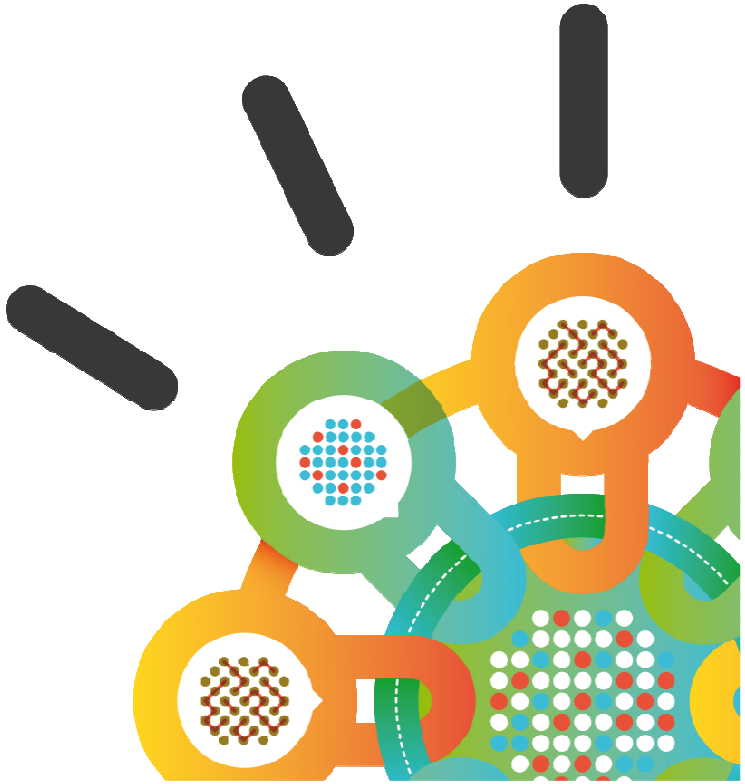
Security Intelligence.
Think Integrated.

IBM Security Systems

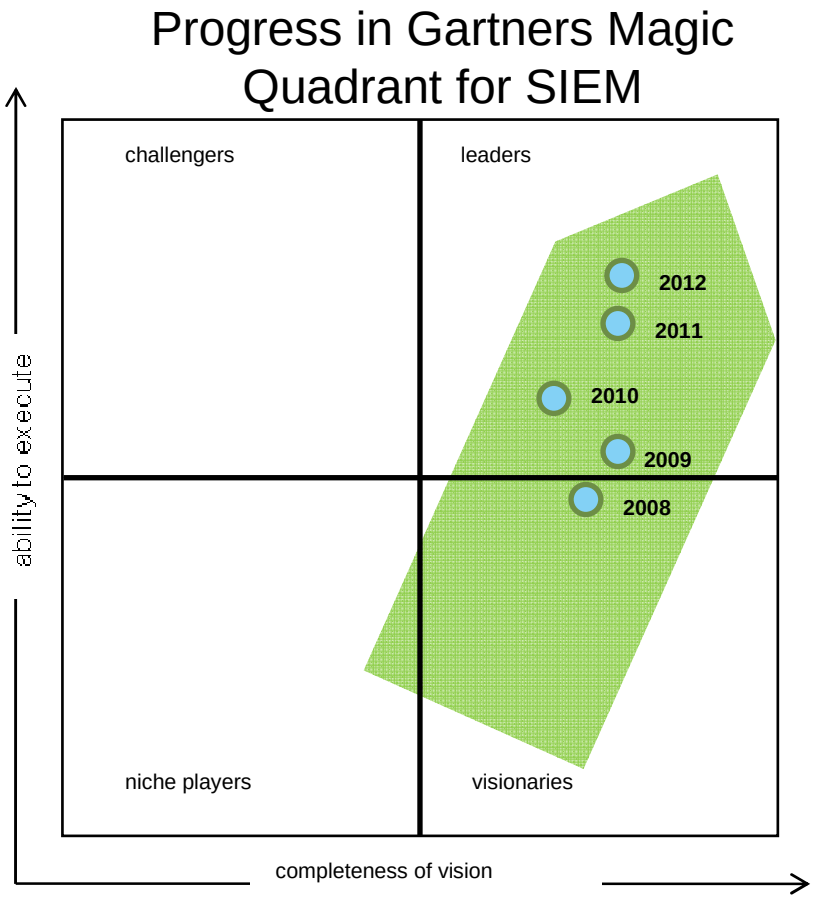
Security wird intelligent



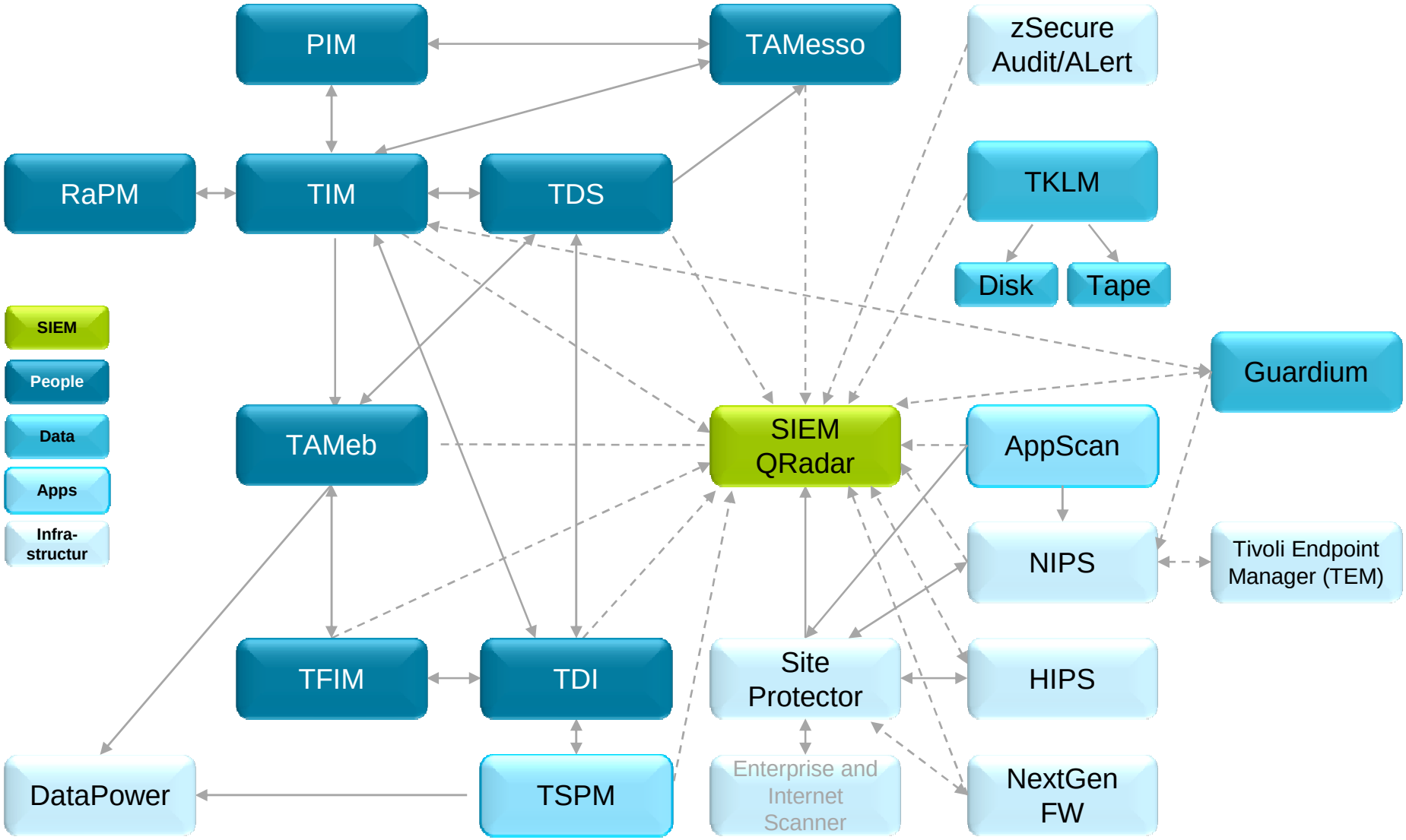
Jürgen Eckstein
Regional Sales Manager
+49-151-12747517
juergen.eckstein@de.ibm.com

