IBM Security
QRadar Virtual Meet Up

twitter.com/IBMSecurity
Linkedin.com/showcase/ibm-security

Overview

- **News and Announcements**
- **QRadar Roadmap and Strategy**
- **Technical Support update**
- **Meeting Discussion: User Behavior Analytics**

News and Announcements

Jerry Frady
North America Technical Sales Leader, IBM Security
jerryfrady@ibm.com

Daily Offering Demos

The Daily Demo Series showcase how our offerings can meet today's security challenges. We invite any customer or security professional to tune in to see a client use case, watch a demo, and ask questions to our experts.

https://ibm.biz/securitycommunityevents

Monday

Mobile Security Monday (2:00 pm)

Abstract: Join us on Mobile Security Mondays for a demonstration from our experts on IBM's market leading Unified Endpoint Management solution. IBM MaaS360 minimizes the steps, resource requirements, and manual activities associated with endpoint management, giving IT practice visibility, security, and control over users devices, apps, content and data – all from one place

Speakers:
- Eric Geller, Technical Sales Engineer
- Ryan Schwartz, Product Marketing Manager

Tuesday

Fraud Prevention Tuesday (10:00 am)

Abstract: Join us for Fraud Prevention Tuesdays where our experts will demo how IBM's Trusteer solutions can quickly & transparently establish digital identity trust

Speaker:
- Eric Geller, Technical Sales Engineer
- Valerie Bradford, Product Marketing Mgr

Data Security Tuesday (2:00 pm)

Abstract: Join us on Data Security Tuesday for a demo on how IBM Security Guardium helps orgs. take a smarter, more adaptive approach to safeguarding their critical data

Speakers: Ken Anderson, Cybersecurity specialist, Rob Young, Tech Product Mkting

Wednesday

IAM Wednesday (2:00 pm)

Abstract: Join us for Identity and Access Management Wednesdays. Weekly content will vary between Cloud Identity, Secret Server, and Identity Governance & Intelligence.

Speakers:
- Eugene Torgovitsky, Client Technical Specialist
- Malik Merchant, Senior Cybersecurity Client Technical Specialist
- Katherine Cola, Product Marketing Manager
- Michael Keane, Product Marketing Manager for Access Management

Thursday

Threat Mngmt Thursday (2:00 pm)

Abstract: Join us on Threat Management Thursdays, where our experts will demonstrate various aspects of how IBM's Threat Management solutions can help you detect and respond to attacks far more effectively and efficiently.

Speakers:
- Jason Brinning, Cybersecurity Technical Specialist
- Jamie Cowper, Security Marketing Leader, Resilient

Friday

CP4S Friday (2:00 pm)

Abstract: Join us for "Into The Future With Cloud Pak for Security Fridays", where our experts will describe our participation in the Open Cybersecurity Alliance (OCA) and how this is manifesting into an open, standards based approach to enabling visibility, detection and response across previously disconnected hybrid multicloud environments and security solutions.

Speakers:
- Charlie Niemi, CTP, IBM Resilient
- Carry Resor, Product Marketing, CP4S

Threat Management at Think 2020

May 5-6

ibm.com/events/think

#IBMThink2020

Session name	Session ID	Session Type	Speakers
Detect & Respond to Accelerating Threats	7114	Featured Session	John Wheeler, Wendi Whitmore
Staying a Step Ahead: Applying Advanced Algorithms to Insider Threats	3233	Technical Session	Joe Mobisa (HMS), Christopher Meenan
The Importance of Automation in Today's Cybersecurity	3358	Technical Session	Jared Fagel (Allette), Ted Julian
Cybersecurity Incident Response: Fight Like You Train, Train Like You Fight	6923	Technical Session	JC Vega, Allison Ritter
Best practices for managing connected security data, no matter where it resides	7107	Technical Session	Christopher Meenan
Threat Intel and Sharing in the 21st Century, or How I Bought One of Everything	1717	Technical Session	Kevin Albano, Nick Rossman, Paul Kurtz
Manage Your Use Cases in IBM QRadar	2007	Scheduled Lab	Shane Lundy, Mutaz Alsallal
IBM Resilient SOAR Integration Workshop	2906	Scheduled Lab	Shane Curtin, Roland Wolters, Gerald Trotman
Using IBM QRadar's Different Search Functions, with a Focus on Advanced Searches	6383	Scheduled Lab	Andreas Grasmück
Secure Your Home Network with the pfSense Open Source Firewall and IBM QRadar Community Edition	5653	Scheduled Lab	Luis Leopoldo Aguirre Rodriguez
Migrate Existing Security Solutions to IBM Cloud Pak for Security	4538	Scheduled Lab	Brent Peterson

