[secure] ®

ISC8

SDN : Radically New Network Architecture

Deserves Radically New Cyber Security Protection

Llewellyn Derry

CISSP, CISM, C|EH

Vice President - Business Development

October 8, 2013

SECTOR

Security Education Conference

Company Proprietary

©2013 ISC8 Inc. All rights reserved

Safe Harbor Statement

All statements included or incorporated by reference in these slides, other than statements or characterizations of historical fact, are forward looking. These forward looking statements include guidance we will provide on our future operating results as well as the prospects for our various businesses and the development and status of new products and technologies. These forward looking statements and our assumptions about the factors that influence them, are based on the limited information available to us at this date. Such information is subject to change, and we may not inform you when changes occur. We do not undertake any obligation to revise or update publicly any forward looking statement, except as required by law.

Forward-looking statements are not guarantees of future results and are subject to risks, uncertainties and assumptions that are difficult to predict. Therefore, our actual results could differ materially and adversely from those described in statements you hear today as a result of various factors. We refer you to our current Form 10-K, subsequent Form 10-Qs and other filings with the SEC, which discuss some of the important risk factors that could contribute to such differences or otherwise affect our business, results of operations and financial condition.

©2013 ISC8 Inc. All rights reserved

Company Profile

Overview

- Founded in 1974, public in 1981, restructuring into Pure Play Cyber Security Company in 2011, divested of non-cyber assets in 2012, acquired 2 Cyber Security Products from Bivio Networks in 2012
- ~200 patents, $160mm of government R&D funding, $240mm of private funding
- HQ in Dallas, TX with Branch Offices in San Francisco Area, Europe, Asia and the Middle East

Product Groups

- Network cyber security
  - adAPT® – signature-less technology that identifies advanced malware movement at the core of the enterprise network
  - NetFalcon® – big data forensics of network activity for cyber security and intelligence
  - NetControl – carrier-grade content control platform

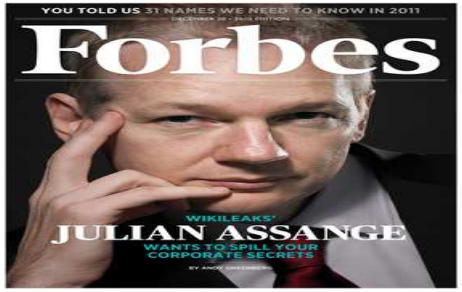
Customers/ Partners

- Service providers
- Law enforcement and government agencies
- Enterprises

©2013 ISC8 Inc. All rights reserved

“All War is Based on Deception”

- Sun Tzu
Author of the Book : “The Art of War”



Innovations in Deviance

"Researchers find APT malware that monitors mouse clicks to evade detection"

2-April-2013

Mouse Movement

"APT attackers getting more evasive, even more persistent"

5-April-2013

Waterhole

"The Changing Face of Advanced Persistent Threat"

19-August-2013

Box.com

This Is Not Your Father's Malware

[secure]®
ISC8

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

The State of Cyber Security Defense

Defense in Depth is Inadequate By Itself

- …but that is the defacto barometer of protection
- Several Hundred Billion Dollar Installed Base
- Network technology is focused on Connectivity not Awareness

Manual/Reactive Analysis is Too Late

- The horse has left the barn
- Today's cyber attacks are very stealthy
- Medical Examiner vs. Physician
- Networks are Growing – 10Gbs and Higher

Perimeter Defenses Leave Core Ignored

- Firewalls
- IDS/IPS
- Proxy Server
- A/V Server
- Malware Server

Patches/Updates are Ineffective

- They are late
- The 1st Release is largely ineffective
- Compatibility Issues w/existing HW/SW

Log File are Growing Exponentially

- 10Gbs Network Produces >200TBs of data PER DAY
- Expertise of Existing IT Staff
- Bandwidth of Existing IT Staff

Hacker Tactics Have Evolved, Enterprise Defenses Have Not

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

The Illusion of Today's Corporate Leadership

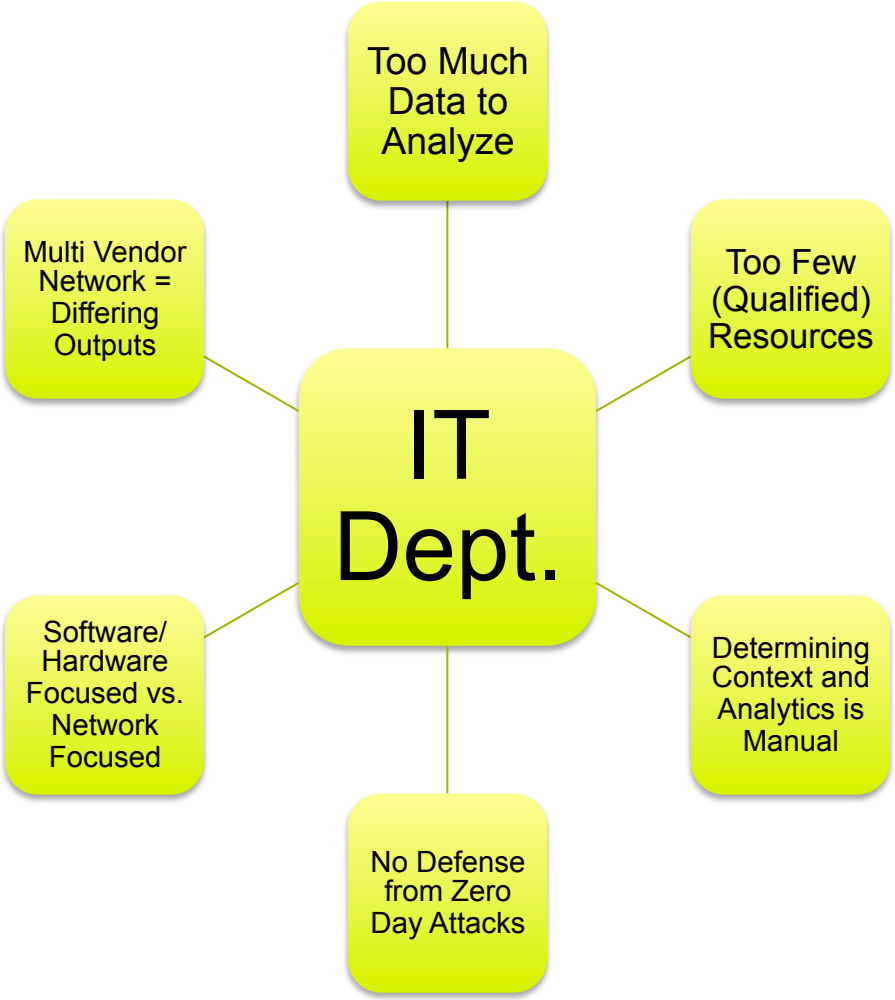
Latest Equipment & Upgrades + Absence of Alerts + Current Software Patches/ Updates + Defense In Depth Installed + IT Staff w/ Certifications ≠ Secure Enterprise Network

"The Disposition of the HW & SW on your Network is not an Accurate Barometer of the Cyber Security Posture of your Network."

