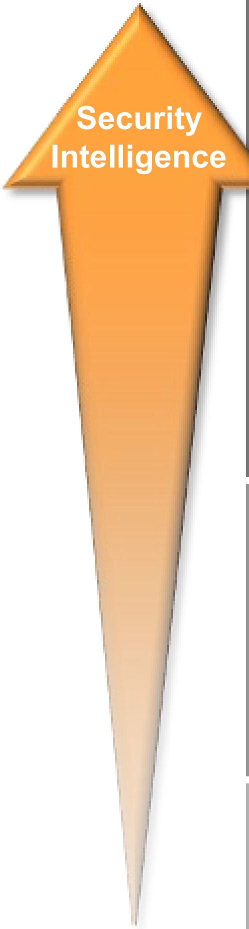
Degustare la crescita

Un percorso in 4 tappe alla scoperta delle soluzioni IBM

**Security Intelligence:
visione unificata e informazioni dettagliate sui rischi**

**Domenico Ercolani
IBM Software Group Security Systems**

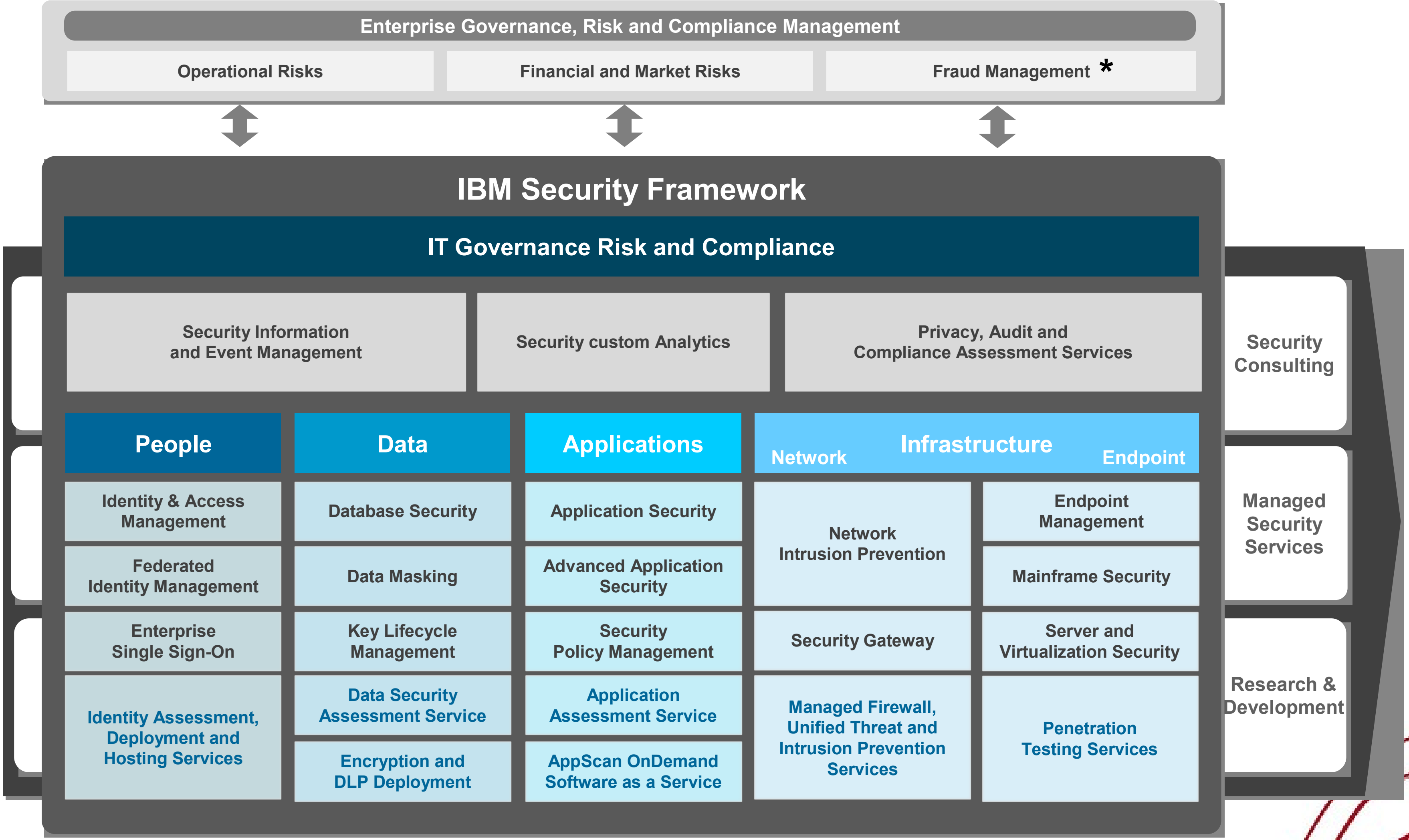
Security Intelligence is enabling progress to optimized security



	People	Data	Applications	[illegible]
Optimized	**Security Intelligence:** Information and event management Advanced correlation and deep analytics External threat research			
	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Security rich systems
Proficient	User provisioning Access management Strong authentication	Database activity monitoring Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset management Endpoint / network security management
Basic	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus

JK 2012-04-26

IBM Security Framework



Enterprise Governance, Risk and Compliance Management

Operational Risks

Financial and Market Risks

Fraud Management *

IBM Security Framework

IT Governance Risk and Compliance

Security Information and Event Management

Security custom Analytics

Privacy, Audit and Compliance Assessment Services

People	Data	Applications	Infrastructure Network	Infrastructure Endpoint
Identity & Access Management	Database Security	Application Security	Network Intrusion Prevention	Endpoint Management
Federated Identity Management	Data Masking	Advanced Application Security		Mainframe Security
Enterprise Single Sign-On	Key Lifecycle Management	Security Policy Management	Security Gateway	Server and Virtualization Security
Identity Assessment, Deployment and Hosting Services	Data Security Assessment Service	Application Assessment Service	Managed Firewall, Unified Threat and Intrusion Prevention Services	Penetration Testing Services
	Encryption and DLP Deployment	AppScan OnDemand Software as a Service		