QRadar WFH/Remote User Security Check Up

60 minutes with a QRadar Technical Expert to "look under the hood" to review the following:

- Security logs - determine if proper logs are being collected and analyzed
- Flows – determine the correct flows and correct locations are enabled
- Remote access security - determine if remote network access is being properly monitored
- Content – determine if applicable content packs are installed and enabled
- Tuning and Administration – Net Hierarchy, VPN ranges, 3rd party cloud, rule tuning, etc.
- User behavior monitoring - determine if and how users are being monitored
- Third party integrations - suggest integrations where applicable / App exchange

After completion, you'll receive a tune up report with next steps and suggestions to optimize your QR deployment.

Please contact craig@ibm.com to schedule the check up.

IBM **Security** a Leader for 11 consecutive years

Clear leader in ‘Completeness of Vision’

Source: Gartner (February 2020)

IBM **Security**'s SIEM market leadership

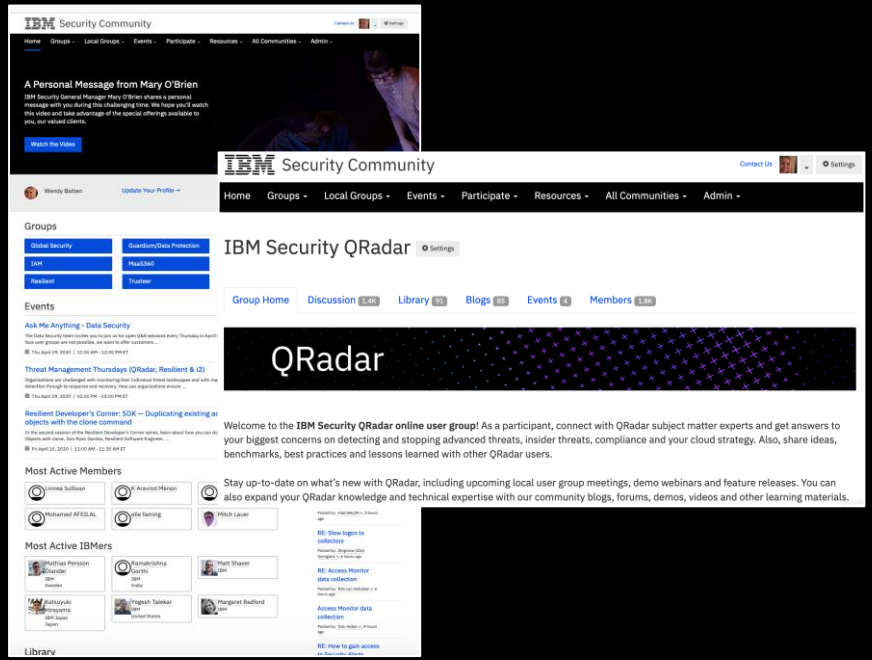
Gartner Magic Quadrant for SIEM

2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2020

Stay Connected: 2 Actions to Take

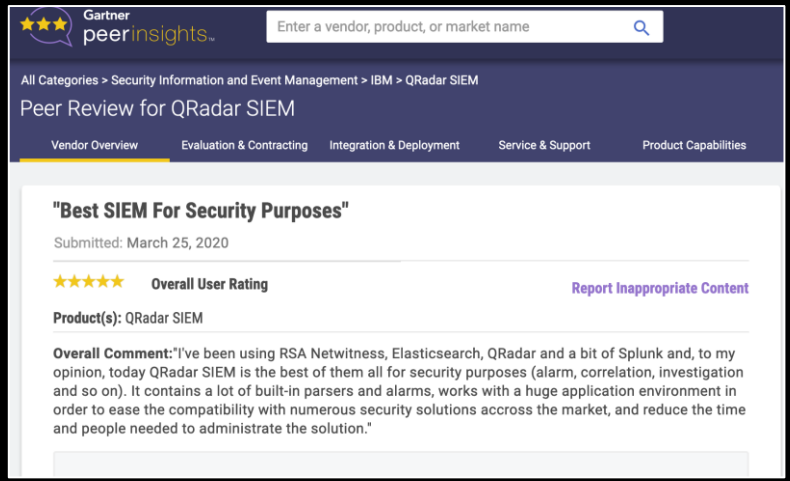
Join the IBM Security Community & the QRadar Community

Your Action: community.ibm.com/security



Share a review on Gartner Peer Insights

Your Action: Email Wendy Batten (wjbatten@us.ibm.com) for details



IBM Security QRadar Roadmap and Strategy

Sophia Sampath
QRadar Offering Manager
sophia@ca.ibm.com

Unfortunately we're unable to share the roadmap slides, as they are future-state and subject to change.

Please reach out directly to learn more about our roadmap and strategy.

