



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

May 6, 2015



ISOAG May 6, 2015 Agenda

- | | |
|--|---------------------------------------|
| I. Welcome & Opening Remarks | Michael Watson, VITA |
| II. MACH37 Cybersecurity Accelerator project | David Ihrie, CIT |
| III. ISO Knowledge Sharing Committee Update | Andrew Hallberg, ABC |
| IV. SEC501-09 | Mark Martins, VITA |
| V. Upcoming Events | Bob Baskette/Michael Watson, VITA |
| VI. Partner/Operation Update | Bob Baskette, VITA, Michael Clark, NG |



Welcome and Opening Remarks

Michael Watson

May 6, 2015



Information Security Officers Advisory Group

Presentations by Mach37 Startup Companies

May 6, 2015

David Ihrle
David.Ihrle@CIT.Org

CTO, Center for Innovative Technology
CTO, Mach37 Cybersecurity Accelerator

Dan Woolley
Dan.Woolley@Mach37.com

Partner, Mach37 Cybersecurity Accelerator

MACH37 Project

Project Presentations

- 1. Eunomics
- 2. Shevirah
- 3. Anatrope
- 4. Atomicorp
- 5. MSB
- 6. Axon
- 7. Syncurity
- 8. Bijoti



Industrial Networks

(Cybersecurity for the real world)

John Nelson

john@eunomicnetworks.com

Eunomic Team

- Founders: John Nelson and Jim Harris
- 20+ years manufacturing product management
- 10+ years cybersecurity for critical infrastructure
- **Security software suite designed for industrial networks**



IBM



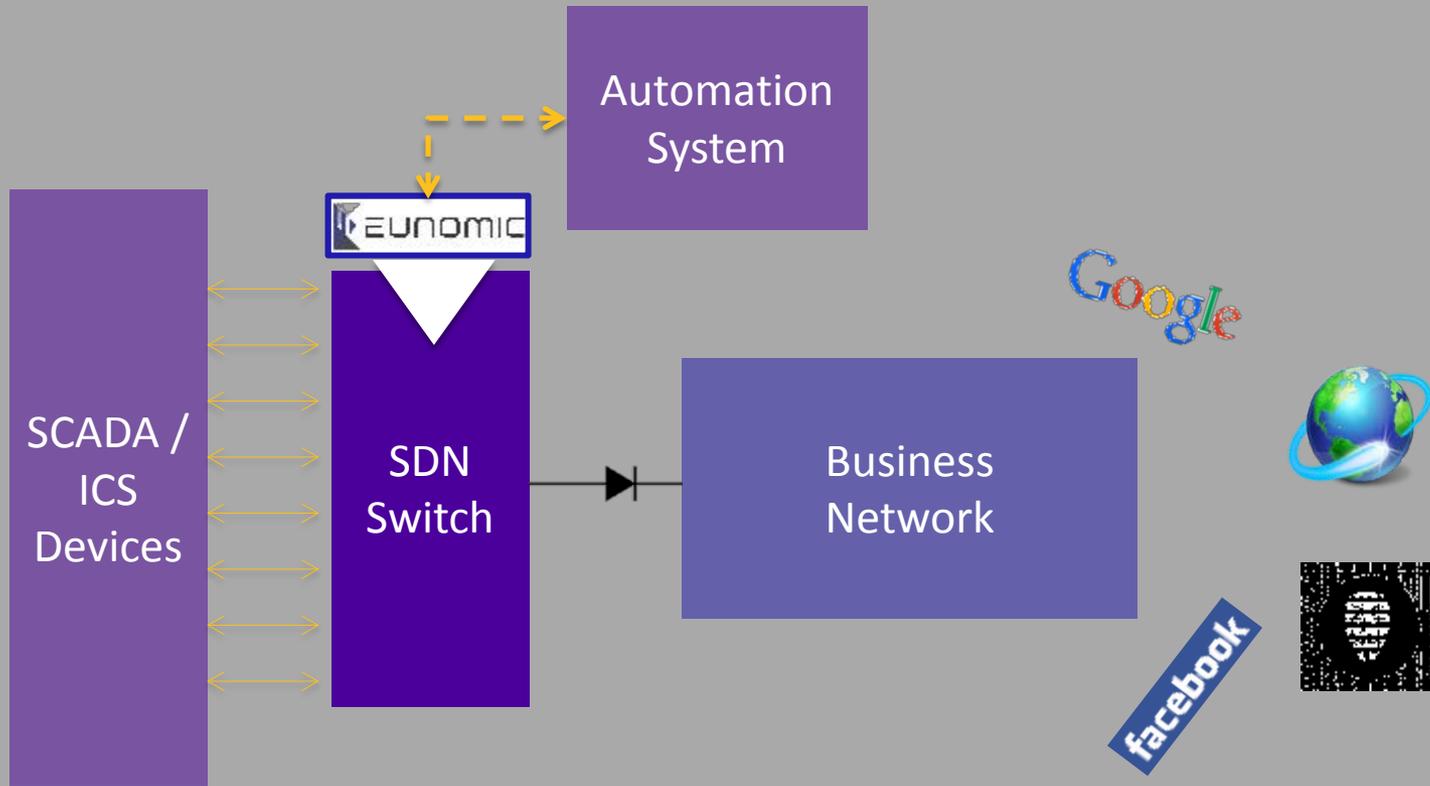
FBI

Industrial Modernization Stalled

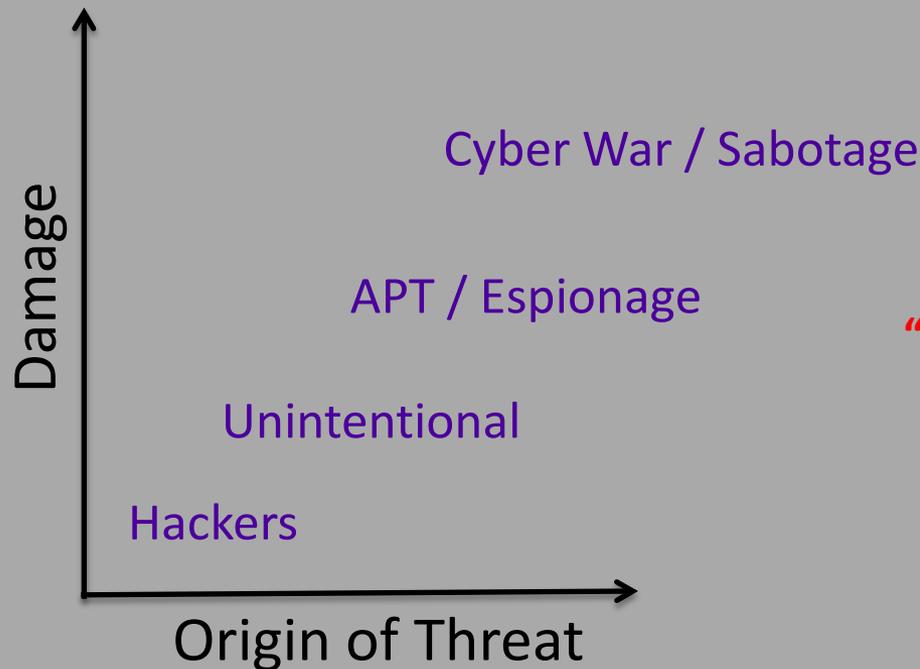
- Current control systems are obsolete
- New control systems are vulnerable



Eunomic Software Solution



Cyber Threats are Real

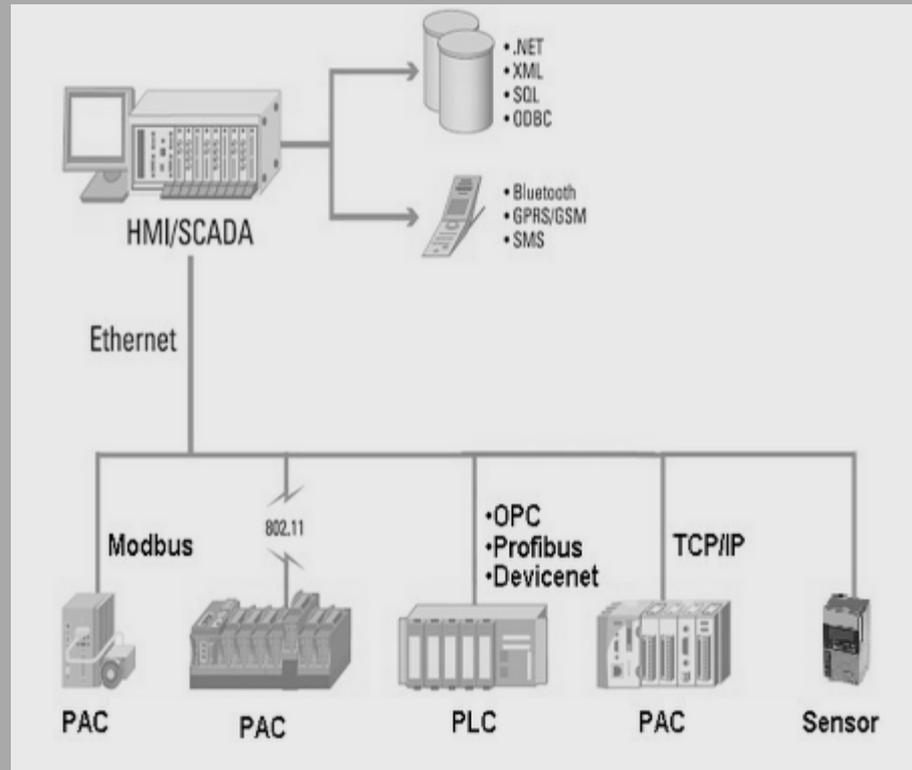


**“Cyberattack on German Steel Plant
Caused Significant Damage”**

ES ISAC

Electricity Sector Information
Sharing Analysis Center

Industrial Networks \neq Business Networks



ICS Priorities

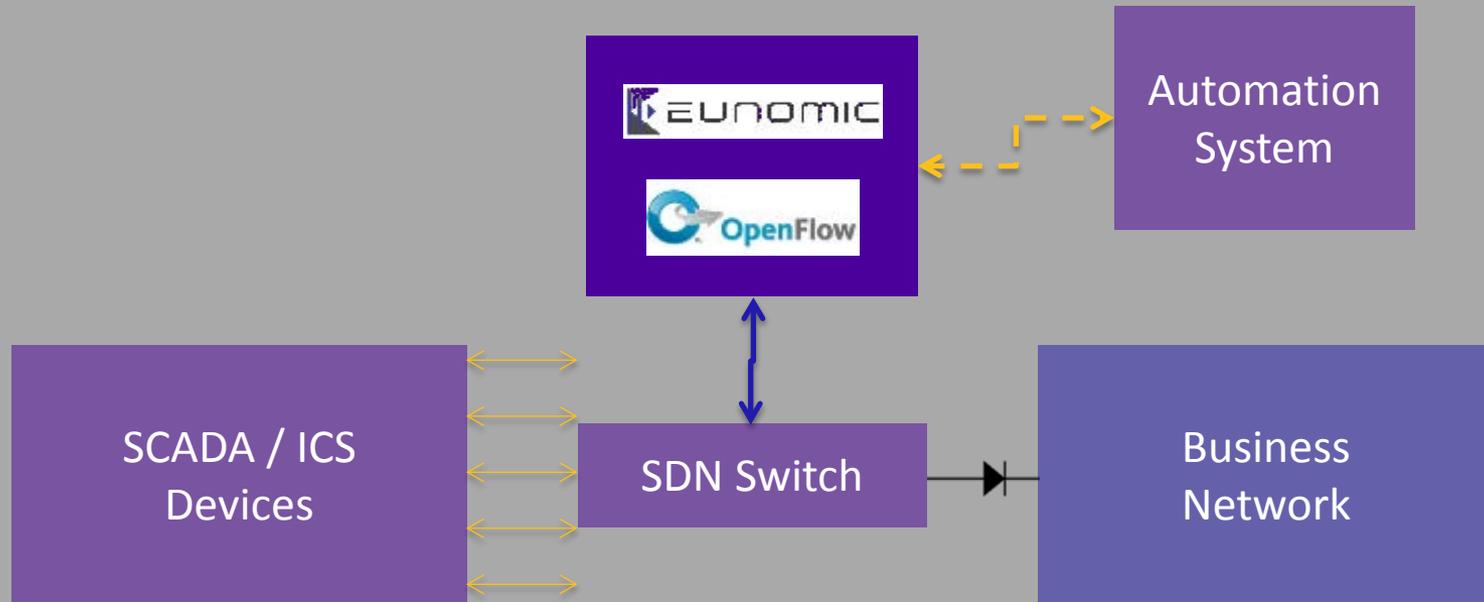


IT Cyber solutions are misdirected for ICS



Industrial Control System (ICS)

Eunomic ICS Network Controller

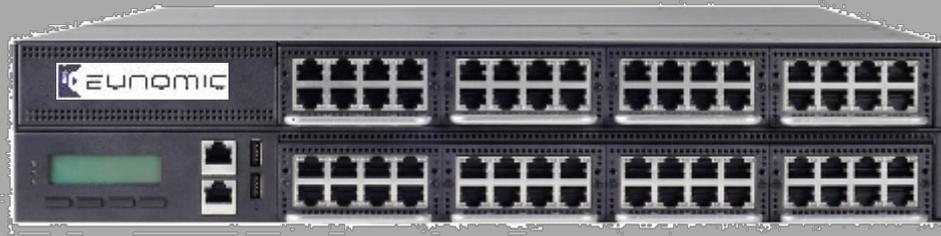


Dynamic Micro-segmentation

Virtualized Security Applications

Pilot System

Eunomic ICS Network Controller (ICS-NC)



Replaces
Network Switch

Integrates network management
with ICS Automation System

Pilot Tests of Eunomic ICS-NC

Customers

- New micro-turbine power plants
- Plant modernization
- Utility clients in the Americas

Strategic Partners

- Automation systems
- SDN hardware and software
- Virtualized security appliances

John Nelson

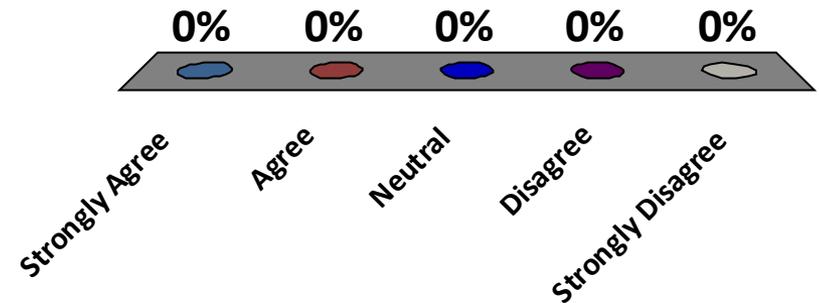
john@eunomicnetworks.com

Phone: +1 703-402-0753



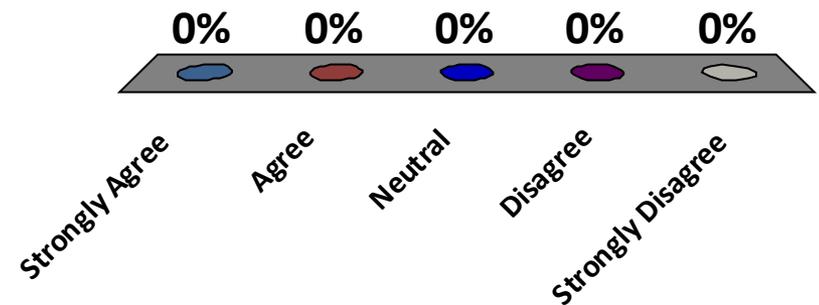
Do you feel the presenter explained their product thoroughly?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



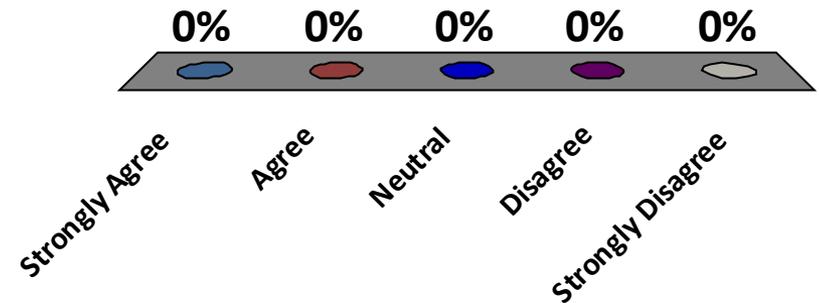
Do you think you this product will provide benefit directly to your environment?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree





Shevirah

Penetration Testing

A Hands-On Introduction to Hacking



Georgia Weidman

Foreword by Peter Van Eckhoutte



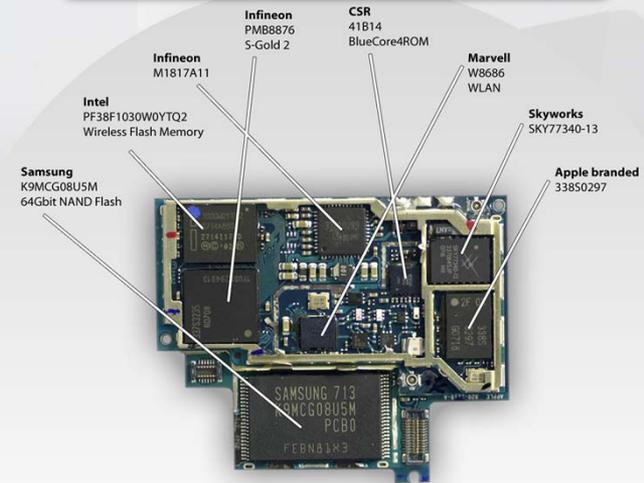
Phone?