Quick Facts Q1 Labs

- Founded 2000, as NBAD toolset
- Products since 2006: Log Management, SIEM, Risk Manager
- QRadar 7.0 achieved the Common Criteria Certification (EAL-3+)
- Leader in Gartner Magic Quadrants 2009, 2010, 2011 and 2012



Product Interconnectivity



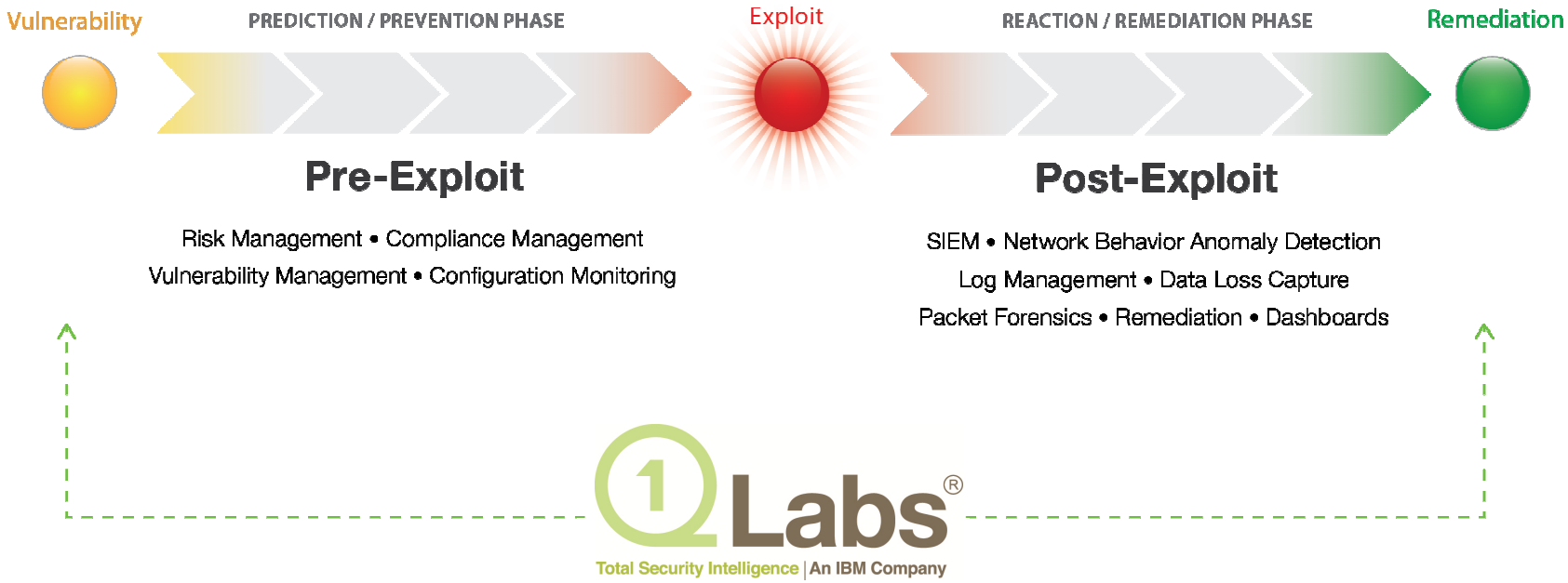
Aktuelle Herausforderungen vieler Unternehmen

- **Compliance & Policy**
  - Compliance-Validierung erfordert Protokollierung und Berichterstattung
  - Neue Vorschriften haben fortwährend Auswirkungen auf viele vertikale Märkte
  - Configuration Audits, manuelle Prozesse

- **Tägliche Schwemme von Logs und Events**
  - Informationen liegen vor, werden aber nicht analysiert, aggregiert und korreliert
  - Fehlende Reduktion zur effektiven Managebarkeit von Verdachtsfällen

- **Sichtbarkeit bei Bedrohungen & Security**
  - Abwehr von Betrugsversuchen, gezielten Angriffen und Cyber-Kriminalität erfordert intelligente Sichtbarmachung
  - Intelligente Telemetriesysteme sind traditionell separierte Insellösungen
  - Breite Überwachung und Integration, um alle Bedrohungen sichtbar zu machen
  - Isolierte Tools zur Adressierung von Risiko-Management Lebenszyklen

Was ist „Security Intelligence“?



Durch Korrelation ergibt sich ein umfassendes Bild

Network and User Context

Event:	**Exploit:** getdrvs.exe ODBC Sample InformationDisclosure
Target:	**96.16.242.135 (vulnerable)**
Host OS:	**Windows XP**
Applications:	**IIS**
Location:	**Headquater**
User ID:	**bboss**
Full Name:	**Big Boss**
Department:	**Executive Branch**

Network Context

Event:	**Exploit:** getdrvs.exe ODBC Sample Information Disclosure
Target:	**96.16.242.135 (vulnerable)**
Host OS:	**Windows XP**
Applications:	**IIS**
Location:	**Headquater**

No Context

Event:	**Exploit:** getdrvs.exe ODBC Sample Information Disclosure
Target:	**96.16.242.135**

Next-Generation SIEM: volle Analyse der Auswirkungen

Before Attack | **During Attack** | **After Attack**

Next-Generation SIEM: Behavior and Context

PROFILING

Who is the attacker?

Where has he been?

What did he do before?

Are my assets prepared?

DETECTION

What is the attack?

Where is it happening?

What rules are firing?

What targets are involved?

FORENSICS

Was it successful?