Technical Support Update

Paul Mollins
L2 Support Services Manager
paul.mollins@ca.ibm.com

- 8 Years as Level 2 Support manager
- 13 years with QRadar
- 32 years industry experience mostly in the support field

Steven Crawford
Squad Lead, IBM Advanced Threat Support
stevenac@ca.ibm.com

- 3 Years as Technical lead
- Specialization in WinCollect
- 5.5 years with QRadar
- 23 years industry experience

Technical Support Update

Supporting our customer during Covid-19 Pandemic

- No support staff have been cut.
- Any data shared with support does not leave our secure environment.
  - ❑ Ecurep
  - ❑ Hursley
  - ❑ Blue Diamond
- Daily meetings to ensure everyone is able to function from home.

Technical Support Update

Escalating a case

If at any point you feel we are not meeting our commitments, call more attention to your Case:

1. Contact the Support Engineer (via a Case update, Slack, or direct phone – if provided) and clarify the business impact of your issue.

2. Raise the Severity Level of the problem using the My Support portal.
   "I am increasing the severity for my case and am requesting additional assistance. Please contact me with an update at 555-123-4567".

3. If you still need to escalate further, you can call 1-800-426-7378 and ask to speak to the Duty Manager

   What is the duty manager?
   The magic words to help with tough situations. Asking for a Duty Manager will call the phone of an IBM Support Duty Manager and they can assist with your issue. This is available to all customers 24 hours a day, 7 days a week. The Duty Manager will work with our technical staff to ensure your request is being handled appropriately.

   "I require a duty manager for case #TSxxxxxx. The duty manager can contact me at 555-123-4567.