Super Computer?



Inside Apple's iPhone



Shevirah

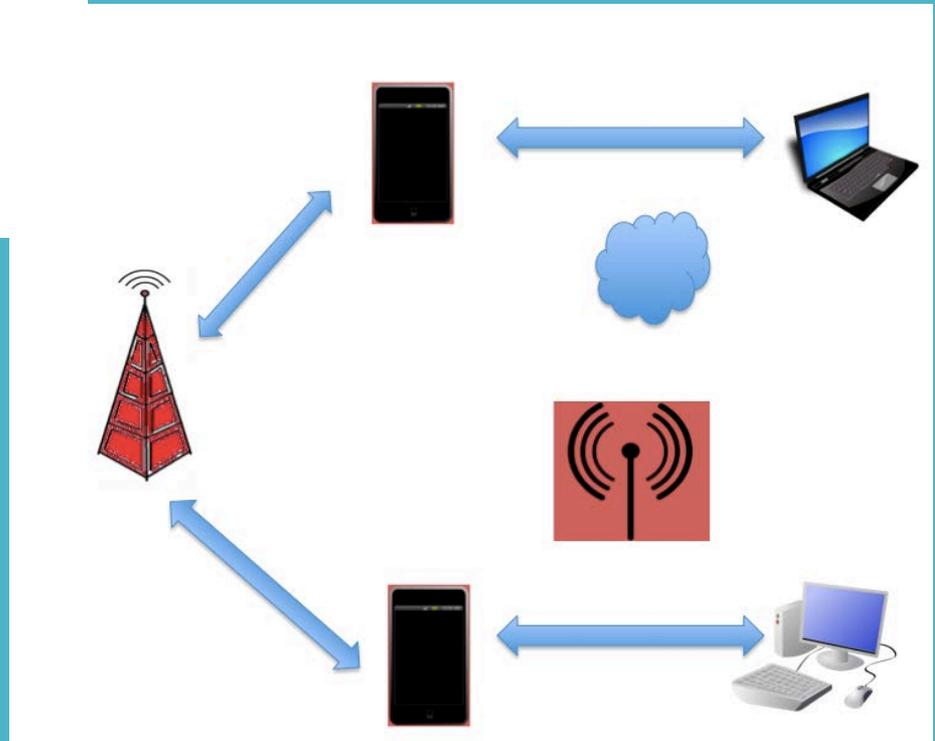
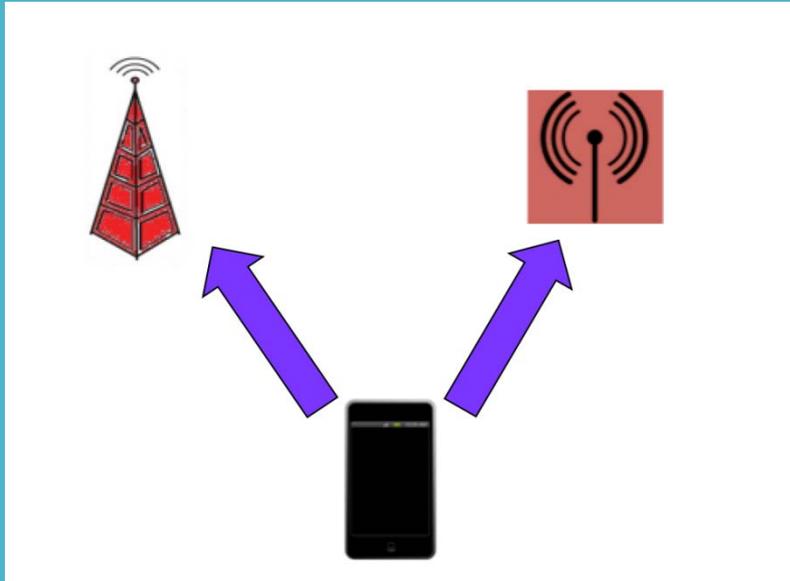
Vulnerability assessments around BYOD

Reports on security posture of mobile devices

Remediation recommendations

Integrates into SEIMs and other security tools

Enterprise Mobile Threats



Mobile Threats

Remote Attacks – Default SSH password, SIM card attacks

Client Sides – Webkit, Document Readers

Social Engineering – text message phishing, QR codes

Malicious Apps – backdoored version of legitimate app, master key issues

What Attackers Can Do on A Phone

Remote Control

Steal data

Undermine security controls

Discover nearby devices

Pivot attacks onto nearby devices

Mobile Security

Mobile Device Management

Mobile Antivirus

Data Containers

Other apps that have stored data or functionality that can be manipulated (2 factor SMS app, VPN app)

Gartner

By 2019, 80% of vulnerability assessment (VA) vendors will offer enterprise mobility management (EMM) integration capabilities to assess mobile devices, up from 20% today.

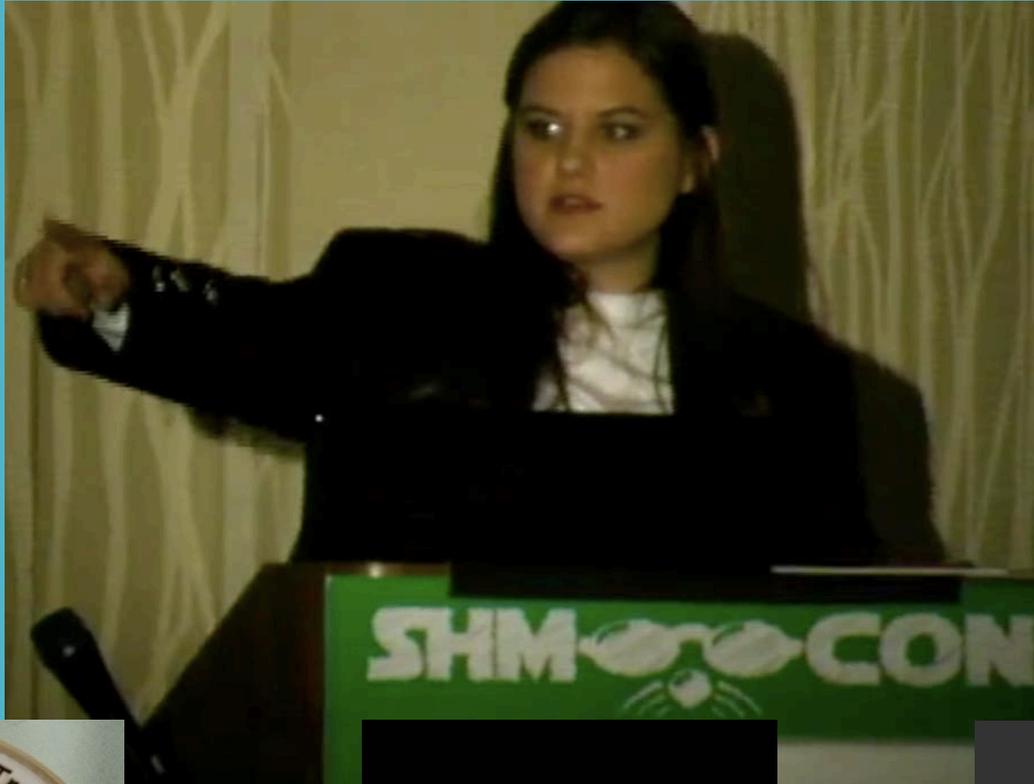
By 2017, 40% of enterprises will deploy or extend their VA solution to cover smartphones and tablets, up from 5% today.

Article: [Four Ways to Close the Gap Between Enterprise Mobility and Vulnerability Management](#)

Mobility and security specialists who assume enterprise mobility management tools are mature and work like legacy PC management tools can lose control of their devices.

Article: [How to Avoid the Top 10 EMM/MDM Deployment Mistakes](#)

The Team



Pilots

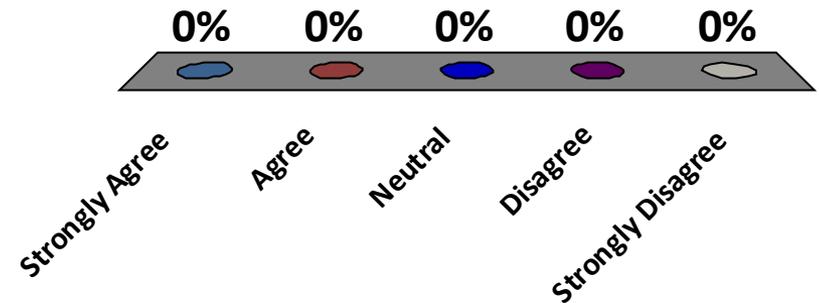
www.shevirah.com

georgia@shevirah.com

[@shevirahsec](#)

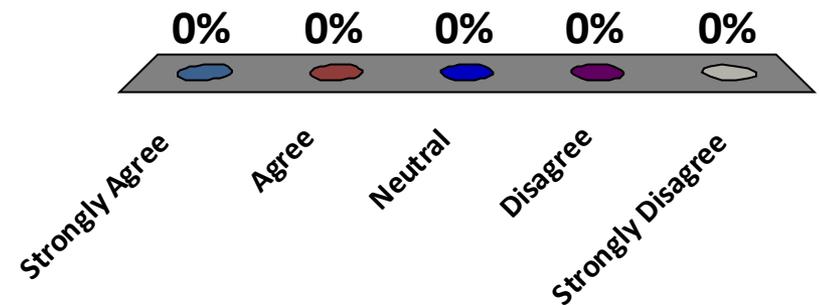
Do you feel the presenter explained their product thoroughly?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



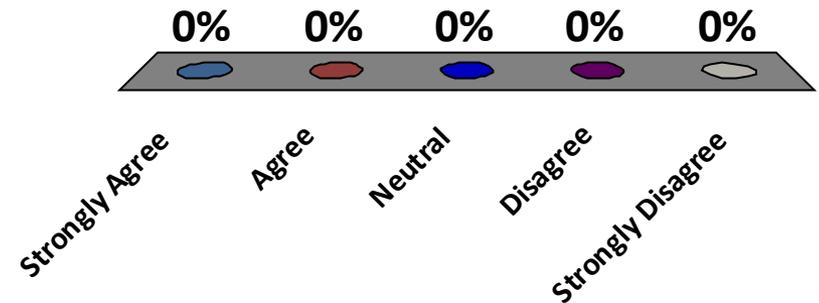
Do you think you this product will provide benefit directly to your environment?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



Anatrobe

*Business Intelligence Through Wireless
Automotive Technologies*

The Problem

People spend a lot of time in their cars.
Your car is continuously broadcasting unique data.
The location-based data is not being utilized.

The Solution

What if you can access and analyze those unique IDs for business intelligence associated with advertising/marketing, perimeter detection for security and fleet management for asset management and fee collection?

- **What**

- Your customers' cars

- **Why**

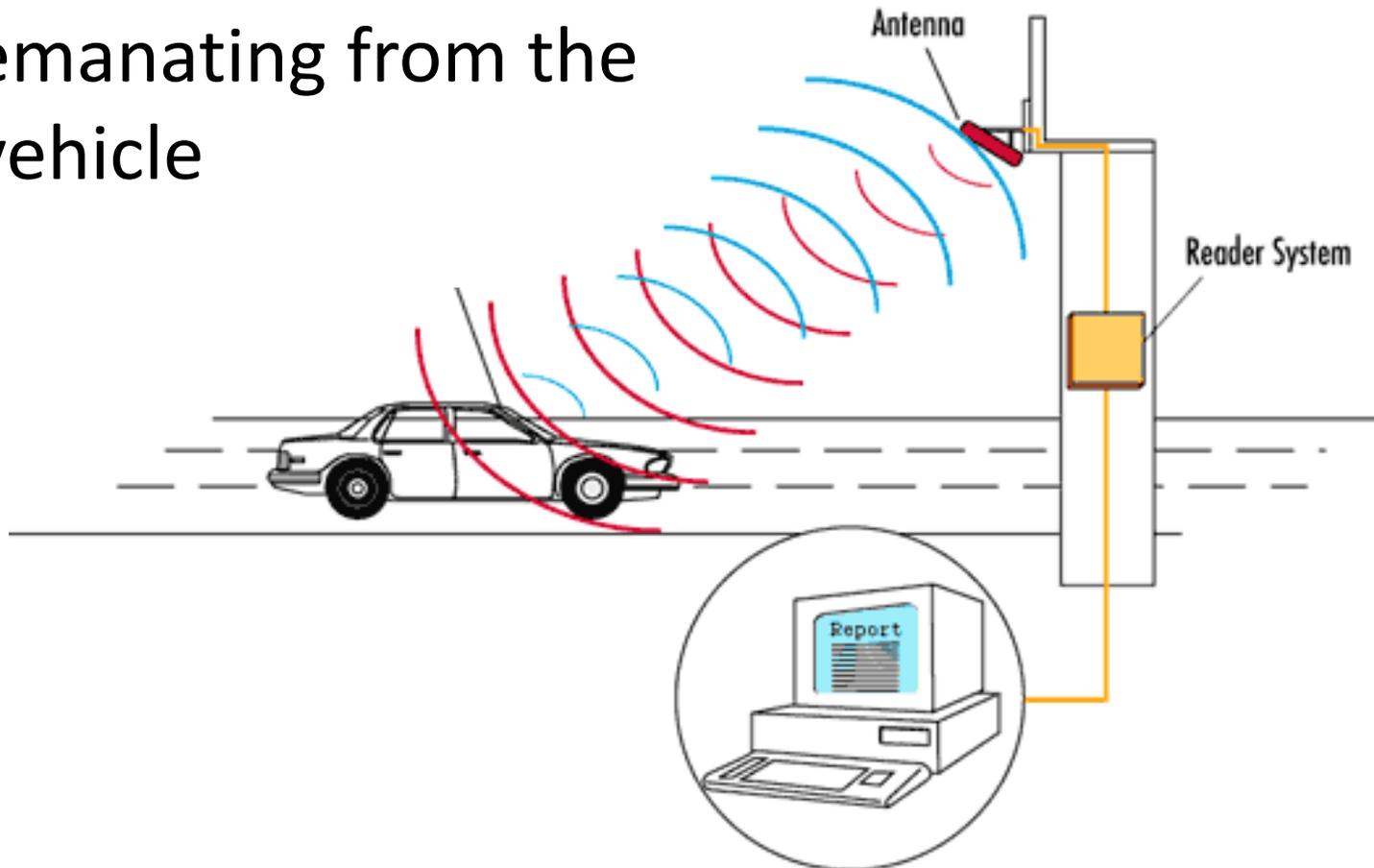
- Targeted consumer advertising with location-based services
- Fleet management
- Perimeter access