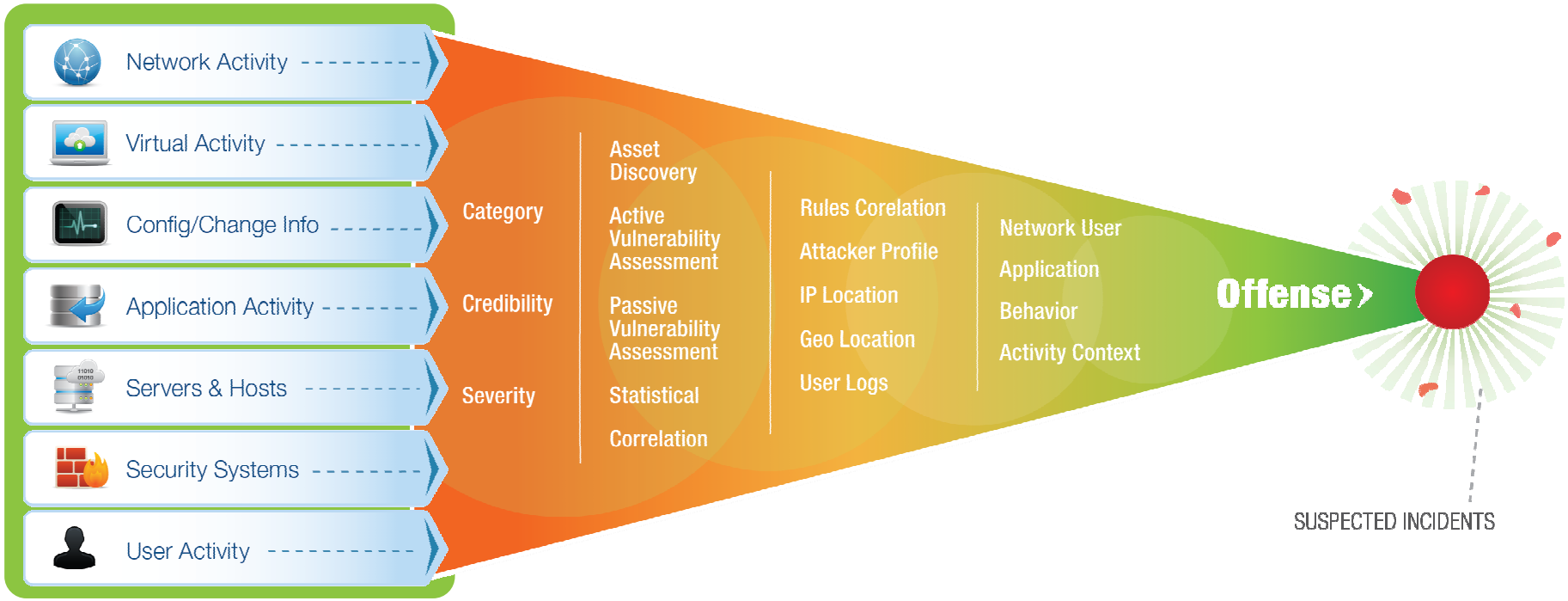
Where has the attack moved to?

What was stolen?

Where is my evidence?

Data Explosion

IBM is integrating across IT silos with Security Intelligence solutions

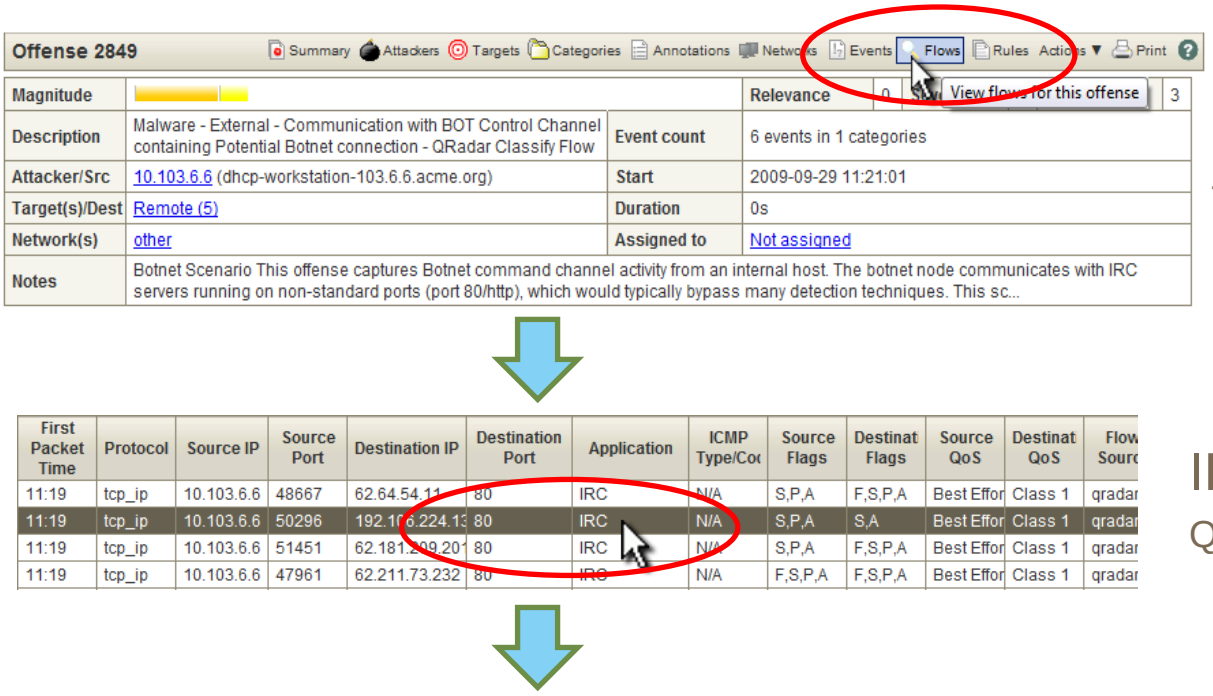


Log-Quellen + QRadar-Intelligenz = genaueste & umsetzbare Erkenntnisse

Offense Management

Klare, präzise und umfassende Bereitstellung von relevanten Informationen:

The Value of Flows – Malware Detection



Potential Botnet Detected?

This is as far as traditional SIEM can go.

IRC on port 80?

