Discover, Analyze, Remediate

The Nanjgel Cyber Security Framework

Jude Pereira
Managing Director
Nanjgel Solutions FZ-LLC

NANJGEL Solutions

Our Focus:
Solving Wicked Hard Problems

COUNTER-TERRORISM

Quick Reaction Capabilities

CYBER

Mission Grade Cyber Defense

Secure Cloud Computing

Cyber Network Operations - Operations, Development, Training

GEOSPATIAL

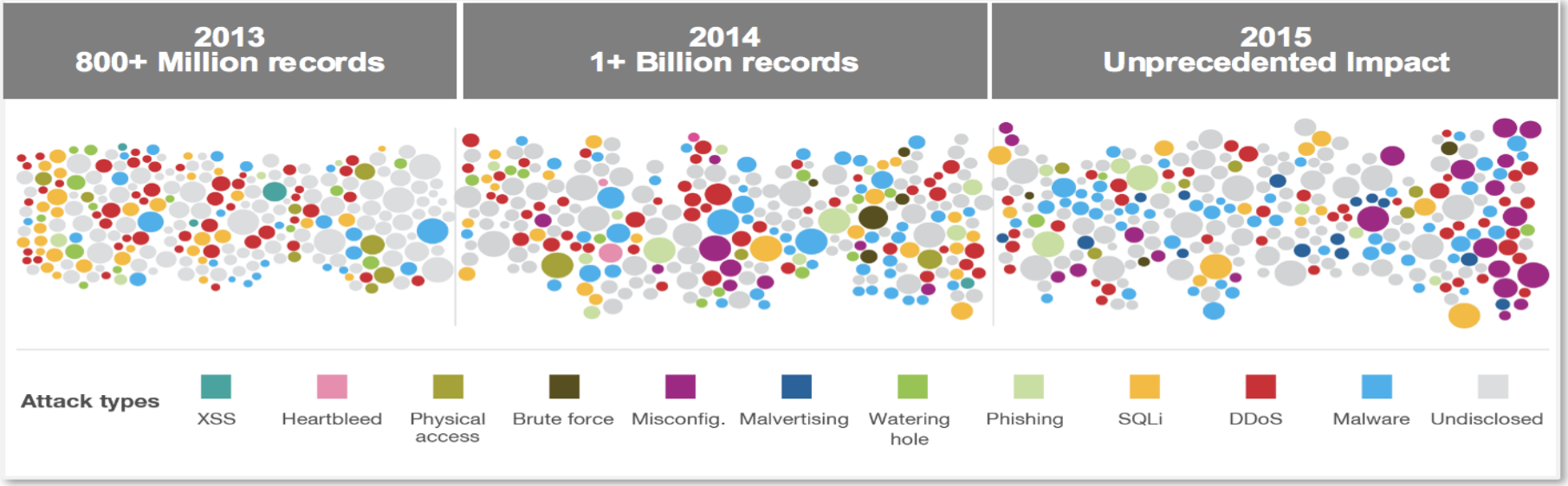
Geospatial Data Management & Analysis

Geospatial Data Collection

Sensor Development & Integration

NANJGEL Solutions

Attackers break through conventional safeguards every day



average time to detect APTs

256 days

average cost of a U.S. data breach

$6.5M

NANJGEL Solutions

We are in an era of continuous breaches

2013

Operational Sophistication

Year of the Security Breach

2014

Near Daily Leaks of Sensitive Data

40% increase in reported data breaches and incidents

2015

Relentless Use of Multiple Methods

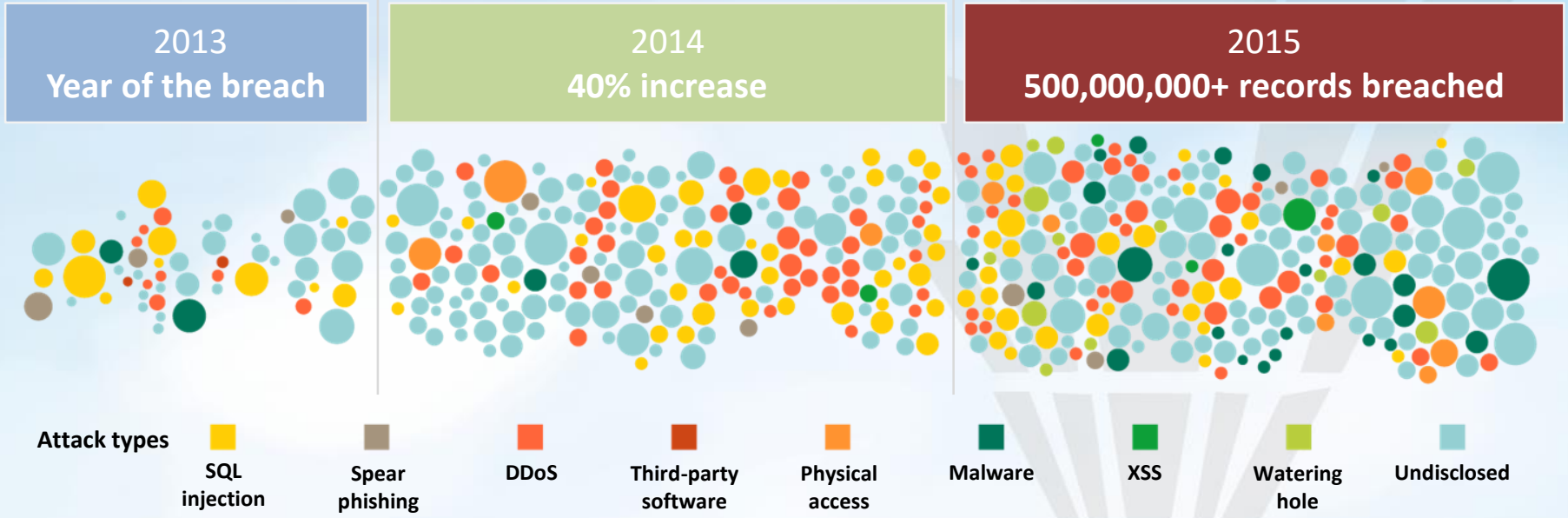
500,000,000+ records were leaked, while the future shows no sign of change

Attack types

- SQL injection
- Spear phishing
- DDoS
- Third-party software
- Physical access
- Malware
- XSS
- Watering hole
- Undisclosed

NANJGEL Solutions

The era of continuous breaches carry on…



Note: Size of circle estimates relative impact of incident in terms of cost to business