How Does Your Company Measure It's Cyber Security Protection?

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

The Challenge of Today's IT Manager

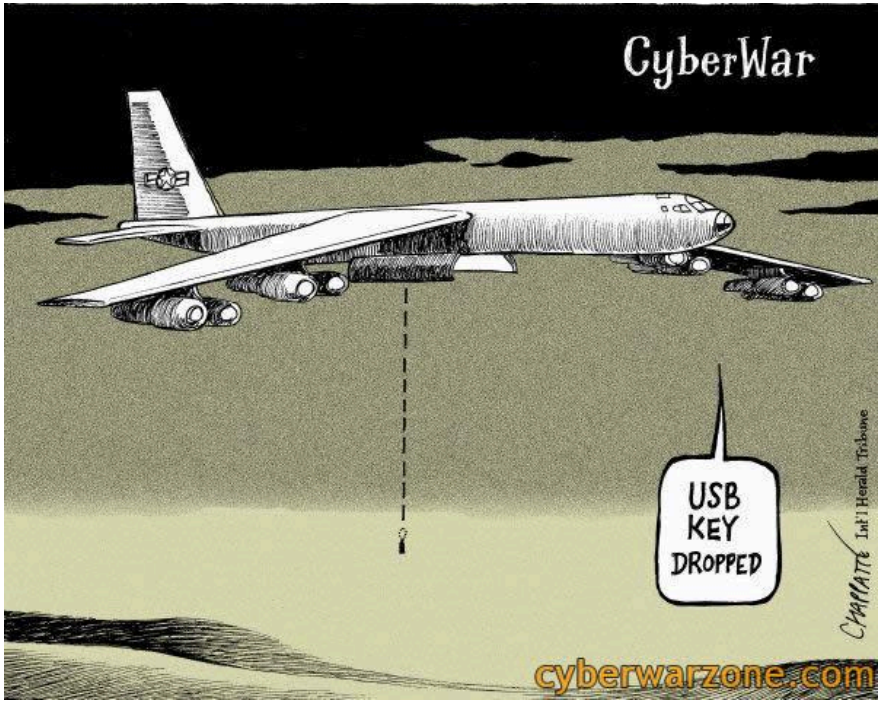


How Do You Lower Your MTTK?

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

The New Cyber Norm

- Stealth
- Well Funded
- Black Market
- Very Knowledgeable
- Very Shrewd
- Large Numbers (and Growing)
- Multiple Enemies in Multiple Geographies



You are outnumbered & outgunned everyday

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

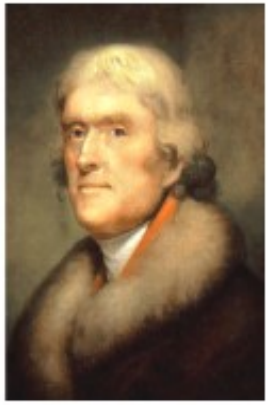
The Face of Cyber War : "Preparing For and Responding to the Enduring Threat"*

- A Defensible Architecture
- Global Situational Awareness
- A Common Operating Picture
- A Concept for how to Operate in Cyber Space
- Trained and Ready Cyber Forces
- The Capacity to Take Action When Authorized

Source : General Keith Alexander Commander : US Cyber Command & NSA/CSS. Speech to the Senate Committee on Appropriations* – June 2013

The price of freedom is eternal vigilance.

- Thomas Jefferson (1743 - 1826)