- **How**

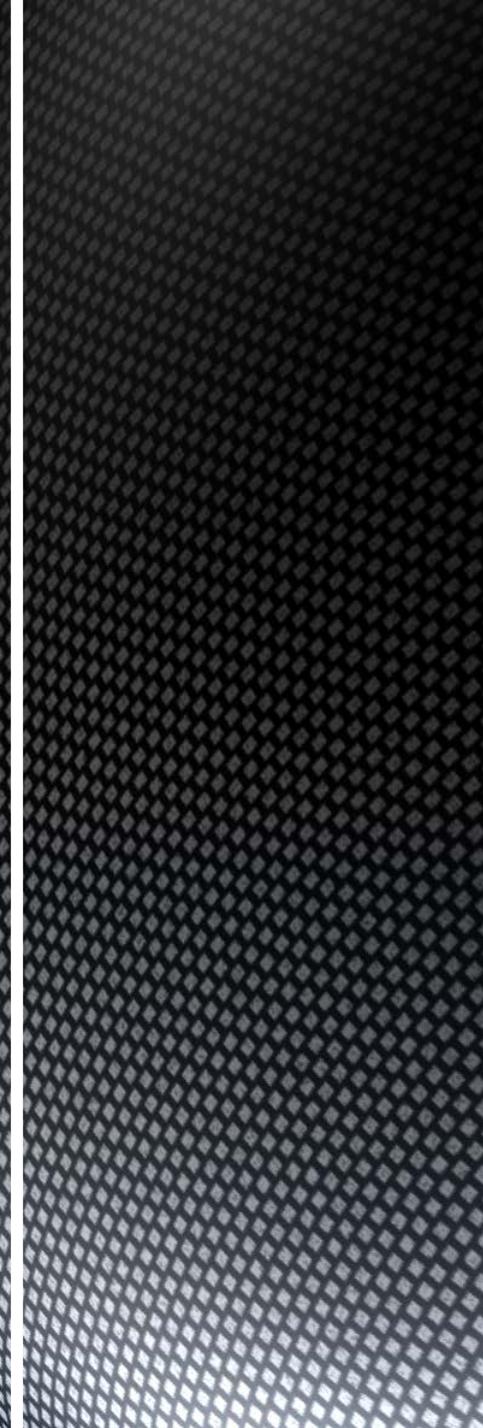
- Radio signals emanating from vehicles MMY 2005+
- Sensors placed on bollards, fences, gates to park lots and garages, toll collection booths, locations with high-crime

The Technology

- Identify vehicles remotely using signals emanating from the vehicle



Access Control

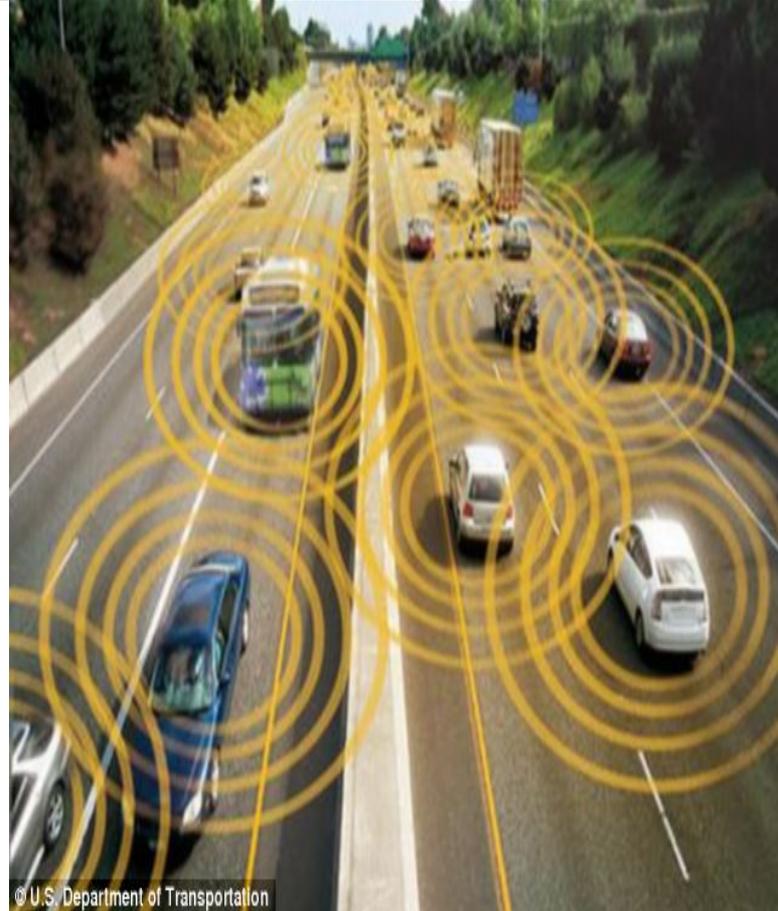




Identify if a vehicle has been returning to a location and query the last time & date seen

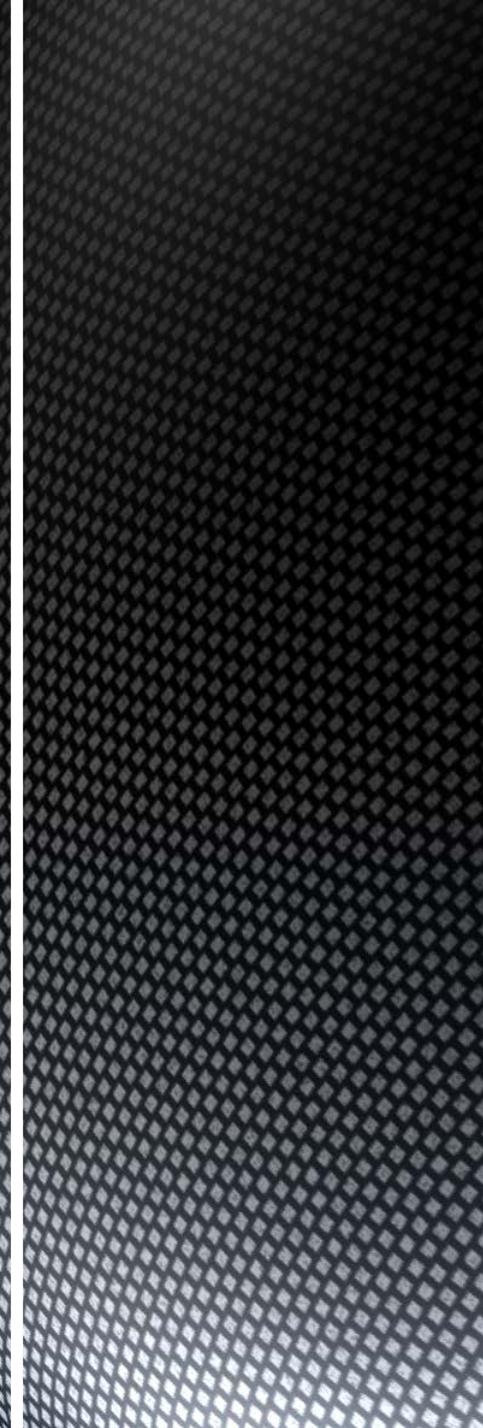
Perimeter intrusion detection system using portable sensors

Location based services



Images: "The Italian Job" and DOT

Targeted
Consumer
Advertising
and Business
Intelligence



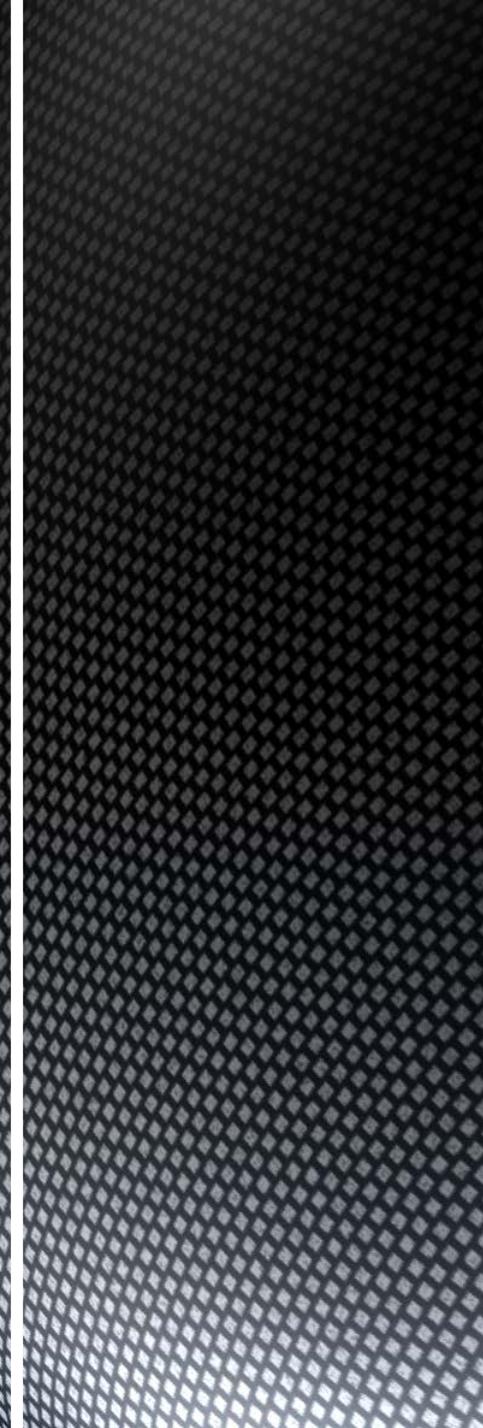


Sensors at gas stations, truck stops, fast food restaurants

Images: <http://www.ctpost.com/news/article/State-checks-trucker-violations-as-part-of-safety-1421102.php#photo-1049436>
<http://detroit.cbslocal.com/2011/02/14/gas-station-tv-sees-record-breaking-revenues-profits/>



Fleet Management





Remotely ID
vehicles as
they enter or
exit fleet lots

Uniquely
identify
vehicles in a
garage and
collect fees



Solution

Remotely, Anatrope's sensors and platform can provide perimeter security, location-based services, and can empower fee collection technology.

Utilize a new data point for business intelligence without the requirement for adding hardware to vehicles.

■ **Tiffany Rad, BS, MBA, JD**

- Independent security research, 10+ years of industry experience including Forbes 20 companies and US defense contractors for vehicle research
- Board Member of the National Academies of Science's *Protection of Transportation Infrastructure from Cyber Incidents* Panel
- Co-author of *Cyber-Enabled Economic Warfare Against the Transportation Sector* report for the US Senate Intelligence Committee
- Computer Security Engineer for Battelle Institute's Center for Advanced Vehicle Engineering (CAVE), 1.5 years

Teague Newman, GIAC-GPEN, GIAC-GCIH

- Independent security researcher
- SANS Advanced Penetration Testing Subject Matter Expert
- Professional penetration tester
- Lead Training Partner for Core Security Technologies
- Physical/Electronic security consultant
- Vehicle racing, computer tuning & modification hobbyist for over 15 years

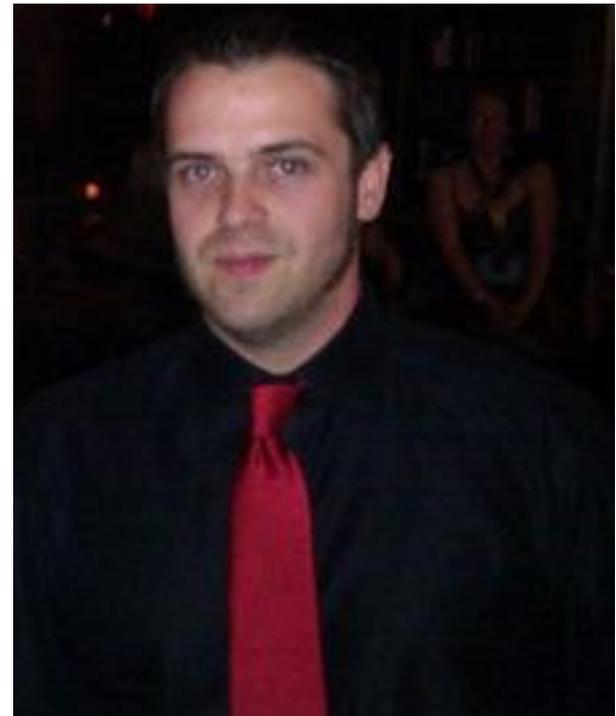
Contact Anatrope, Inc.

Tiffany Rad, CEO

Tiffany@anatrope.com

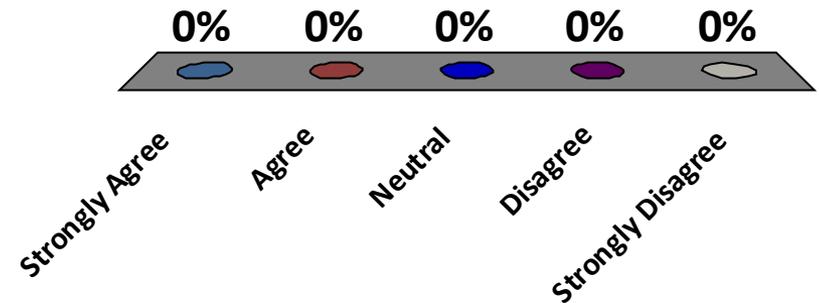
Teague Newman, CTO

Teague@anatrope.com



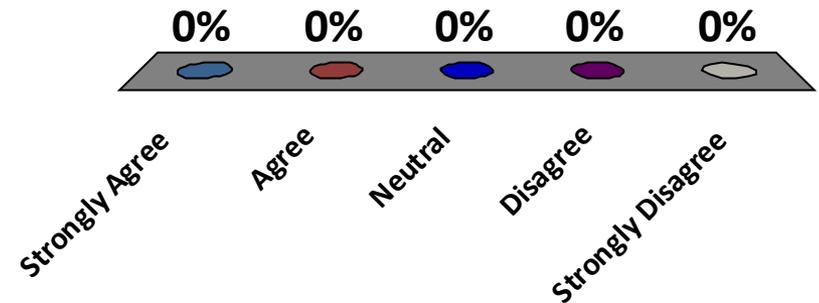
Do you feel the presenter explained their product thoroughly?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



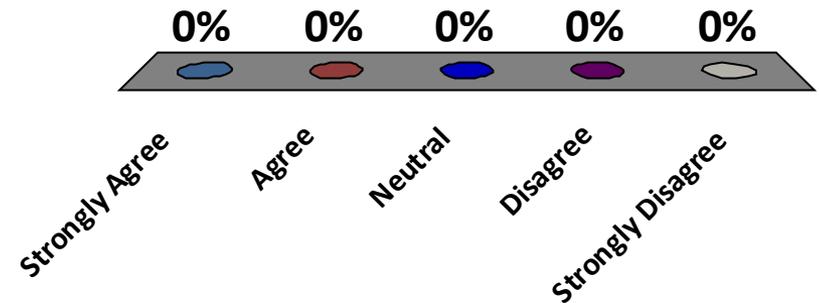
Do you think you this product will provide benefit directly to your environment?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree

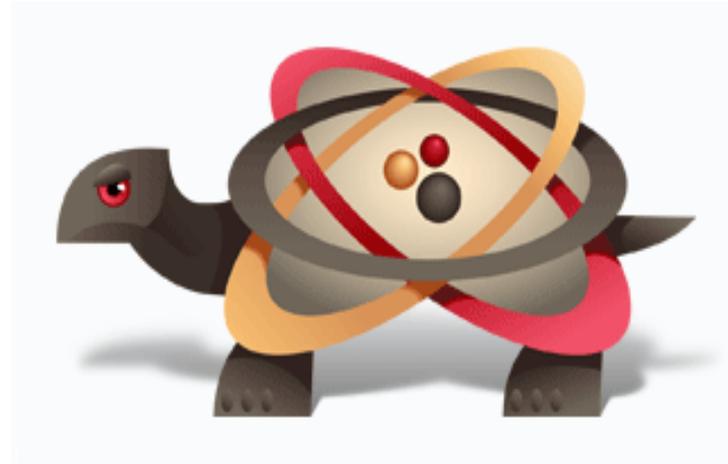


Do you think there are other parties within the State or Local government that would benefit from this type of product?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