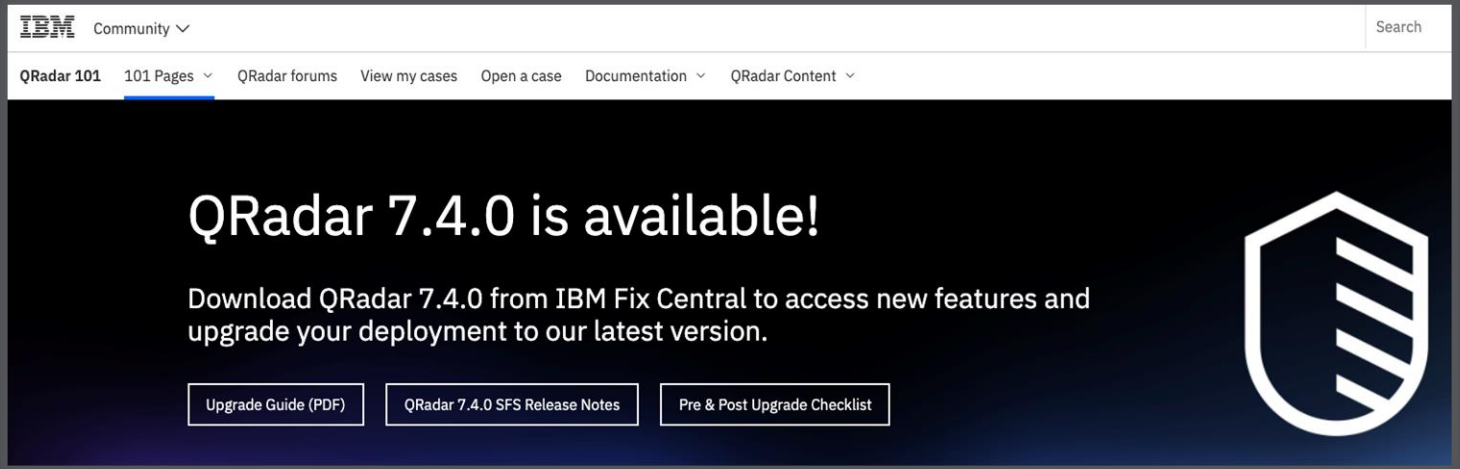
4. Escalate direct to IBM Support management contacts (During normal business hours)

Technical Support Update

QRadar 101

- QRadar 101 site contain a wealth of knowledge.
- 101 Pages:
  APAR 101
  Disk Space 101
  Support 101
  Tech Notes 101
  WinCollect 101
- QRadar Forums
- View My Cases
- Open a Case
- Documentation Links
- QRadar Content:
  IBM Support YouTube
  Learning services
  QRadar Community (user group)

  Where?
  https://www.ibm.com/community/qradar/



Technical Support Update

QRadar Support (short) URLs

- Forum quick link: http://ibm.biz/qradarforums
- Firmware quick link: http://ibm.biz/qradarfirmware
- Software quick link: http://ibm.biz/qradarsoftware
- Open/View Support Cases: http://ibm.biz/qradarsupport
- RFE quick link: http://ibm.biz/RFEQRadar
- IBM Learning Academy: http://ibm.biz/learnqradar
- Open Mic quick link: http://ibm.biz/qradaropenmic
- X-Force quick link: http://ibm.biz/qradarxforce
- Get logs information quick link: http://ibm.biz/QRadarlogs
- Lifecycle information quick link: http://ibm.biz/QRadarlifecycle
- Ask Developers App questions: http://ibm.biz/QRadarappdev
- Get QRadar Support information http://ibm.biz/qradarsupport101
- QRadar App Developer Center http://ibm.biz/QRadarsdk
- QRadar101 https://www.ibm.com/community/qradar
- IBM Support handbook
  https://www.ibm.com/support/customercare/sas/f/handbook/getsupport.html

Meeting Discussion: IBM QRadar User Behavior Analytics

Surfacing Unknown Threats

Milan Patel
Program Director, IBM Security Offering Management
milpatel@us.ibm.com

IBM Security

IBM

Agenda

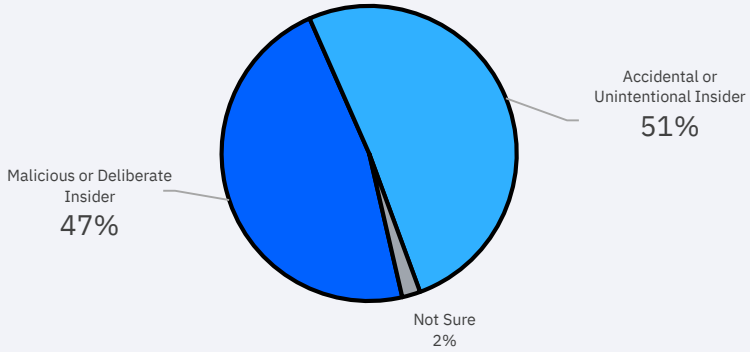
- Insider threats overview
- IBM’s approach
- User behavior use cases
- Demo