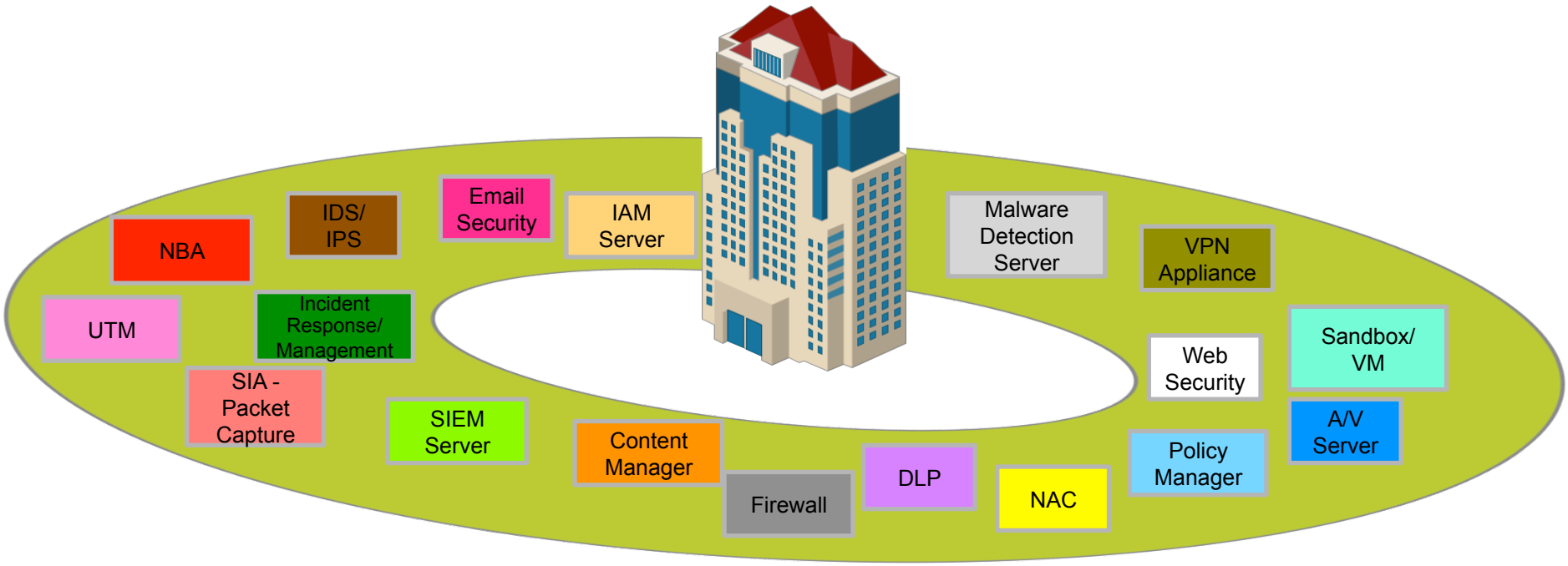


The U.S. DoD Game Plan

©2013 ISC8 Inc. All rights reserved

Perimeter Solutions Alone are Not Effective

Advanced Malware



[secure]®

ISC8

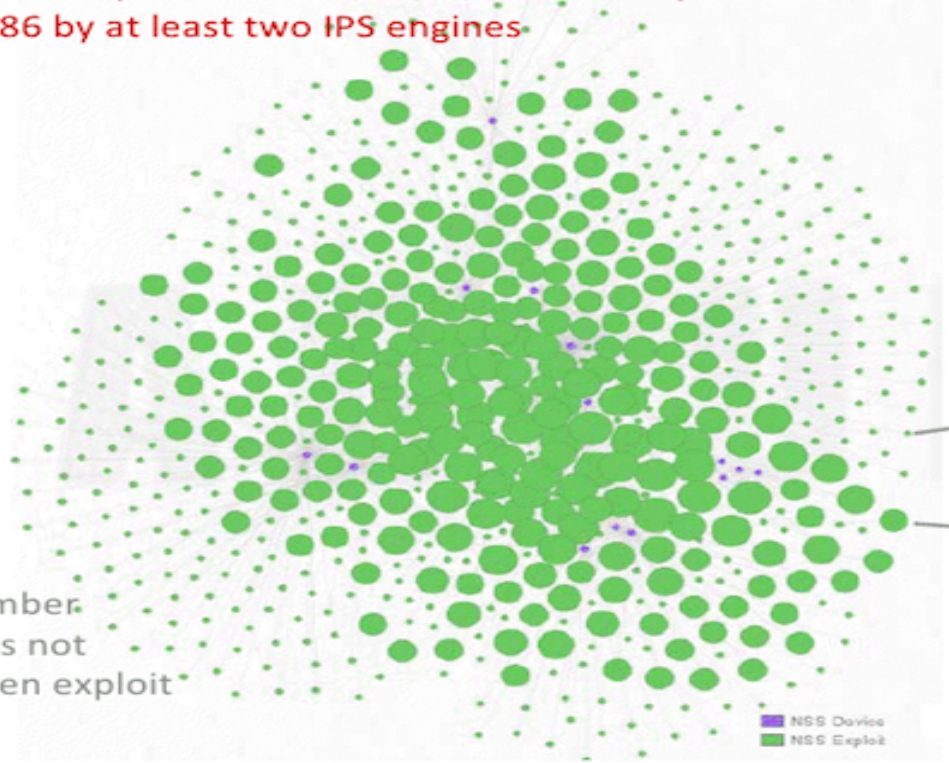
Question…Where is Your Perimeter?

The Emasculation of Defense in Depth

Correlation of undetected Exploits

Many exploits are not detected by several IPS engines

714 of 1,486 exploits tested are not detected by at least one IPS engine, 40% or 286 by at least two IPS engines