Security Consulting

Managed Security Services

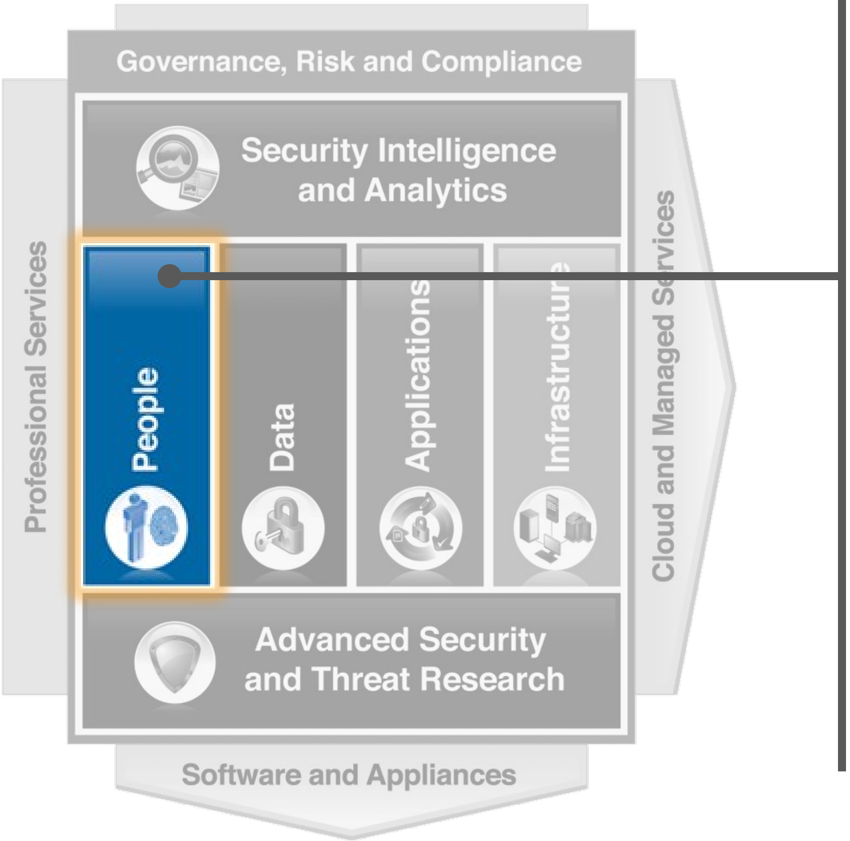
Research & Development

(*) Per la gestione delle Frodi in ambito Financial Services IBM ha elaborato ulteriormente il Framework con una contestualizzazione specifica: una sorta di Framework nel Framework.

People

Area of Focus

Manage and extend enterprise identity context across security domains with comprehensive Identity Intelligence


Governance, Risk and Compliance
Security Intelligence and Analytics
Professional Services
People
Data
Applications
Infrastructure
Cloud and Managed Services
Advanced Security and Threat Research
Software and Appliances

Portfolio Overview

IBM Security Identity Manager

- Automate the creation, modification, and termination of users throughout the lifecycle
- Identity control including role management and auditing

IBM Security Access Manager Family

- Automates sign-on and authentication to enterprise web applications and services
- Entitlement management for fine-grained access enforcement

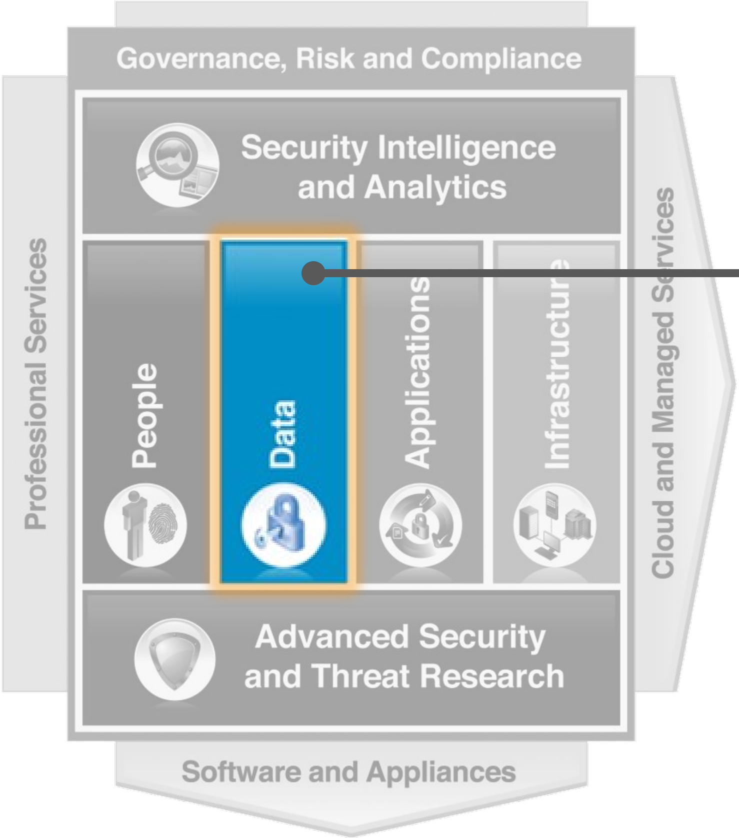
IBM Security zSecure suite

- User friendly layer over RACF to improve administration and reporting
- Monitor, audit and report on security events and exposures on mainframes

