Why Breach Detection is Your New Must-Have, Cyber Security Tool

John McCarty

Regional Vice-President, East

Seculert

Why Breach Detection Is Your New Must-Have, Cyber Security Tool

John McCarty
Regional Vice President

cyber security
breach
Column

Popular Posts


Facebook Slingshots Itself In The Face By...
5 days ago


Elon Musk Is Right, Burning Man Is Silicon...
5 days ago


China Telecom Posts iPhone 6 Pre-Order...
4 days ago


Yes, Google Will Now (Probably) Replace Your...
5 days ago


Nasty Gal Lays Off Up To 10 Percent Of Its...
5 days ago


Logitech Releases A Surprisingly...
6 days ago


Live From Apple's iPhone Event In...
2 hours ago

Why Breach Detection Is Your New Must-Have, Cyber Security Tool

Posted Sep 6, 2014 by Paz Eshel, Bucky Moore, Shiran Shalev

7 Share 4 Share 602 Tweet 291

Editor's note: *Paz Eshel is a vice president, and Bucky Moore and Shiran Shalev are associates, at Battery Ventures. Eshel and Shalev are based in Battery's Israel office, while Moore works from Menlo Park. For a full list of Battery's portfolio investments, please click here.*

Biggest Breaches 2014

Retail

Michaels THE ARTS AND CRAFTS STORE®

P.F. CHANG'S

SPEC'S

Neiman Marcus

ebay

THE HOME DEPOT

Finance

JPMorganChase

Paytime Integrated Payroll Solutions

Government

MONTANA

DEPARTMENT OF VETERANS AFFAIRS · UNITED STATES OF AMERICA

UNIVERSITY OF MARYLAND 18 56

Other

VETERANS OF FOREIGN WARS OF THE UNITED STATES

ups

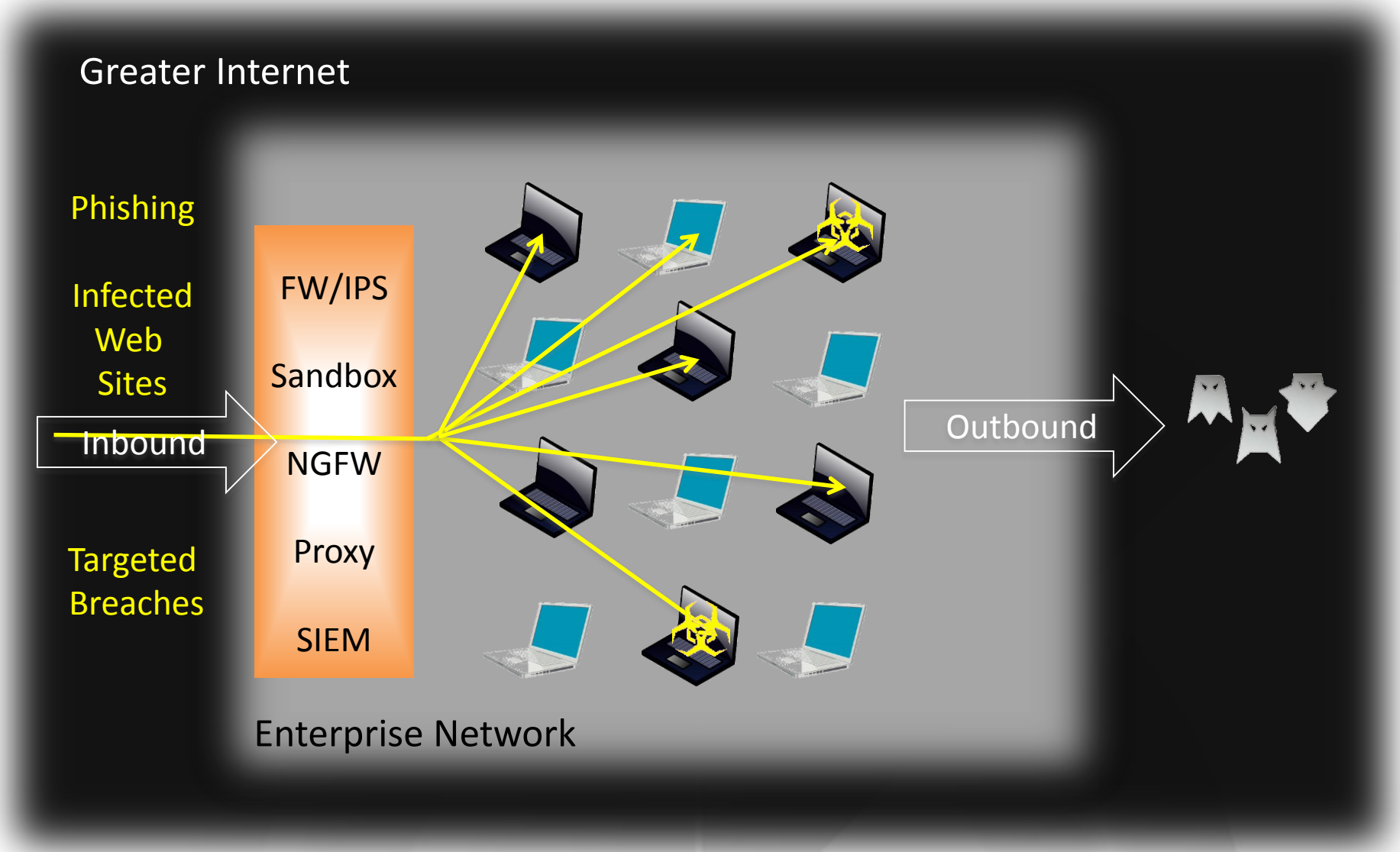