Undetected by one IPS

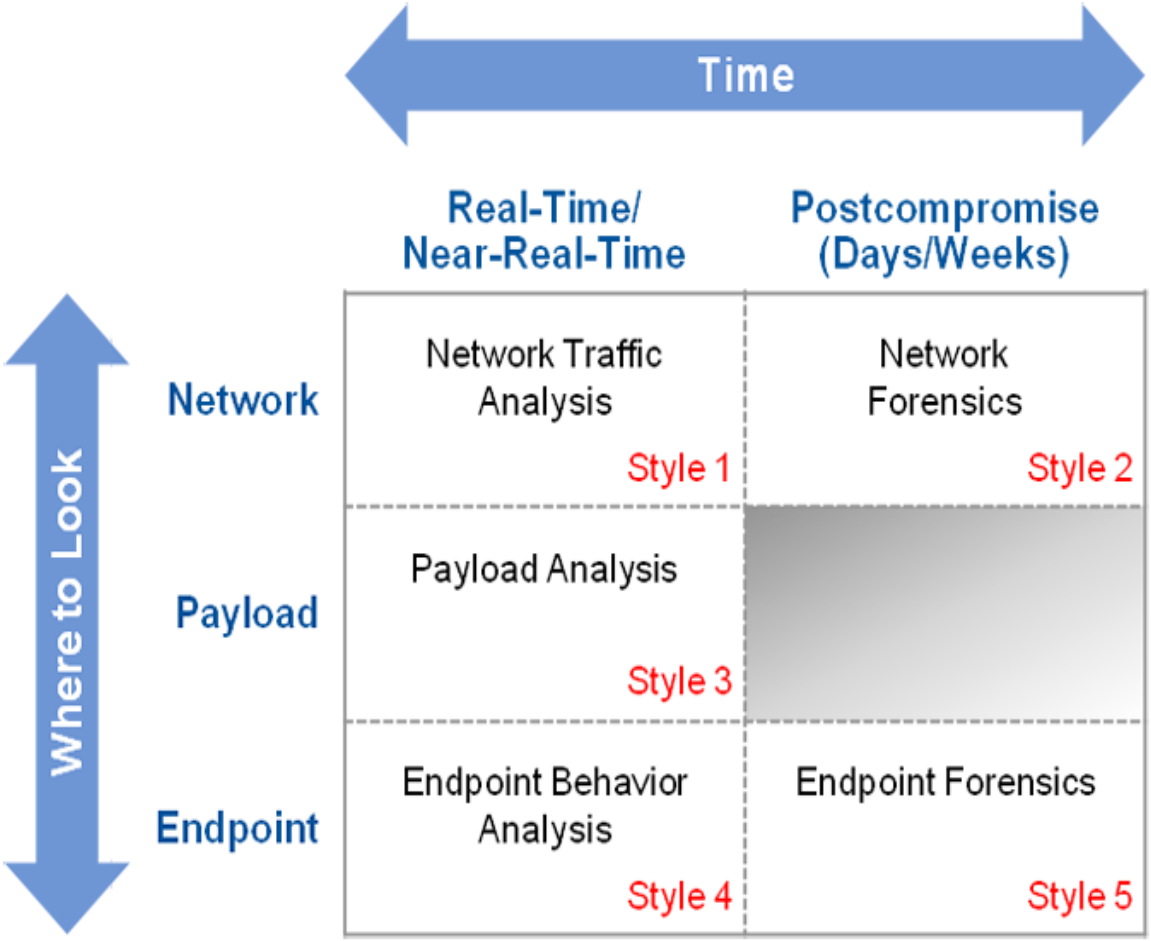
Undetected by multiple IPS

Bubble size indicates number of IPS engines not detecting given exploit

Source : NSS Labs February 2013

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

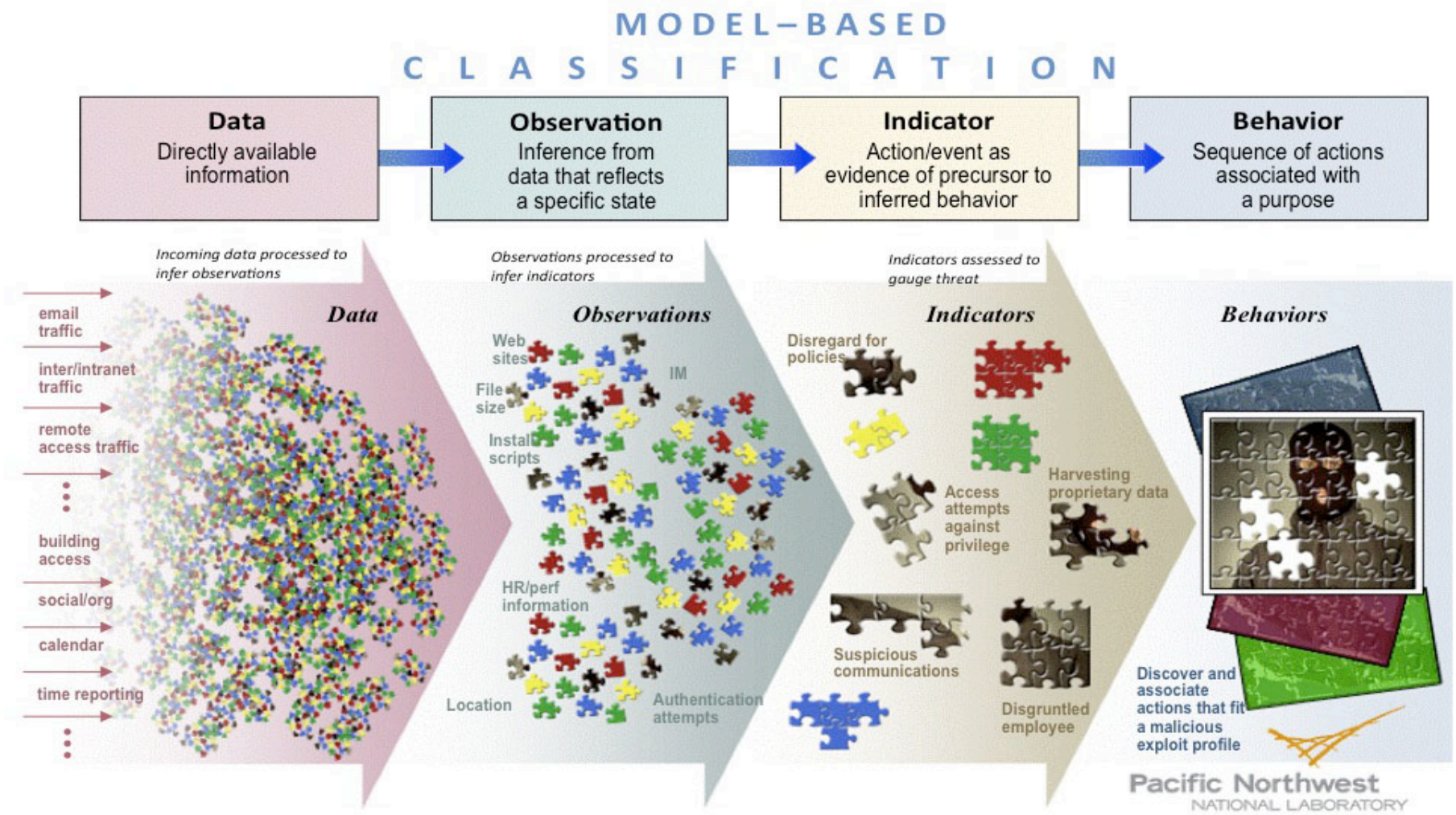
What Does Advanced Threat Defense Look Like?



Source :
"Five Styles of Advanced Threat Defense"
Gartner : August 2013 via FierceITSecurity.com

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

Next Gen High Fidelity Cyber Sensor



Effective Analytics & Correlation

Source : Pacific Northwest National Laboratory

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

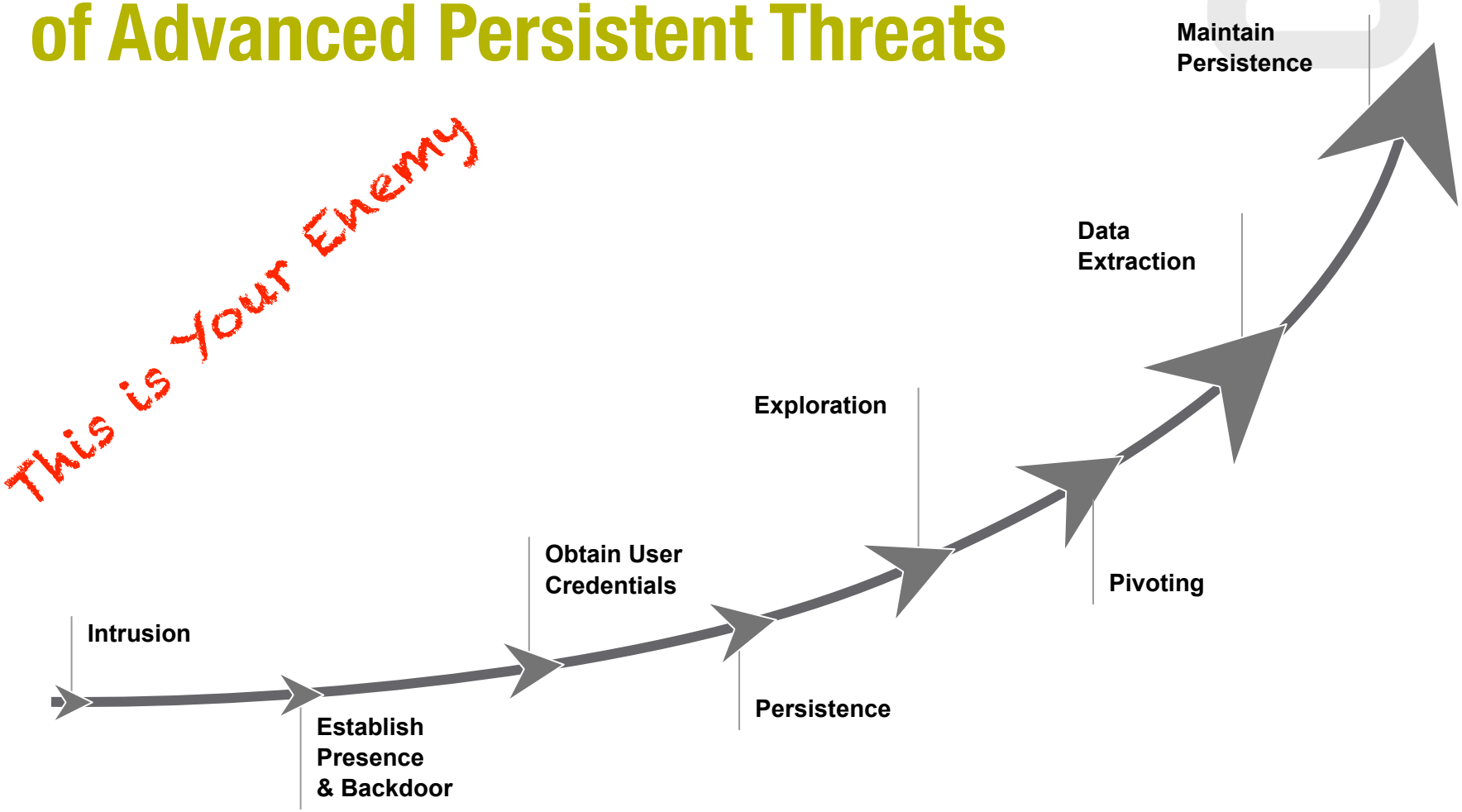
These Are NOT Your Enemies…

[secure]®

ISC8

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

The Cyber Kill Chain – The Attack Lifecycle of Advanced Persistent Threats



Is it Really War When One Side Does not Fight Back?