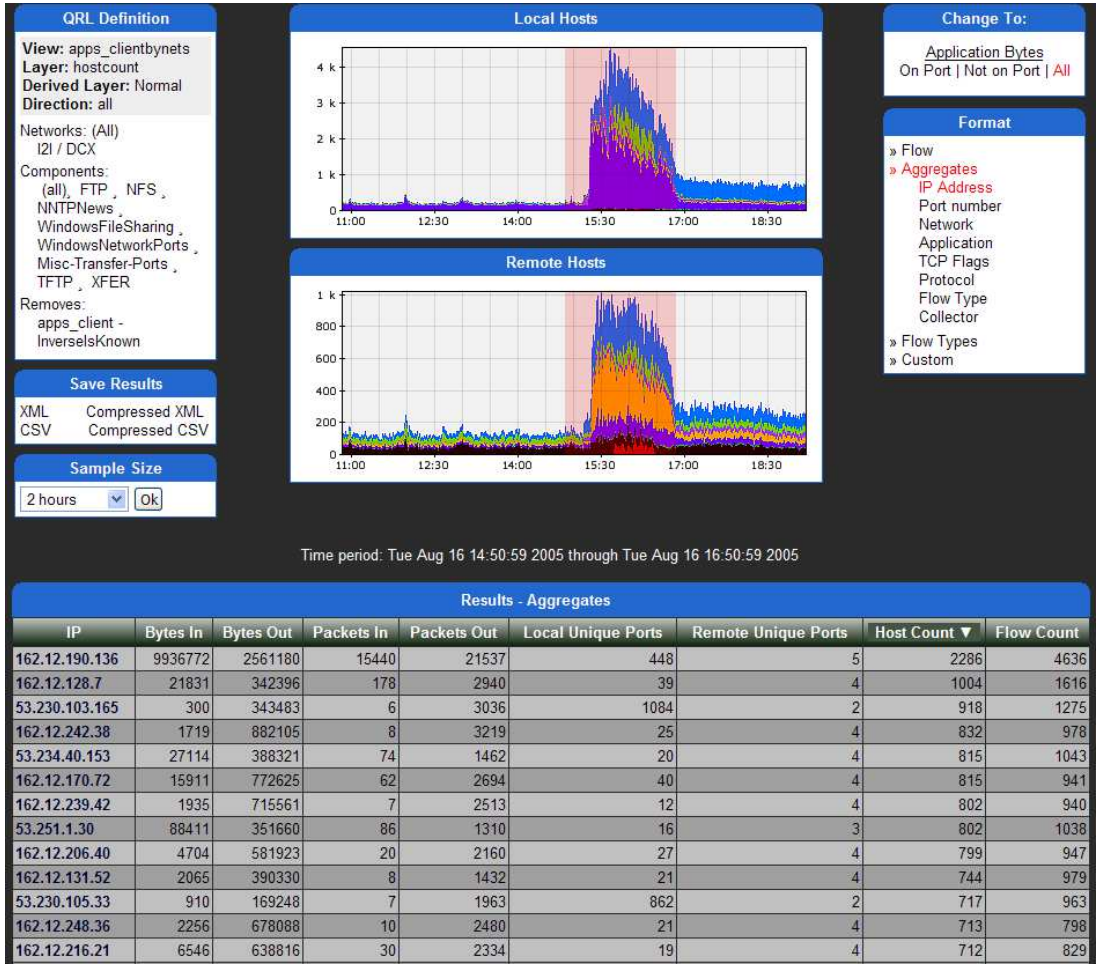
QFlow enables detection of a covert channel.

Irrefutable Botnet Communication

Layer 7 data contains botnet command and control instructions.

The Value of Flows – Anomaly Detection

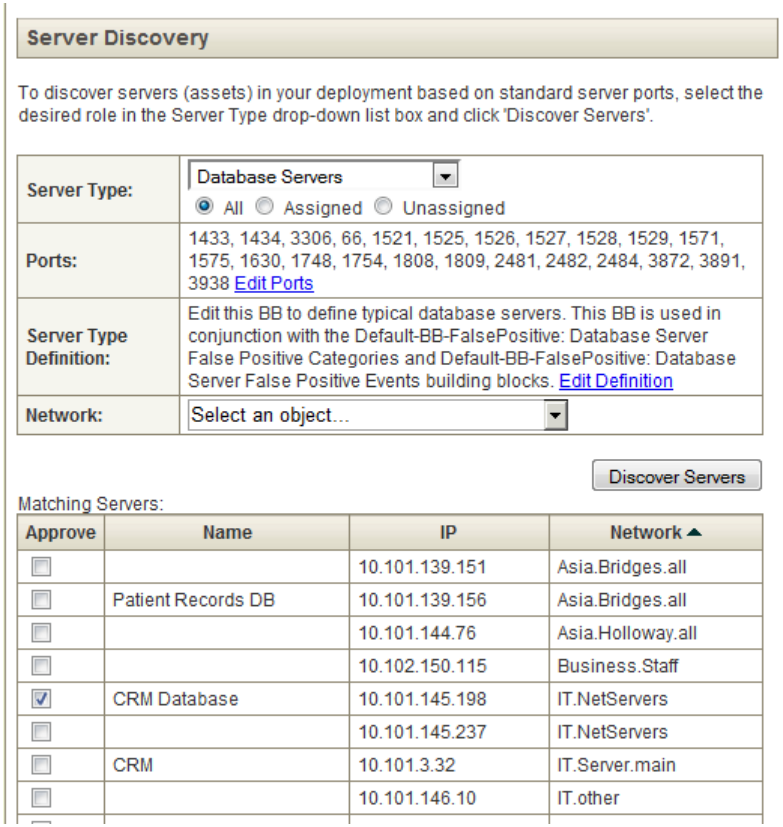
Large Manufacturer –
Detected a worm outbreak affecting their production facility during evaluation using only flow data. This worm was not detected by existing signature based sources



IP	Bytes In	Bytes Out	Packets In	Packets Out	Local Unique Ports	Remote Unique Ports	Host Count ▼	Flow Count
162.12.190.136	9936772	2561180	15440	21537	448	5	2286	4636
162.12.128.7	21831	342396	178	2940	39	4	1004	1616
53.230.103.165	300	343483	6	3036	1084	2	918	1275
162.12.242.38	1719	882105	8	3219	25	4	832	978
53.234.40.153	27114	388321	74	1462	20	4	815	1043
162.12.170.72	15911	772625	62	2694	40	4	815	941
162.12.239.42	1935	715561	7	2513	12	4	802	940
53.251.1.30	88411	351660	86	1310	16	3	802	1038
162.12.206.40	4704	581923	20	2160	27	4	799	947
162.12.131.52	2065	390330	8	1432	21	4	744	979
53.230.105.33	910	169248	7	1963	862	2	717	963
162.12.248.36	2256	678088	10	2480	21	4	713	798
162.12.216.21	6546	638816	30	2334	19	4	712	829

The Value of Flows – Passive Asset Discovery

Port	Risk / Severity	Last Seen	First Seen
514	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
7676	1	2009-09-29 21:30:12 (Passive)	2009-09-28 02:30:11 (Passive)
7777	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
7778	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)
8009	1	2009-09-29 20:00:12 (Passive)	2009-09-28 02:30:11 (Passive)

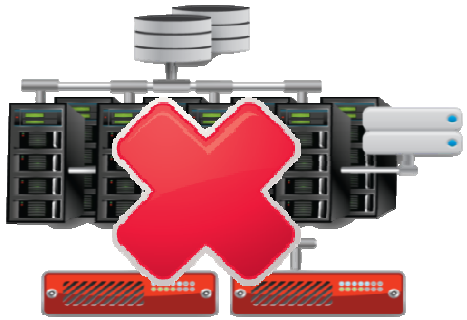


- Automatic Asset Discovery
  QRadar creates host profiles as network activity is seen to/from
- Passive Asset Profiling
  QRadar identifies services and ports on hosts by watching network activity
- Server Discovery
  QRadar identifies and classifies server infrastructure based on these asset profiles
- Correlation on new assets & services
  Rules can fire when new assets and services come online