Deltek

Healthcare

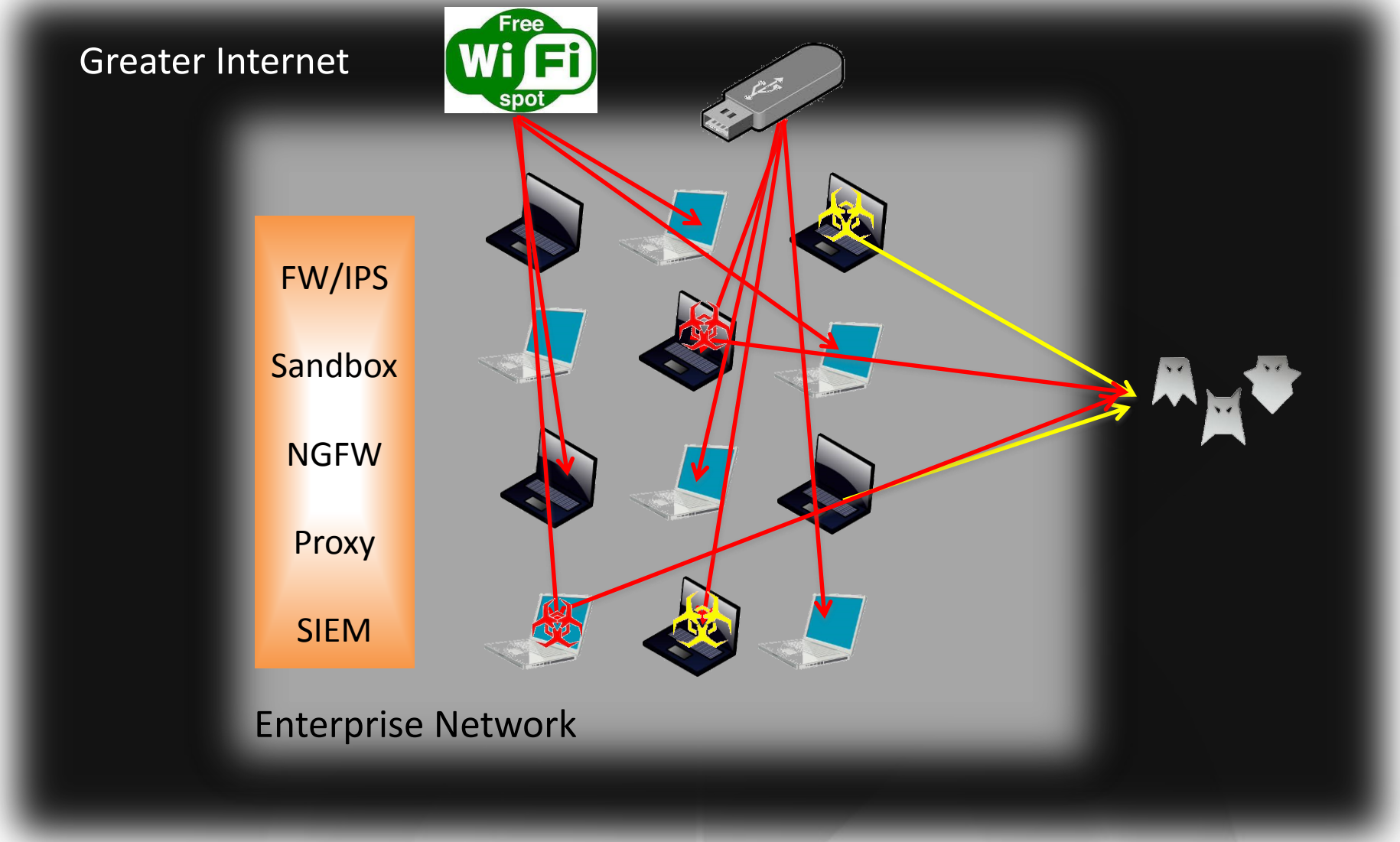
SUTHERLAND HEALTHCARE SOLUTIONS

CHS Community Health Systems

The Inevitable Breach



The Inevitable Breach

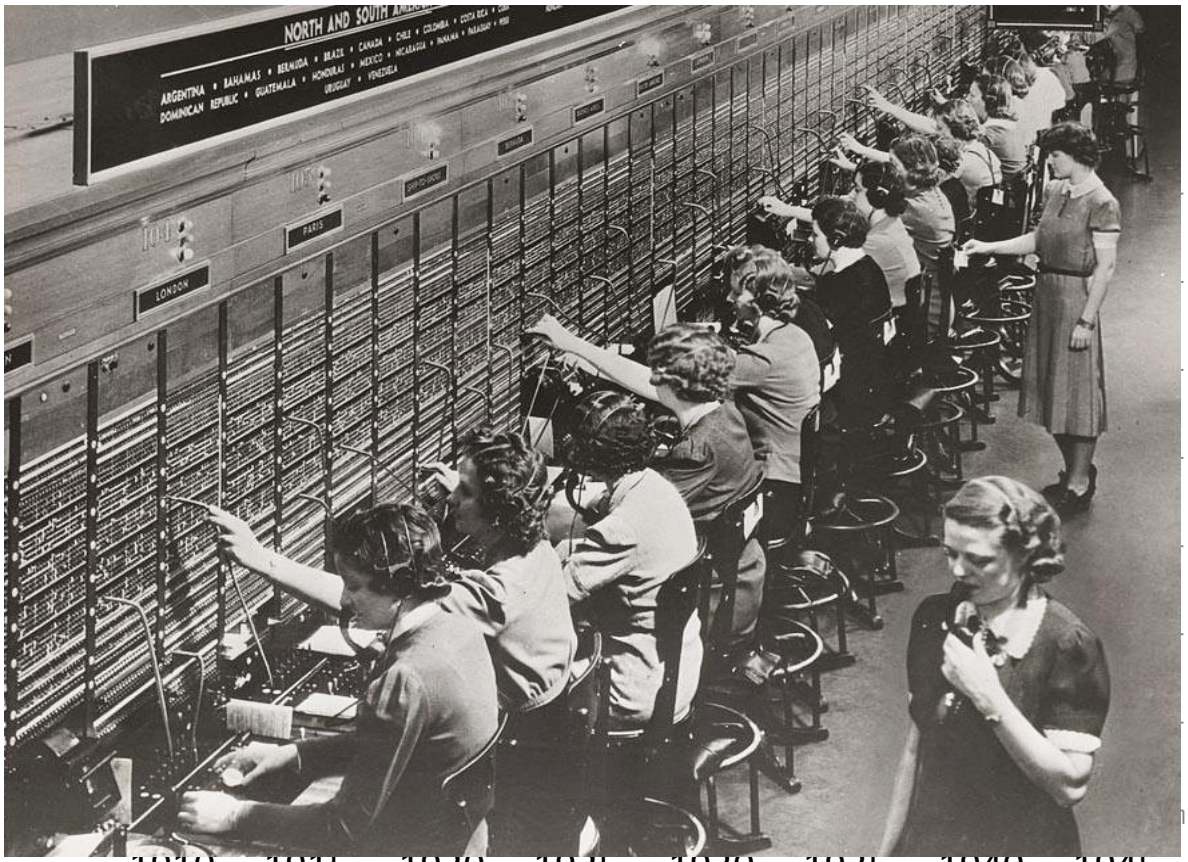


Current Challenges

- Starting point: “We are already infected with undetected persistent malware”
- Prevention solutions provide real-time coverage on the way in, with black lists blocking on the way out. 85-95% effective*
- Everyone one has network blind spots through which malware passes unexamined
- Large volume of alerts into the SIEM
- SIEM/Threat Intelligence correlation process is too manual, too many false positives
- Huge pressure on limited SOC resources
- Detection of new attack types still a challenge