Data

Area of Focus

Enterprise-wide solutions for helping secure the privacy and integrity of trusted information in your data center



Governance, Risk and Compliance
Security Intelligence and Analytics
Professional Services
People
Data
Applications
Infrastructure
Cloud and Managed Services
Advanced Security and Threat Research
Software and Appliances

Portfolio Overview

IBM InfoSphere Guardium Product Family

•Database Activity Monitoring – continuously monitor and block unauthorized access to databases

•Privileged User Monitoring – detect or block malicious or unapproved activity by DBAs, developers and outsourced personnel

•Database Leak Prevention – help detect and block leakage in the data center

•Database Vulnerability Assessment – scan databases to detect vulnerabilities and take action

•Audit and Validate Compliance – simplify SOX, PCI-DSS, and Data Privacy processes with pre-configured reports and automated workflows

IBM Security Key Lifecycle Manager

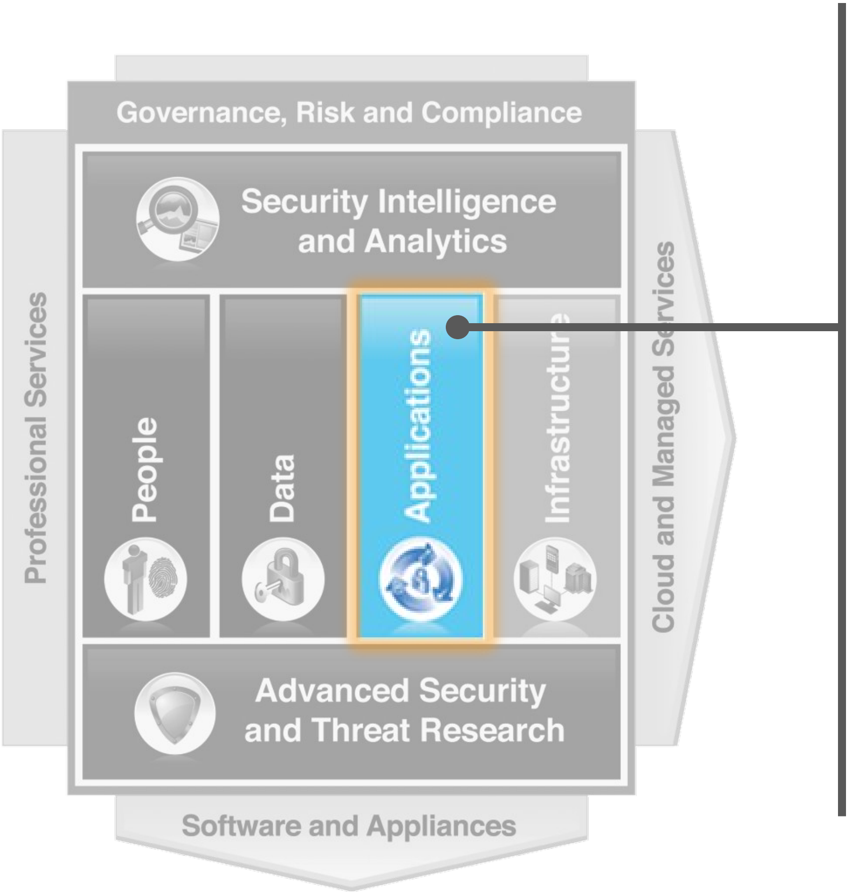
•Centralize and automate the encryption key management process

•Simplify administration with an intuitive user interface for configuration and management

Applications

Area of Focus

Reducing the cost of developing more secure applications



Governance, Risk and Compliance
Security Intelligence and Analytics
Professional Services
People
Data
Applications
Infrastructure
Cloud and Managed Services
Advanced Security and Threat Research
Software and Appliances

Portfolio Overview

AppScan Enterprise Edition

•Enterprise-class solution for application security testing and risk management with governance and collaboration

•Multi-user solution providing simultaneous security scanning and centralized reporting

AppScan Standard Edition

•Desktop solution to automate web application security testing for IT Security, auditors, and penetration testers

