Stream Keynote: Security Intelligence

Pulse2013

Optimizing the World's Infrastructure

Equifax Customer Story

Tony Spinelli

Senior Vice President &
Chief Information Security Officer
Equifax

Empowering With Trusted Information

- Credit scoring and reporting
- Identity protection

- Business credit reporting / monitoring
- Business risk monitoring

- Risk management
- Fraud prevention
- Marketing solutions

Managing Unique, Diverse Data Globally

Worldwide

- 572M+ consumers
- 81M+ businesses
- 200M+ employee files
- 4.4B+ trade accounts
- 108M+ public records
- 2B trade lines / month
- 15 countries

- Firmographic data
- Consumer
  - Demographics
  - Income and employment
  - Asset / wealth
  - Property
  - Credit
  - Unemployment claims
- Fraud and authentication
- Securities compliance
- Telephone / utility exchanges

Evaluate Security Maturity

- Re-validate security maturity by country, domain and program*
- Establish benchmarks (ISO, world class, financial services)
- Model and apply 2011 – 2013 goals and directives

	Policy	Organ-ization	Data Security	Information systems
Canada	9	10	8	10
US	10	10	10	8
Argentina	9	8	9	10
Brazil	10	8	9	9
Total	9.5	9.0	9.2	8.9

*Sample information

Create and Implement New Controls

- Create 2011 – 2013 global security plans
- Create programs to address threats

Group	Project	Risk Area	Threat Category	Cost
Engineering	Https decryption	DLP	Employees	H
Engineering	Centralized FW logging	Alarm / alert monitoring	Network compromise	H
Fraud and investigation	Fraud detection	Fraud prevention	Data exposure	M

EQUIFAX

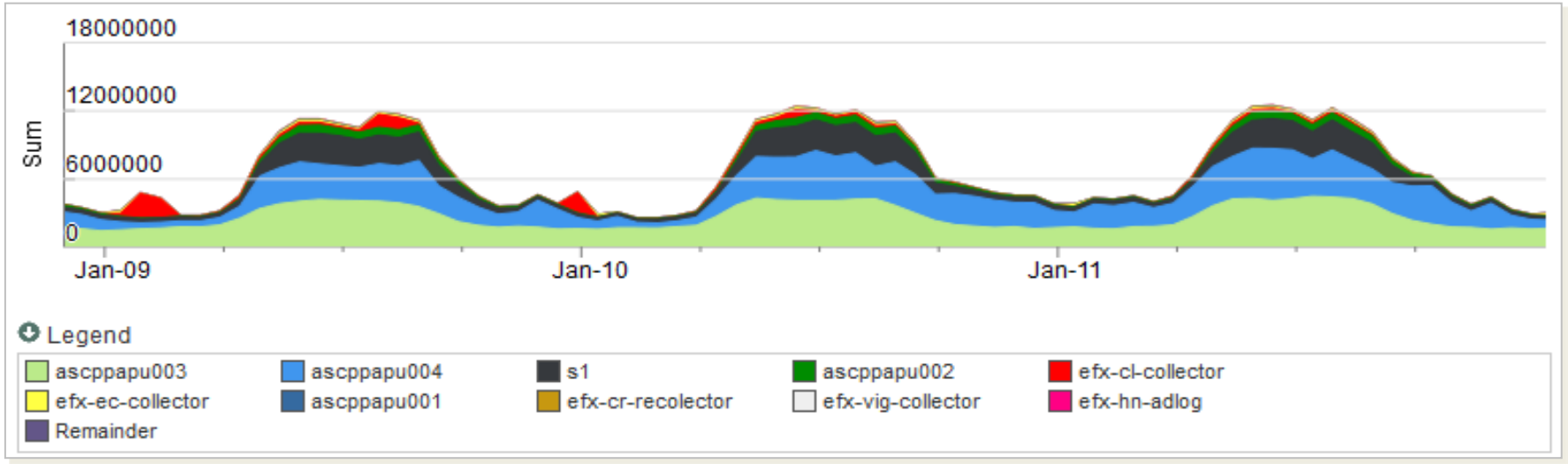
Strategic Capability Playbook

Increasing Risk

Kill Chain	Detect	Deny	Disrupt	Degrade	Deceive
Recon	E-Beast, Sec Intel, IPS, HoneyPot	IPS, FW			Canary, Web Banners, HoneyPot
Weaponization	Efraud Network	IPS			
Delivery	Anti MW, E-Beast, Security Intel	Email AV, Proxy, FW, Non-Cat	External Mail Tag	Email Queuing	
Exploit	HIPS	AV, GPO rules, patch	DEP		
Installation	HIPS	Temp Dir Disable	HIPS, DEP		
Command & Control	Anti MW	Proxy, FW, IPS, Non-Cat	FW, Null Route, IPS		
Actions	HIPS, Sec Intel	DLP, IPS, FW	DLP, Non-Cat, Null Route		HoneyPot

Post Infiltration

Current Focus – Data Fusion Management



Data Volume: QRadar currently processes 1 billion events per day with an average of 10,000 events per second

Stream Keynote: Security Intelligence

Pulse2013

Optimizing the World's Infrastructure