Atomicorp



Security for Everyone

The Problem

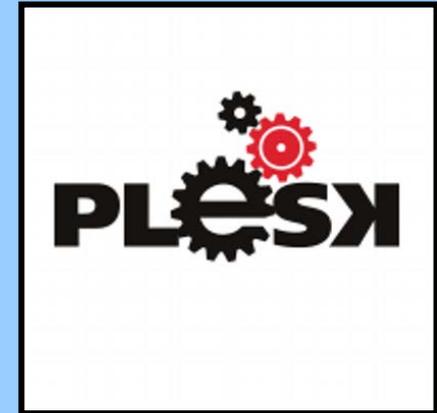
- Security solutions are complicated
- No defense in depth
- Lack fundamental foundations
- No compatibility



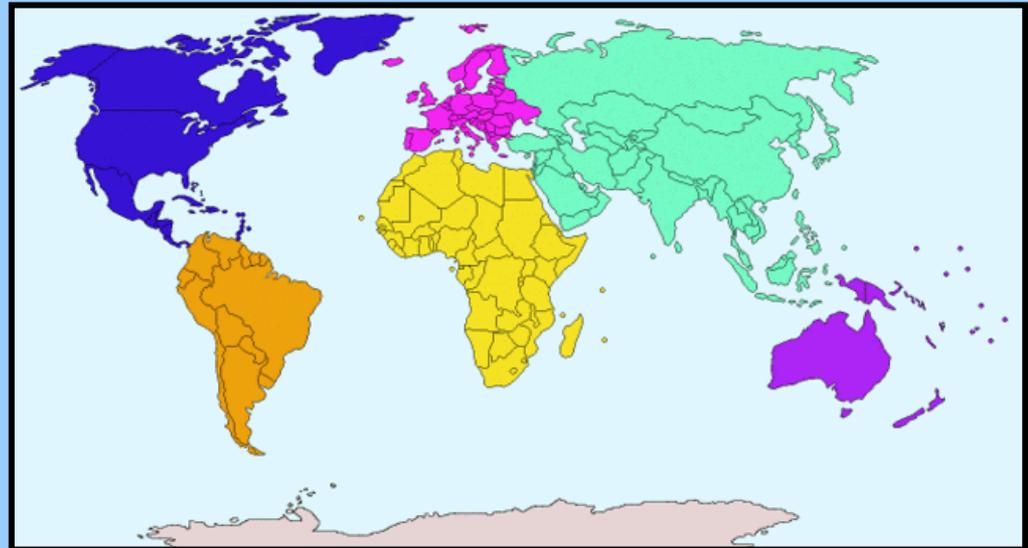
The Problem



The Company



- Grown to over 1200 global customers in 24 months



The Solution

- Build defense depth
- Automate routine security functions
- Reduce costs



The Atomic Secure Product Line

- Hardened Kernel
- Web Application Firewall
- Host Intrusion Detection System
- Virtual patching
- Threat intelligence

The screenshot displays the Atomic Secure System Monitor interface. The main window is titled "System Monitor" and contains several sections:

- Memory:** 5273 MB (indicated by a green progress bar).
- Swap:** 36 MB (indicated by a grey progress bar).
- System Load:** A line graph showing system load over time, with values ranging from 0.00 to 1.00.
- Vulnerability:** A pie chart showing the distribution of vulnerabilities by severity: Critical (red), High (orange), Moderate (yellow), and Low (green).
- System Updates:** A table listing installed updates and their status:

Component	Status
Atomic Secured Linux	✓
Malware Detection Engine	⚠
Intrusion Detection System / Intrusion Preventions System	✓
Kernel Intrusion Prevention System	✓
Web Application Firewall	✓
Denial of Service Protection	✓

An "UPDATE" button is visible at the bottom right of the System Updates section.

- Vulnerability Details:** A list of detected vulnerabilities with "Read More..." links:

- Operating System: Un-Applied updates for your system were detected. A full list of available updates is available in `/var/asl/data/updates_pending.log`
- PHP: warn-only mode for detecting and disabling dangerous PHP functions.
- PHP: function `curl_exec()` allows an attacker to execute shell commands through php.
- PHP: function `curl_multi_exec()` allows an attacker to execute shell commands through php.

The background shows other parts of the interface, including a "Security Events" section with "Alerts" and "Events" tabs, a "Countries" list (US, ??, DE, ES, GB), and a "Level" dropdown menu (Level 1 to Level 16).



The Benefits

- AS/L installs on your existing server
- Hardens existing infrastructure without additional hardware
- Works in harmony with other security products (Symantec, McAfee, Palo Alto, etc.)
- Real-time defense as threats are detected across the AS/L network of users





Top Source Countries

CN	244
US	217
GB	96
PK	82
TW	45
IN	31
VN	30
AU	26
BR	24
JP	24

Top Source IP Addresses

69.52.135.38	44
167.114.117.104	21
190.255.167.122	12
117.241.34.179	11
110.248.209.151	8
112.226.188.156	8
111.166.199.241	8
85.255.233.158	8
123.75.49.208	8
49.240.55.240	8



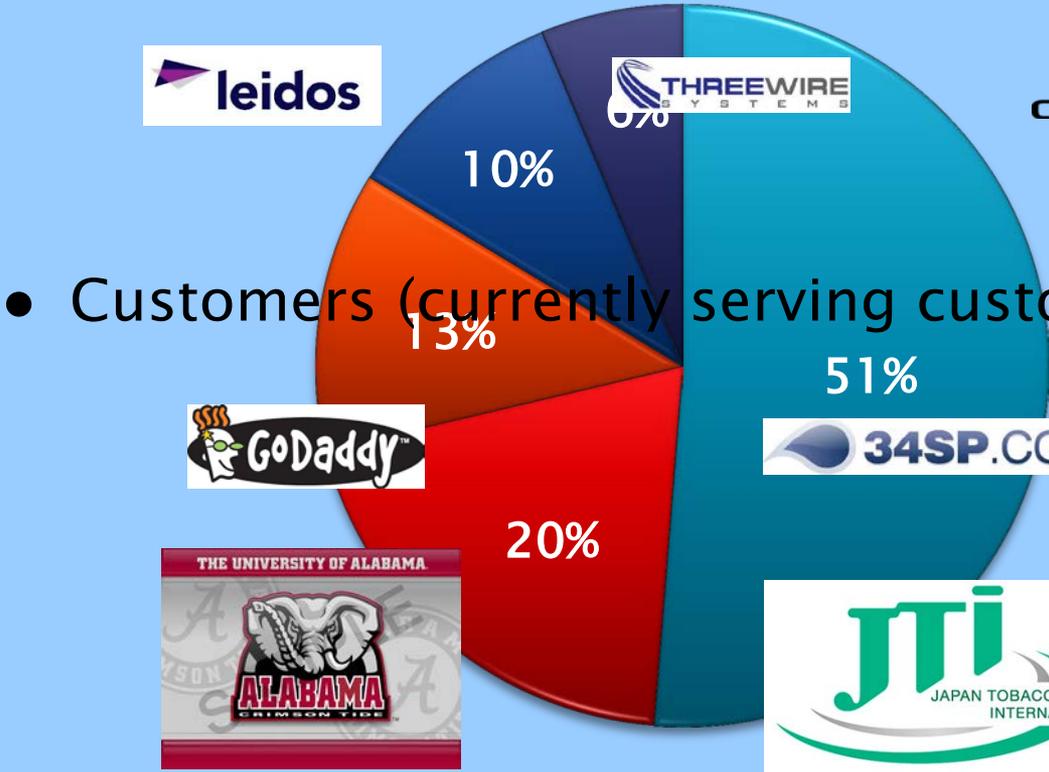
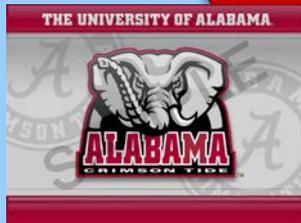
Partners and Customers

% of Sales

- Partners



- Customers (currently serving customers on all 7 continents)



Questions / Comments

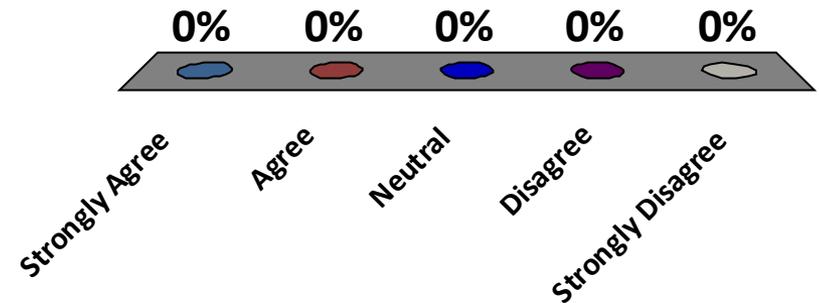
From Terra Firma to the Cloud
We've got you covered
ATOMIC SECURED by ATOMICORP



Contact Cliff Richardson @ 703-266-6006

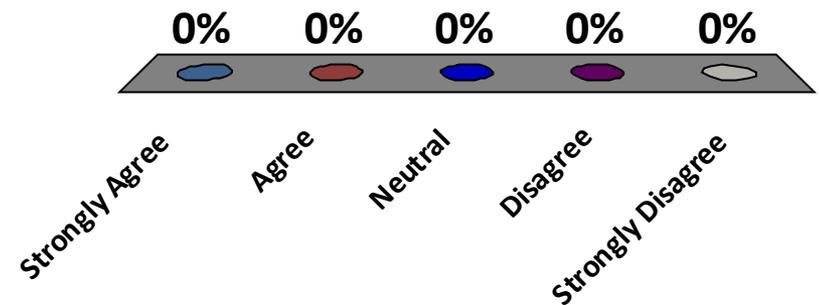
Do you feel the presenter explained their product thoroughly?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



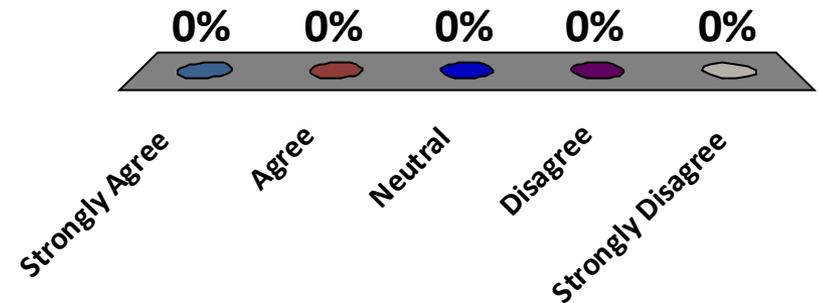
Do you think you this product will provide benefit directly to your environment?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



Security i-Cue[™]

Prioritize Security Risk. Intelligently.



Do you ever feel like this guy?



* t.scudiero.com

Overwhelming security threats & changes

Example: 400-1000 new vulnerabilities identified
every month



This is not a new problem...



...But it's getting worse

Minneapolis Post

Shareholder advisory firm: Target should drop most board members

Institutional Shareholder Services suggested that members of Target's audit committee, including Austin, should be removed from the board in the wake of the data breach.

NEGLIGENCE

The Gazette

Target's 1Q profit down 16% as it deals with customer data breach fallout

Target cut its annual profit outlook Wednesday and said its first-quarter earnings fell 16 percent as it took another hit from a massive customer data breach.

PROFITS DOWN

Target cut its annual profit outlook Wednesday and said its first-quarter earnings fell 16 percent as it took another hit from a massive customer data breach and a troubled expansion in Canada.

Target Seeks New Chief Information Officer After Data Breach

Target Corp, still reeling from a security breach that exposed the personal information of tens of millions of customers, is seeking a top technology executive to help prevent future attacks.

The company is searching externally for a candidate to replace Beth Jacob, who resigned today after holding the chief information officer post since 2008. The new executive will help revamp

FIRINGS

Target CEO Gregg Steinhafel resigns following last year's security breach

Target CEO is the latest casualty of the widespread data breach that allowed hackers steal personal data and credit card information from millions of customers.

On Monday, the Minneapolis-based retail chain announced that 35-year company veteran Gregg Steinhafel had stepped down effective immediately.



Data analysis requires legions of staff

EXTERNAL DATA

Vulnerabilities

Threats

Environmental Factors

INTERNAL DATA

SIEM

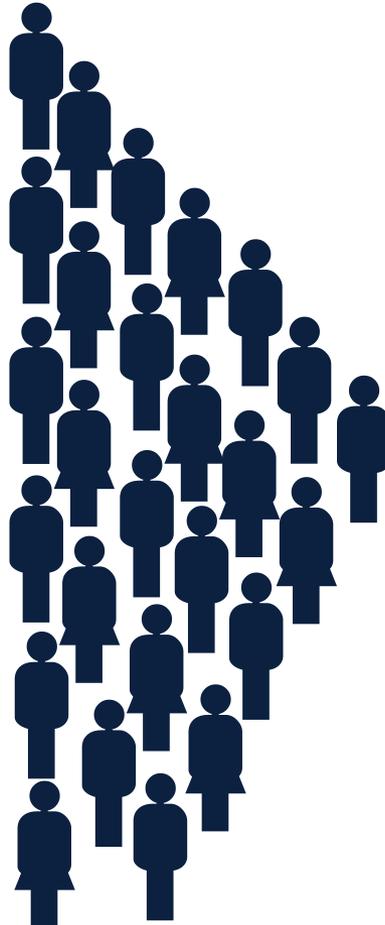
Vulnerability Scanning

Policies & Procedures

Consulting

Compliance

Asset Management



Security i-Cue™ solves this problem

EXTERNAL DATA

Vulnerabilities

Threats

Environmental Factors

INTERNAL DATA

SIEM

Vulnerability Scanning

Policies & Procedures

Consulting

Compliance

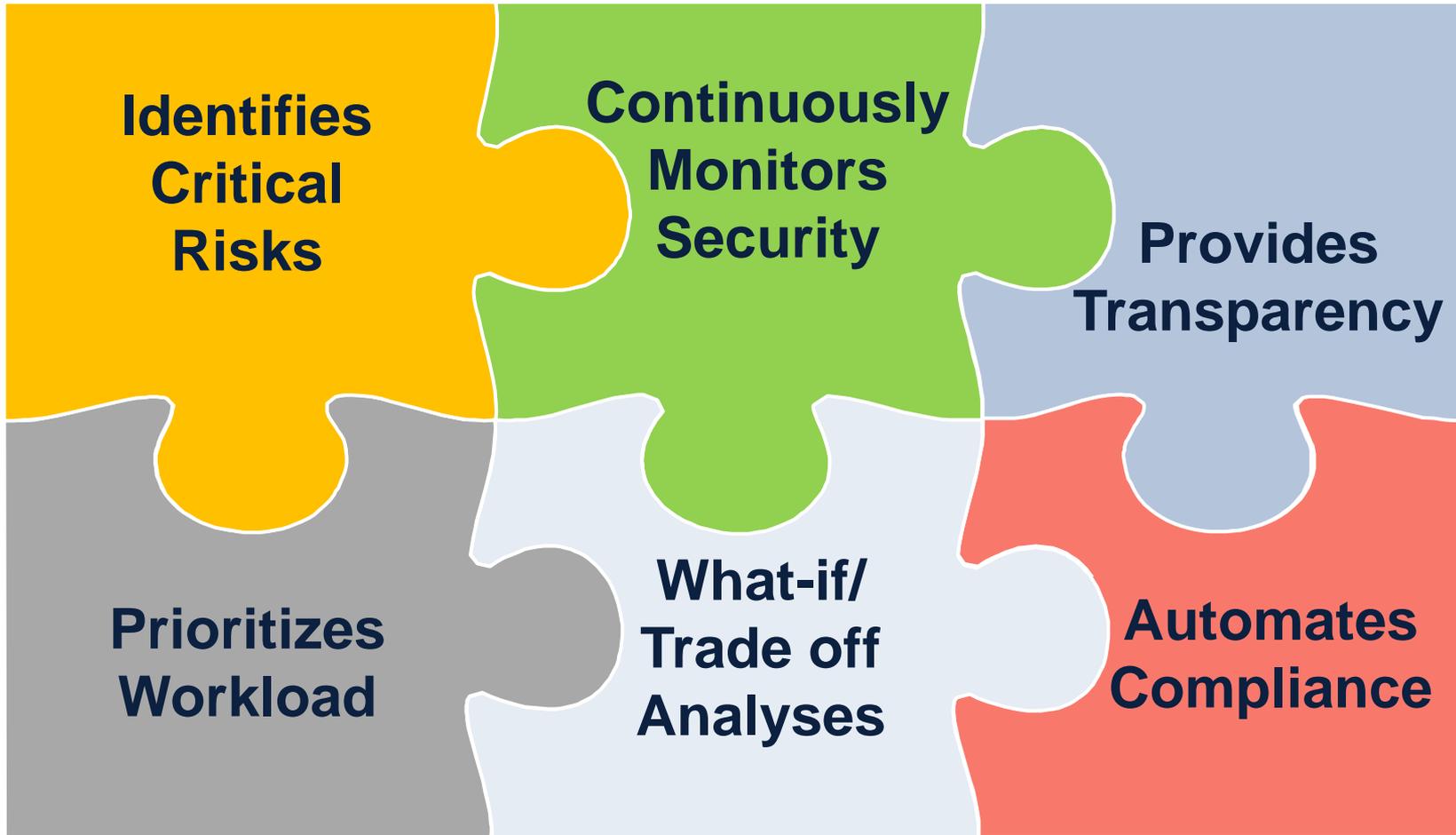
Asset Management



Automated analysis for risk prioritization



Security i-Cue™ delivers...