All made possible by Netflow & QFlow

QRadar: Integration verhindert die falsche Wahl zwischen Möglichkeiten & Einfachheit

Bolted Together Solution



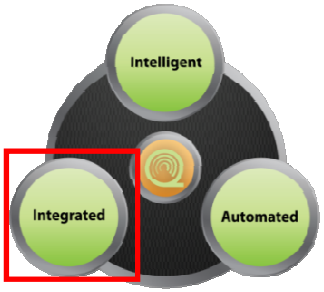
- Scale problems
- Disparate reporting, searching
- No local decisions
- Complex High Availability
- Multi-product admin and DBA
- Forklift upgrades
- Duplicate log repositories
- Operational bottleneck

QRadar Integrated Solution

- Highly scalable
- Common reporting, searching
- Distributed correlation
- Integrated High Availability
- Unified administration
- Seamless expansion
- Logs stored once
- Total visibility

Unified Administration
Time spent managing security events was reduced by 80% compared to siloed systems

Roto



QRadar Security Intelligence Solutions - Deploy, Expand at Your Pace

Log Management

QRadar Log Manager

QRadar Log Manager Free Edition

- Turnkey log management
- SME to Enterprise
- Upgradeable to enterprise SIEM

SIEM/SEM

QRadar SIEM

- Integrated log, cyber threat, risk and compliance management
- Sophisticated event analytics
- Asset profiling and flow analytics

Risk Management

QRadar Risk Manager

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

Scale

QRadar High Availability

- Event Processors
- Network Activity Processors
- High Availability
- Stackable Expansion
- Embedded, real-time database

Visibility/ Network Activity

QFlow Collector

VFlow Collector

- Layer 7 application monitoring
- Content capture
- Network Analysis

QRadar Security Intelligence Solutions - Deploy, Expand at Your Pace

Log Management

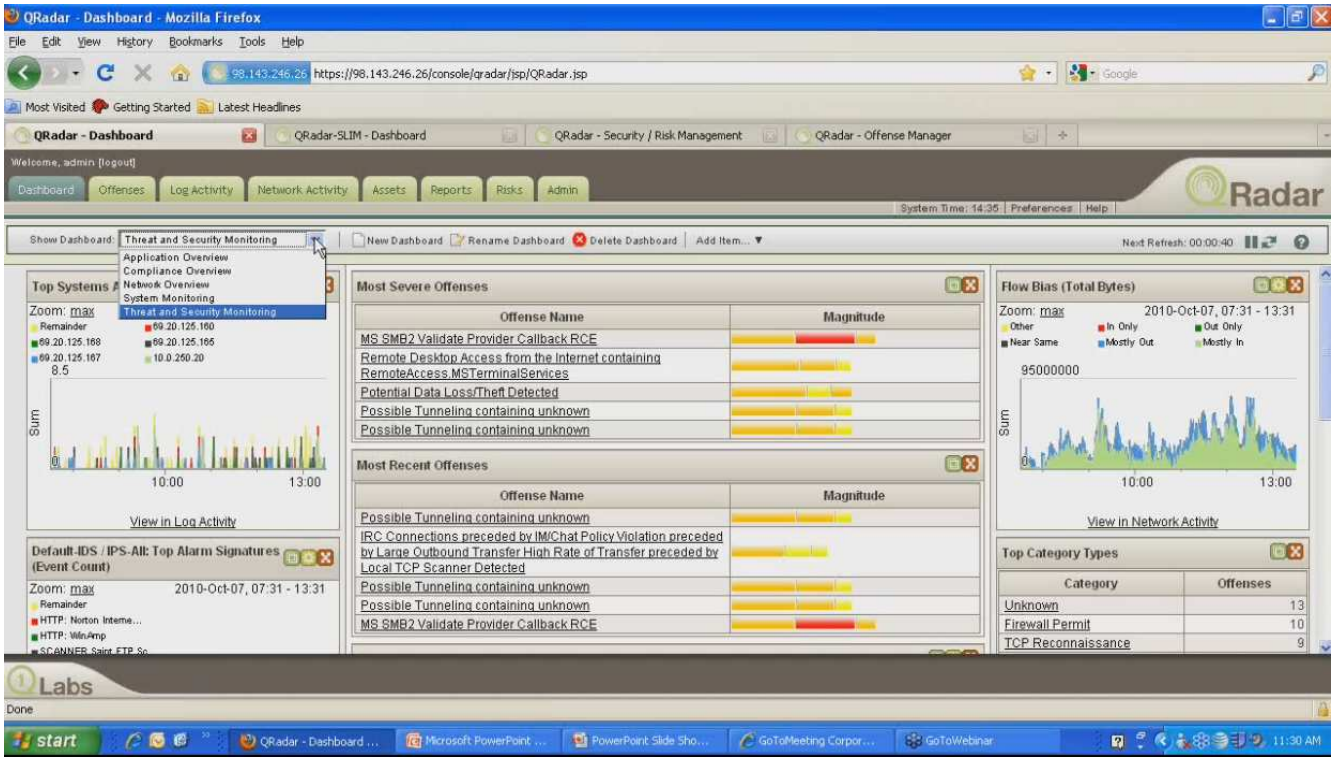
SIEM/SEM

Risk Management

Scale

Visibility/ Network Activity

One Console Security



QRadar: Automation Drives Simplicity and Cost Effectiveness




Monitor

- Auto-discovery of log sources
- Auto-discovery of applications
- Auto-discovery of assets
- Auto-grouping of assets
- Centralized log management
- Automated configuration audits

Analyze

- Auto-tuning
- Auto-detect threats
- Thousands of pre-defined rules
- Easy-to-use event filtering
- Advanced security analytics

Act

- Thousands of predefined reports
- Asset-based prioritization
- Auto-update of threats
- Auto-response
- Directed remediation

Efficient, Immediate, Custom

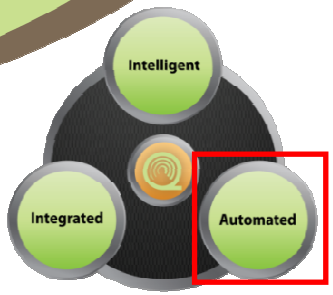
"Where it would take 10 days on our old system to build and test rules, it takes us just 10 minutes in QRadar."

logica

Automation Drives Operations Efficiency

"We were pleased with QRadar being extremely automated, equipped with compliance-driven report templates that were very useful out of the box, which spared us the manpower and resources of having to develop them ourselves."