Insider threats: Threat surface and vector

Threat Facts

- Insiders are responsible for **more than 50%** of data breaches – Forrester 2017
- **74% named user intervention -** clicking a link, opening an attachment - as the top ways threats enter - SANS 2017
- **90% of Organizations** feel vulnerable to insider threat – Cybersecurity Insiders

Motivations



Types of insiders posing risk

***#1** Regular Employees*

***#2** Privileged Employees*

***#3** Contractors*

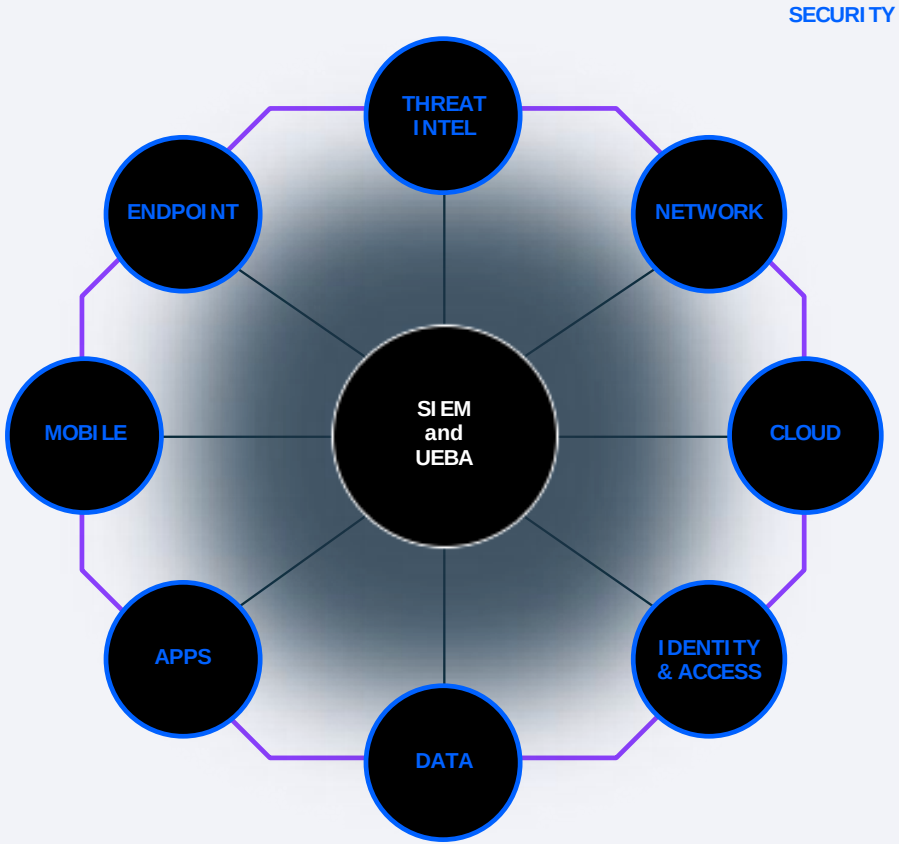
Organizational Cost

- Most **vulnerable** data: Confidential business info, privileged account information and sensitive PII
- Average cost **100.000 to 500.000** USD per successful insider attack

*Cybersecurity Insiders 2018**

Detecting insider threats requires a 360° view

Both Logs and Flows



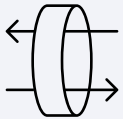
Why IBM QRadar User Behavior Analytics?