Automated calculation of business risks

Proprietary Analytics Engine




Security i-Cue

Security i-Cue Dashboard - 5/13/2013 12:24:29 PM Overview Data

Device Name	IP	Device Description	System Name	Result	# of Findings	Criticality
01 Computer_1	192.168.2.1	MS Laptop	MS Laptop	Pass	0	1
01 Computer_2	192.168.2.2	MS Laptop	MS Laptop	Pass	0	1
01 Computer_3	192.168.2.3	MS Laptop	MS Laptop	Pass	0	1
01 Computer_4	192.168.2.4	MS Laptop	MS Laptop	Pass	0	1
01 Computer_5	192.168.2.5	MS Laptop	MS Laptop	Pass	0	1
01 Computer_6	192.168.2.6	MS Laptop	MS Laptop	Pass	0	1
01 Computer_7	192.168.2.7	MS Print Server	MS Print Server	Pass	0	1
01 Computer_8	192.168.2.8	MS Desktop	MS Desktop	Pass	0	1
01 Computer_9	192.168.2.9	MS Desktop	MS Desktop	Pass	0	1
01 Computer_10	192.168.2.10	MS Desktop	MS Desktop	Pass	0	1
01 Computer_11	192.168.2.11	MS Desktop	MS Desktop	Pass	0	1
01 Computer_12	192.168.2.12	MS Desktop	MS Desktop	Pass	0	1
01 Computer_13	192.168.2.13	MS Desktop	MS Desktop	Pass	0	1
01 Computer_14	192.168.2.14	MS Desktop	MS Desktop	Pass	0	1
01 Computer_15	192.168.2.15	MS Desktop	MS Desktop	Pass	0	1
01 Computer_16	192.168.2.16	MS Desktop	MS Desktop	Pass	0	1
01 Computer_17	192.168.2.17	MS Desktop	MS Desktop	Pass	0	1
01 Computer_18	192.168.2.18	MS Desktop	MS Desktop	Pass	0	1
01 Computer_19	192.168.2.19	MS Desktop	MS Desktop	Pass	0	1
01 Computer_20	192.168.2.20	MS Desktop	MS Desktop	Pass	0	1
01 Computer_21	192.168.2.21	MS Desktop	MS Desktop	Pass	0	1
01 Computer_22	192.168.2.22	MS Desktop	MS Desktop	Pass	0	1
01 Computer_23	192.168.2.23	MS Desktop	MS Desktop	Pass	0	1
01 Computer_24	192.168.2.24	MS Desktop	MS Desktop	Pass	0	1
01 Computer_25	192.168.2.25	MS Desktop	MS Desktop	Pass	0	1
01 Computer_26	192.168.2.26	MS Desktop	MS Desktop	Pass	0	1
01 Computer_27	192.168.2.27	MS Desktop	MS Desktop	Pass	0	1
01 Computer_28	192.168.2.28	MS Desktop	MS Desktop	Pass	0	1
01 Computer_29	192.168.2.29	MS Desktop	MS Desktop	Pass	0	1
01 Computer_30	192.168.2.30	MS Desktop	MS Desktop	Pass	0	1
01 Computer_31	192.168.2.31	MS Desktop	MS Desktop	Pass	0	1
01 Computer_32	192.168.2.32	MS Desktop	MS Desktop	Pass	0	1
01 Computer_33	192.168.2.33	MS Desktop	MS Desktop	Pass	0	1
01 Computer_34	192.168.2.34	MS Desktop	MS Desktop	Pass	0	1
01 Computer_35	192.168.2.35	MS Desktop	MS Desktop	Pass	0	1
01 Computer_36	192.168.2.36	MS Desktop	MS Desktop	Pass	0	1
01 Computer_37	192.168.2.37	MS Desktop	MS Desktop	Pass	0	1
01 Computer_38	192.168.2.38	MS Desktop	MS Desktop	Pass	0	1
01 Computer_39	192.168.2.39	MS Desktop	MS Desktop	Pass	0	1
01 Computer_40	192.168.2.40	MS Desktop	MS Desktop	Pass	0	1

Security i-Cue

Security i-Cue Evaluation Summary - 5/13/2013 12:24:29 AM Overview

Evaluation Risk Indexes by Threat

Top 10 Control Potential

Control	Score	Weighted Potential
ACT	88	149.85
ADG	87	82.91
EN3	85	52.45
CM4	85	40.4
ACD	87	66.28
ACT2	79	64.4
AK2	87	83.25
PE2	73	46.58
AT5	53	43.91
L4G	47	31

Security i-Cue

Security i-Cue Threat Custom Dashboard - 5/13/2013 12:34 PM Evaluation

Evaluation Risk Indexes

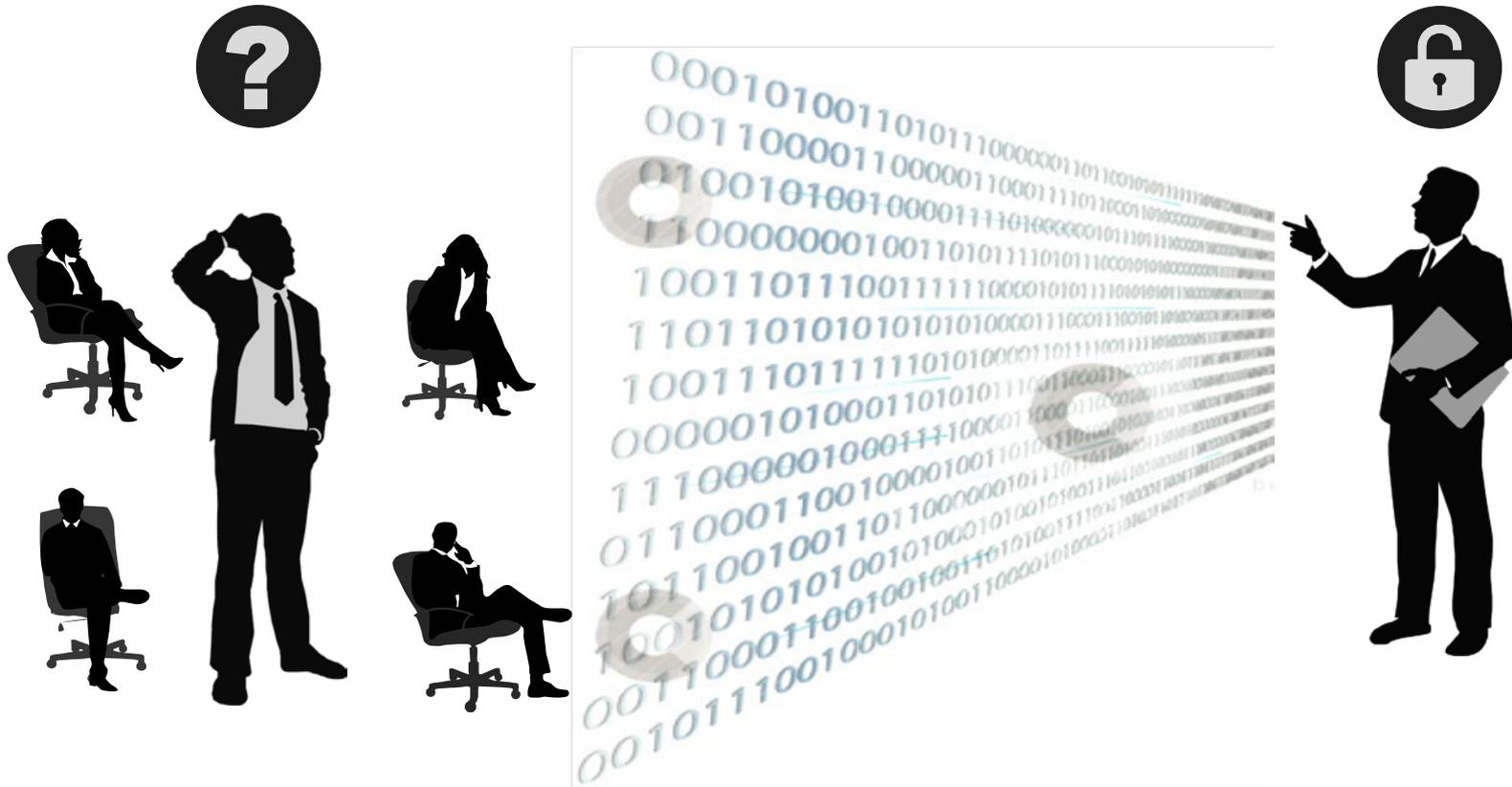
Form Control Scores

Security i-Cue

Control Report Matrix

Control ID	Control Name	Control Type	Control Status	Control Category	Control Subcategory	Control Score	Control Weight	Control Potential
AC1	Network Management	Network	Compliant	Network	Network	100	100	10000
AC2	Network Configuration	Network	Compliant	Network	Network	100	100	10000
AC3	Network Performance	Network	Compliant	Network	Network	100	100	10000
AC4	Network Security	Network	Compliant	Network	Network	100	100	10000
AC5	Network Availability	Network	Compliant	Network	Network	100	100	10000
AC6	Network Reliability	Network	Compliant	Network	Network	100	100	10000
AC7	Network Scalability	Network	Compliant	Network	Network	100	100	10000
AC8	Network Flexibility	Network	Compliant	Network	Network	100	100	10000
AC9	Network Interoperability	Network	Compliant	Network	Network	100	100	10000
AC10	Network Compatibility	Network	Compliant	Network	Network	100	100	10000
AC11	Network Portability	Network	Compliant	Network	Network	100	100	10000
AC12	Network Expandability	Network	Compliant	Network	Network	100	100	10000
AC13	Network Upgradeability	Network	Compliant	Network	Network	100	100	10000
AC14	Network Maintainability	Network	Compliant	Network	Network	100	100	10000
AC15	Network Recoverability	Network	Compliant	Network	Network	100	100	10000
AC16	Network Resiliency	Network	Compliant	Network	Network	100	100	10000
AC17	Network Fault Tolerance	Network	Compliant	Network	Network	100	100	10000
AC18	Network Availability	Network	Compliant	Network	Network	100	100	10000
AC19	Network Reliability	Network	Compliant	Network	Network	100	100	10000
AC20	Network Scalability	Network	Compliant	Network	Network	100	100	10000

Boards are demanding security risk information



Security i-Cue™ is the answer to:



- Understanding and analyzing cybersecurity data
- Providing a common language for business and security
- Identifying the critical business risks

Security i-Cue[™]

Prioritize Security Risk. Intelligently.

CEO Alfred Seifert, CISSP

aseifert@msbai.com

703-553-2571



Back up Slides

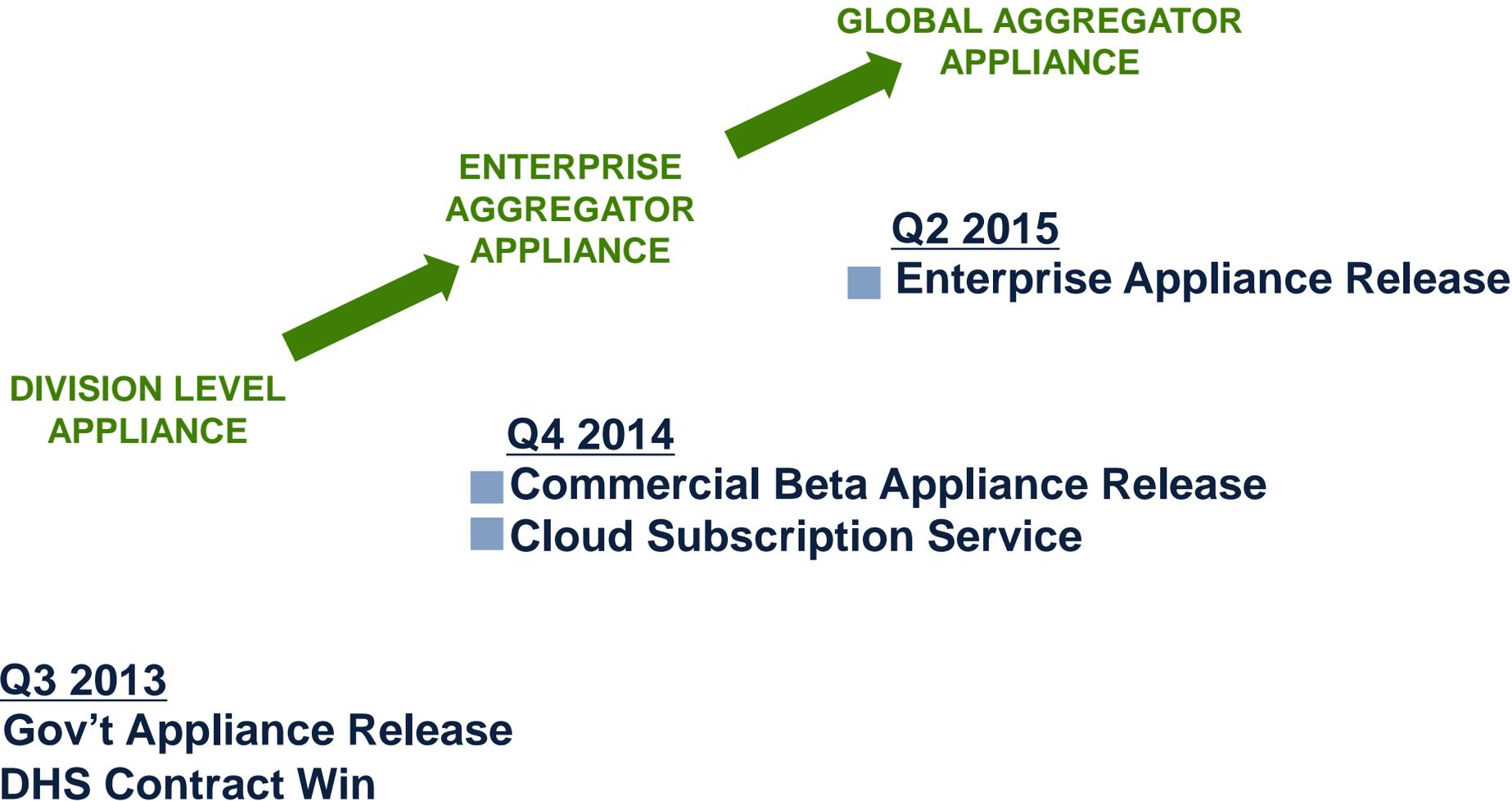
Large market opportunity

- Targeting Fortune 1000 & large government entities
- Market size is \$5B – growing to \$9.9B by 2018
- Timing is right