ISC8 [secure]®
ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

Challenges of Legacy Network Architectures

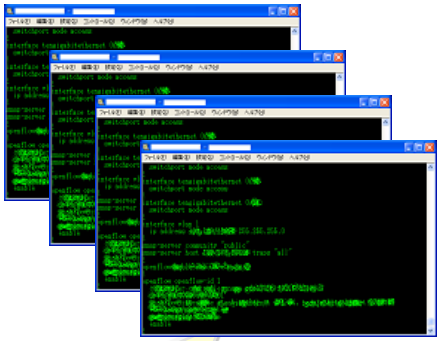
- Escalating Operating Costs
- Lack of QoS End to End
- No SLA's
- Stability
- Management Difficulties in Multi-Vendor Environment
- Lack of End to End Visibility
- Corporate Policy Implementation

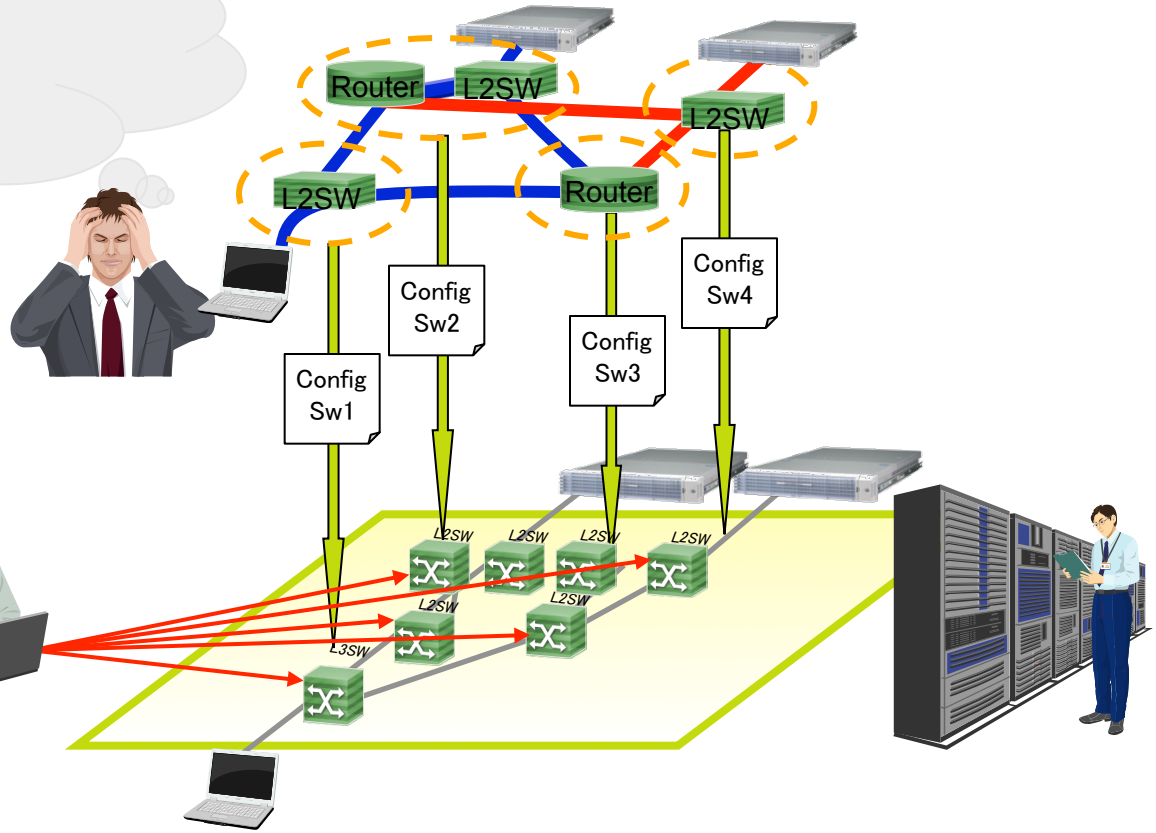
It is a 30+ Year Old Architecture

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

Traditional IT Network Management

- Physical Network Structure
- Logical Network Structure
- Redundant Route
- Resource Design…