REGULUS



QRadar Architecture

Event Processor (EP)	Collect, Normalize, Correlate, Store Events
Flow Processor (FP)	Collect, Normalize, Correlate, Store Flows
Database (DB)	Purpose built DB „Ariel“
Management (MG)	Management, Rules, Reporting, Correlation

QRadar Architecture

All-In-One Appliance

Event Processor (EP)

Flow Processor (FP)

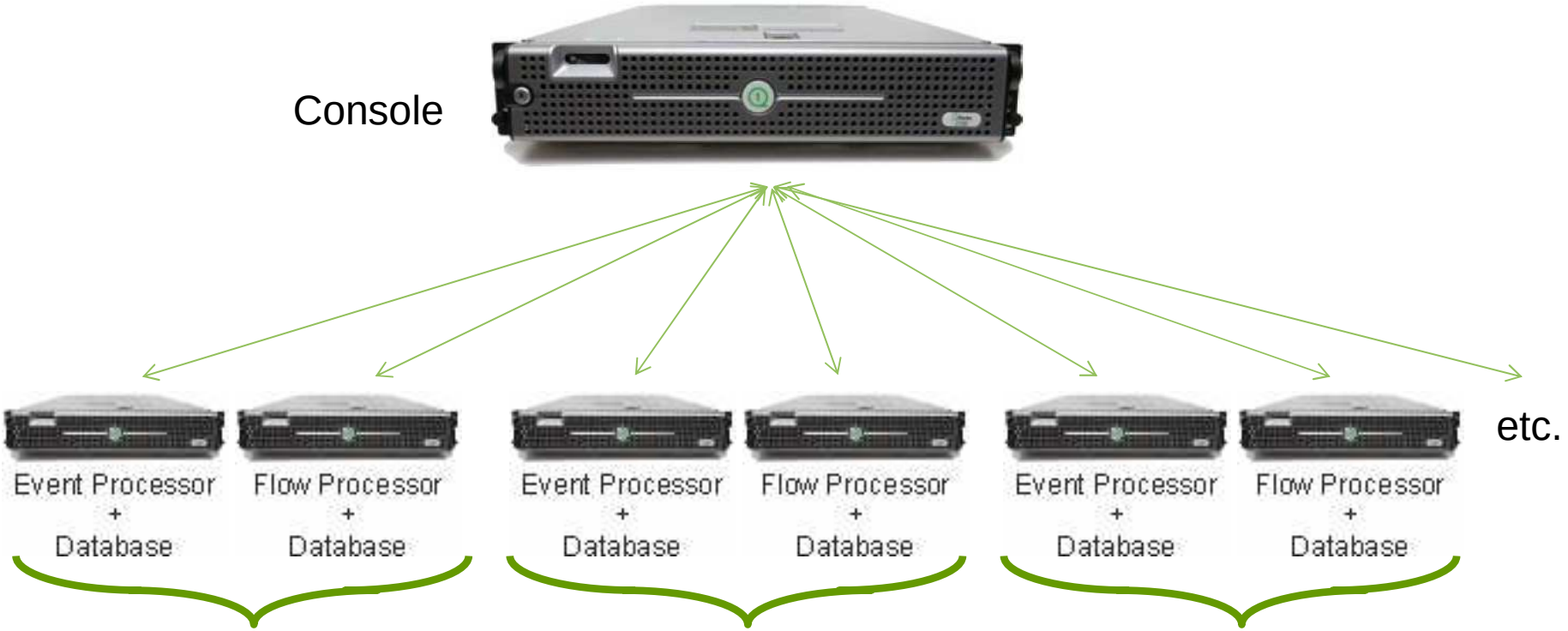
Database (DB)

Management (MG)

Up to:
5K Events/Second (correlated!)
200K Flows/Minute (correlated!)

QRadar Architecture

Distributed Environment



up to 20K EPS correlated
up to 600K FPM correlated

up to 20K EPS correlated
up to 600K FPM correlated

up to 20K EPS correlated
up to 600K FPM correlated

QRadar Lizenzmodell

Basics

- Die QRadar Plattform wird grundsätzlich als Hardware-, Software-, und Virtual-Appliance angeboten (Software-Appliances müssen auf Kundenserver mit RedHat Enterprise Server 5.4 oder 5.7 installiert werden; Virtual-Appliances sind derzeit auf max. 1.000 Events/Sekunde beschränkt)
- Die Lizenzierung besteht aus dem Kauf der entsprechenden Appliance (gilt für Hard-, Soft- und Virtual-Appliance plus Kauf von Lizenzen für Events/Sekunde, Flows/Minute und Anzahl Log Sources.
- Alle Appliances können eine gewisse Anzahl an Events und/oder Flows verarbeiten. Das Deployment erfolgt entweder über eine All-In-One Appliance, welche alle benötigten Komponenten in einer Appliance vereint, oder über eine verteilte Umgebung, falls die maximale Anzahl Events und/oder Flows für eine einzelne Appliance überschritten wird.
- In einer verteilten Umgebung wird immer eine Console für das Management und mindestens ein Event- und/oder Flow- und/oder kombinierter Event/Flow Prozessor benötigt.
- In einer verteilten Umgebung können mehrere Event- und/oder Flowprozessoren eingesetzt werden falls die maximale Anzahl für einen Event- und/oder Flowprozessor überschritten wird
- Kombinierte Event/Flow Prozessoren können die Kosten senken, es können mehrere Event/Flowprozessoren an eine Console angeschlossen werden.

Modell 1: All-In-One Appliance

QRadar 2000:
kommt Basislizenz für
Events/Sec: 200
Flows/Minute: 30000
Log Sources*: 250

Nicht erweiterbar!

QRadar 2100:
kommt mit Basislizenz für
Events/Sec: 1000
Flows/Minute: 50000
Log Sources*: 750

Erweiterbar auf max.
Flows/Minute: 100000

QRadar 31XX:
kommt mit Basislizenz für
Events/Sec: 1000
Flows/Minute: 50000
Log Sources*: 750

Erweiterbar auf max.
Events/Sekunde: 5000
Flows/Minute: 400000

*Log Sources = Anzahl der Geräte die Logdaten generieren und diese zur Analyse an QRadar senden. LogSources können auf eine bliebige Anzahl erweitert werden, solange die insgesamte Anzahl Events/Sekunde die maximale Menge des gesamten Systems nicht übersteigt.

** Die QRadar 31XX Series wird als 3100 mit 3TB, als 3105 mit 6TB und als 3124 mit 16TB internem Festplattenspeicher angeboten, Basislizenz ist identisch.

Modell 2: Verteilte Umgebung mit dedizierten Event- und/oder Flowprozessoren

Console

Eventprozessor

Flowprozessor

QRadar 31XX* Console:
kommt Basislizenz für
Log Sources 750

QRadar 16XX* Eventprozessor:
kommt mit Basislizenz für
Events/Sec: 2.500

Erweiterbar auf max.
Events/Sekunde: 20.000

QRadar 17XX* Flowprozessor
kommt mit Basislizenz für
Flows/Minute: 200.000

Erweiterbar auf max.
Flows/Minute: 1.200.000

* Alle Appliances werden als XX00 mit 3TB, als XX05 mit 6TB und XX24 mit 16TB internem Festplattenspeicher angeboten, Basislizenzen sind identisch.