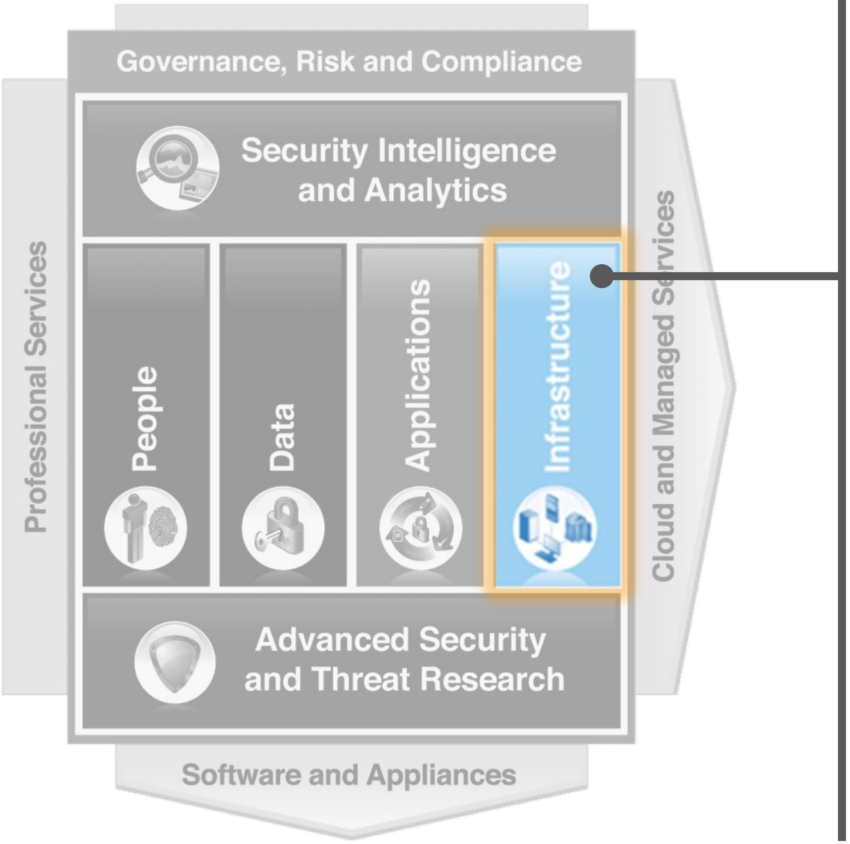
AppScan Source Edition

- Adds source code analysis to AppScan Enterprise with static application security testing

Infrastructure (Network)

Area of Focus

Help guard against sophisticated attacks with insight into users, content and applications


Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

Portfolio Overview

IBM Security Network Intrusion Prevention (IPS)

•Delivers Advanced Threat Detection and Prevention to help stop targeted attacks against high value assets

•Proactively improves protection with IBM Virtual Patch® technology

•Helps protect web applications from threats such as SQL Injection and Cross-site Scripting attacks

•Integrated Data Loss Prevention (DLP) monitors data security risks throughout your network

•Provides Ahead of the Threat® protection backed by world renowned IBM X-Force Research

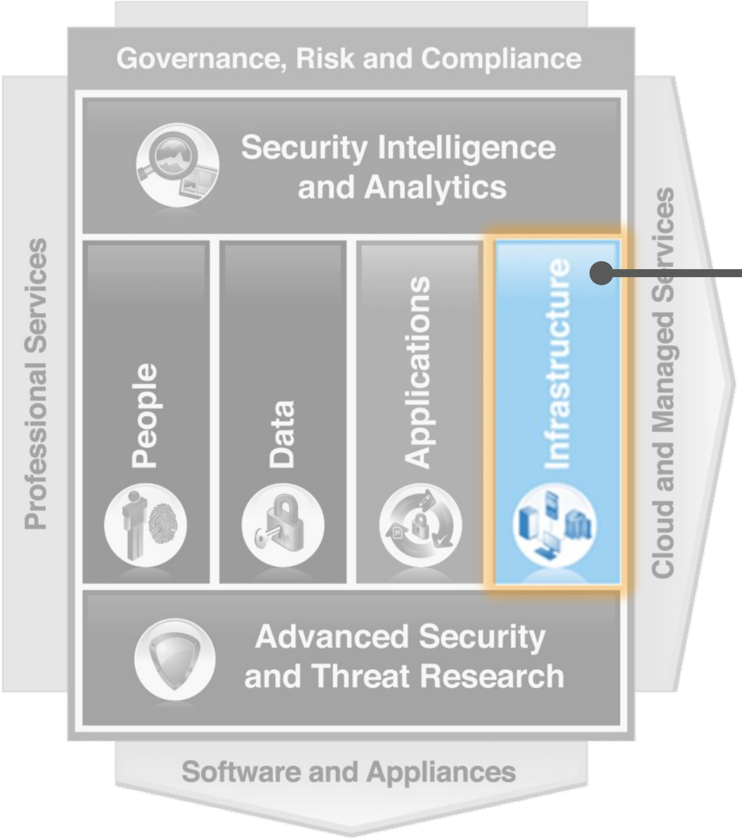
IBM Security SiteProtector

•Provides central management of security devices to control policies, events, analysis and reporting for your business

Infrastructure (Endpoint and Server)

Area of Focus

Helping endpoints, servers, and mobile devices remain compliant, updated, and protected


Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

Portfolio Overview

IBM Endpoint Manager for Security and Compliance

•Addresses distributed environments with endpoint and security management in a single solution

IBM Endpoint Manager for Core Protection

•Helps protect endpoints from malware and other threats in real-time

IBM Endpoint Manager for Mobile Devices

- Manage and help secure traditional endpoints as well as iOS, Android, Symbian, and Microsoft devices

IBM Security Server Protection

- Helps provide multilayered protection against threats, supporting a broad range of operating systems

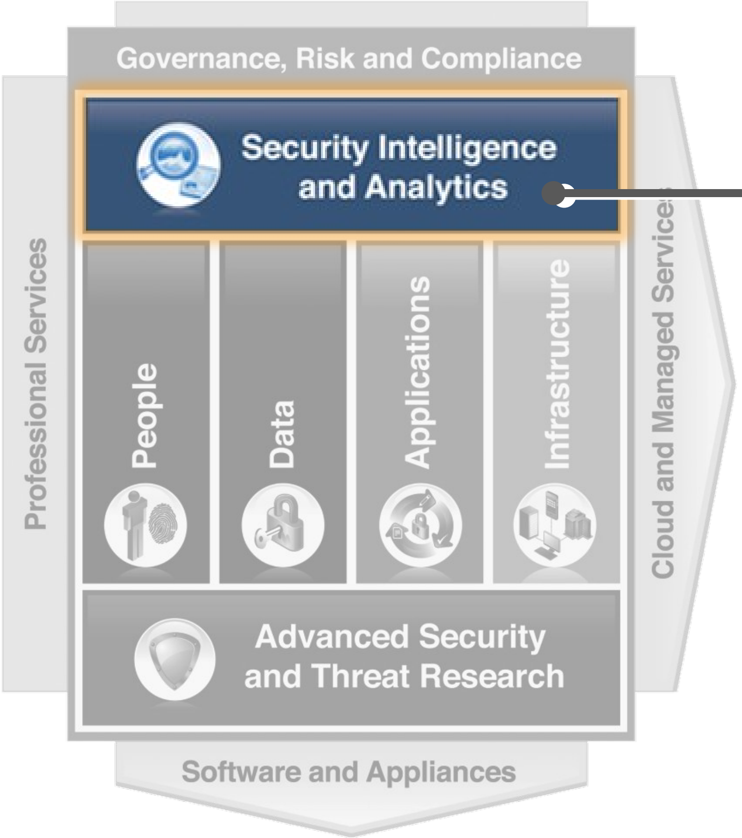
IBM Security Virtual Server Protection for VMware