Customer Interest



Product Roadmap and Go-To-Market Milestones



Founding team

- Four startups
- Successful exits
- Long work history
- Security credentials

Al Seifert



Stuart Kurkowski, PhD



Eric Garnett



Financial Assumptions

Projected sales cycle – 9 to 18 months

License Fees

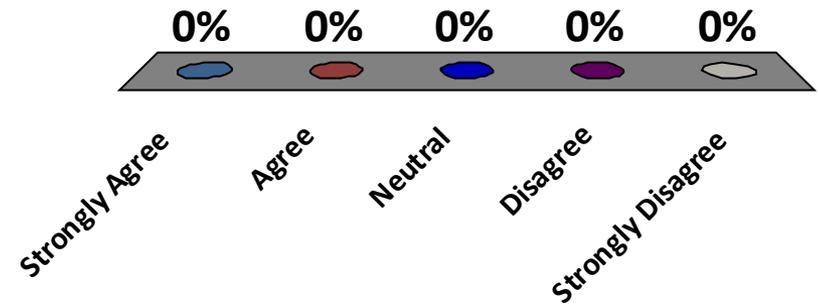
- Enterprise suite– comprehensive installations at \$2.0M to \$3.9M
- Large company– 6 to 10 Units at \$1.3M to \$1.95M
- Medium size company– 2 to 5 Units \$310K to \$730M
- Maintenance Fee – 20% per installation price

Revenue Targets

Year	Units	Revenue
2014	1	\$50,000
2015	15	\$2.6 million
2016	36	\$6.3 million
2017	110	\$19.2 million
2018	175	\$30.6 million
2019	300	\$52.5 million

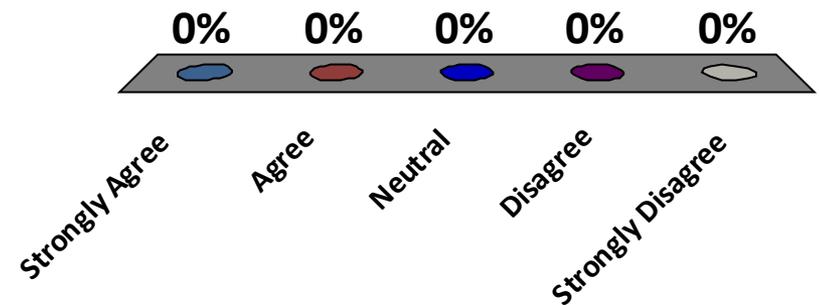
Do you feel the presenter explained their product thoroughly?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



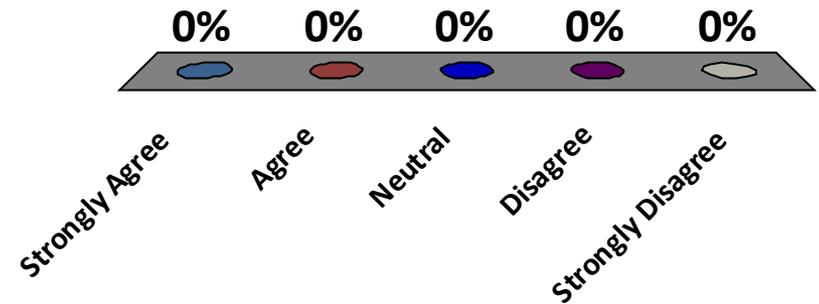
Do you think you this product will provide benefit directly to your environment?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



AXON *Ghost Sentinel*

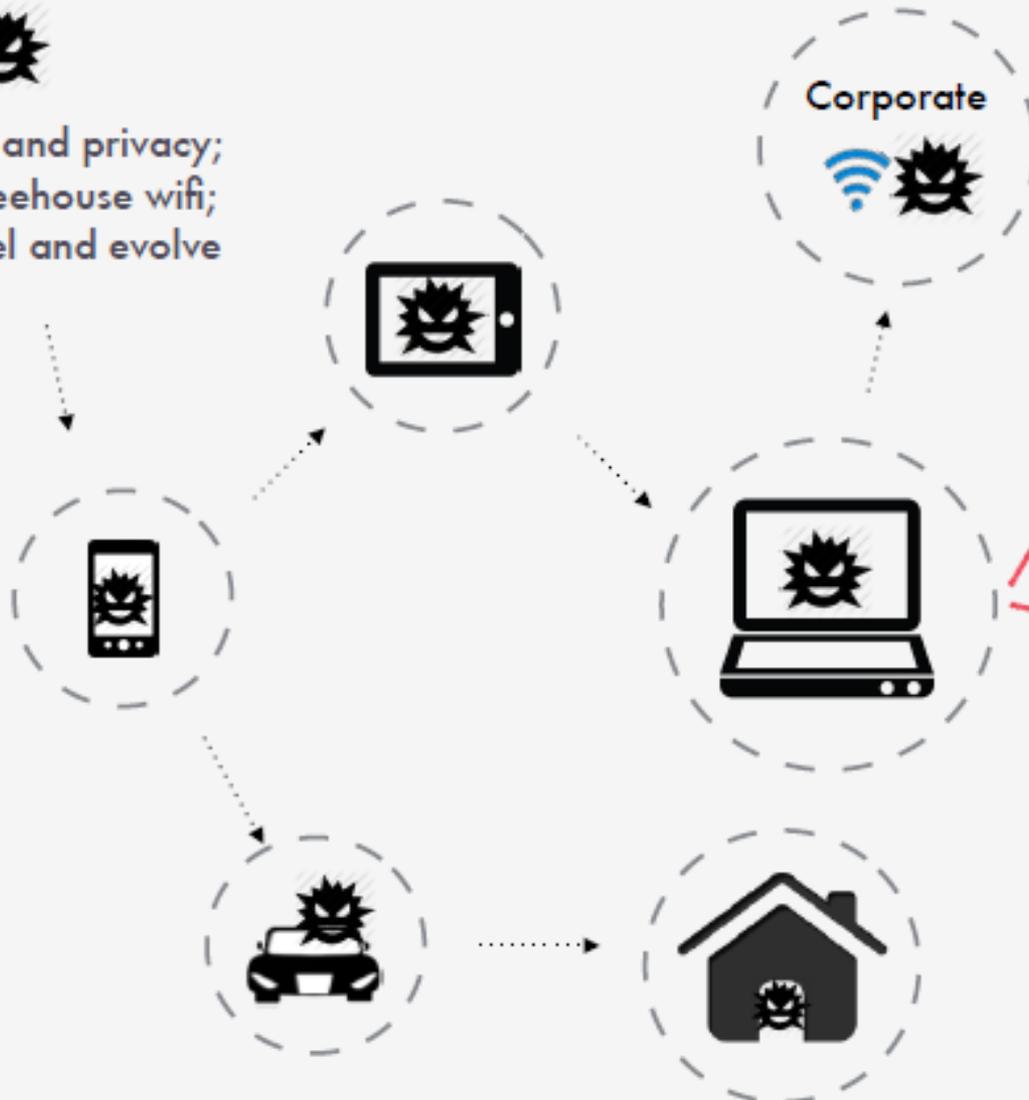
Michael Markulec
President & CEO
mmarkulec@axonghostsentinel.com

January 2015

Securing the Borderless Network



Steals IP, \$, and privacy;
lives in coffeehouse wifi;
likes to travel and evolve



Current defenses are
slow, intrusive, and
can't learn

Traditional Endpoint Security

Containerization



- Container applications limit what applications user can run on their device
- Constrains and severely limits device use and frustrates users
- Leads to non-compliance; new class of malware specifically targeting containers

Traditional Endpoint Agents



- Computer program on device that tracks and logs device behavior over time
- Analyze data locally or in cloud, with analysis indicating compromise
- Jeopardizes device performance, delays threat analysis, and difficult to port to different OS and devices

Centralized Data Analysis



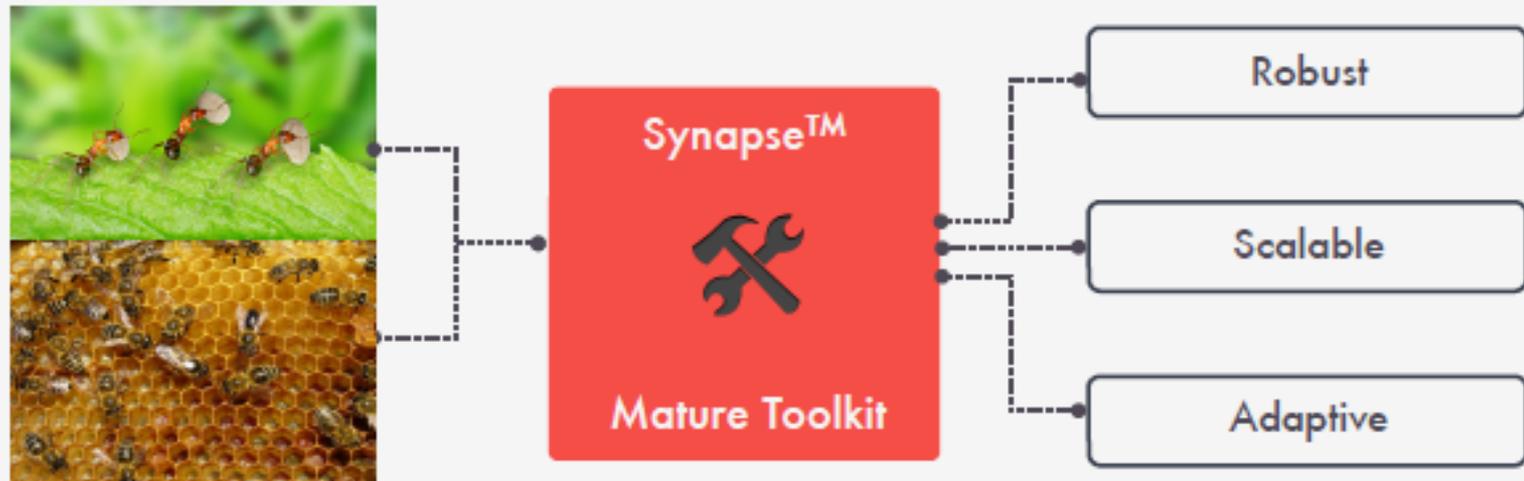
- Collect data into central repository for analysis, then push threat warnings to users
- Often requires investment in server racks, and restricts bandwidth
- Delays threat warnings and algorithms usually unable to detect attacks in a timely manner

Underlying Swarm Intelligence

Current approaches cannot handle non-linear complexity and are expensive

Inspired by natural self-organizing systems

Rapidly create solutions



Generate cost and efficiency savings - Solves problems that others cannot

End Point Anomaly Detection

1



The user downloads AGS technology onto their device or the technology comes pre-installed. The program downloaded is called a "Hive" and it contains a "Colony" of "Ghosts".

2

"How much memory is being used?"



Each ghost, like a bee is a computationally simple and lightweight entity. It samples specific information about the device. The ghosts NEVER collect any personal information or look at the content generated by the user.

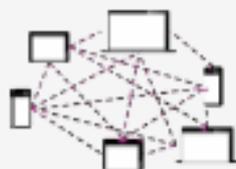
3

"How is your device doing?"



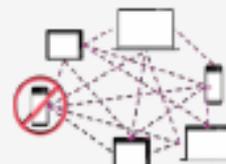
The Colony on one device then queries Colonies on other devices via the P2P overlay. This communication between devices establishes the "Apiary", which is a specific collection of devices and networks. For example, a company that wants to deploy AGS technology could have their own Apiary.

4



A Colony queries other Colonies about their assessment of the device's behavior. In simplistic terms, ghosts in one device speak to ghosts in other devices and ask them how their device is doing and what their device is doing. Ghosts that say their device is behaving abnormally generate more queries from other ghosts, thereby creating a "swarming" effect.

5



The more abnormal a device is behaving, the greater the "swarming" effect. Abnormality is defined by our special algorithms. At a certain threshold of "swarming", the system tells the administrator or user that something is wrong and, if programmed to, takes preemptive action.

Carnica - Mobile Device Security

Our products use swarm intelligence and peer-to-peer processing to:

- provide early-warning detection of threats in all devices
- preemptively take customized actions to stop attacks
- provide situational awareness of networks
- not interfere with device use and performance
- free the user from worry

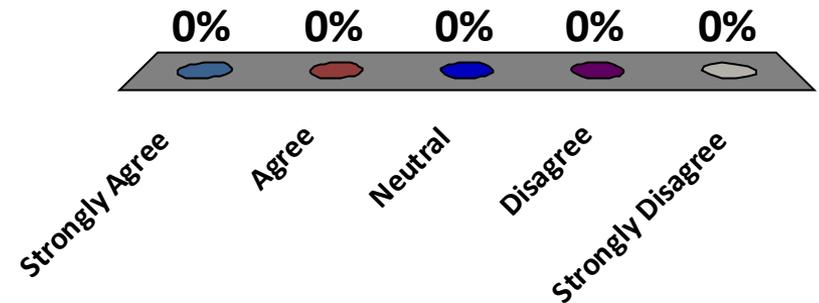
“No one today is using this type of advanced swarming technology to protect devices... and there is great opportunity in the market for a real solution to mobile security” - Gartner, VP - Wireless Mobile Security



AXON *Ghost Sentinel*

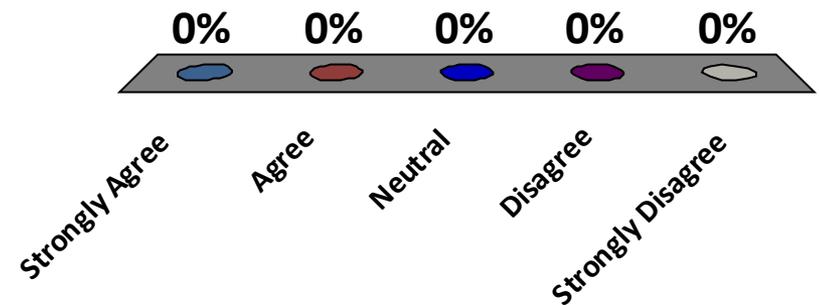
Do you feel the presenter explained their product thoroughly?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



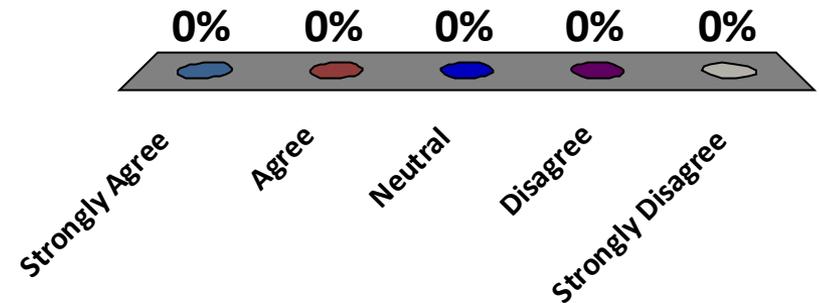
Do you think you this product will provide benefit directly to your environment?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



SYNCURITY NETWORKS



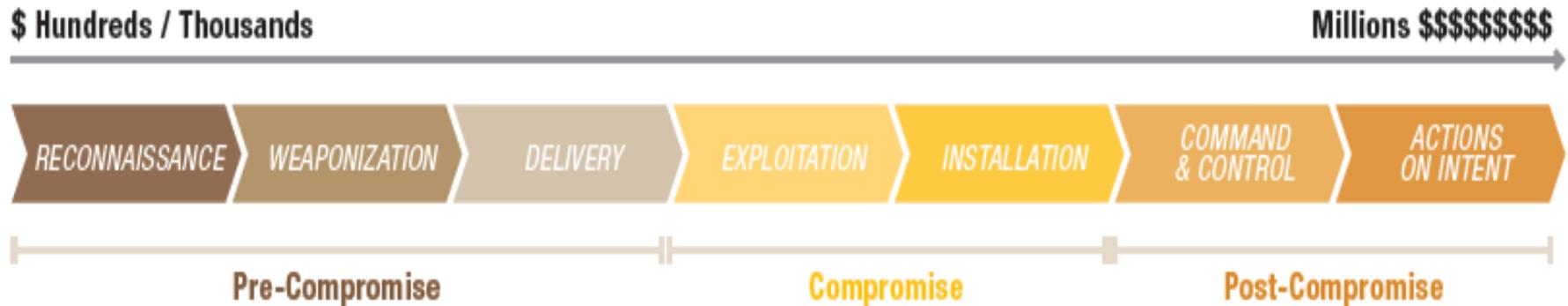
IR-Flow Introduction

JP Bourget, Founder and CEO

Our software, IR-Flow streamlines cyber security alert and incident response management, enabling companies to respond in a consistent, repeatable and measurable manner, in a single pane of glass.