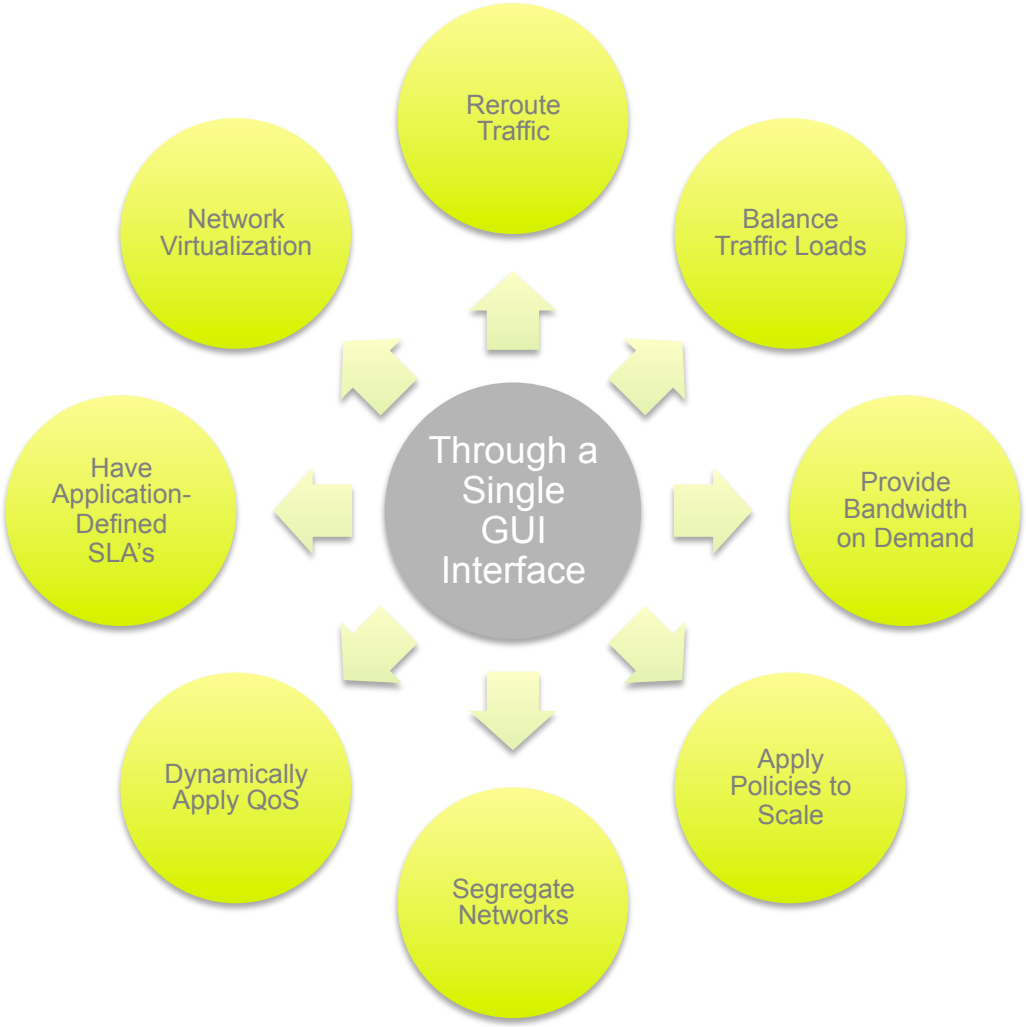


The segregated configuration of each and every switches must be managed.

Oh, By the Way, You Have to Protect This Network From Ever-Advancing Threats

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

Through the Promise of SDN You Can….