- Helps provide dynamic security for virtualization with VM rootkit detection, auditing, network intrusion prevention

Security Intelligence and Analytics

Area of Focus

Helping customers optimize security with additional context, automation and integration


Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

Portfolio Overview

QRadar SIEM

- Integrated log, threat, compliance management
- Asset profiling and flow analytics
- Offense management and workflow

QRadar Risk Manager

- Predictive threat modeling and simulation
- Scalable configuration monitoring and audit
- Advanced threat and impact analysis

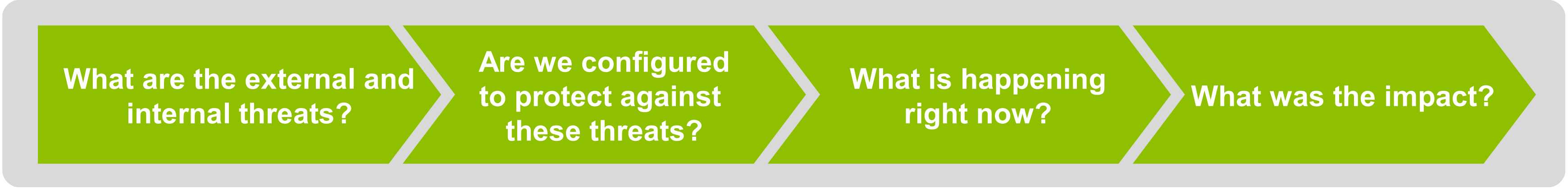
QRadar Log Manager

- Turnkey log management
- Upgradeable to enterprise SIEM

Network Activity Collectors (QFlow / VFlow)

- Network analytics, behavior and anomaly detection
- Fully integrated with SIEM

Solutions for the Full Compliance and Security Intelligence Timeline

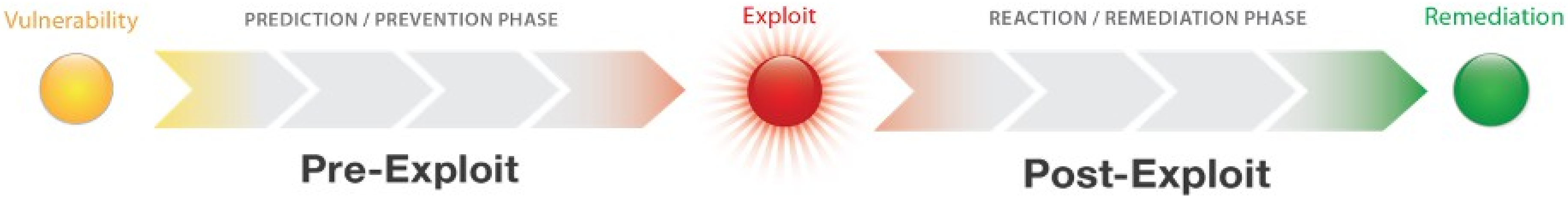


What are the external and internal threats?

Are we configured to protect against these threats?

What is happening right now?

What was the impact?



Prediction & Prevention

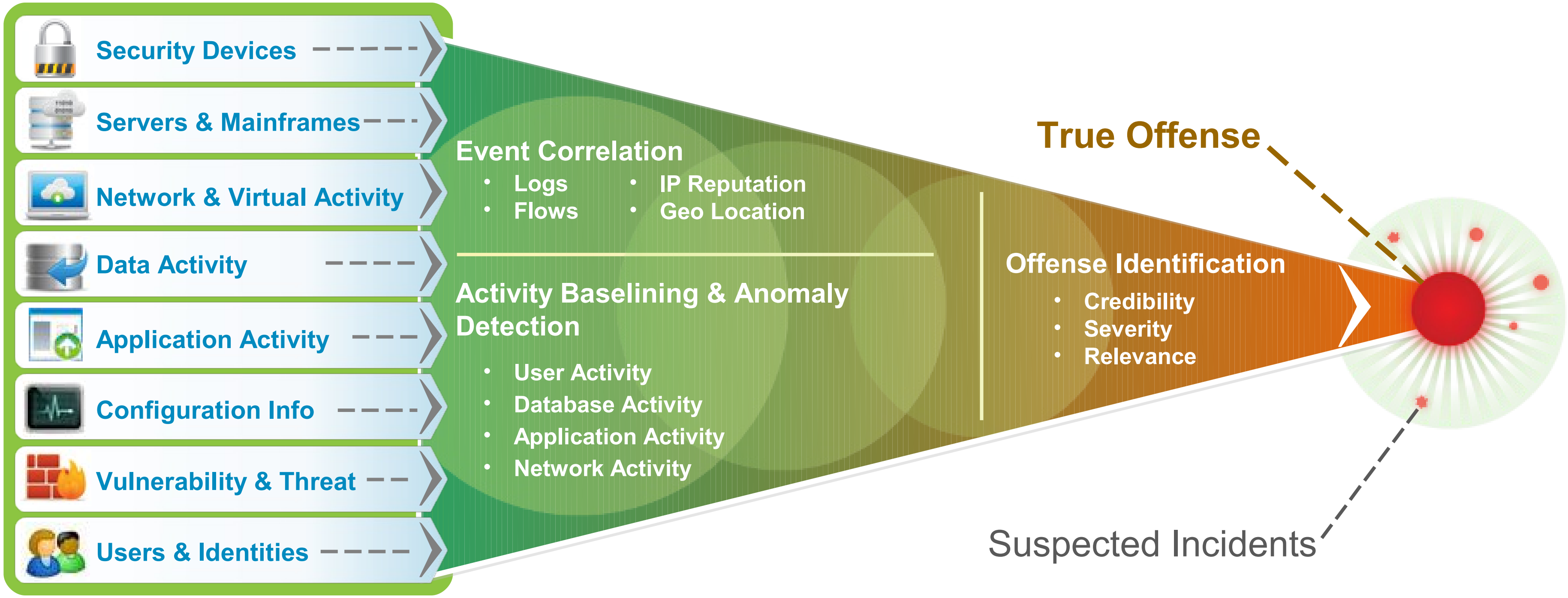
Risk Management. Vulnerability Management.
Configuration Monitoring. Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management. Reporting and Scorecards.