Innovative technology changes everything

1 trillion connected objects

1 billion mobile workers

Social business

Bring your own IT

Cloud and virtualization

NANJGEL Solutions

PARADIGM SHIFT

In Crime

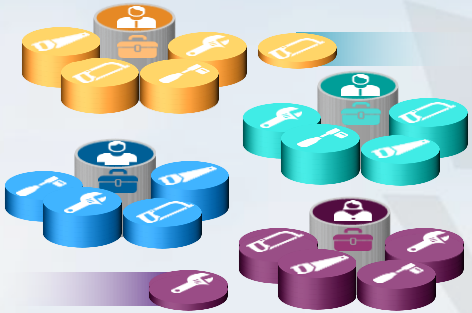
NANJGEL Solutions

Today's challenges

Escalating Attacks

- Increasingly sophisticated attack methods
- Disappearing perimeters
- Accelerating security breaches

Increasing Complexity



- Constantly changing infrastructure
- Too many products from multiple vendors; costly to configure and manage
- Inadequate and ineffective tools

Resource Constraints

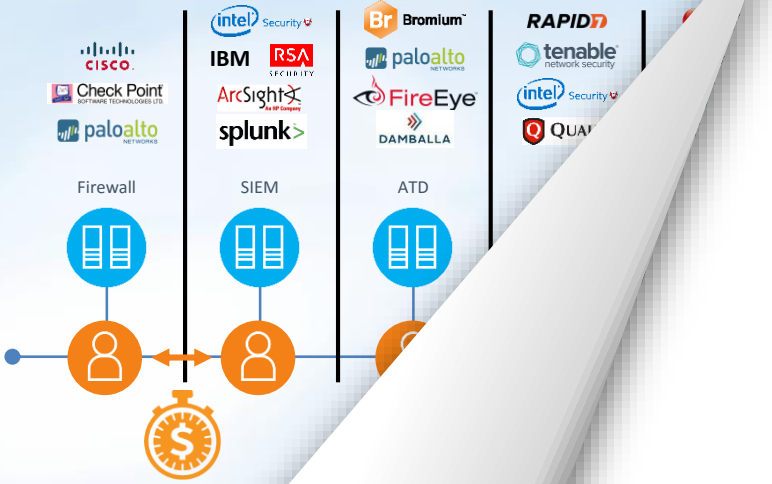
- Struggling security teams
- Too much data with limited manpower and skills to manage it all
- Managing and monitoring increasing compliance demands

NANJGEL Solutions

The Fact of Reality?

NANJGEL Solutions

IT Security Challenges



Fragmented security lets attackers in

“70 to 90 percent of all malicious incidents could have been prevented or found sooner if existing logs and alerts had been monitored”

Verizon Data Breach Investigations Report

“Average time to contain a cyber attack is 31 days”

Ponemon Institute “2014 Global Report on the Cost of Cyber Crime”

Yesterday's practices are not working

$3.5M+

Average cost
of a data breach

85 tools from

45 vendors

NANJGEL Solutions

Your security team sees noise

We need a new approach – *The power to act* – at scale

NANJGEL Solutions

Organizations Need to Speed Up Breach Detection

On average, organizations take **229 days** to detect a data breach, according to a recent study from a cybersecurity firm.

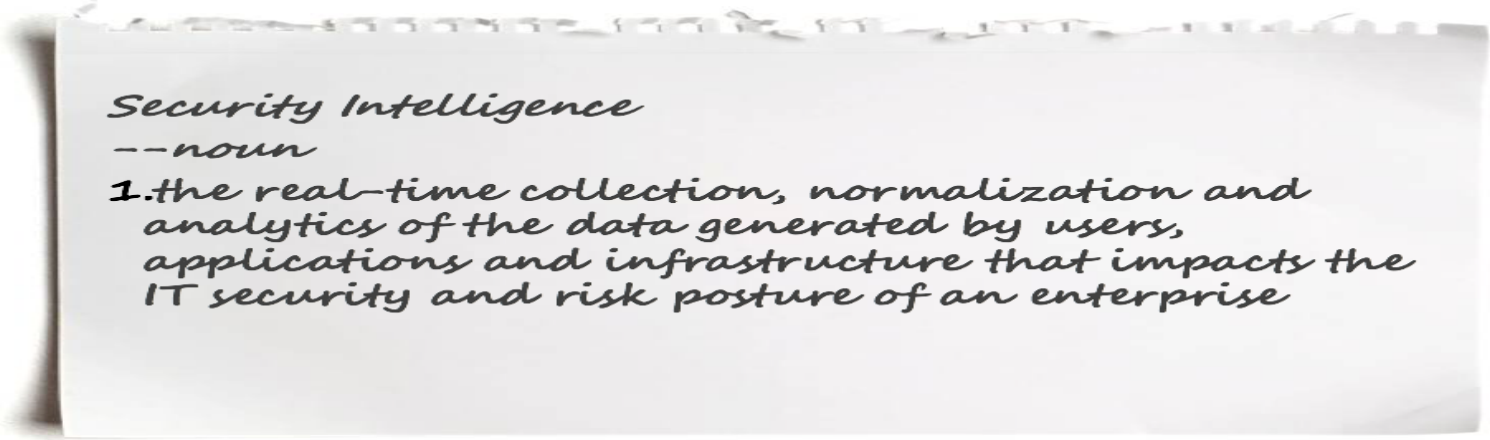
One reason for the lengthy detection time is two-thirds of organizations are told about a breach by a third party, rather than discovering it themselves.

Organizations looking to speed up breach detection on their own, rather than relying on others, need to improve their data analytics capabilities, prioritize the type of data they want to collect and analyze, and ensure they have appropriate staff who can take the time to review the data for suspicious activity.

By Jeffrey Roman, November 25, 2014.