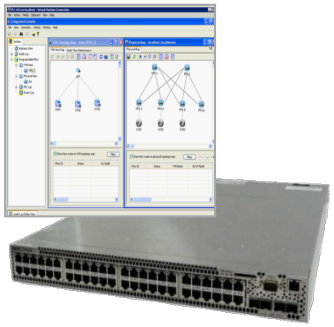


It's Not One to Many, It's One to Any

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

SDN : An Open Network Model

Network



Applications

Management | Security | Optimization

openstack

Northbound API

OPEN DAYLIGHT

Control

Southbound API

OpenFlow

Data

Physical | Virtual

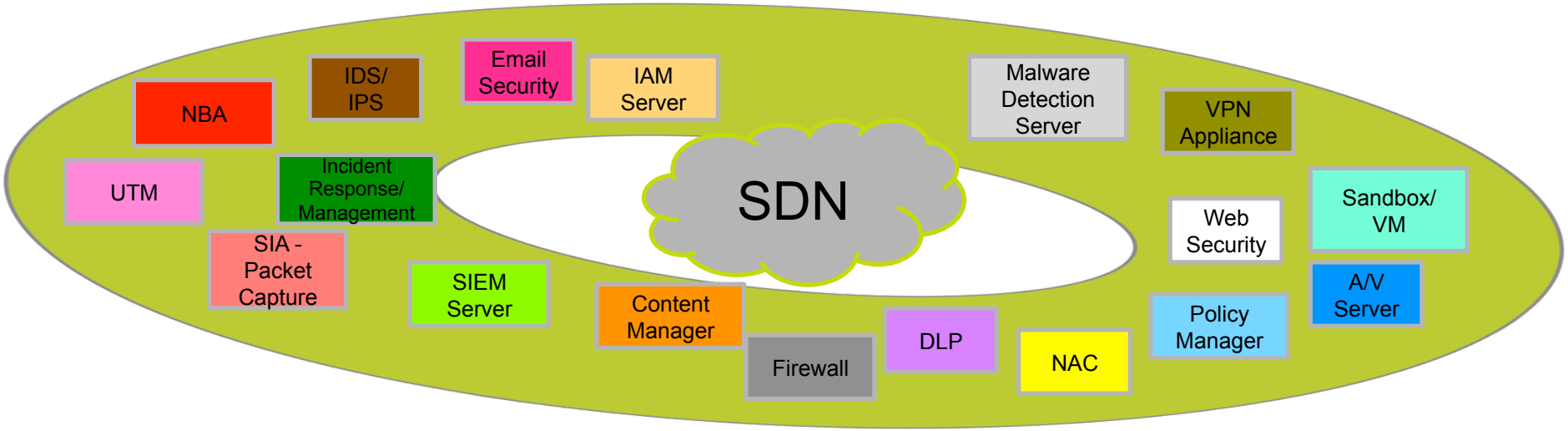
[secure]®

ISC8

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

Source : NEC

SDN with Legacy Cyber Security Protection

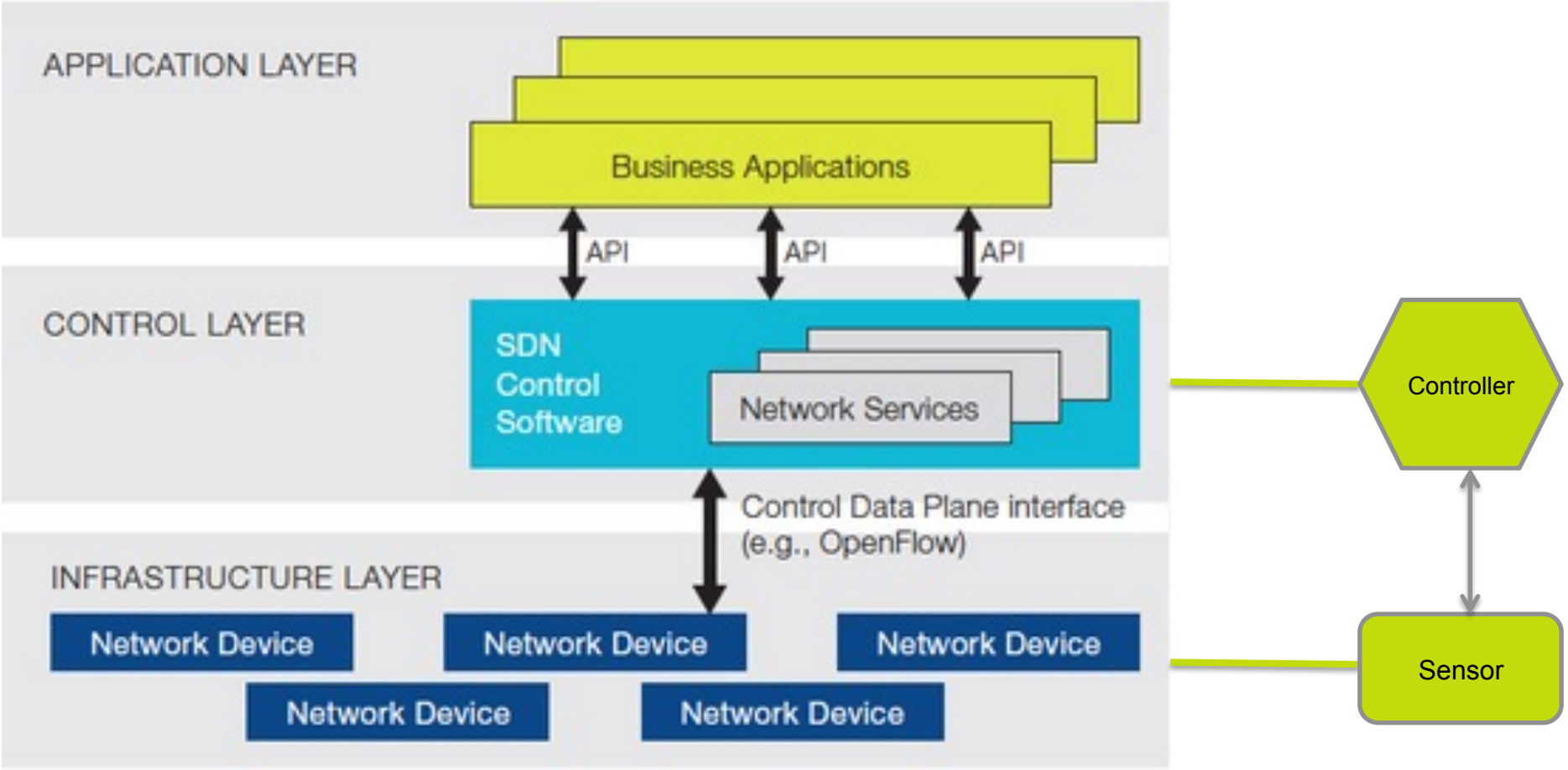


How are you going to look for malware in this environment?
Dynamic Network Provisioning
Custom Flow Management
Flexible and Real-time Network Optimization
Dynamic QoS Profiles
Application-Defined SLA's

Which One of Your Perimeter Tools will Protect You?

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

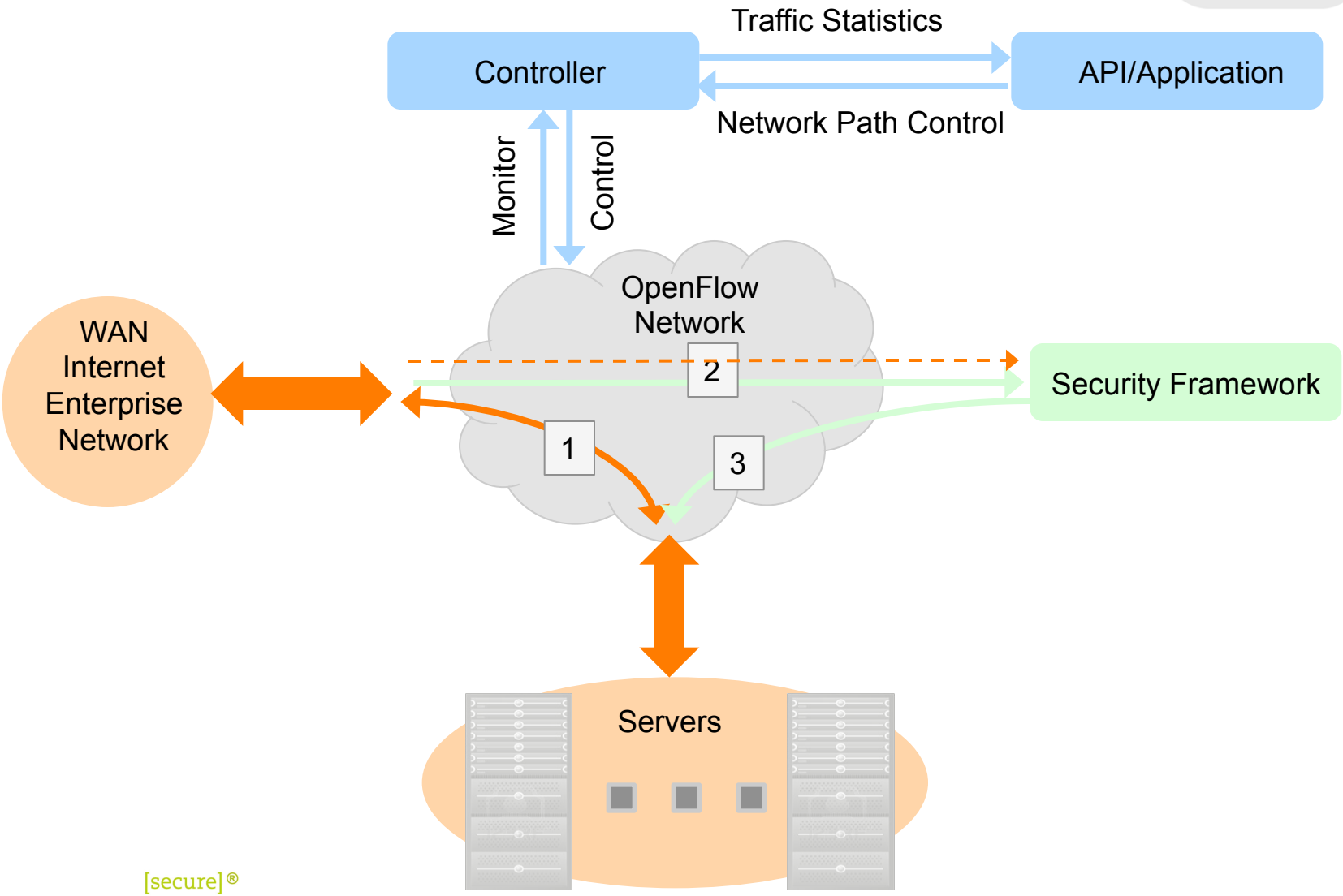
You Need Monitoring from the Inside Out



Source : NEC

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

SDN w/Advanced Security Protection



ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

Questions to Ask you SDN Vendor

- How do you define SDN vis a vis the ONF?
- How does Your Solution Prevent Vendor Lock-In?
- How Does Your Technology Features Match to my Business Requirements?
- What percent of your SDN solution is provided by you vs a 3rd Party?
- How are you going to provide cyber security protection and attestation with your SDN Solution?

