to help them mitigate cybersecurity risk and navigate an ocean of security data

68% of cybersecurity pros say their organization is overwhelmed by the volume of security data

76% believe their cybersecurity team is often reactive instead of proactive

believe big data analytics would significantly improve their agency's cybersecurity

With data volumes rising agencies need help even more than ever to keep on top of security with limited resources

say at least some of their security data goes unanalyzed due to a lack of time or skill

are hiring new security staff

Big data analytics makes it safe to go in the water

Government cybersecurity pros who say they can detect 90% of cyber-incidents before they become harmful

40% today

56% with big data analytics

9 OUT OF 10 Big data analytics will significantly improve cybersecurity almost 9 out of 10 times

4 reasons to use big data analytics for cybersecurity

1. Detect breaches that are currently happening
2. Monitor streams of data in real time
3. Identify a breach that has already occurred
4. Conduct a conclusive root cause analysis following a breach

5 ways to use Splunk for cyberthreat analysis

1. Perform research on adversarial threats posed to systems, operations and missions
2. Analyze collected data to derive facts, inferences and projections concerning attacks
3. Use context to more accurately determine false-positives and false-negatives
4. Identify attacks by piecing together snippets of abnormal behavior spread over time and across systems
5. Contribute to profiling adversarial behavior

Learn how big data analytics can help navigate the waves of cybersecurity.
www.splunk.com/cybersecurity

Sources:
Except where noted all information is based on a survey of 302 government cybersecurity professionals from federal, state and local agencies/organizations conducted by MeriTalk in April 2015
Access the survey report at: http://www.meritalk.com/go-big-security.php

* "Report: 4 in 10 Government Security Breaches Go Undetected," The Washington Free Beacon, February 5, 2014, http://freebeacon.com/national-security/report-4-in-10-government-security-breaches-go-undetected/; sourced from "The Source of Security," MeriTalk, 2015, http://www.meritalk.com/source-of-security.php

splunk> listen to your data