74% of companies believe they will be the target of an APT attack.*

Is your organization doing enough to fight this threat?

CyberSentinel **detects complex cyber security threats** that traditional security methods can't. It combines state-of-the-art techniques like

- *advanced machine learning,*
- *statistical analysis, and*
- *proprietary algorithms*

to fight APTs, insider threats, and other types of sophisticated attacks.

CyberSentinel is a **next-generation** weapon in the cyber security arsenal that will work on top of the tools you already have, decreasing your information security risk and reducing your management costs—all with an impressive time to value, since **CyberSentinel can go from installation to production *in just a week*.**

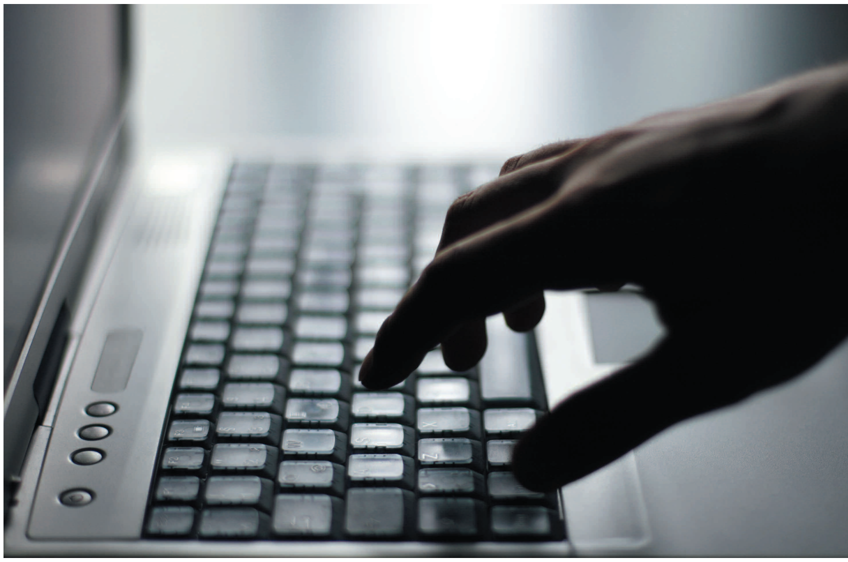
** ISACA Study, 2015 Advanced Persistent Threat Awareness—Third Annual, Oct. 2015.*

www.jeskell.com/cybersentinel

Executive Overview

You can build a higher wall. You can dig a deeper moat. You can lay a thousand trip wires—but a stealthy, well-funded attacker will still find a way into any fortress.

For most organizations, these kinds of attacks are already happening. If you want the ability to disrupt these attacks mid-strike, then you need more than just cyber security. You need a cyber **sentinel** to keep watch.



A sentinel may not know exactly what it's looking for, but it'll know when something's out of the ordinary. Unlike static walls, moats, and trip wires, **a sentinel has the ability to learn the norms** of its environment. And it will know that abnormalities—even if they *seem* harmless—may indicate an underlying problem.

That's how CyberSentinel works. Unlike standard cyber security practices like firewalls, IPS and IDS, signature-based analysis, encryption, and log management systems—all crucial elements of cyber security—CyberSentinel has the ability to do *more*. Through a combination of advanced machine learning, state-of-the-art analytics software, and proprietary algorithms developed by IBM Research, CyberSentinel learns the norms of its environment so that it can detect anomalies. This allows it to identify unusual activity on the network and adapt to changes as the organization itself changes.