Choose Your Business Requirements Before You Choose The SDN Technology

[secure]®
ISC8

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

Futures for SDN

- Data Center Interconnect
- Disaster Recovery
- Business Continuity
- More Granular Security
- Inter-Service Provider SLA's

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

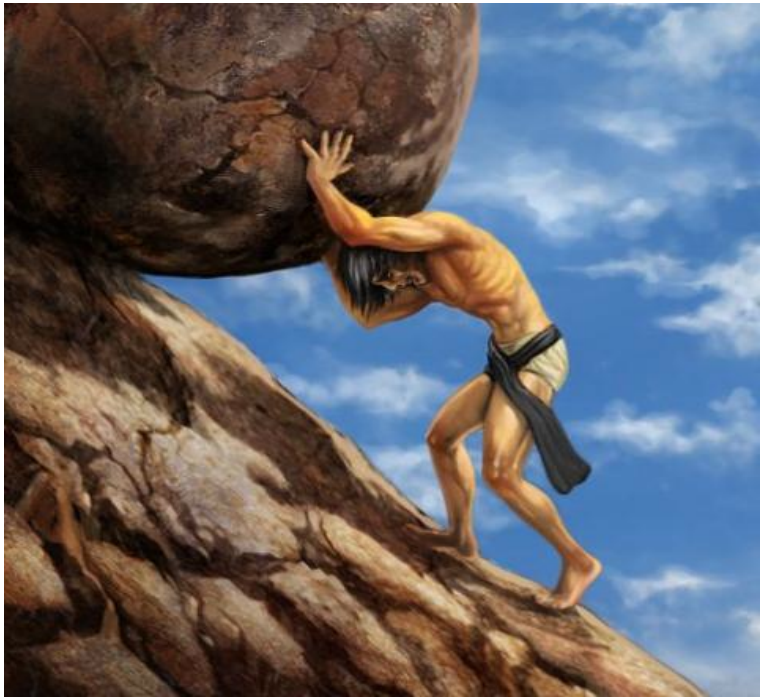
Today's Cyber Vendor Landscape

What you Have….	What you Need…
Signature Based	Signature-less
Anomaly Detection	Malware Detection
Manual Analytics Provided by IT Staff	Analytics Engine and Analysis Included
Disposition of S/W & H/W Vendor Equip	Movement of Malware at Network Core
Placed at Network Perimeter	Placed at Network Core
"Stacked" 10G (1GxN)	10G Line Speed Connectivity (each way)
Number of New Vulnerabilities per Week	Number of New Threat Tactics per Week
MTTK is measured in days or weeks	MTTK is perpetual and ongoing
Manually Build Forensic Evidence across Multiple Products	Forensic Data Analysis is Included
Large Data Store with ad hoc tools to be analyzed by humans – DAILY	Small Data Store that identifies Malware based upon it's presence and movement

What am I Protecting, the Components or the Ecosystem?

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

Let's Not Become the Sisyphus of the 21st Century

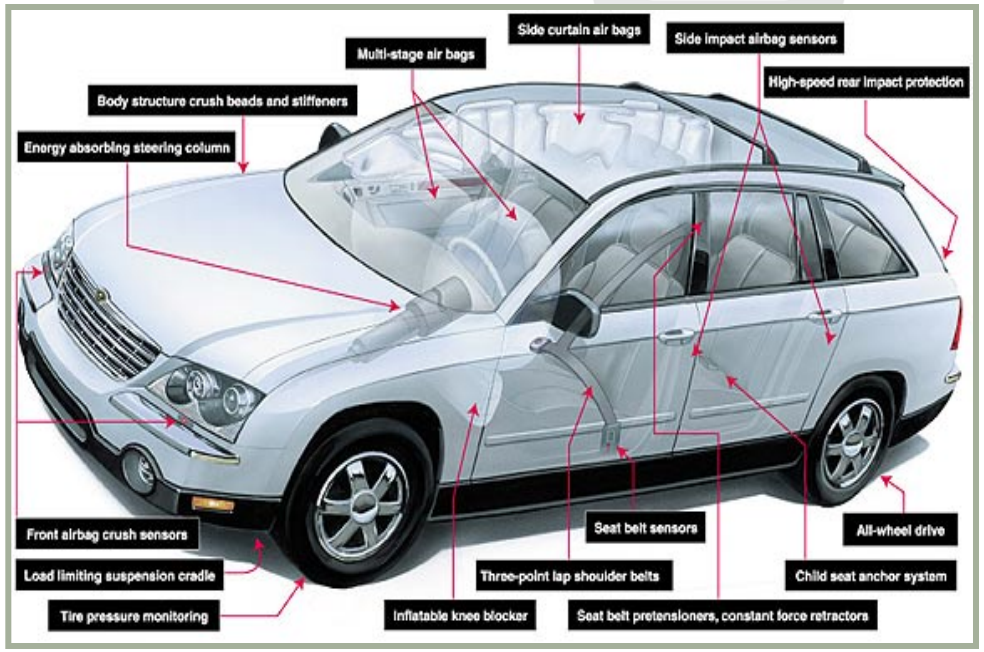


- Compliance Reporting Alone
- Manual Log Analysis & Correlation
- Internal (vs External) Pen Testing
- Vendor-specific Analysis
- Focusing on Prevention Instead Detection and Response

The Definition of Insanity Is….

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

We've Tried Bolt-On Security…Last Century



Security as an Afterthought

- More Expensive to "install" and "maintain"
- Difficult to Integrate
- Does not scale well
- Takes Resources Away from Primary Corporate Focus
- Low and Decreasing Efficacy

Security as an Integral Part of the System

- Integrated at Production
- Seamless Collaboration
- Purpose-Built for this System
- Understands Normal Operations
- Extensible Throughout System

Let's Choose to Act and Not React…

The Name of the Game is Situational Awareness – From the Network Core to the Perimeter

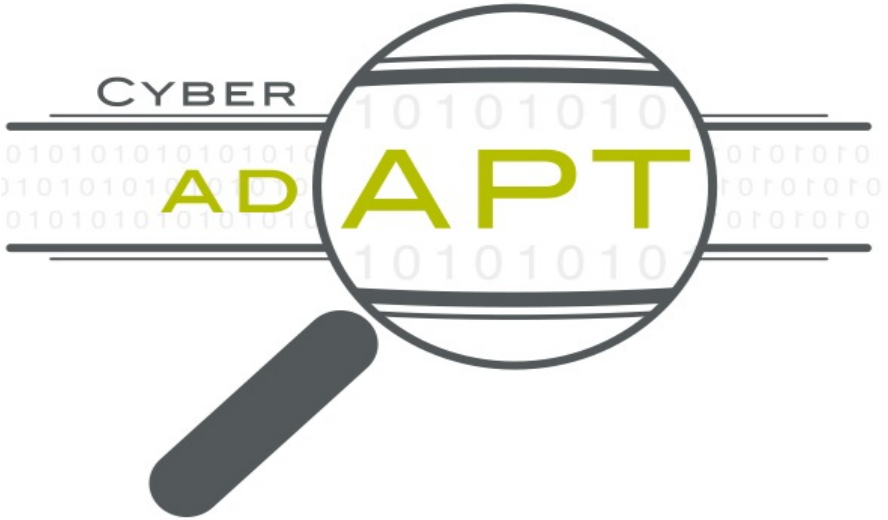
"Cyber Security Posture Attestation (from the Core to the Perimeter) is the Holy Grail of Tomorrow's CISO."

- ISC8

Whose Definition of 'Secure" are You Using?

ISC8 Company Proprietary
©2013 ISC8 Inc. All rights reserved

Thank You For Your Time



Cyber Attacks Happen in Real-Time…
Now Cyber Security Does Too.

Questions?

[secure]
ISC8