Modell 2: Verteilte Umgebung mit kombiniertem Event- und Flowprozessor

Console

Event- und Flowprozessor

QRadar 31XX* Console:
kommt Basislizenz für
Log Sources 750

QRadar 18XX* Event- und Flowprozessor:
kommt mit Basislizenz für
Events/Sec: 1.000
Flows/Minute: 50.000

* Der 18XX Event- und Flowprozessor wird als 1801 mit 1,5TB angeboten, welcher bis max. 1.000 Events/Sekunde 100.000 Flows/Minute und als 1802 mit 3TB angeboten, welcher bis max. 5.000 Events/Sekunde und 400.000 Flows/Minute erweitert werden kann

Selling Q1 Labs Solutions

Ziel Kundenprofil

- **Ziel-Unternehmensgröße**: $200M+ Umsatz; 750+ Mitarbeiter

  Ideale Unternehmen: 10,000+ Mitarbeiter
- **Ziel Branchen**: Energie & Versorgungsunternehmen; Bundes-, Landesbehörden; Fertigung; Industrie; Automobilindustrie, Banken, Versicherungen, Healthcare, Retail etc.
- **Ziel Abteilungen**: Network security; network; security; IT operations; risk management, compliance & policy
- **Ziel Ansprechpartner**: CIO/CISO; VP/Director of Security und/oder Security; VP/Director of IT; Compliance & Risk Mgmt.
- **Übliche Compliance Driver**: **PCI**, **SOX**, **ISO2700x**, etc.
- **Andere Eigenschaften**: Kein zentralisiertes Log Management; manuelle Vorfall-Management Prozesse; keine verteilte Netzwerk-Sniffing-Fähigkeiten

Sales Cycle: Functional Drivers

Title	Scenario
CISO / CIO	• Besseres Erkennen von externen und internen Bedrohungen und Bereiche der Nichteinhaltung von Regularien • Verbesserung der allgemeinen Sichtbarkeit, Früherkennung von Sicherheitsrisiken für das Unternehmen • Reduktion der Verbreitung von Anbieter und Technologien durch Konsolidierung
VP / Director of IT or Security	• Adressierung der erhöhten Komplexität und Anzahl der Angriffe, die ihre Netzwerke durchdringen • Verbesserung des Risoko-Managements zahlreicher Schwachstellen bevor Erfolgreiche Attacken und Einbrüche auftreten • Verbesserung der betrieblichen Effizienz von Netzwerk-und Security-Teams • Wählen Sie flexible Lösungen, die zukunftssicher sind und skalieren können, um Veränderungen und Wachstum zu unterstützen
Security / Network Engineer	• Anomales Verhalten und schwer zu erkennende Bedrohungen im gesamten Netzwerk identifizieren • Aufdeckung von Betrug • Zeitersparnis durch bessere Priorisierung der Vorfälle und schnellere Indentifizierung von Bedrohungen
Compliance and Policy Officer	• Automatisierte Überwachung von Unternehmensrichtlinien und gesetzlichen Richtlinien wie SOX, PCI, ISO 2700x etc. • Sammlung großer Mengen von Daten und Ereignisse in einer überschaubaren und leicht überprüfbaren Weise • Automatisierung von Compliance-Reports für Audits, um manuellen Aufwand zu reduzieren

Qualifizierende Fragen…

- Welche Arten der Sicherheit und Compliance-Risiken müssen Sie heute berücksichtigen?
- Hatten Sie in der Vergangenheit bei Compliance-Audits Unregelmäßigkeiten?
- Wie führen Sie die Überwachung Ihrer Netzwerk-und Security-Geräte durch? Haben Sie das Gefühl Sie können alle Bedrohungen für Ihre Infrastruktur identifizieren?
- Nutzen Sie bereits heute schon Log-Management oder SIEM-Lösungen? Sind Sie zufrieden mit deren Leistung und Benutzerfreundlichkeit?
- Haben Sie eine wichtige Security-bzw. Netzwerk-Initiativen im Gange oder geplant für die nahe Zukunft?
- Mit welchen Herausforderungen sehen Sie sich bei der Netzsicherheit heute konfrontiert?
- Welche kurz- und/oder langfristigen Veränderungen planen Sie für Ihre Infrastruktur?

Schlagworte um QRadar Opportunities zu identifizieren: “Wir müssen…”

- ...das Reporting für Compliance-Audits stärken / automatisieren
- ...Kosten und Aufwand für die Einhaltung für SOX, PCI, Unternehmenspolicy etc. reduzieren
- ...unsere Log-Management oder SIEM-Lösung upgraden / ersetzen
- ...Sicherheitslücken und Risiken schneller erkennen
- ...anomale Netzwerk- / Benutzer- / Anwendungs-Aktivitäten identifizieren
- ...internen Diebstahl, Betrug oder hinterlistige Aktivitäten entdecken
- ... Social-Media oder Mobile-Aktivität in Bezug auf Datensicherheitsrisiken überwachen
- ...Netzwerk-Aktivitäten in virtuellen und Cloud-Umgebungen monitoren
- ...die Kosten oder den manuellen Aufwand unserer SIEM / Log Mgmt. Lösung reduzieren
- *Wettbewerb*: HP ArcSight, RSA, NitroSecurity (McAfee)

Hauptunterscheidungsmerkmale

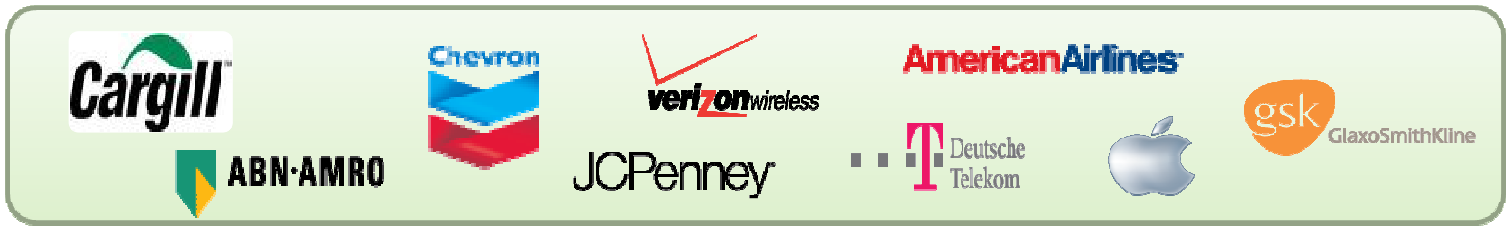
1) Meist Intelligent
   - Bedrohungserkennung - Flow-Analyse für Netzwerk-, Anwender-und Applikations-Monitoring
   - Massive Datenreduktion, um die „Nadel im Heuhaufen“ zu finden
   - Pre-exploit security awareness