Reaction & Remediation

SIEM. Log Management. Incident Response.
Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Loss Prevention.

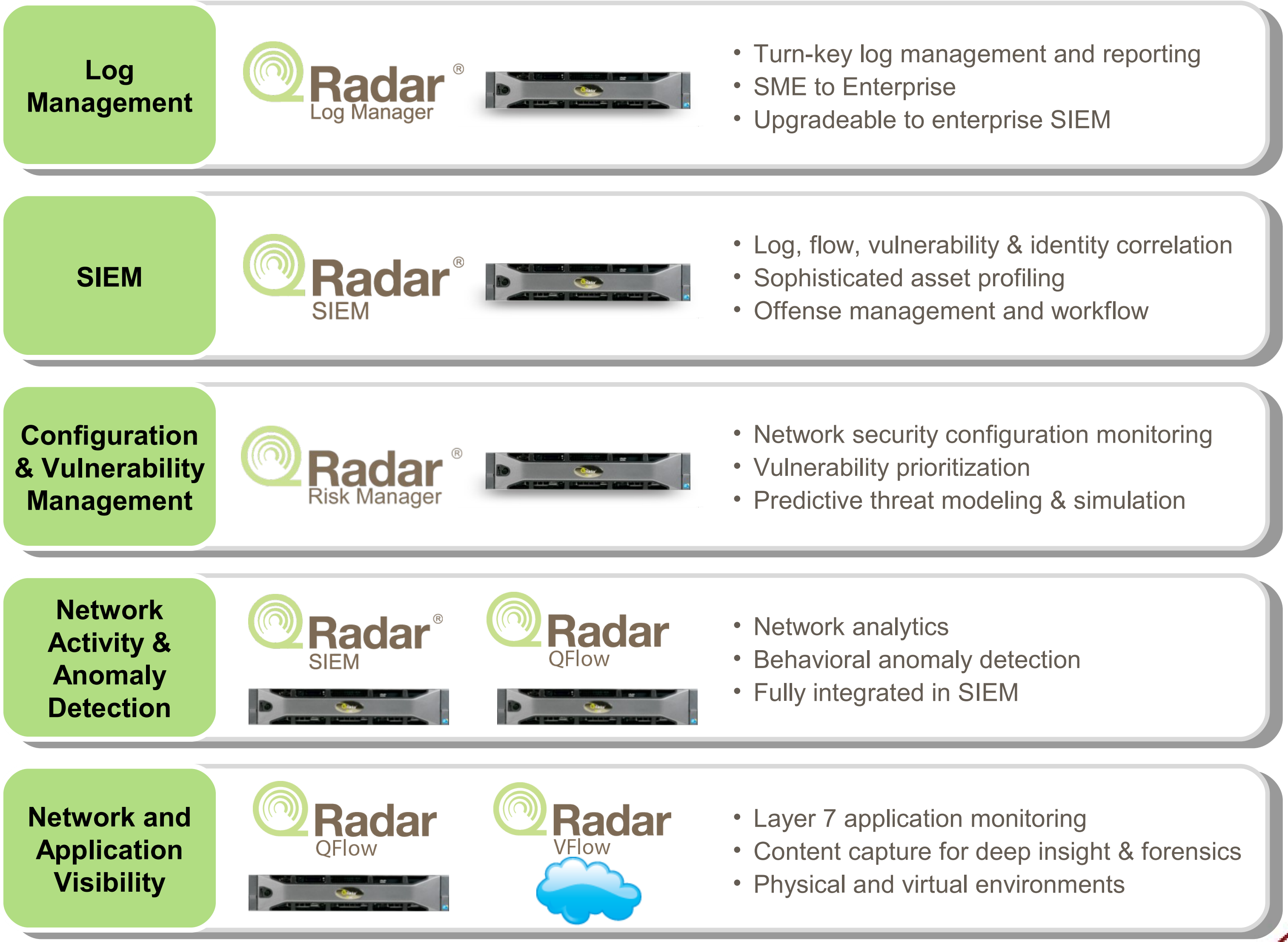
Total Security Intelligence | An IBM Company

Context and Correlation Drive Deepest Insight



Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

Fully Integrated Security Intelligence



Log Management

QRadar® Log Manager

- Turn-key log management and reporting
- SME to Enterprise
- Upgradeable to enterprise SIEM

SIEM

QRadar® SIEM

- Log, flow, vulnerability & identity correlation
- Sophisticated asset profiling
- Offense management and workflow