Advantages of an integrated UBA Solution

- **Complete visibility** across end point, network and cloud infrastructure with both log **and flow** data.
- **Avoids reloading and curating data** faster time to insights, lowers opex, frees valuable resources
- **Out-of-the-box analytic models** that leverage and extend the security operations platform
- **Single Security operation processes** with integration of workflow system and other security solutions ex) QRA
- **Easily extend** to third-party analytic models including existing insider threats use cases already implemented
- **Leverage UBA insights** in other integrated security analytics solutions
- **Get more from your QRadar ecosystem**

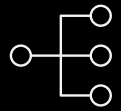
What the new normal ‘outside the perimeter’ looks like

User working from home office



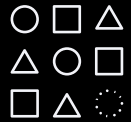
connected via corporate VPN

Data Centers



Internal Networks

Clouds



SaaS Applications

Critical Data

To the corporate estate

Online Shopping

Video Games

Streaming Services

And everything else

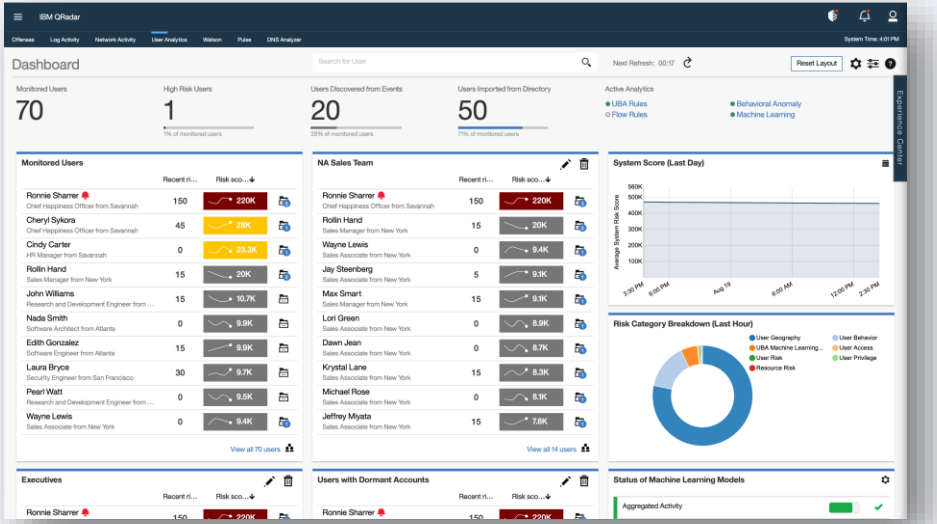
IBM QRadar User Behavior Analytics

190+ rule and ML driven use cases addressing 3 major insider threat vectors

Compromised or Stolen Credentials

Careless or Malicious Insiders

Malware takeover of user accounts



User Behavior Analytics Client Stories

Regional US Bank
Exfiltrate customer data

US Entertainment Company
Compromised credentials & exfiltration

US Healthcare Processor
Immortal user & higher expected usage of machine accounts

MSSP (50+ UBA Customers)
Unauthorized account use, account harvesting, PowerShell abuse

Large Canadian Bank & US IT Vendor
Credential sharing

Large European Bank
Malware beaconing

Detecting Compromised Credentials

70% of phishing attacks are to steal credentials
81% of breaches are with stolen credentials
$4M average cost of a data breach

	Phishing	Download	C & C	Access Privileges	Download IP	Exfiltration
Attacker Tactics & Techniques	• Phishing Emails • Suspicious Web Links	• Weaponized malware	• Outbound communication with C2 server	• Lateral Movement • Privilege Escalation • Change to access or authorization • Change in access geography or time	• Change in downloads	• Change in outbound attempts • Volume outbound transfers • DGA
UBA Use Cases	• Browsed to Malicious Website • Browsed to Phishing Website • Browsed to Scam/Illegal Website	• User Accessing Risky IP, Botnet • User Accessing Risky IP, Malware	• User Access Login Anomaly • User Geography Change • User access at Unusual Times • Account or Group or Privileges Added, Modified • User Accessing Account from Anonymous Source • Unusual Authentication Activity (ML), Access Activity (ML)		• Data Downloaded (ML) • Defined peer group (ML) • Risk Posture (ML)	• Large Outbound Transfer by High Risk User • Suspicious Access Followed by Data Exfiltration • Data Uploaded to Remote Networks (ML) • Outbound Transfer Attempts (ML) • Potential Access to DGA Domain
Data Sources	• Firewall and Web Gateways	• Threat Intel feeds	• Firewall, VPN gateways, Network • Access, Authentication logs, Jump servers, Web gateway • Windows security events • Servers, Applications, Database logs • Active Directory • Cloud		• Network switches, routers and gateways • Proxy servers • Active Directory	• Network Security • DNS