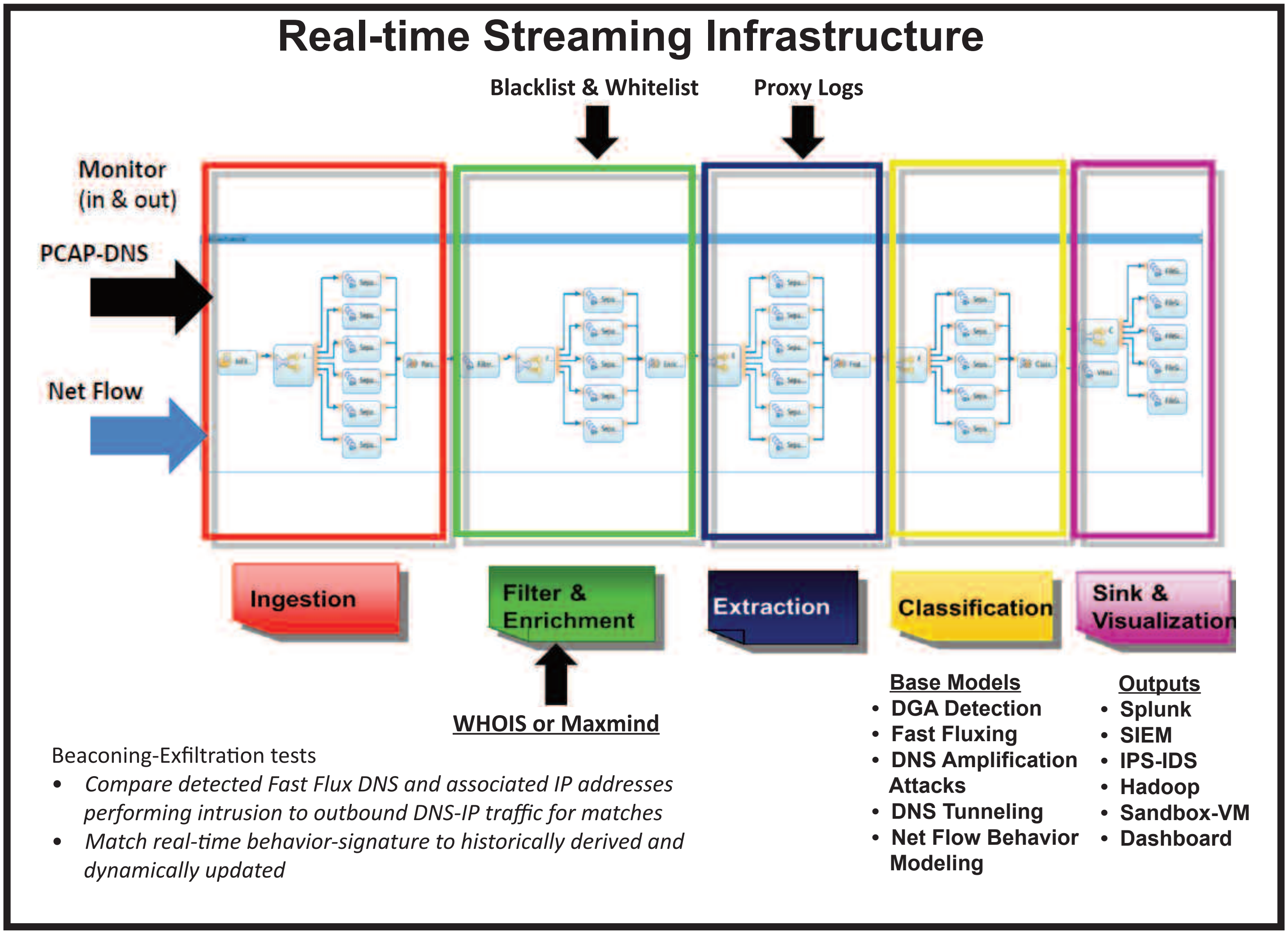
So if your business has made the investment to ***keep threats out***, now is the time to make sure you invest in detecting threats ***once they're already in***.

This is more than rules and signatures. This is next-generation. *This is CyberSentinel.*

How It Works

IBM Analytic and Big Data technologies form the core of CyberSentinel. These market-leading and mature technologies are designed to enable security specialists to conduct proactive network defense with a system that is optimized for cyber security. CyberSentinel features the following components:

- ***Modeling Framework** based on IBM SPSS Modeler 16 and InfoSphere Streams SPSS Analytics Toolkit for the creation of new custom models like Time series, Regression, Clustering, Association, & more*
- ***Machine Based Learning Models** for cyber, including: Fast Fluxing, beaconing and exfiltration detection, DNS tunneling, Domain Generation Algorithm (DGA) detection, DNS amplification, and Deep Packet Inspection*
- ***Big Data Analytics Interoperability** with many of the popular big data repository and cyber solutions, including: IBM InfoSphere BigInsights, IBM QRadar, Cloudera, Hortonworks, Accumulo, Mongo DB, Splunk/Hunk, and HP ArcSight*
- ***Rich Toolset** that provides ease-of-use and advanced streaming computing environments for real-time analysis of data in motion like predictive analytics, data mining, advanced visualization and diagnostic analytics*



Real-time Streaming Infrastructure

Base Models

- DGA Detection
- Fast Fluxing
- DNS Amplification Attacks
- DNS Tunneling
- Net Flow Behavior Modeling

Outputs

- Splunk
- SIEM
- IPS-IDS
- Hadoop
- Sandbox-VM
- Dashboard

Beaconing-Exfiltration tests

- *Compare detected Fast Flux DNS and associated IP addresses performing intrusion to outbound DNS-IP traffic for matches*
- *Match real-time behavior-signature to historically derived and dynamically updated*

Image: CyberSentinel real-time streaming architecture

Network Behavior Monitoring & Visualization

CyberSentinel includes pre-trained **Behavior Models for DNS Traffic analysis**, as well as **Netflow Anomaly Detection** to search for Netflow and DNS anomalies over long periods of time (unlike more traditional cyber security tools, which are limited to short term detection). Also included is the necessary **software and pre-configured connections** to automatically deploy cyber security predictive models to a streaming environment, providing real time risk detection across your network traffic. Once a predictive model has been built, tested and validated, it is made available via the included analytical asset repository. With this repository, models can be activated to monitor network data and provide risk scores relative to known or unusual patterns.