2) Meist Integriert
   - Konsolidierung von Insellösungen und Produkten mehrerer Hersteller
   - Extrem hohe Skalierbarkeit - wir liefern was andere nur versprechen
   - Zukunftssicher Ansatz

1) Meist Automatisiert
   - Automatische Erkennung und Auto-Tuning, um Operationen zu vereinfachen
   - Geringe Anforderungen für die Umsetzung, schnelles „Time-to-Value“

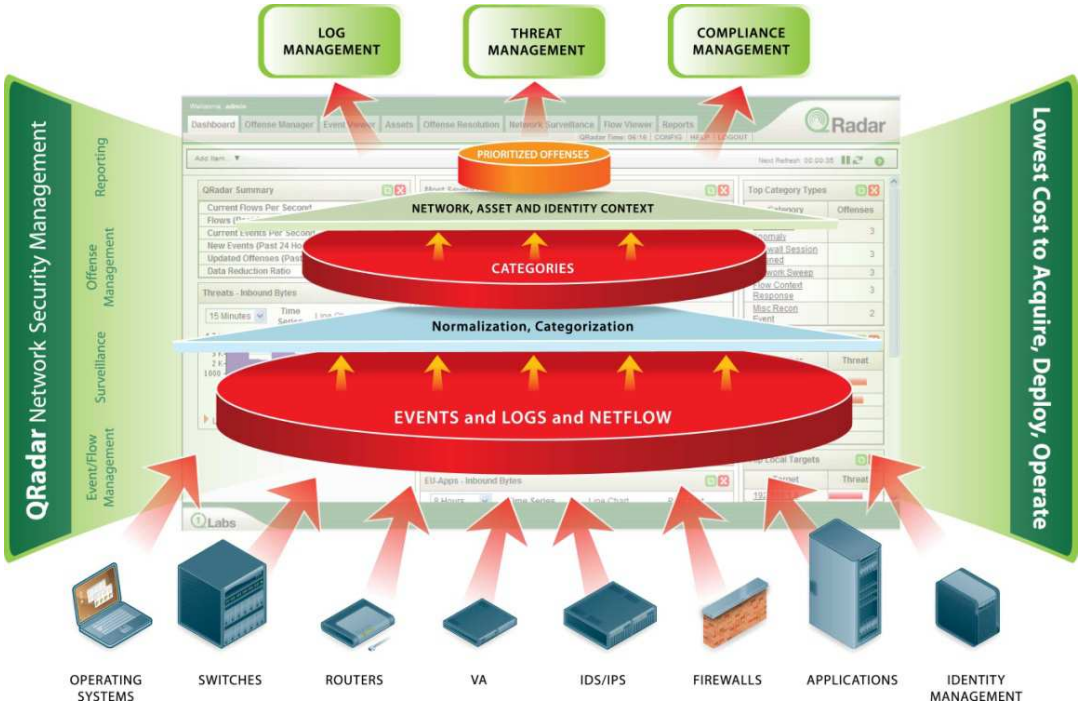
Top Gründe, warum Kunden Q1 Labs gewählt haben

1. Die meist intelligente, integrierte und automatisierte Lösung
2. Die modernste und ausgefeilteste Bedrohungs-Analytik mit umfangreichster Sichtbarkeit für die Verwaltung von Bedrohungen
3. Amortisiert sich innerhalb kürzester Zeit mit geringem Personalbedarf
4. Einfache Skalierbarkeit, wenn Organisation, Bedrohungen und Datensicherheit wachsen
5. Etablierter Marktführer mit exzellenten Kunden-Support
6. Einfach Geschäfte machen, mit den besten Channel-Beziehungen



QRadar PoC deckt auf

- **Was ist erforderlich**
  - Minimalster Aufwand der Mitarbeiter bei der Einrichtung des PoC (ca. 2-4 Stunden)
  - QRadar Hardwareappliance wird mit Werkseinstellungen ins Unternehmens-Netzwerk eingerichtet
  - Event-Log-Quellen (Firewall, Anti-MalWare, IDS, IPS, Applikationen etc.) schreiben ihre Logs zum QRadar

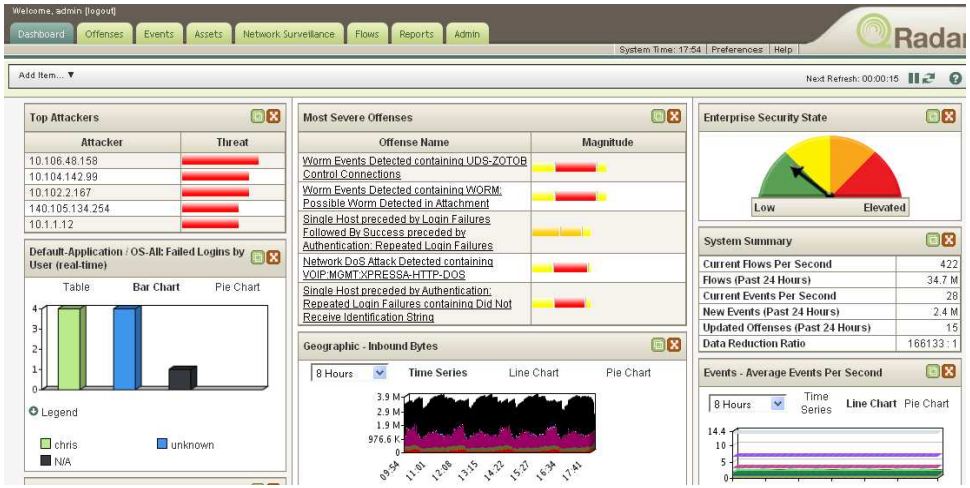


- Mit den ersten ankommenden Logs beginnt die Analyse und Korrelation
- Spezielle Anforderungen können mit geringem Aufwand flexibel umgesetzt werden

Log-Quellen + QRadar-Intelligenz = genaueste & umsetzbare Erkenntnisse

Ergebnis

- **Nach zwei Wochen Besprechung der Resultate**



- Welche Angriffe (Hacking-attacken, Viren, neueste Technologien wie SQL-Slammer, Botnet, DDoS, DMZ jumping etc.)
- Welche Verwundbarkeiten (ungepatchte Systeme, unbekannte Sicherheitslücken, Social Media etc.)
- Welche Betrugsversuche (Data Leakage, Versand von sensiblen Daten z.B. Kreditkarten-Nummern oder unternehmenskritische Daten; verdächtige Authentisierungsaktivitäten (deaktivierte/ abgelaufener Accounts, das Erraten von Kennwörtern etc.)
- Erkennung unberechtigter WAPs oder anderer nicht klassifizierte Geräte
- Datenbankangriffe (brute force account access, administrative Änderungen etc.)
- Verstöße gegen Policies (Nutzung von Peer-to-Peer oder Skype etc.)
- Reporting und vieles mehr...

Thank You!

Jürgen Eckstein
Regional Sales Manager
juergen.eckstein@de.ibm.com