* NSS Report-2014

Automate or Die



1910 1915 1920 1925 1930 1935 1940 1945

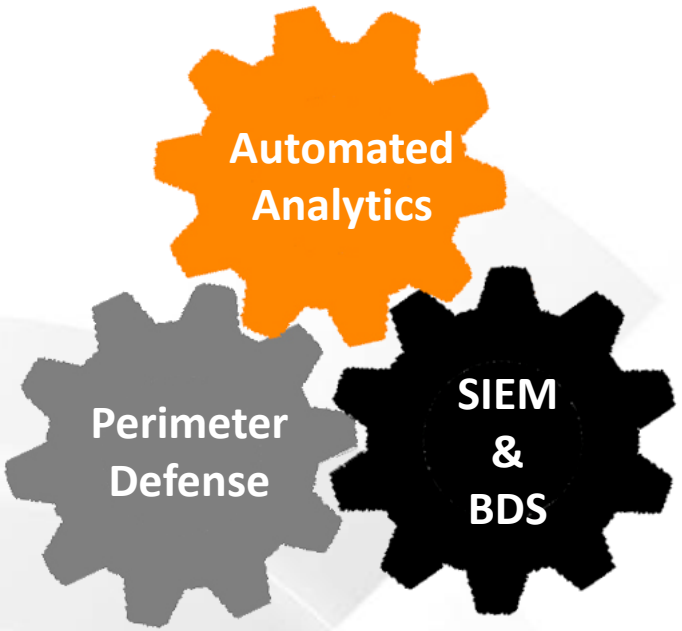
AT&T Operators 1943

Automate or Die

Current Issues

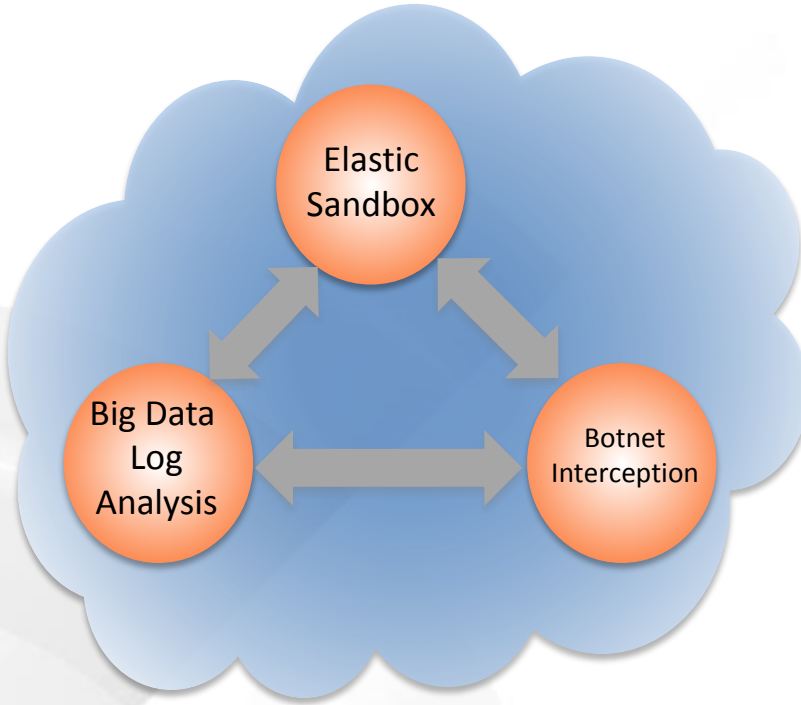
- Threats growing unabated
- Newest threats evade most perimeter defenses
- Not enough qualified security analysts
- Prevention technologies are necessary but insufficient to provide protection

Integrated Detection



Seculert Platform

- Identifies infections found in your network's **blind spots** or that have successfully evaded your prevention solutions
- Only alerts on beaconing communications that are **100% validated**. IR-ready information
- Automates the SIEM/Threat intelligence correlation analytics. P1 Alert helps SOC team **prioritize**
- **Works WITH** existing on premise prevention products
- **All As a Service –** No Hardware, No Software



Automated Breach Detection

John.McCarty@Seculert.com, +1 (484) 994-4878