Companies Are NOT Prepared

INCREASING RISK & COST TO MAINTAIN & REMEDIATE



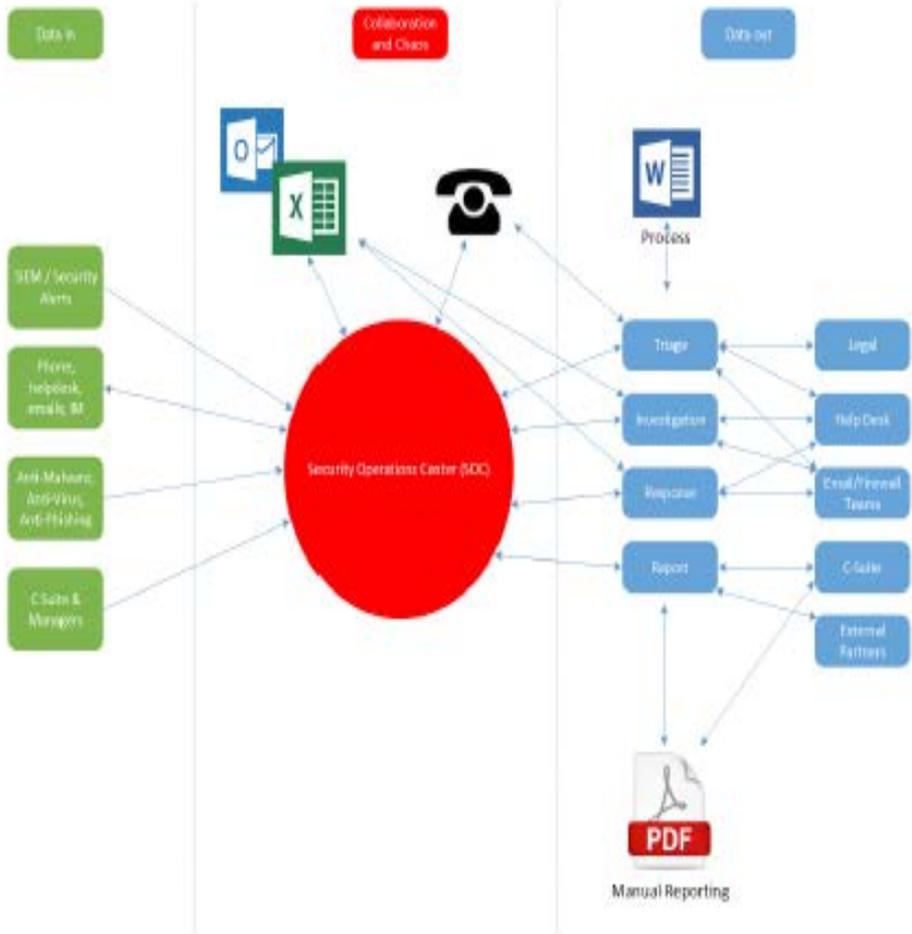
The Problem

Companies are struggling with:

- Responding to the **firehose** of **security alerts** in **email** and **spreadsheets**
- **Collaboration and Visibility** for **alert triage** and **incident response**
- **Enriching** alert data with **existing security tools** and **intelligence**
- **Reporting** and **compliance** is largely **manual** and **time consuming**
- **Inadequate response** leads to **losses**



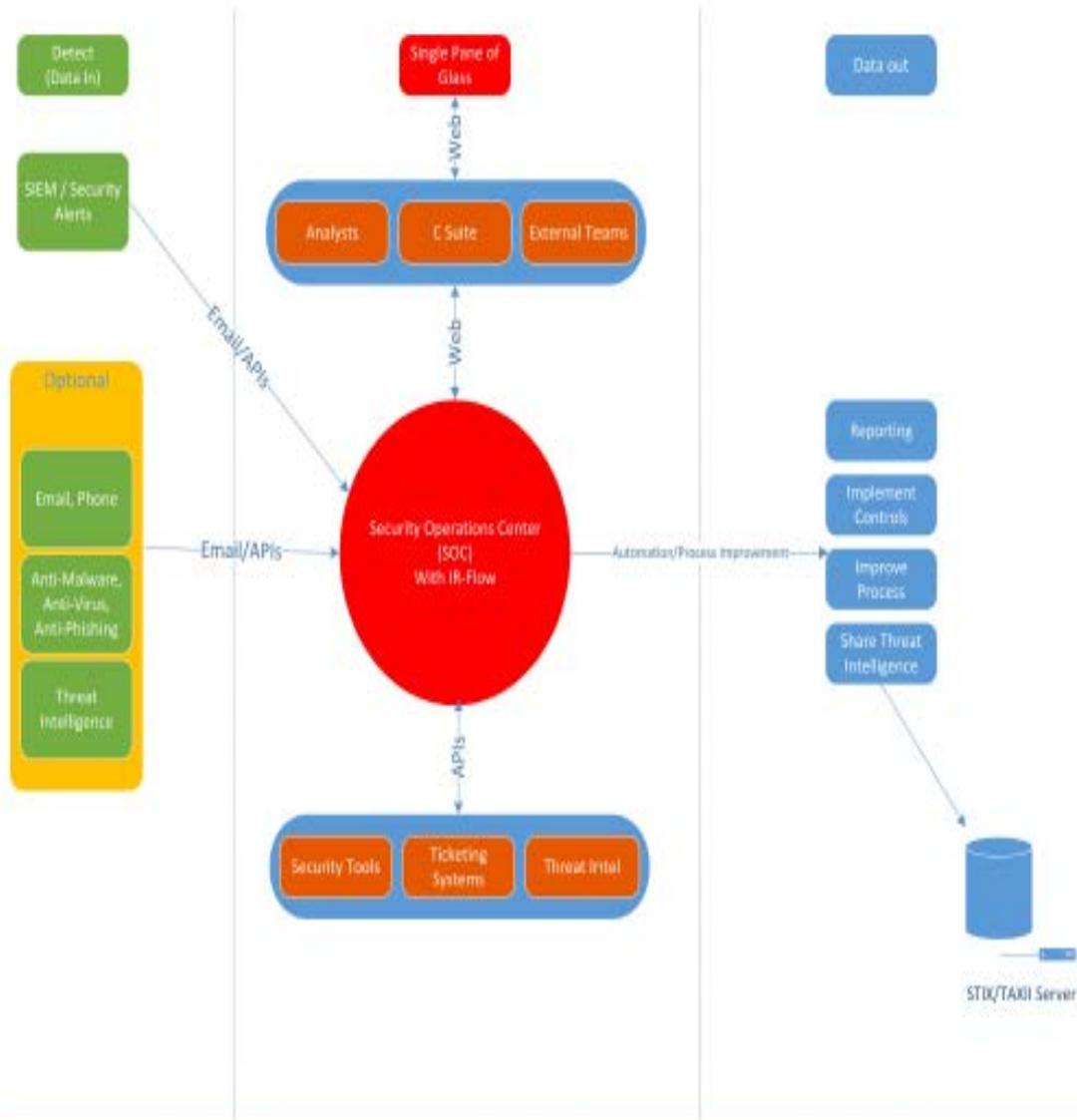
Before IR-Flow



Source: NIST



With IR-Flow



The Solution: IR-Flow

An Incident Response Management Platform

Mitigate before the breach with:

- Event handling -> **Triage** -> **Investigations** -> **Incidents or false positives**
- **Orchestration, visibility**, tool integration and **collaboration**
- Institutional knowledge **capture**
- **Automated** forensic artifact **collection and data enrichment (context)**
- **Reporting** measures performance and attack surface area



SOC Alert Queue

Home | Incoming | Incidents | Tasks | Cases | Engine | Config | Metrics | System

Admin Panel | Logged in as admin | Logout

Incoming Events

New or Parsed evidence or artifacts. Triage Events into Incidents or False positives.

25 records per page

low All Search

Event Num	Creation Time	Event Source	External Links	Notes	Status	Assignee	Incident Num	Actions
42	Mar 10, 2015 06:15:03 PM		Link to Results		New	admin		Create Incident, Add to..., False - ignore
39	Mar 10, 2015 06:12:27 PM		Link to Results		False - ignore			Create Incident, Add to..., Undo False
38	Mar 10, 2015 03:10:26 PM		Link to Results		New	admin		Create Incident, Add to..., False - ignore
37	Mar 10, 2015 03:15:13 PM				False - ignore			Create Incident, Add to..., Undo False
36	Mar 10, 2015 03:14:09 PM				False - ignore			Create Incident, Add to..., Undo False
35	Mar 10, 2015 02:59:24 PM		Link to Results		New	admin		Create Incident, Add to..., False - ignore
34	Mar 10, 2015 02:55:27 PM		Link to Results		False - ignore			Create Incident, Add to..., Undo False
33	Mar 10, 2015 02:52:31 PM		Link to Results		False - ignore			Create Incident, Add to..., Undo False
32	Mar 09, 2015 04:37:27 PM	Other			False - ignore			Create Incident, Add to..., Undo False
31	Mar 09, 2015 05:35:18 PM	Proofpoint URL		I? clicked a phishing link - looks bad - will make incident.	Incident	admin	11	Create Incident, Add to..., False - ignore
30	Mar 09, 2015 05:34:58 PM	Proofpoint URL		Not sure - if what did you do?	Incident	admin	12	Create Incident, Add to..., False - ignore
29	Mar 06, 2015 05:52:01 PM	SIA255 Wildfire URL			New			Create Incident, Add to..., False - ignore
28	Mar 06, 2015 05:52:00 PM	SIA255 Wildfire URL			New			Create Incident, Add to..., False - ignore
27	Mar 06, 2015 05:51:58 PM	Officer Offense ID			New			Create Incident, Add to..., False - ignore
26	Mar 06, 2015 05:51:58 PM	Officer Offense ID			New			Create Incident, Add to..., False - ignore
25	Mar 06, 2015 05:51:56 PM	SIA255 Wildfire URL			New			Create Incident, Add to..., False - ignore
24	Mar 06, 2015 05:51:38 PM	Officer Offense ID			New			Create Incident, Add to..., False - ignore
23	Mar 06, 2015 05:50:36 PM	SIA255 Wildfire URL			New			Create Incident, Add to..., False - ignore



Alert Triage

IR-Flow

Admin Panel Logged in as admin Logout

Incoming Events

New Event

Email

Raw or Parsed evidence or artifacts. Triage Events into Incidents or False positives.

25 records per page

New All

Search:

Event Num	Creation Time	Event Source	External Links	Notes	Status	Triage Progress	Assignee	Incident Num	Actions
82	Apr 30, 2015 02:57:54 PM	Palo Alto Wildfire	SHA256 Wildfire URL		New	<div><div style="width: 20%;"></div></div>			Create Incident Add to... False - Ignore
81	Apr 30, 2015 02:44:53 PM	Phishing	Proofpoint URL		New	<div><div style="width: 20%;"></div></div>			Create Incident Add to... False - Ignore
71	Apr 30, 2015 02:41:04 PM	Palo Alto Wildfire	SHA256 Wildfire URL		New	<div><div style="width: 0%;"></div></div>			Create Incident Add to... False - Ignore
70	Apr 30, 2015 02:41:03 PM	Palo Alto Wildfire	SHA256 Wildfire URL		New	<div><div style="width: 0%;"></div></div>			Create Incident Add to... False - Ignore
69	Apr 29, 2015 09:02:42 PM	Palo Alto Wildfire	SHA256 Wildfire URL		New	<div><div style="width: 20%;"></div></div>			Create Incident Add to... False - Ignore
63	Apr 24, 2015 08:48:47 PM	QRadar	QRadar Offense ID		New	<div><div style="width: 0%;"></div></div>			Create Incident Add to... False - Ignore
62	Apr 24, 2015 04:14:27 PM	QRadar	QRadar Offense ID		New	<div><div style="width: 0%;"></div></div>			Create Incident Add to... False - Ignore
61	Apr 24, 2015 04:14:26 PM	QRadar	QRadar Offense ID		New	<div><div style="width: 20%;"></div></div>	Block		Create Incident Add to... False - Ignore

Showing 1 to 8 of 8 entries

Event #82 - Apr 30, 2015 02:57:54 pm - Assigned To: < No Assigned User >

Incoming Data Group: Palo Alto Wildfire

Source IP : 127.0.0.1
Username : Synchrony-shmpage
Destination IP : 127.0.0.1
SHA256 : 7986c70f016ce14811...

Wildfire URL : urldefense.proofpoi...
Wildfire Verdict : This sample was determin...
ed to be malware. Summary of behaviors o...
bserved during analysis : - Created or modifi...
ed a file - Started a process - Modified the

Triage Check List

40% Complete

- Check MD5 on Virus Total
- Reverse DNS lookup on external IP
- Check Bro File.log for earlier execution
- Validate event

SYNCURITY
NETWORKS



Investigation/Incident Facilitation

iFlow
Admin Panel | Logged in as admin | Logout

Incoming
Incidents
Tools
Cases
Engine
Config
Metrics
System

Incidents / Incident #7

Incident Summary

Owner:	Opened:	14 days and 21 hours ago
# of Tasks Open	Status:	
Severity:	Actions:	<input checked="" type="checkbox"/>
Priority:	Stages:	
Type:	Sub-Type:	Inbound Phishing
Description: Inbound Phishing Message sent to user Davidson, Ray - Looks like it might be phishing for Google Credentials.		

Tasks

ID	Assigned	Priority	Stage	Status	Name	Actions
47	RPeck	High	Identification	Closed	Gather Attack Info	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
48	RPeck	High	Identification	Closed	Determine clickers/submitters	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
49	RPeck	High	Eradication	New	Eradicate the effects of the phishing message	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
50	RPeck	High	Identification	New	Determine who clicked the phishing link	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
51	RPeck	High	Containment	New	Determine who submitted the form	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
52	RPeck	Immediate	Recovery	Waiting	Remediation for users who submitted the form	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
53	RPeck	High	Containment	New	Contain the Phishing Page	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
54	RPeck	Immediate	Identification	New	Submit Honeytoken Credentials	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
55	RPeck	High	Identification	Closed	Get Screenshot/Copy of Actual email	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

[Add Task](#)

Events

Date / Time	Event Type	Data Source	Actions	Source IP	Source Port	Username	Destination IP	Reporting Person	Short Description
2015-02-13 18:19:26		QKadir	<input checked="" type="checkbox"/>	127.0.0.1					Exploit/Malware Events Across Multiple Targets
2015-02-25 18:12:25		Phishing	<input checked="" type="checkbox"/>					ray_davidson@syncurity.net	phish

[Add Event](#)

Parsed Lists

(None found)

File Attachments

[Drop files here or CLICK to upload](#)



Reporting



Charts

Incidents by property

Filters

Status

all

Incident Type

all

Incident Sub-Type

all

Quick Range

Last 90 days

Custom Range

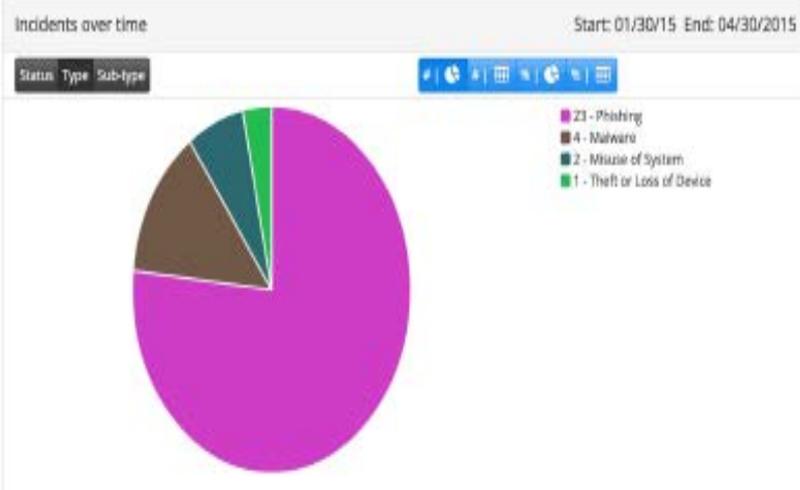
Start Date

01/30/15

End Date

04/30/2015

Update



Where is IR-Flow going?