Configuration & Vulnerability Management

QRadar® Risk Manager

- Network security configuration monitoring
- Vulnerability prioritization
- Predictive threat modeling & simulation

Network Activity & Anomaly Detection

QRadar® SIEM

QRadar QFlow

- Network analytics
- Behavioral anomaly detection
- Fully integrated in SIEM

Network and Application Visibility

QRadar QFlow

QRadar VFlow

- Layer 7 application monitoring
- Content capture for deep insight & forensics
- Physical and virtual environments

Fully Integrated Security Intelligence

Log Management

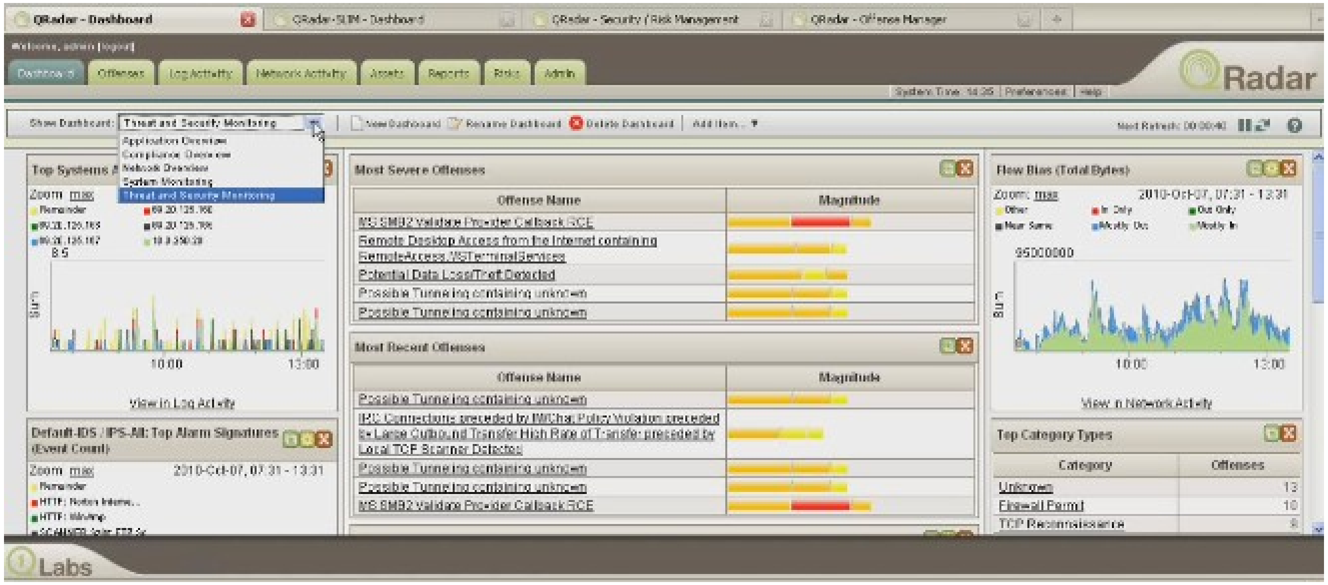
SIEM

Configuration & Vulnerability Management

Network Activity & Anomaly Detection

Network and Application Visibility

One Console Security



Most Severe Offenses

Offense Name	Magnitude
MS SMB2 Validate Provider Callback RCE	
Remote Desktop Access from the Internet containing RemoteAccess.MSTerminalServices	
Potential Data Loss/Theft Detected	
Possible Tunneling containing unknown	
Possible Tunneling containing unknown	

Most Recent Offenses

Offense Name	Magnitude
Possible Tunneling containing unknown	
IRC Connections preceded by IM/Chat Policy Violation preceded by Large Outbound Transfer High Rate of Transfer preceded by Local TCP Scanner Detected	
Possible Tunneling containing unknown	
Possible Tunneling containing unknown	
MS SMB2 Validate Provider Callback RCE	

Top Category Types

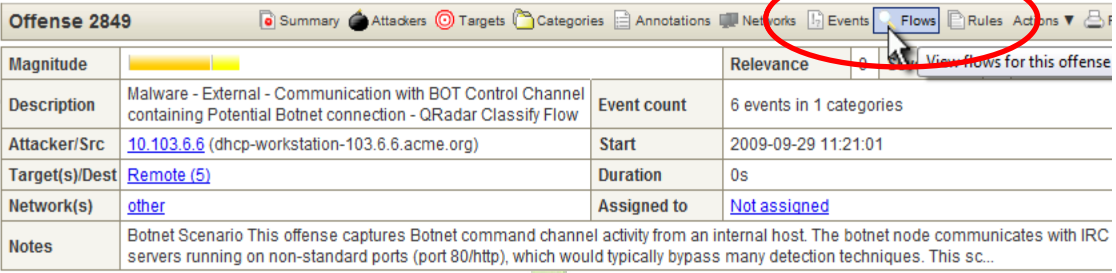
Category	Offenses
Unknown	13
Firewall Permit	10
TCP Reconnaissance	8

Built on a Single Data Architecture

Example 1: Detecting Threats

Potential Botnet Detected?