Jeskell Systems
CyberSentinel
Supervised
Machine Lear

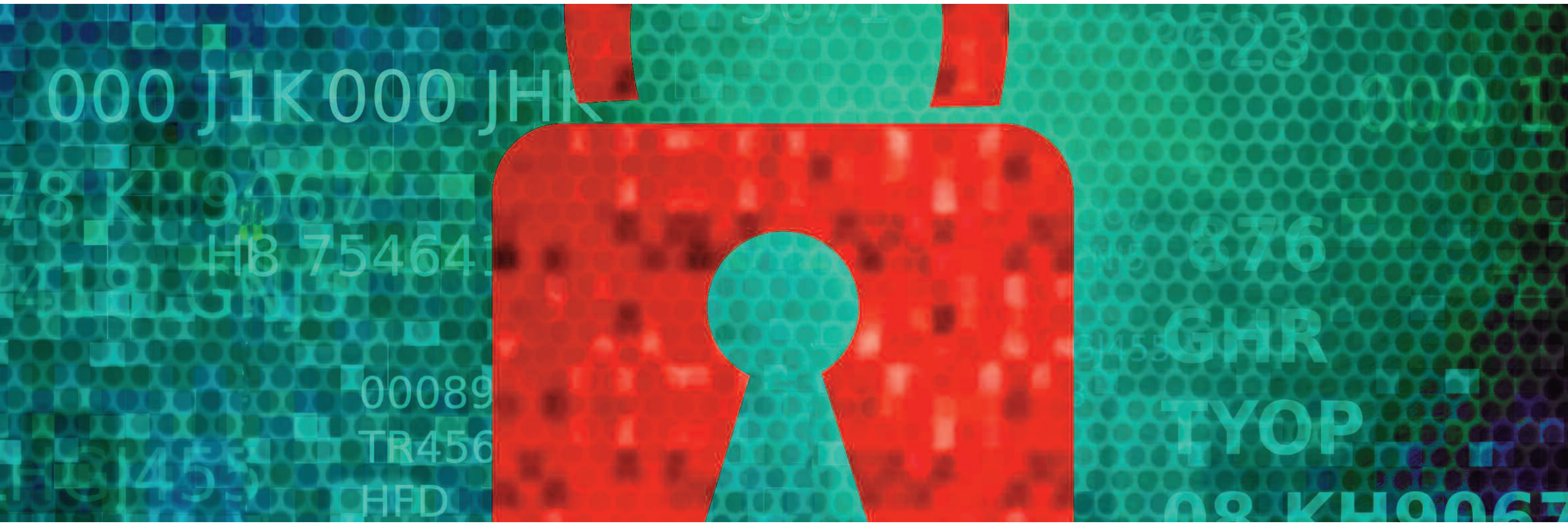
Bruce Brown – CyberSentinel Lead Engineer
December 9, 2015

JESKELL/IBM CONFIDENTIAL

www.jeskell.com

To learn how CyberSentinel can identify and interrupt threats within your environment, watch the demo on our website.

> “We are vulnerable in the military and in our governments, but I think we’re most vulnerable to cyber attacks commercially. This challenge is going to significantly increase. *It’s not going to go away.*[*]”
>
> - Admiral Michael Mullen, USN, Retired



Benefits of CyberSentinel

1. Decreases Information Security Risk

CyberSentinel detects:

- previously unknown threats that rules and signatures based analysis would miss
- botnet communication and exfiltration
- DGA, Tunneling, FastFluxing, and other tactics used by malicious actors

2. Lowers Cost of Management

- Reduced false positives rate
- Reduced amount of time spent tuning with machine learning algorithms
- Features a user-friendly GUI so security specialists don't need to be data scientists or have the service farmed out to a managed services provider

3. Quick Time to Value

- Integrated appliance with installation to production in just one week
- Vendor supported
- Based on IBM’s industry-leading commercial commercial big data platform

[*] http://fortune.com/2012/05/10/adm-mike-mullen-debt-is-still-biggest-threat-to-u-s-security/

Solution Summary

Most cyber security tools and solutions use rule and signature based analyses to detect threats. But CyberSentinel uses machine learning models to identify threats that more traditional security tools can’t. This new cyber security approach will:

- decrease information security risk,
- reduce management and analytic costs, and
- provide quick time to value.

To learn more, visit us on the web at www.jeskell.com/cybersentinel or call us at 1-877-JESKELL.

CyberSentinel
by Jeskell Systems

Premier Business Partner IBM™