- Improved Reporting
- Visualization of Response process (optimization and flexibility)
- More automation (alert context, control recommendations)
- Outbound threat intelligence sharing

Building relationships with ISACs

*ISAC: Information Sharing and Analysis Centers



Syncurity Team



JP Bourget

CEO

*SIEM and IR Consultant
Former RIT Prof
10 Years in Industry*



Mike Volo

VP Engineering

*3rd Software Startup
12 Years software design*



Ryan Peck

Security Analyst

*Former SPARSA president, 3
years of IR*



Brian Gaeddert

Software Engineer

*6 years of Full Stack Web
App Development*



John Jolly

CRO, Redjack

*Former VP, General Dynamics
Responsible for IR Practice*



Ben Walter

Security Op Mgr, Box.com

Built IR team at Salesforce.com



François Bégin

Principal, Catalyst Partners

*30 years consulting for Gov't (DHS,
IC) and Commercial*



Matt Ahrens

VP, Guidepoint Security

*VP at Guidepoint
Former IR Lead, Fishnet*

**SYNCURITY
NETWORKS**



Questions?



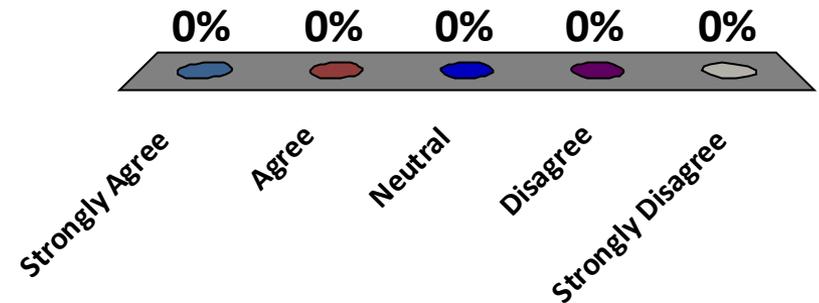
JP Bourget, CEO

jp@syncurity.net
www.syncurity.net
585-319-1706



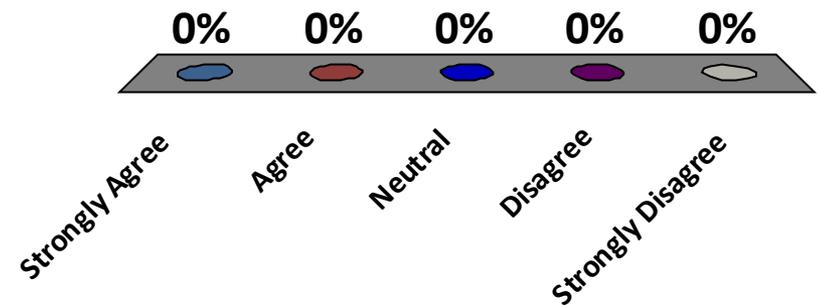
Do you feel the presenter explained their product thoroughly?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



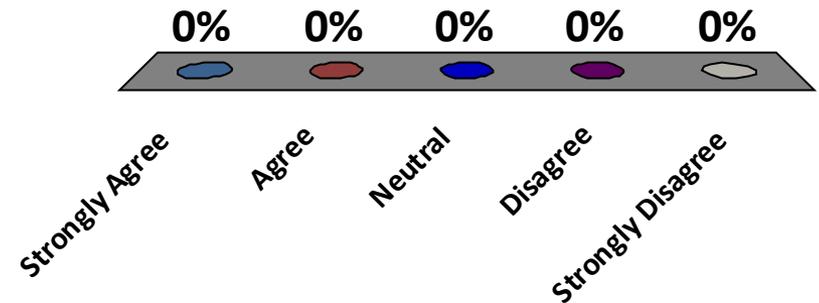
Do you think you this product will provide benefit directly to your environment?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree





BiJoTi

SECURITY PERFORMANCE MANAGEMENT

 [BiJoTi.be](https://www.BiJoTi.be)

 info@BiJoTi.be

Midmarket Cybersecurity Challenges



“Forty percent of the data-security breaches experienced by organizations arise from attacks on their suppliers.” - The Information Security Forum (ISF)

BiJoTi

475 PERSON DEFENS

5 TECHNOLOG

2 IT PE

Case

1 NETWORK

1 APP DEV

1 DIRE



MARSH

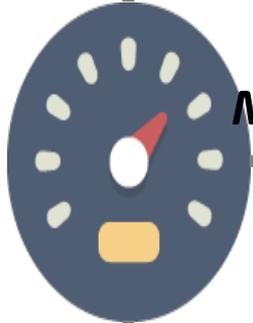
JoTi

Case Study

“Logs?”



Compliance



*Security
Monitoring*



Long Term
Log Storage



Security
Performance
Management

SPM



Modular
Partner
Toolbox

*Actionable
Intelligence*

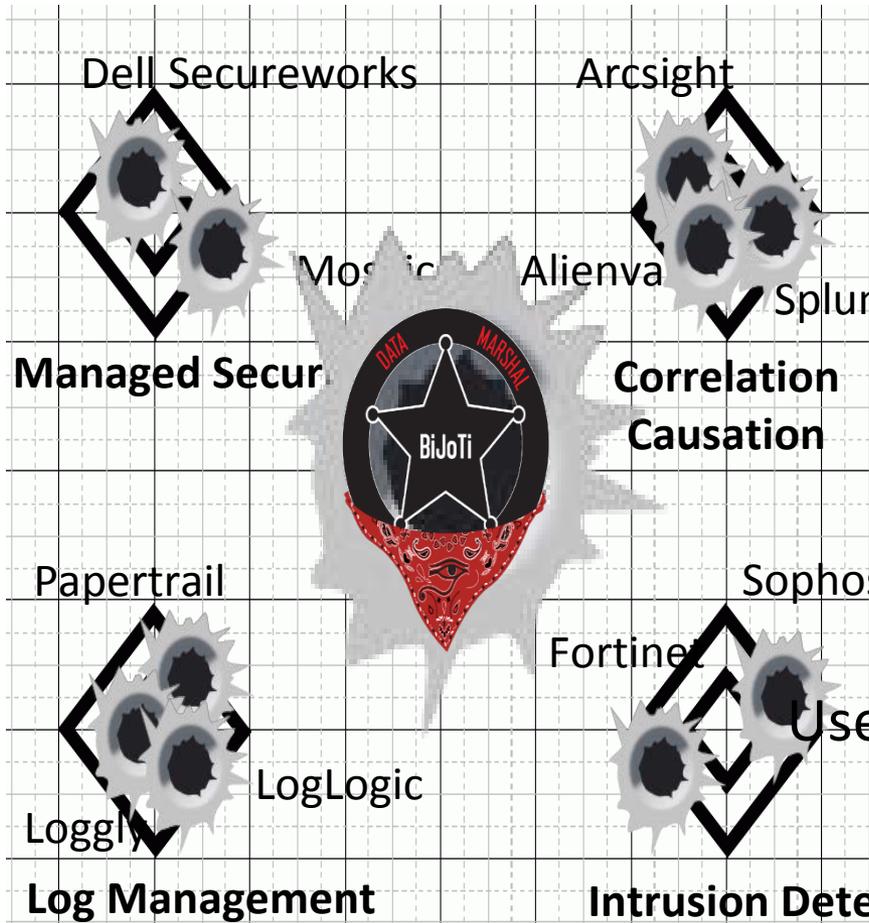


Case
Management

Security Performance Management

- Security as a Service
- Easy-To-Use Web Based Dashboard
- Maximize existing security infrastructure
- Reduce your cost
- Prove your compliance
- Maximize the efficiency of your team





BiJoTi Hits the market

Ease of Implementation

Provable Compliance

Use your existing Security Infrastructure

BiJoTi

Traction

Product Release!



Channel Partner!



Customer!



Market Move

The cloud-based security services market is rising



SOURCE: GARTNER

The Gift





BiJoTi.be

Thank you!



Josh@BiJoTi.be

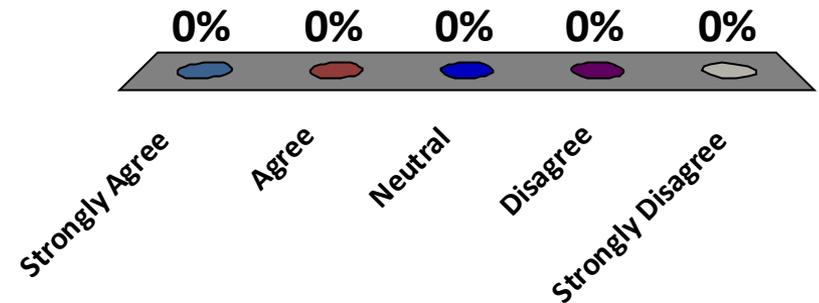


APPENDIX



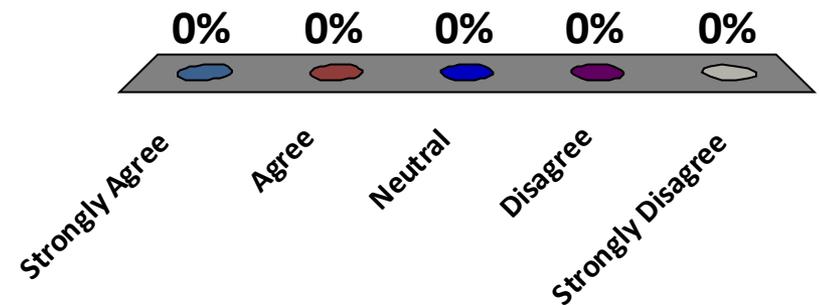
Do you feel the presenter explained their product thoroughly?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



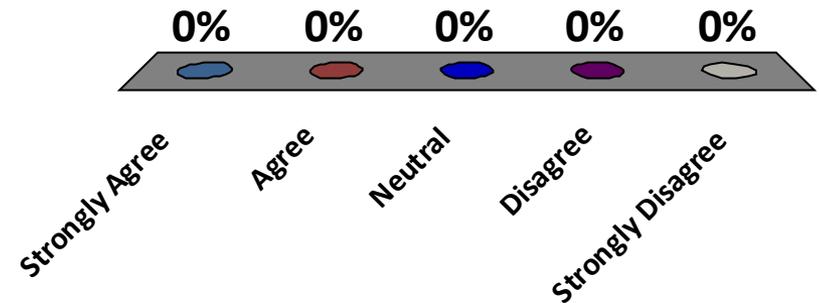
Do you think you this product will provide benefit directly to your environment?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



Do you think there are other parties within the State or Local government that would benefit from this type of product?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree

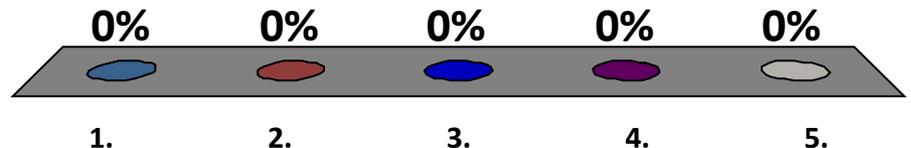


MACH37 Project Presentations

Summary Questions

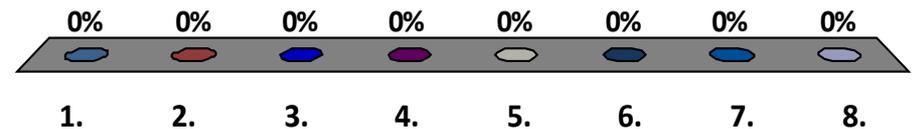
Do you feel you received enough detail about the products and/or services to decide whether to invest in it or not?

1. Strongly Agree
2. Agree
3. Neutral
4. Disagree
5. Strongly Disagree



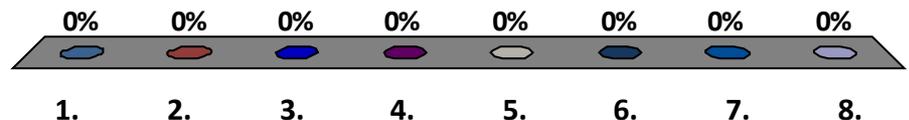
Pick one product which you would recommend investing in first

1. Presenter #1- Eunomics
2. Presenter #2- Shevirah
3. Presenter #3- Anatrope
4. Presenter #4- Atomicorp
5. Presenter #5- MSB
6. Presenter #6- Axon
7. Presenter #7- Syncurity
8. Presenter #8- Bijoti



If there is one product you would be interested in being a POC/Beta evaluator, which one would it be?

1. Presenter #1- Eunomics
2. Presenter #2- Shevirah
3. Presenter #3- Anatrope
4. Presenter #4- Atomicorp
5. Presenter #5- MSB
6. Presenter #6- Axon
7. Presenter #7- Syncurity
8. Presenter #8- Bijoti



MACH37

Thank you!



Andrew Hallberg , ABC

ISO Knowledge Sharing Committee Update

May 6, 2015



SEC501-09

Mark Martens
Information Assurance Specialist

ISOAG
May 6th, 2015



Dates

- ORCA
 - December 24th 2014
- Final Revision
 - February 22nd 2015
- Effective Date
 - May 1st
- Compliance Date
 - August 1st



Changes

Revision 9	02/20/2015	<p>Updated in concert with NIST 800-53 Revision 4 and the Risk Management Framework.</p> <p>New Requirements: AC-2: j, k 12, 13; AC-6: 5, 7, 8; AC-20: 3, 4; AT-2: 1, 2; AU-4: 1; AU-5; AU-6: 1, 6; AU-7: 1; AU-12; AU-13; CA-7: 3; CM-2-COV: 4; CM-3: 6; CM-11; CP-2: 4, 7; CP-7: 6; IA-2: 5; IR-3: 2; IR-4: 1; MA-2: f; MA-5: b, c; MP-5: c; PE-13: 1, 2, 3, 4; PE-14: d; PS-4: b, f; PS-6: a, c; PS-7: b, d; RA-3: d; RA-5: d, e; SA-11: 4, 6, 7; SA-15; SA-16; SA-17; SA-18; SA-19; SA-20; SC-11; SC-18; SC-19; SC-37; SC-41; SC-42; SC-42-COV: 13, 16; SI-10: 2, 3;</p>
------------	------------	--

Identifying Changes in This Document

- See the latest entry in the table above
- Vertical lines in the left margin indicate that the paragraph has changed



Changes Continued

- Not applicable to COV
 - Cost, Effectiveness, Security Posture, etc..



Comments

- 118 Comments
- 14 Commenters
- 9 agencies
- 1 private company



Title not Relevant

Questions

????????????????

You may also send any questions to :
CommonwealthSecurity@VITA.Virginia.Gov



Virginia Information Technologies Agency

Upcoming Events





2015 IS Security Conference

Presentations from last month's Second Annual Commonwealth Security Conference now are posted on the VITA website for security and other IT professionals to use as references. The sold-out event was highly successful.

The presentations can be viewed at the link below:

<http://www.vita.virginia.gov/itac/default.aspx?id=6442472004>



Spring 2015 CISM and CISA Review Courses

Spring 2015 CISM and CISA Review Courses

The ISACA Virginia Chapter is sponsoring our annual 3-day intense Spring CISM and CISA Review Courses. The review program has been developed to assist those who plan to sit for the CISM or CISA exam. This 3-day review course focuses on the key points covered in the exam then followed by class practice questions and discussions. All of this at a very affordable rate.

Register here:

CISM: [CISM 2015 Spring Registration](#)

CISA: [CISA 2015 Spring Registration](#)



Spring 2015 CISM and CISA Review Courses

When: Saturday, May 9, 2015 - from 8:30am to 4:30pm
Saturday, May 16, 2015 - from 8:30am to 4:30pm
Saturday, May 30, 2015 - from 8:30am to 4:30pm

Where: Hilton Richmond Hotel at Short Pump
12042 West Broad Street
Richmond VA 23233

Fees : Member \$450.00
Non-Member \$500.00

Course price includes Continental Breakfast, lunch and refreshments during breaks. Anyone who fails to make payment online will not be considered an attendee unless special arrangements are made with VA ISACA Chapter



IS Orientation

When: Thursday, June 16th, 2015

Time: 1:00 pm to 3:00 pm

Where: CESC , Room 1211

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



Future ISOAG

June 3, 1:00 - 4:00 pm @ CESC

Speaker: Bruce Bryant, CA Technologies

ISOAG meets the 1st Wednesday of each month in 2015

ADJOURN

THANK YOU FOR ATTENDING