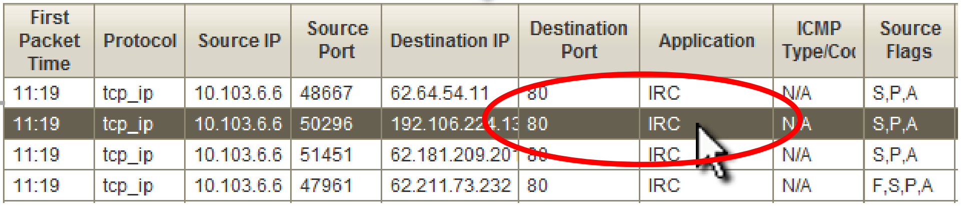
This is as far as traditional SIEM can go



Magnitude		Relevance	0
Description	Malware - External - Communication with BOT Control Channel containing Potential Botnet connection - QRadar Classify Flow	Event count	6 events in 1 categories
Attacker/Src	10.103.6.6 (dhcp-workstation-103.6.6.acme.org)	Start	2009-09-29 11:21:01
Target(s)/Dest	Remote (5)	Duration	0s
Network(s)	other	Assigned to	Not assigned
Notes	Botnet Scenario This offense captures Botnet command channel activity from an internal host. The botnet node communicates with IRC servers running on non-standard ports (port 80/http), which would typically bypass many detection techniques. This sc...		

IRC on port 80?

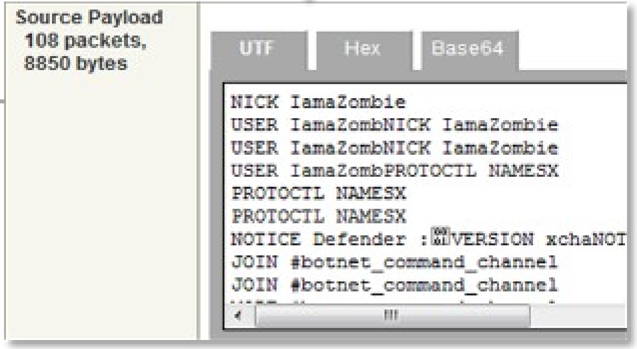
IBM Security QRadar QFlow detects a covert channel



First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Co	Source Flags
11:19	tcp_ip	10.103.6.6	48667	62.64.54.11	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	50296	192.106.224.13	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	51451	62.181.209.20	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	47961	62.211.73.232	80	IRC	N/A	F,S,P,A

Irrefutable Botnet Communication

Layer 7 flow data contains botnet command control instructions

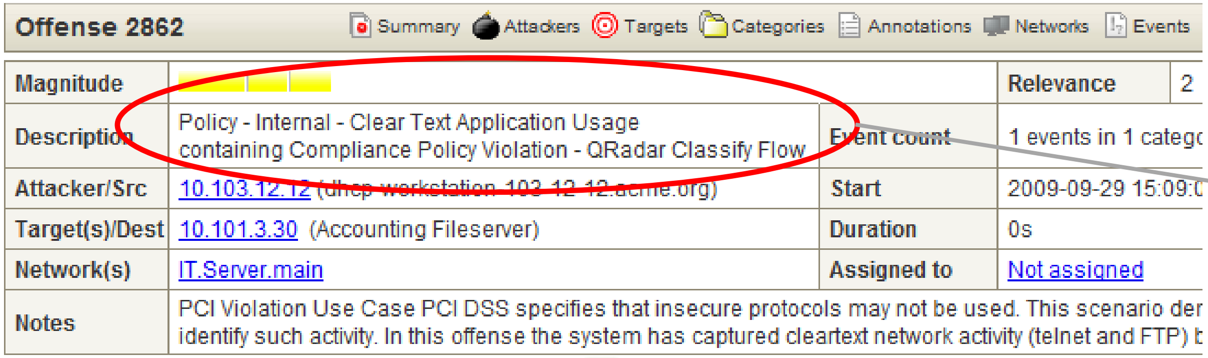


Source Payload
108 packets,
8850 bytes

```
NICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombNICK IamaZombie
USER IamaZombPROTOCTL NAMESX
PROTOCTL NAMESX
PROTOCTL NAMESX
NOTICE Defender :VERSION xchaNOT
JOIN #botnet_command_channel
JOIN #botnet_command_channel
```

Application layer flow analysis can detect threats others miss

Example 2: Addressing Regulatory Mandates

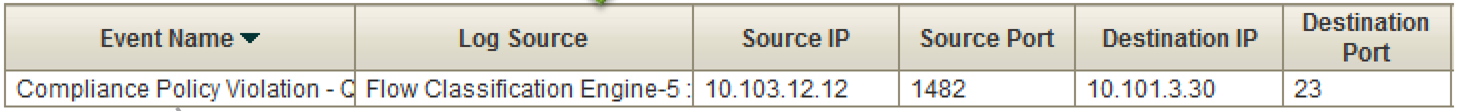


Offense 2862

Magnitude	▮▮▮	Relevance	2
Description	Policy - Internal - Clear Text Application Usage containing Compliance Policy Violation - QRadar Classify Flow	Event count	1 events in 1 catego
Attacker/Src	10.103.12.12 (dhcp-workstation-103-12-12.acme.org)	Start	2009-09-29 15:09:0
Target(s)/Dest	10.101.3.30 (Accounting Fileserver)	Duration	0s
Network(s)	IT.Server.main	Assigned to	Not assigned
Notes	PCI Violation Use Case PCI DSS specifies that insecure protocols may not be used. This scenario der identify such activity. In this offense the system has captured cleartext network activity (telnet and FTP) b		

PCI compliance at risk?

Real-time detection of possible violation



Event Name ▾	Log Source	Source IP	Source Port	Destination IP	Destination Port
Compliance Policy Violation - C	Flow Classification Engine-5 :	10.103.12.12	1482	10.101.3.30	23

Unencrypted Traffic

IBM Security QRadar QFlow saw a cleartext service running on the Accounting server

PCI Requirement 4 states: Encrypt transmission of cardholder data across open, public networks

Compliance Simplified

Out-of-the-box support for major compliance and regulatory standards

Automated reports, pre-defined correlation rules and dashboards