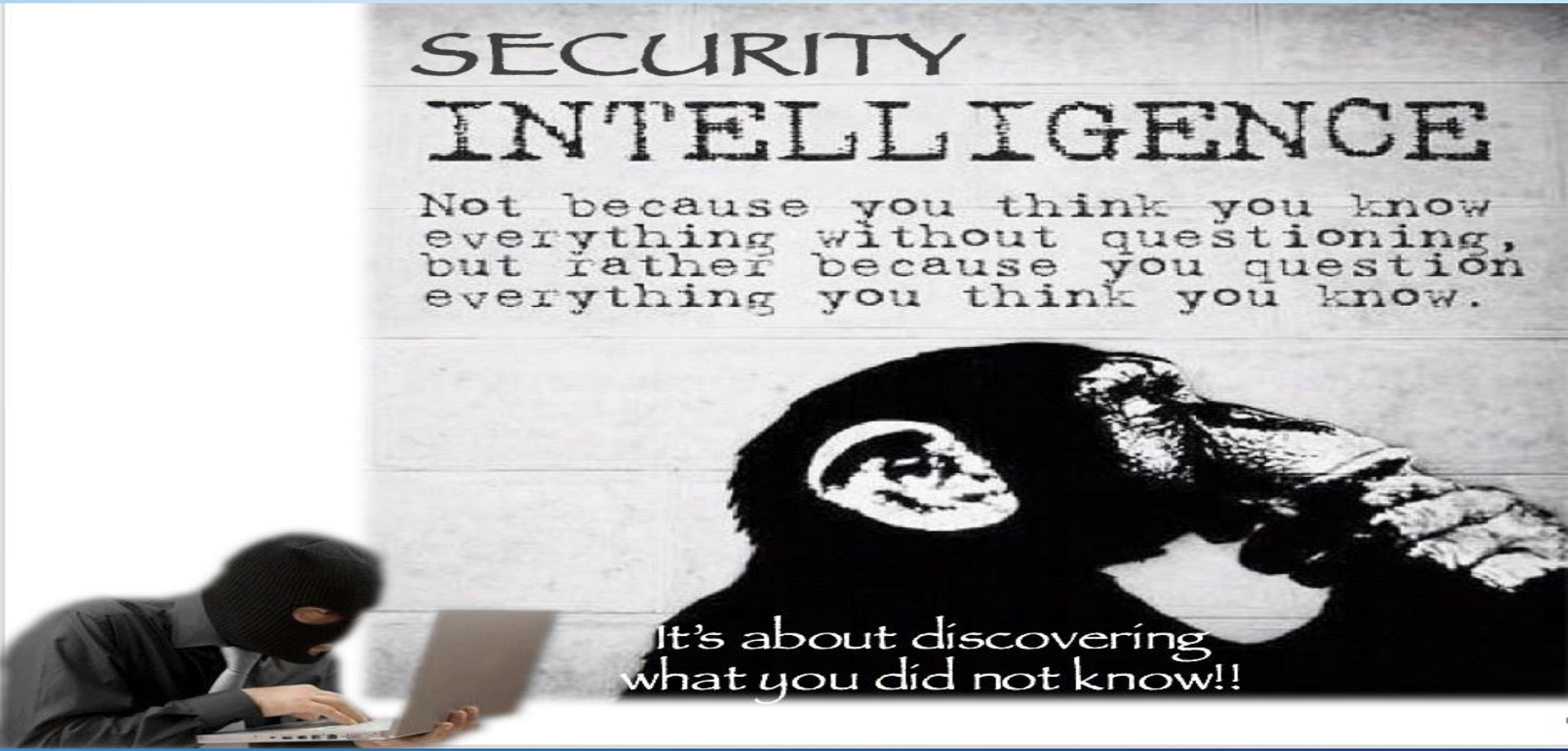
NANJGEL Solutions

Security Intelligence –
Core Functionality for Cyber Security

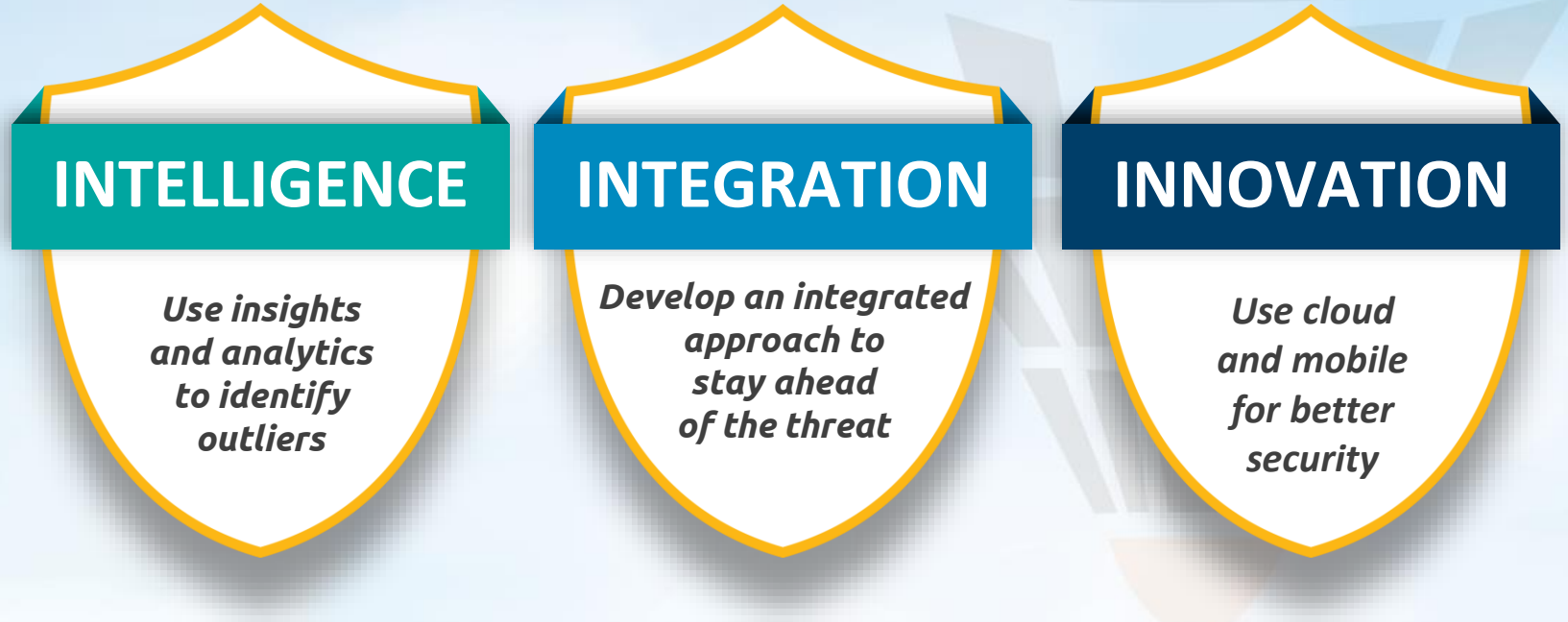


Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation

NANJGEL Solutions



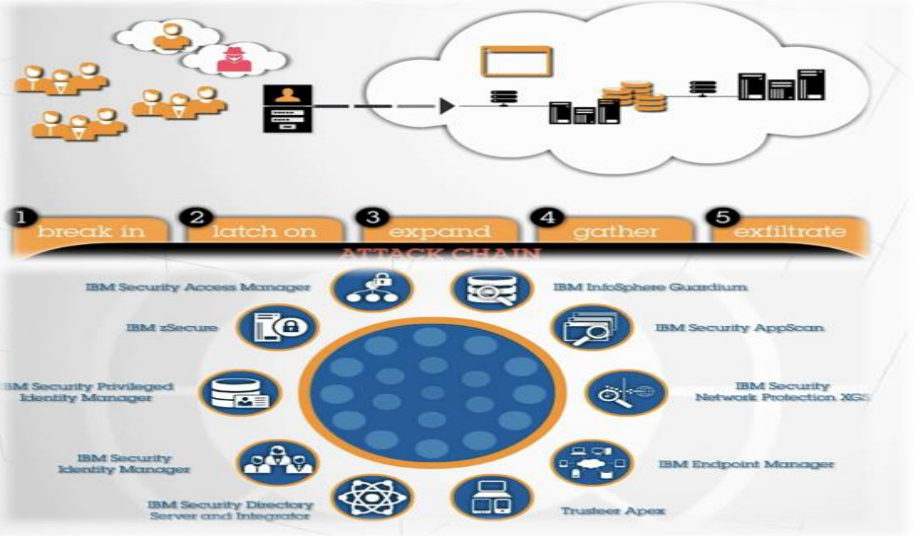
Our Approach



NANJGEL Solutions

”More Context” means more Integration

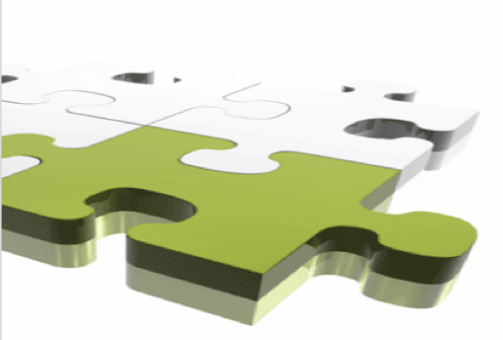
- Security Systems solutions offer integration and interoperation, for the benefit of customers who need their security infrastructure to support relevant standards and integrate and interoperate for ease of operations and for broad span of coverage.



Integration” means easier & more comprehensive

Security skills and staffing continues to lag at enterprise organizations.

Data points to a pretty substantial skills gap:

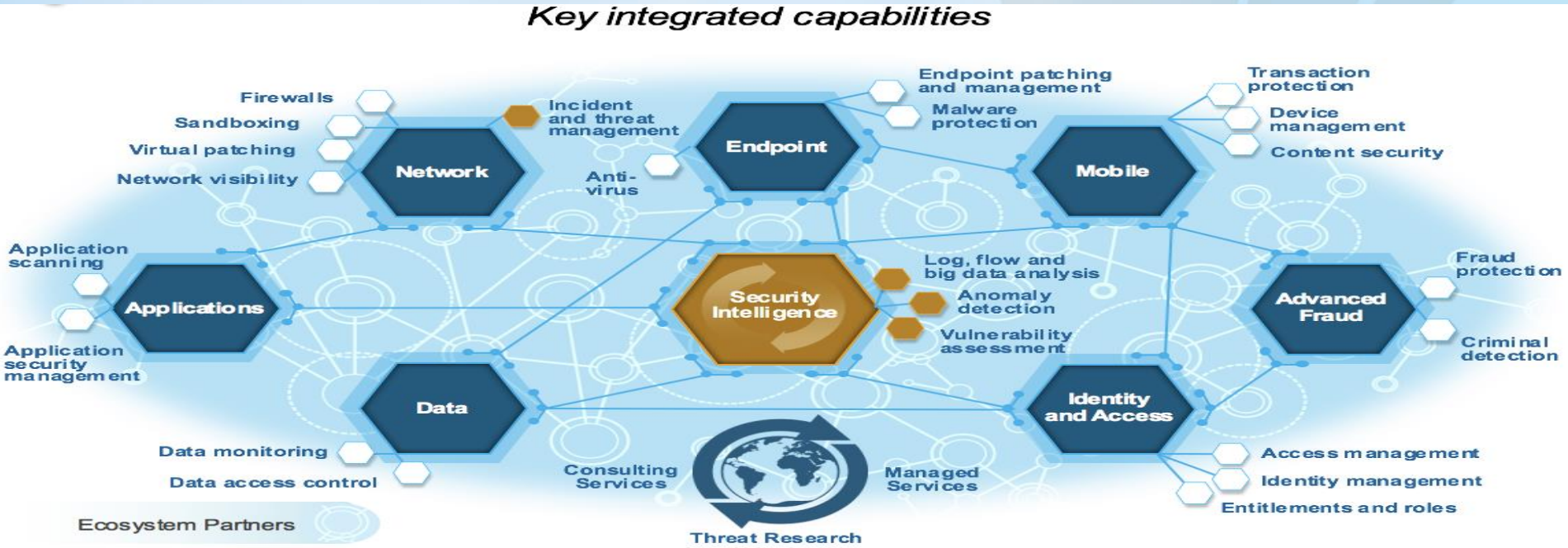


- *30% of organizations say that the network security skills of the infosec staff are inadequate in some, most, or all cases.*
- *44% of organizations say that the number of networking/security staff with strong knowledge in both security and networking technology is inadequate in some, most, or all cases.*
- *38% of organizations say that the ability of the security staff to keep up with network security changes is inadequate in some, most, or all cases.*
- *37% of organizations say that the ability of the security staff to keep up with the threat landscape is inadequate in some, most, or all cases.*
- *47% of organizations say that the number of employees dedicated to network security is inadequate in some, most, or all cases.*

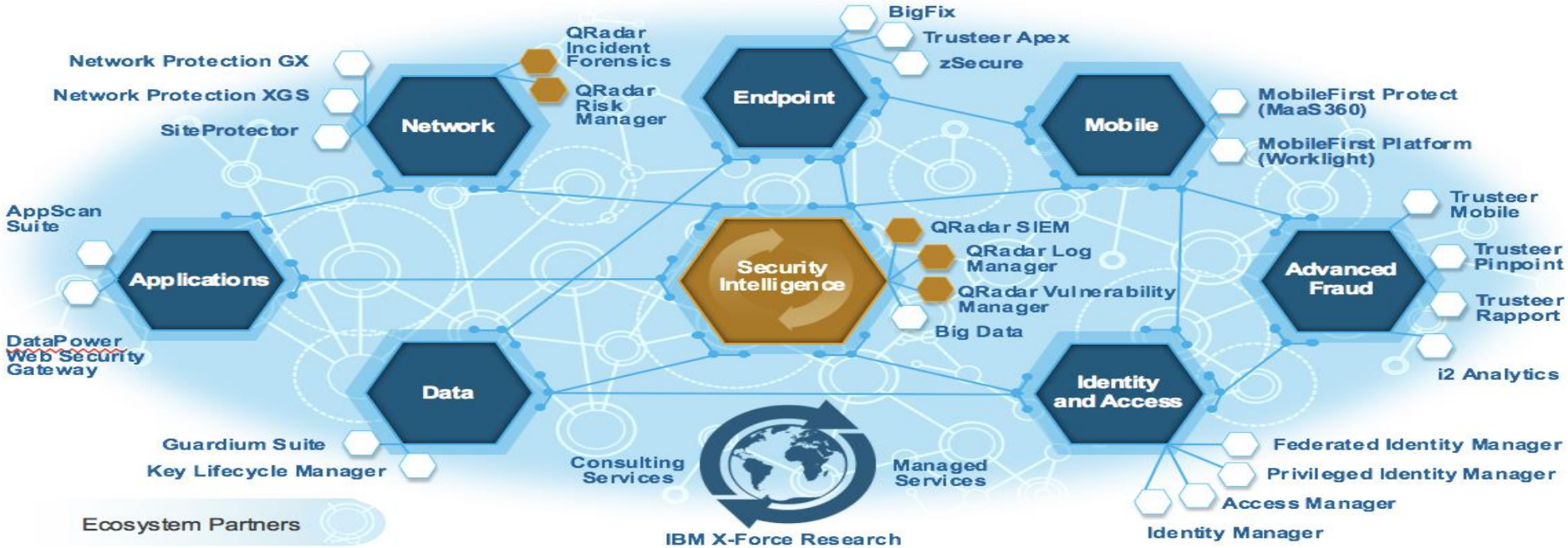
Large organizations have been segmenting networks, filtering packets, and managing firewalls, IDS/IPS, network proxies, and assorted gateways for years. In spite of this experience however, they remained under-skilled and understaffed and thus more vulnerable than they should be.

NANJGEL Solutions

Establish Security as a System



Establish Security as an Eco-System



Our Methodology

What we need to do ?

- **Visibility**
  Get full visibility into your Environment, Understand what is happening & what is not.

- **Detect**
  External & Internal Threats, Vulnerabilities, User Activity, Loss of System and personal or sensitive Data.

- **Report**
  Provide evidence in investigation, Historic & Real Time Data gathering.

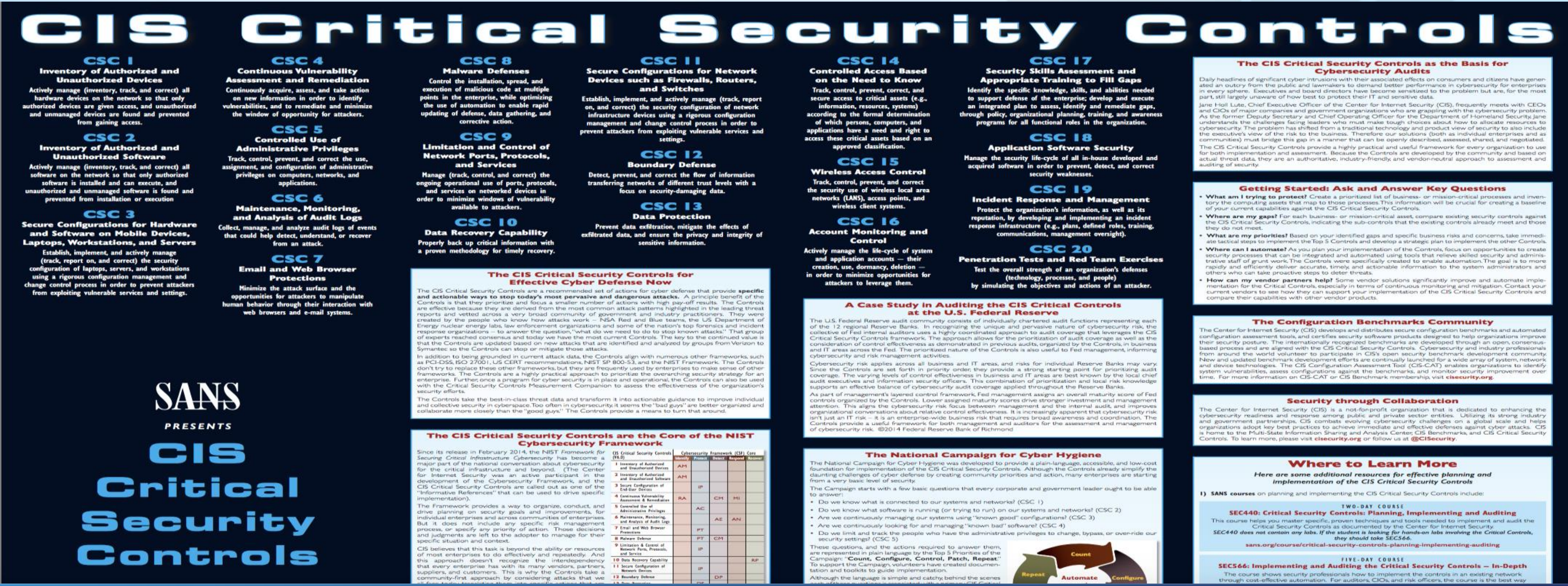
NANJGEL Solutions

What we else also do ?

- **Respond**
  Virtual Firewalling, Data Protection, Block Access, Turn off switch Port , Notification.

- **Remediate**
  Incident management, Open Trouble Ticket, Self Remediation, Integration with 3rd Party tools

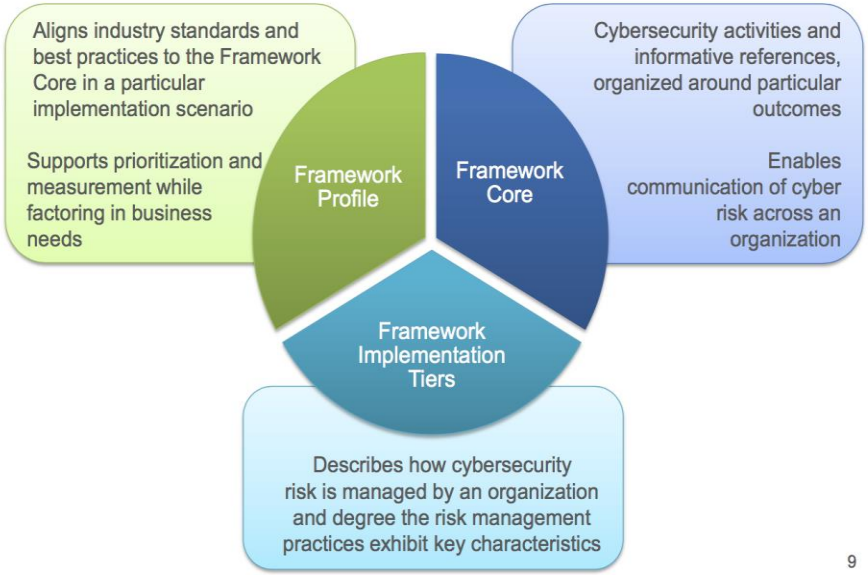
SANS 20 CRITICAL CONTROLS



NANJGEL Solutions

NIST – CYBER SECURITY FRAMEWORK

Framework Components

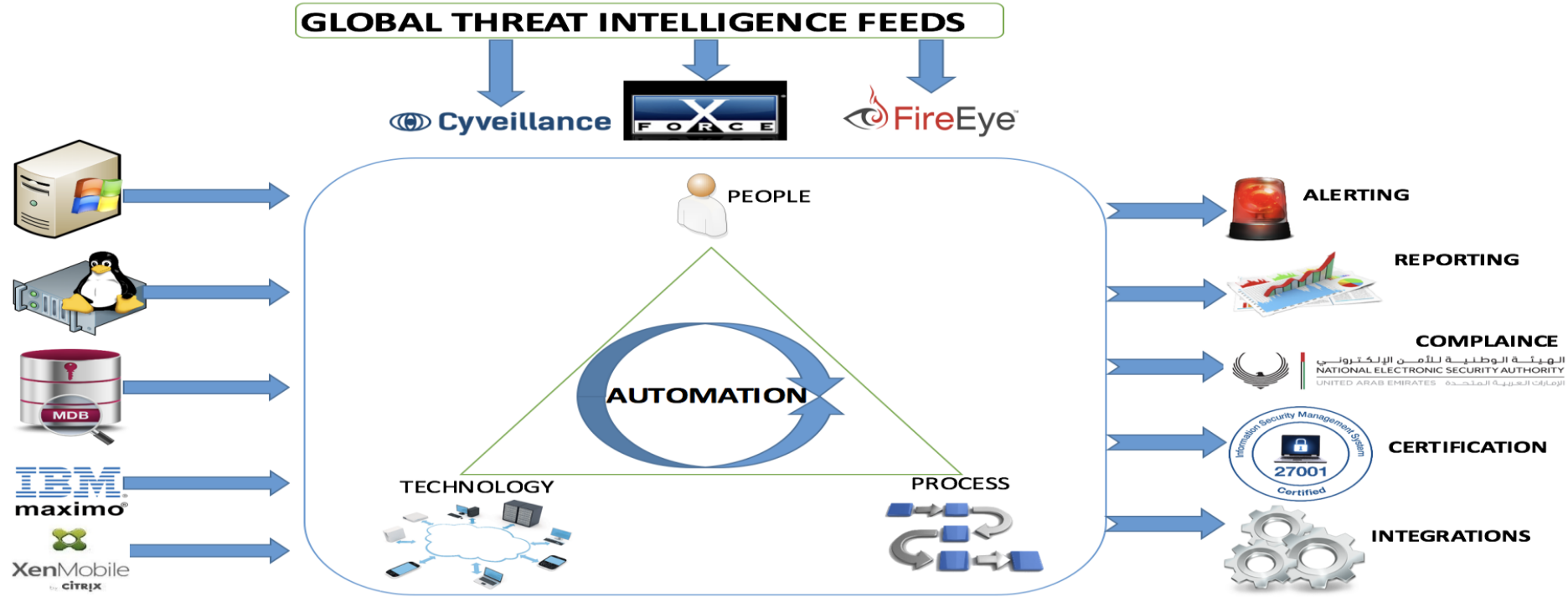


9

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

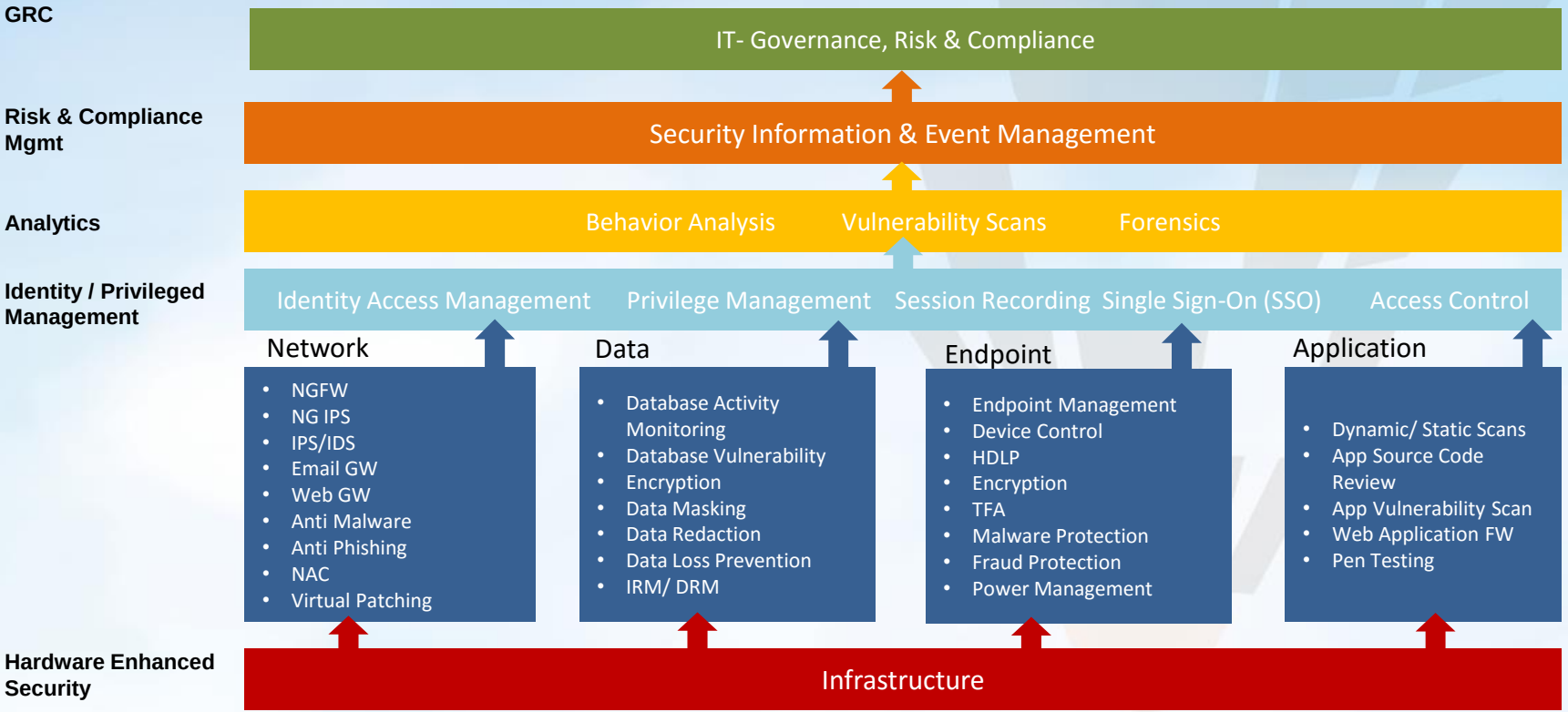
NANJGEL Solutions

NANJGEL AUTOMATED CYBER SECURITY FRAMEWORK

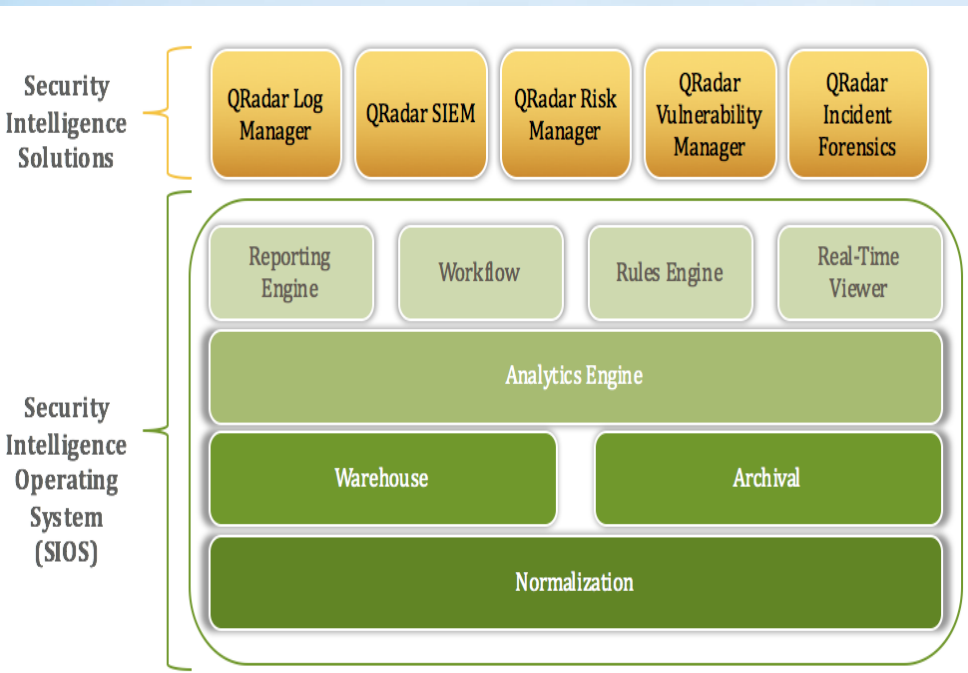


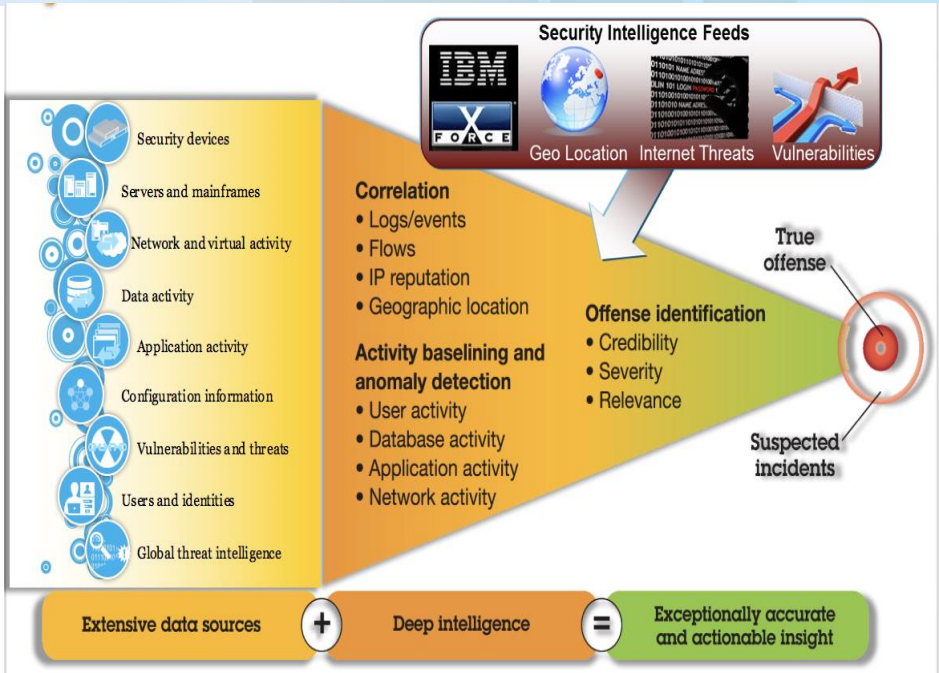
NANJGEL Solutions

Automated Framework Architecture



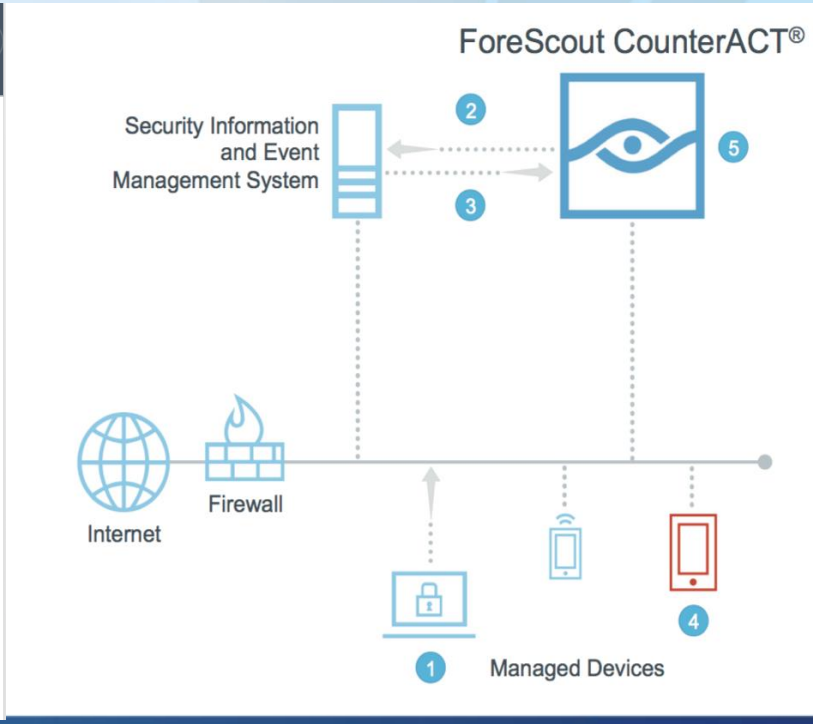
Cyber Analytics – Using IBM QRadar





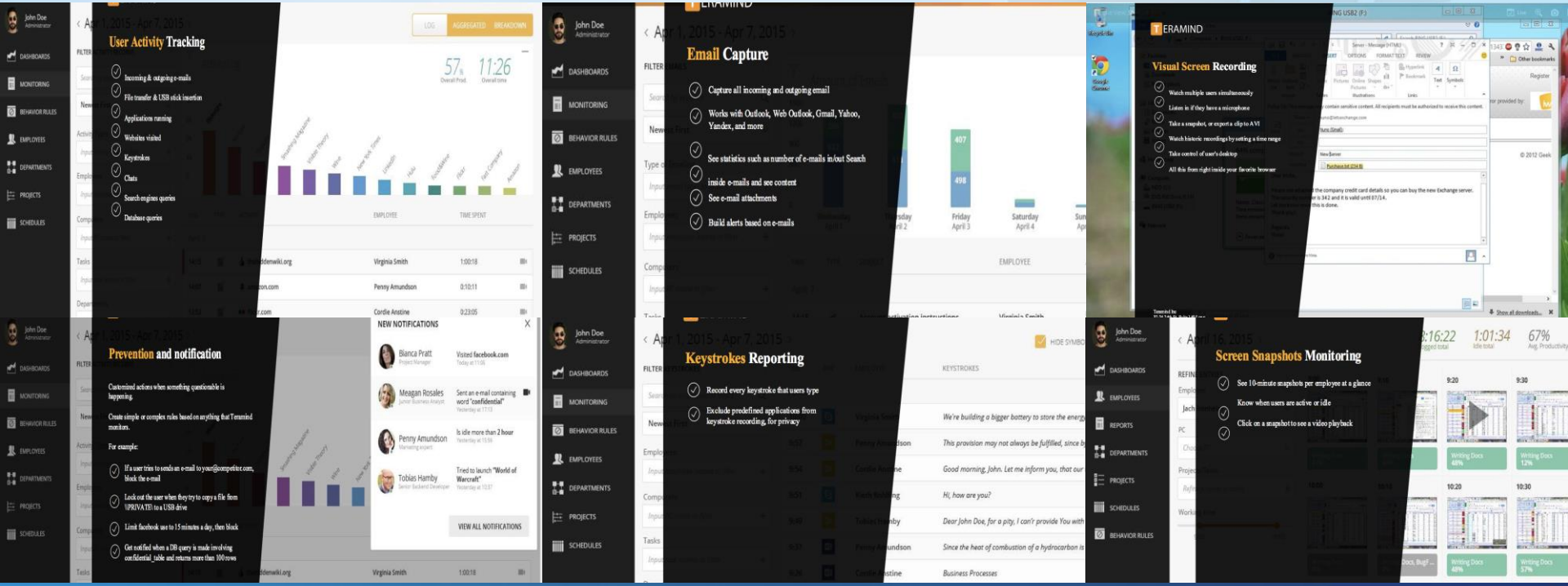
NANJGEL Solutions

Cyber Security Automation – EVAS – ForeScout



NANJGEL Solutions

Automated End User Risk Analysis



NANJGEL Solutions

Automated Global Threat Intelligence

LookingGlass monitors the broadest possible set of sources to maximize detection and speed

Anti-Phishing Take down Service

Anti Spoofing DMARC Email Service

C-Level ID Theft Fraud Detection

Social Media Monitoring Facebook, Twitter etc

Domain Name Registrations and "Go Live" Alerts

Patented Site-Seal Early-Detection System

NANJGEL Solutions

About Us

Established in **2005** providing IT Security Solutions

We lead the way in a different approach to information security

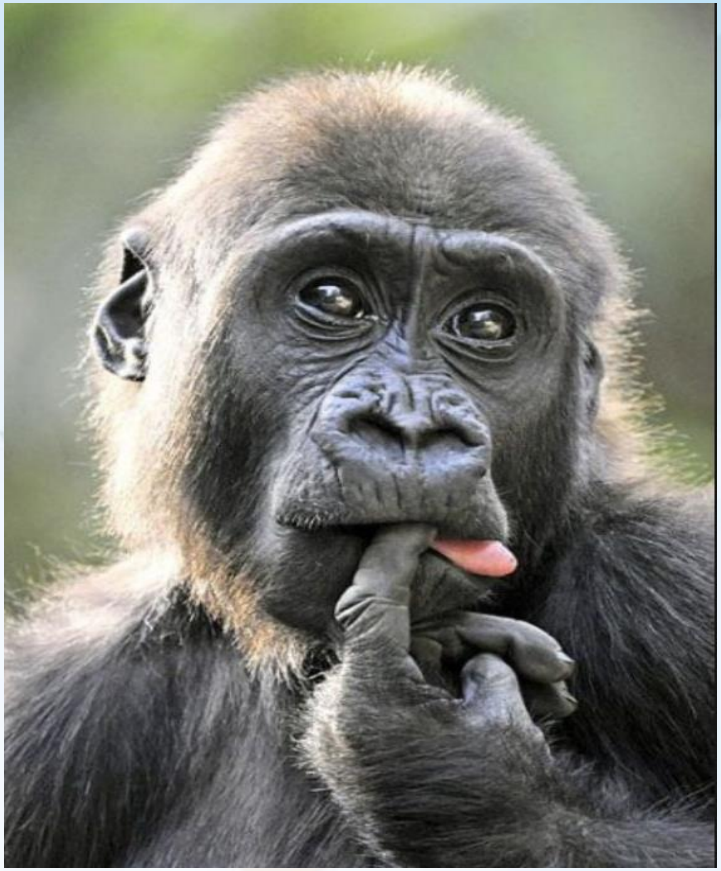
Presence in **Middle East , Europe & India** with over **12 strategic partners & alliances**

Long standing **customer relationships** across all **verticals**

We provide next generation IT solutions for secured business operations

NANJGEL Solutions

Any question?



NANJGEL Solutions