Malicious behavior comes in many forms

Scenario 1

	VPN access with coworker credentials	Abnormal login time	Abnormal file access and download	Excessive printing
Attacker Tactics & Techniques	• Using someone's VPN certificate	• Logins outside of normal hours	• Change access & authentication • Approvals and declines • Activity/frequency change • Escalation of privileges	• Larger transfer of files to print server
	Abnormal Drop in File Activity	**Abnormal drop in email activity**	**Abnormal drop in web activity**	**Visits to job search sites**
UBA Use Cases	• VPN Certificate Sharing • User Accessing Account from Anonymous Source	• User Access at Unusual Times	• Authentication Activity (ML), • Access Activity (ML) • Data Downloaded (ML) • Defined peer group (ML) • Unauthorized Access • Failed Access to Critical Assets	• UBA : Data Exfiltration by Print
	Abnormal login time	**Abnormal file access and download**	**USB device inserted**	**Write to USB**
Data Sources	• Firewall, VPN • Network switches, routers	• Access, Authentication logs • VPN Directory, Active Directory	• Access, Authentication logs, Jump servers • Windows security events • Servers, Applications, Database logs • Active Directory	• Endpoint logs • Print server logs • DLP

Maturing into User Behavioral Analytics

https://ibm.co/2TljBfX

Getting Started

- Log sources input; parsing properly
- LDAP setup; Reference Maps
- User ID Coalescing
- KYUC & Align with Biz needs
- Config and Tune UCs

Step 1

Focus on accounts and access

Step 2

Expand to USER views with network & session data

Step 3

Build and compare to PEER GROUP

Analytic Outcomes

- **Account** anomalies
- **Access** deviations

- Surface abnormal **user** behavior

- Detect users deviating from self or from peer **groups**

Data Intelligence

- LDAP, AD, Authentication Logs
- Proxy, Firewall, Web GW, VPN's, IPDS, Flow
- End point, SaaS Apps, Cloud

Tactical UBA approach (Security Expert Labs)

Everything **starts with** understanding

The QRadar environment

- QRadar performance
- QRadar health-check/QLean or QRadar Value Assessment

Available data (Maturity model for reference)

- LDAP, AD, Access and Authentication logs
- Network, Routers , Proxy, Firewall, servers, VPN, IPS
- Endpoints, Cloud, Flows, Applications, Policy

Number of offenses x Number of SOC Analysts

Understand the CISO’s priorities:

- Discuss the cyber security needs of the business and the relative priority of attack vectors

Tactical UBA approach (Security Expert Labs)

UBA Quick-start

- 3 Days, simple deploy
  - Installation
  - Identity mapping
  - Enable up to 5 rules
  - Basic threshold tuning

UBA In Depth

- Based on organization size and need
- Starts with 5 days
  - Installation
  - Identity mapping
  - Enables up to 10 default rules (can be changed based on needs)
  - Deploys up to 5 custom use-cases (can be changed based on needs)

QRadar UBA delivers value to the SOC

Analyst Effectiveness

- Detect known and unknown threats
- Reduce time to detection
- Identify activities of interest quickly

Analyst Efficiency

- Expedite investigations
- Reduce time to respond
- Reduce deep data expertise

ROI

- Get more from your investments
- Leverage existing QRadar skills
- Available at no charge

Time to Value

- Easy to acquire
- Quick to deploy and configure
- Easy to tune

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity