QRadar SIEM
health check in one day

Karl Jaeger

Pro4bizz GmbH
https://www.pro4bizz.de
karl.jaeger@pro4bizz.de
0721-909 81 722

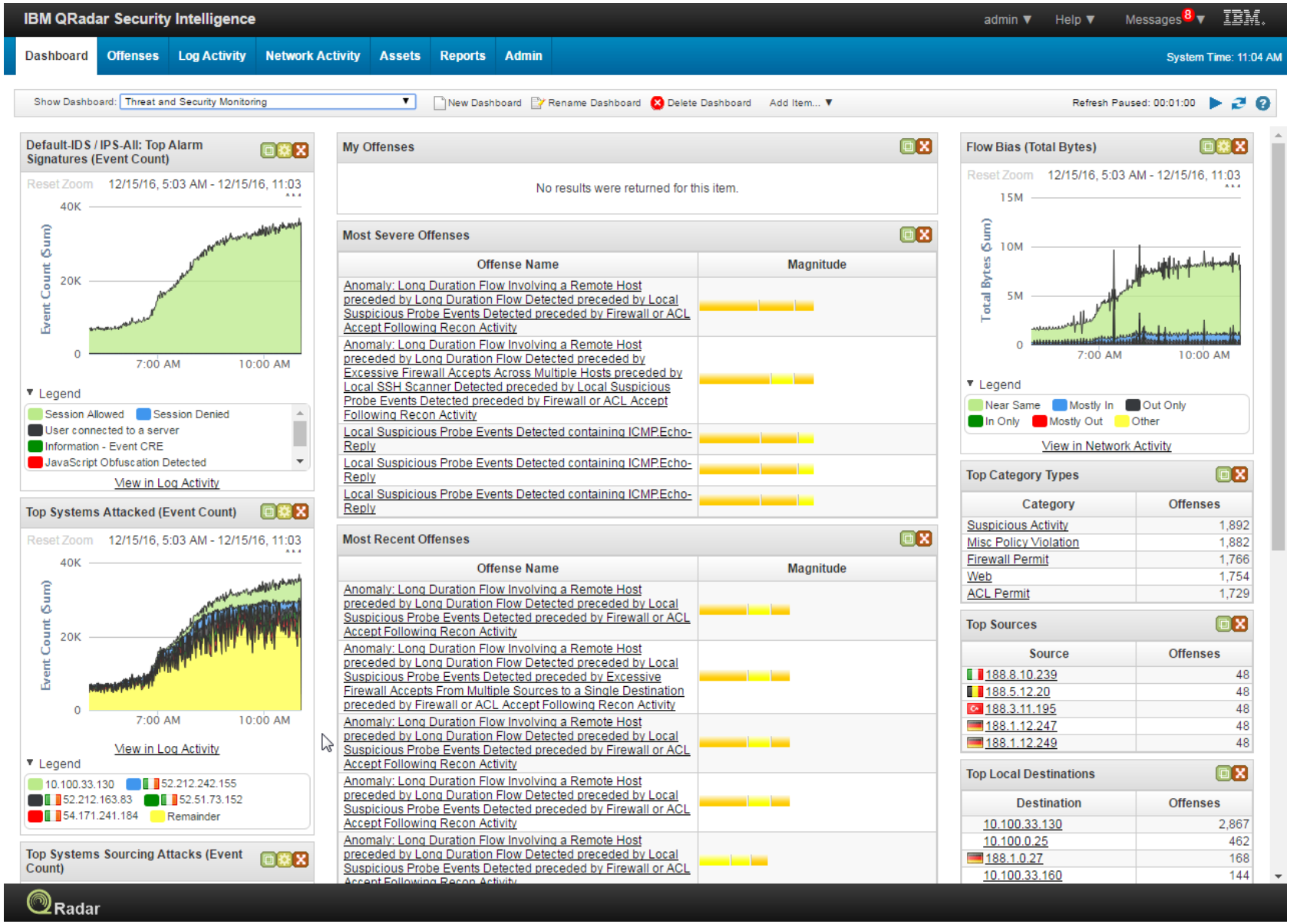
Agenda

- strukturierte Istanalyse
- Regelwerkanalyse & PKI
- Maßnahmen Finetuning
- Security Policy und Use Cases
- Projektplanung

pro4bizz
protect.your.business

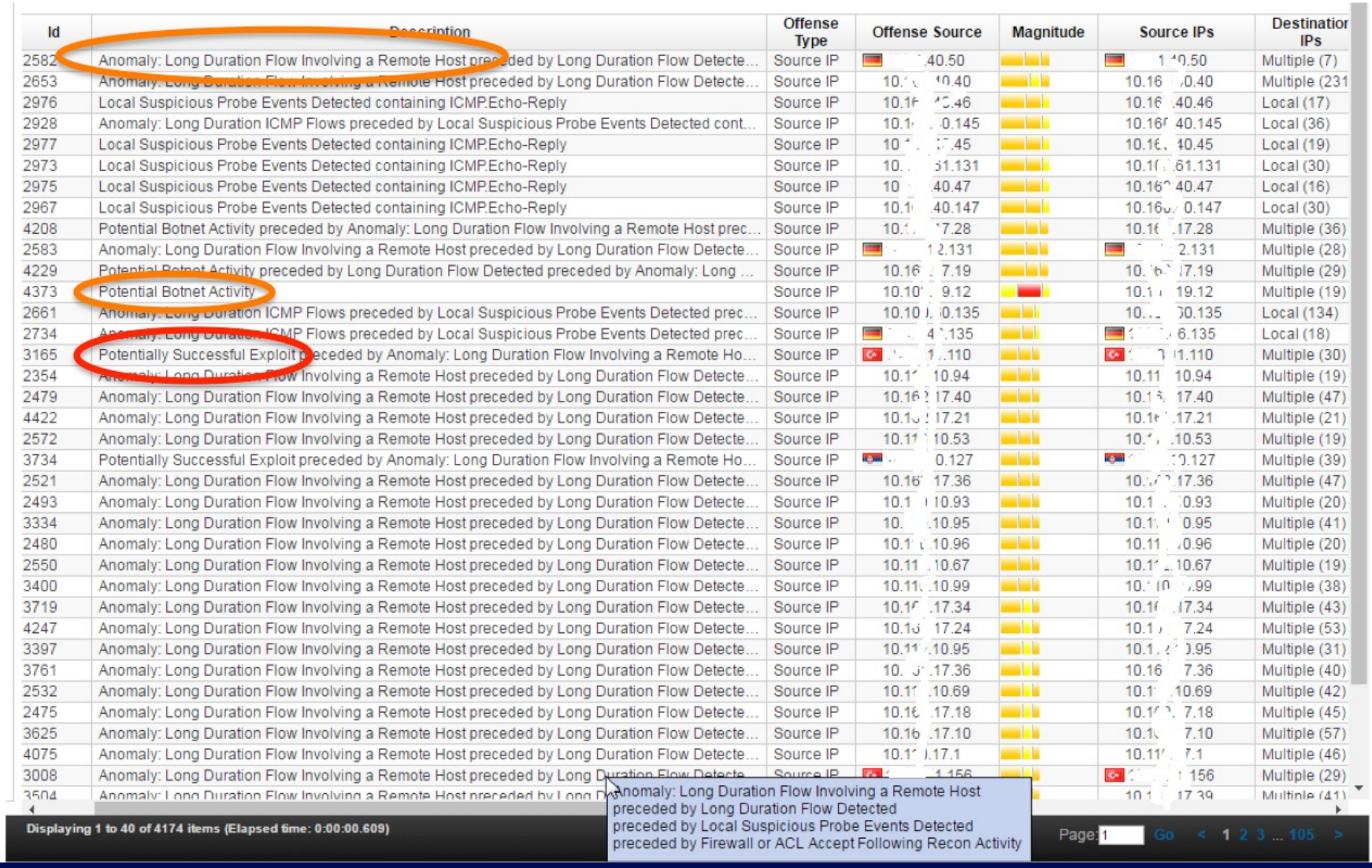
10.000 ft

structured drilldown



Sicherheitsalarm? (SI)

categories mapped, BBs triggering, rules firing



Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs
2582	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	.40.50		1 .0.50	Multiple (7)
2653	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10. .40		10.16 .0.40	Multiple (231
2976	Local Suspicious Probe Events Detected containing ICMP:Echo-Reply	Source IP	10.16 .46		10.16 .40.46	Local (17)
2928	Anomaly: Long Duration ICMP Flows preceded by Local Suspicious Probe Events Detected cont...	Source IP	10.1 .0.145		10.16 40.145	Local (36)
2977	Local Suspicious Probe Events Detected containing ICMP:Echo-Reply	Source IP	10 .45		10.16 .40.45	Local (19)
2973	Local Suspicious Probe Events Detected containing ICMP:Echo-Reply	Source IP	10. .61.131		10.1 .61.131	Local (30)
2975	Local Suspicious Probe Events Detected containing ICMP:Echo-Reply	Source IP	10 .40.47		10.16 40.47	Local (16)
2967	Local Suspicious Probe Events Detected containing ICMP:Echo-Reply	Source IP	10.1 .40.147		10.16 0.147	Local (30)
4208	Potential Botnet Activity preceded by Anomaly: Long Duration Flow Involving a Remote Host prec...	Source IP	10. .7.28		10.16 .17.28	Multiple (36)
2583	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	1 2.131		2.131	Multiple (28)
4229	Potential Botnet Activity preceded by Long Duration Flow Detected preceded by Anomaly: Long ...	Source IP	10.16 .7.19		10. .7.19	Multiple (29)
4373	Potential Botnet Activity	Source IP	10.10 .9.12		10.1 .19.12	Multiple (19)
2661	Anomaly: Long Duration ICMP Flows preceded by Local Suspicious Probe Events Detected prec...	Source IP	10.10 .0.135		10. .0.135	Local (134)
2734	Anomaly: Long Duration ICMP Flows preceded by Local Suspicious Probe Events Detected prec...	Source IP	4 .135		6.135	Local (18)
3165	Potentially Successful Exploit preceded by Anomaly: Long Duration Flow Involving a Remote Ho...	Source IP	1 .110		1.110	Multiple (30)
2354	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.1 10.94		10.11 10.94	Multiple (19)
2479	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.16 17.40		10.1 17.40	Multiple (47)
4422	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.1 17.21		10.1 .17.21	Multiple (21)
2572	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.1 10.53		10. .10.53	Multiple (19)
3734	Potentially Successful Exploit preceded by Anomaly: Long Duration Flow Involving a Remote Ho...	Source IP	0.127		.0.127	Multiple (39)
2521	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.16 17.36		10. .17.36	Multiple (47)
2493	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.1 10.93		10.1 .0.93	Multiple (20)
3334	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10. .10.95		10.1 0.95	Multiple (41)
2480	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.1 10.96		10.11 .0.96	Multiple (20)
2550	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.11 .10.67		10.1 10.67	Multiple (19)
3400	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.11 .10.99		10. 10 .99	Multiple (38)
3719	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.1 .17.34		10.16 .17.34	Multiple (43)
4247	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.1 17.24		10.1 7.24	Multiple (53)
3397	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.11 .10.95		10.1 .0.95	Multiple (31)
3761	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10. .17.36		10.16 7.36	Multiple (40)
2532	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.11 .10.69		10.1 10.69	Multiple (42)
2475	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.16 .17.18		10.1 7.18	Multiple (45)
3625	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.16 .17.10		10.1 7.10	Multiple (57)
4075	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	10.1 .17.1		10.11 7.1	Multiple (46)
3008	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Duration Flow Detecte...	Source IP	1 .156		1 156	Multiple (29)
3504	Anomaly: Long Duration Flow Involving a Remote Host preceded by Long Du...				10.1 17.39	Multiple (41)

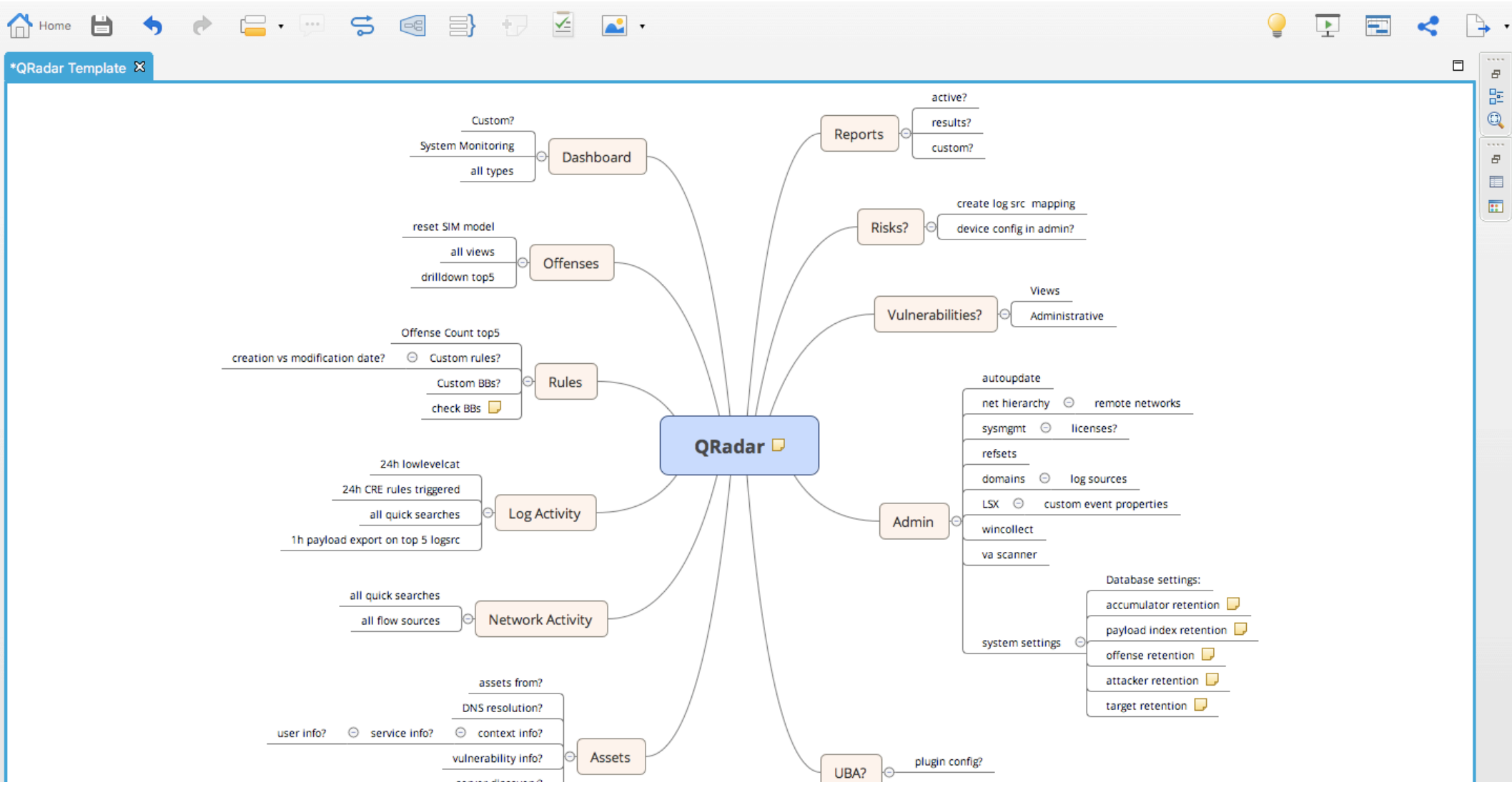
Displaying 1 to 40 of 4174 items (Elapsed time: 0:00:00.609)

Anomaly: Long Duration Flow Involving a Remote Host
preceded by Long Duration Flow Detected
preceded by Local Suspicious Probe Events Detected
preceded by Firewall or ACL Accept Following Recon Activity

Page: 1 Go < 1 2 3 ... 105 >

strukturierte Istanalyse

xmind

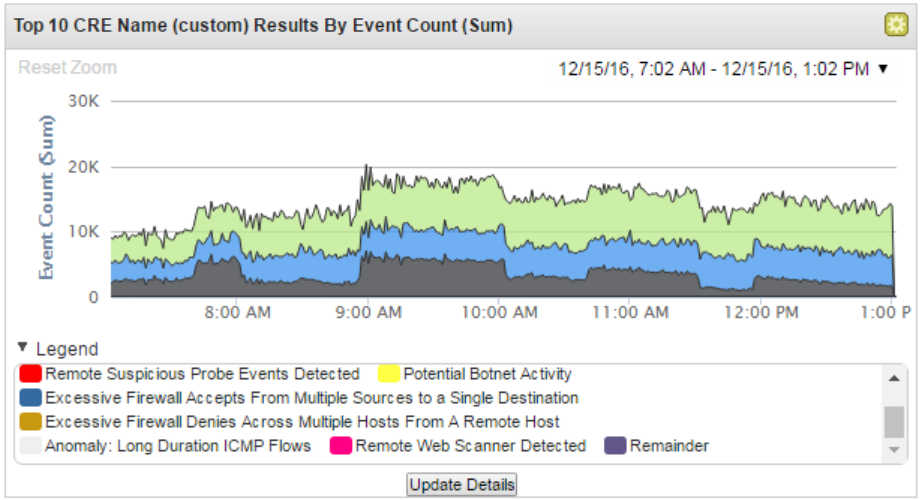


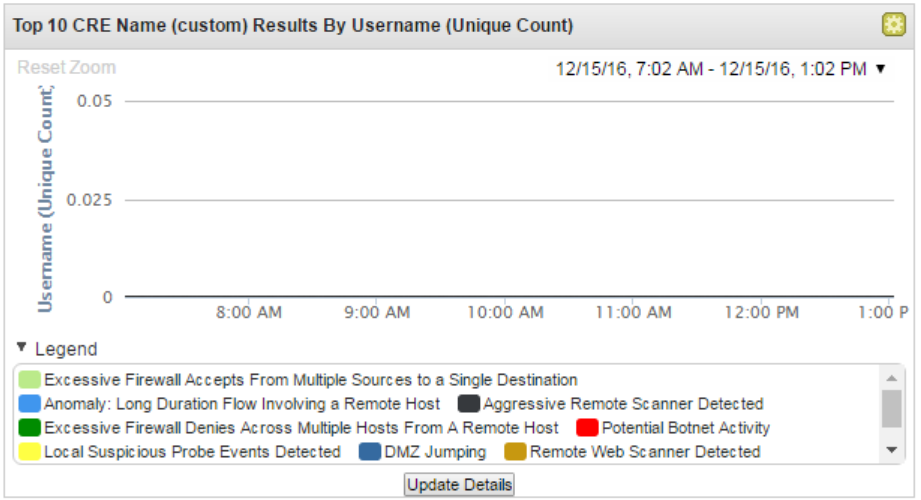
Analyse Security Incidents

Category Name	Offense Count	Local Destination Count	Source Count	Event/Flow Count
Application	[illegible]	5,491	1,995	37,950,070
Suspicious Activity	**1,893**	**129**	**1,893**	**5,740,069**
Suspicious Activity	[illegible]	127	1,893	5,740,062
Information Leak	1	2	1	7
Policy	**1,883**	**21**	**1,883**	**14,116**
Misc Policy Violation	[illegible]	21	1,883	14,116
Access	**1,785**	**4,252**	**1,759**	**103,525,089**
Firewall Permit	[illegible]	4,010	1,741	60,726,906
ACL Permit	1,730	2,404	1,704	12,153,626
Firewall Deny	1,670	250	1,670	30,642,352
ACL Deny	39	2	39	1,905
Firewall Session Opened	1	1	1	300
Recon	[illegible]	934	1,715	7,925,803
Exploit	**70**	**25**	**70**	**124**
Misc Exploit	[illegible]	25	70	120
Buffer Overflow	1	1	1	1
Format String Vulnerability	[illegible]	1	1	3
Malware	**33**	**0**	**33**	**555**
Misc Malware	[illegible]	0	33	555
System	**14**	**4**	**14**	**1,213**
Warning	10	0	10	268
Misc System Event	2	2	2	856
Successful Configuration Modification	2	2	2	4
System Status	1	0	1	1
Information	1	1	1	84
VIS Host Discovery	8	8	8	8
Asset Profiler	**5**	**0**	**5**	**5**
Asset IP Address Created	5	0	5	5
Authentication	**2**	**2**	**2**	**15**
Misc Login Succeeded	2	2	2	8
Misc Logout	2	2	2	4
Host Login Failed	1	1	1	3
SIM Audit	2	2	2	8
DOS	**2**	**2**	**2**	**7**
Brute force login	[illegible]	2	2	7
Potential Exploit	**1**	**0**	**1**	**1**
Potential Botnet Connection	[illegible]	0	1	1
Risk	**1**	**0**	**1**	**4**
Data Loss Possible	1	0	1	4

Analyse Metaevents CRE 24h

KPIs per CSV Export





(Hide Charts)

CRE Name (custom)	Event Name (Unique Count)	Low Level Category (Unique Count)	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Us (Ui Co	Magnitu (Minimui	Event Count (Sum)	Count
Local Suspicious Probe Events Detected	Multiple (2)	Host Query	Multiple (1,473)	Multiple (318)	Multiple (111)	...	5	2,346,950	2,346,950
Firewall or ACL Accept Following Recon Activity	Firewall or ACL Accept Follow...	ACL Permit	Multiple (1,403)	Multiple (574)	Multiple (61)	...	2	1,552,621	1,552,621
Anomaly: Long Duration Flow Involving a Re...	Anomaly: Long Duration Flow ...	Suspicious Activity	Multiple (1,632)	Multiple (315)	Multiple (463)	...	4	1,218,134	1,218,134
Long Duration Flow Detected	Long Duration Flow Detected	Misc Policy Violation	Multiple (1,307)	Multiple (218)	Multiple (38)	...	3	7,977	7,977
Remote Suspicious Probe Events Detected	Remote Suspicious Probe Ev...	Host Query	Multiple (4)	Multiple (316)	Multiple (4)	...	2	366	366
Potential Botnet Activity	Potential Botnet Activity	Misc Malware	Multiple (22)	Multiple (13)	53	...	7	160	160
Excessive Firewall Accepts From Multiple So...	Excessive Firewall Accepts Fr...	Firewall Permit	Multiple (106)	Multiple (16)	443	...	8	149	149
Excessive Firewall Denies Across Multiple Ho...	Excessive Firewall Denies Acr...	Network Sweep	Multiple (4)	Multiple (62)	Multiple (4)	...	6	65	65
Anomaly: Long Duration ICMP Flows	Anomaly: Long Duration ICMP...	Suspicious Activity	Multiple (15)	Multiple (13)	0	...	4	44	44
Remote Web Scanner Detected	Remote Web Scanner Detected	Web Reconnaissance	Multiple (3)	Multiple (38)	8080	...	2	38	38
DMZ Jumping	DMZ Jumping	Suspicious Activity	Multiple (5)	Multiple (7)	Multiple (12)	...	5	19	19
Excessive Firewall Accepts Across Multiple H...	Excessive Firewall Accepts Ac...	Firewall Permit	Multiple (2)	Multiple (15)	Multiple (2)	...	8	15	15
Multiple Vector Attacker Detected	Multiple Vector Attacker Detect...	Misc Exploit	Multiple (10)	Multiple (10)	Multiple (8)	...	4	10	10
Remote TCP Scanner Detected	Remote TCP Scanner Detected	TCP Reconnaissance	Multiple (2)	Multiple (6)	Multiple (2)	...	2	6	6
Local SSH Scanner Detected	Local SSH Scanner Detected	Misc Recon Event	Multiple (2)	Multiple (2)	22	...	7	2	2
Aggressive Remote Scanner Detected	Aggressive Remote Scanner ...	Network Sweep	195.2.253.2	Multiple (2)	8080	...	3	2	2
Remote Mail Scanner Detected	Remote Mail Scanner Detected	Mail Reconnaissance	91.200.14.71	185.32.244.189	25	...	2	1	1

Regelwerkanalyse

- TOP 20 Rules
- Ermittlung der KPIs
- Empfehlungen für Finetuning

Custom Rule	Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)
UBA : User Time, Access at Unusual Times	UBA : User Access at Unusual Times	Multiple (7)	Multiple (2)	0	User Time	Other	Multiple (9)
BB:HostDefinition: Local Assets	UBA : User Access at Unusual Times	Multiple (7)	Multiple (2)	0	User Time	Other	Multiple (9)
System: Load Building Blocks	UBA : User Access at Unusual Times	Multiple (7)	Multiple (2)	0	User Time	Other	Multiple (9)
BB:NetworkDefinition: Client Networks	UBA : User Access at Unusual Times	Multiple (7)	Multiple (2)	0	User Time	Other	Multiple (9)
Magnitude Adjustment: Destination Network ...	UBA : User Access at Unusual Times	Multiple (7)	Multiple (2)	0	User Time	Other	Multiple (9)
Magnitude Adjustment: Context is Local to Lo...	UBA : User Access at Unusual Times	Multiple (7)	Multiple (2)	0	User Time	Other	Multiple (9)
Magnitude Adjustment: Destination Asset Exi...	UBA : User Access at Unusual Times	Multiple (7)	Multiple (2)	0	User Time	Other	Multiple (9)
UBA : Common Event Filters	UBA : User Access at Unusual Times	Multiple (7)	Multiple (2)	0	User Time	Other	Multiple (9)
Magnitude Adjustment: Source Network Weig...	UBA : User Access at Unusual Times	Multiple (7)	Multiple (2)	0	User Time	Other	Multiple (9)
Magnitude Adjustment: Source Asset Exists	UBA : User Access at Unusual Times	Multiple (6)	Multiple (2)	0	User Time	Other	Multiple (9)
BB:CategoryDefinition: Superuser Accounts	UBA : User Access at Unusual Times	Multiple (4)	Multiple (2)	0	User Time	Other	Multiple (3)
UBA : Unusual Times, Overnight	UBA : User Access at Unusual Times	Multiple (5)	Multiple (2)	0	User Time	Other	Multiple (7)
UBA : Unusual Times, Evening	UBA : User Access at Unusual Times	Multiple (6)	10.10.100.251	0	User Time	Other	Multiple (6)
BB:CategoryDefinition: Suspicious Event Cat...	X-Force Risky IP - Dynamic	Multiple (1,616)	Multiple (1,653)	Multiple (67)	Suspicious IP Ad...	Multiple (4)	None
BB:CategoryDefinition: Suspicious Events	X-Force Risky IP - Dynamic	Multiple (1,616)	Multiple (1,653)	Multiple (67)	Suspicious IP Ad...	Multiple (4)	None
X-Force Risky IP, Dynamic	X-Force Risky IP - Dynamic	Multiple (1,616)	Multiple (1,653)	Multiple (67)	Suspicious IP Ad...	Multiple (4)	None
BB:NetworkDefinition: Client Networks	X-Force Risky IP - Dynamic	Multiple (1,615)	Multiple (1,610)	Multiple (66)	Suspicious IP Ad...	Multiple (4)	None
Magnitude Adjustment: Destination Network ...	X-Force Risky IP - Dynamic	Multiple (1,615)	Multiple (1,610)	Multiple (66)	Suspicious IP Ad...	Multiple (4)	None

Displaying 1 to 100 of 151 items (Elapsed time: 0:00:00.185)

Regelwerkanalyse

export Regelwerk als XLS (pro4bizz hack!)

	Rule Name	Tests	Enabled	Building Block	ID	Notes	Response	Create Offense	E
2	Database: Failures Followed by User Changes	when we see an event match any of the following BB:HostDefinition: Database Servers							
3	when we see at least 2 of these BB:Database: System Action Deny, in any order, with the same destination IP followed by at least 1 of these BB:Database: User Addition or Change in any order with the same IP from the previous source, within 5 minutes								
4	true false 319 Reports when there are failures followed by the addition or change of a user accoun	New Event	true						
5	Database: Concurrent Logins from Multiple Locations	the Source is Remote							
6	when we see an event match any of the following BB:HostDefinition: Database Servers								
7	when we see any of these BB:CategoryDefinition: Authentication Success with the same destination	IP more than 5 times, across more than 5 source IP(s) within 10 minutes							
8	true false 320 Reports when there are a number of authentications to a database server across ma	New Event	true						
9	Policy: Upload to Local WebServer	when we see an event match any of the following BB:CategoryDefinition: Upload to Local WebServer							
10	false false 321 Detects potential file uploads to local web servers. To change the parameters of thi	New Event	true						
11	Anomaly: Devices with High Event Rates	when any of these BB:DeviceDefinition: Devices to Monitor for High Event Rates with the same log source more than 500 times, across more than 0 destination IP within 1							
12	false false 1443 Monitors devices for high event rates. The default threshold is set very low for mc	New Event	true						
13	DDoS: DDoS Events with High Magnitude Become Offenses	when the event category for the event is one of the following DOS.Distributed DoS, DOS.Distributed High Rate DoS, DOS.Distributed High Rate ICMP DoS, DOS.Distributed							
14	when an event matches any of the following BB:CategoryDefinition: High Magnitude Events								
15	true false 1444 Rule forces offense creation for DoS based event with high magnitude."		false						
16	DDoS: DDoS Attack Detected	when any of these BB:CategoryDefinition: DDoS Attack Events with the same QID more than 3 times, across exactly 1 destination IP within 5 minutes							
17	true false 1445 Reports network Denial of Service (DoS) attacks on a system. "	New Event	true						
18	Malware: Treat Key Loggers as Offenses	when an event matches any of the following BB:CategoryDefinition: Key Loggers							
19	false false 100001 Enable this rule if you wish all events categorized as key loggers to create offenses."		false						
20	BB:CategoryDefinition: VPN Access Denied	when an event matches any of the following BB:CategoryDefinition: Authentication Failures, BB:CategoryDefinition: Authentication to Disabled Account, BB:CategoryDefin							
21	when an event matches any of the following BB:DeviceDefinition: VPN								
22	true true 100010 This rule identifies VPN events that are considered denied access."		false						
23	BB:CategoryDefinition: VPN Access Accepted	when an event matches any of the following BB:CategoryDefinition: Authentication Success							
24	when an event matches any of the following BB:DeviceDefinition: VPN								
25	true true 100019 This rule identifies VPN events that show permitted access."		false						
26	BB:CategoryDefinition: Database Access Denied	when an event matches any of the following BB:CategoryDefinition: Authentication Failures, BB:CategoryDefinition: Authentication to Disabled Account, BB:CategoryDefin							
27	when an event matches any of the following BB:DeviceDefinition: Database								
28	true true 100020 This rule identifies Database events that are considered denied access."		false						
29	BB:CategoryDefinition: Database Access Permited	when an event matches any of the following BB:CategoryDefinition: Authentication Success							
30	when an event matches any of the following BB:DeviceDefinition: Database								
31	true true 100021 This rule identifies Database events that show permitted access."		false						
32	BB:BehaviorDefinition: Post Compromise Activities	when an event matches any of the following BB:CategoryDefinition: Authentication User or Group Added or Changed, BB:ReconDetected: All Recon Rules, Anomaly: Poten							
33	true true 100022 Edit this BB to include categories that are considered the be part of events seen after typical compromises."		false						
34	SuspiciousActivity: Consumer Grade Equipment	when an event matches any of the following BB:DeviceDefinition: Consumer Grade Routers, BB:DeviceDefinition: Consumer Grade Wireless APs							
35	false false 100038 This rule will identify assets that appear to be consumer grade equipment."	New Event	false						
36	SuspiciousActivity: Communication with Known Watched Networks	when an event matches any of the following BB:NetworkDefinition: Watch List Addresses, BB:NetworkDefinition: Darknet Addresses							
37	false false 1453 This rule will identify events that are involved with networks that are defined as ne	New Event	false						
38	SuspiciousActivity: Communication with Known Online Services	when an event matches any of the following BB:NetworkDefinition: DLP Addresses							
39	false false 1454 This rule will identify events that are involved with networks that are defined as pc	New Event	false						
40	System: Host Based Failures	when an event matches any of the following BB:CategoryDefinition: Failure Service or Hardware							
41	false false 100044 This rule fires when the system sees events that indicate failures within services or hardware."		false						
42	System: Critical System Events	when an event matches any of the following BB:HostBased: Critical Events							

Blatt1

Maßnahmenkatalog erarbeiten

M1: disable superfluos anomaly or recon rules (offense tab -> Rules)

M2: disable offense action / metaevent response only

M3: modify database settings (admin tab -> system settings -> accumulator retention)

M4: create refset for false pos tuning, fill via payload export values or manually

M5: drop events creating false alarms if custom property is (not) in refset

M6: create category for false pos tuning via qidmap, create BB to establish category

M7: use offense index object for events to be tuned, use (not) N/A in rule for test

M8: create custom property for events to be tuned, use (not) N/A in BB or rule for test

M9: enable index on custom property missed (admin tab -> index management)

Regelwerk Finetuning

Beispiel: geplante Maßnahmen aus Istanalyse

rule	count	M
Policy: Remote: Long Duration Flow Detected	1884	set host/network exception in rule
Anomaly: Long Duration Flow Involving a Remote Host	1858	disable offense in rule / CRE event only
Recon: Recon Followed by Accept	1704	disable offense in rule / CRE event only
Recon: Local L2L Suspicious Probe Events Detected	1581	disable offense in rule / CRE event only
Recon: Local L2R Suspicious Probe Events Detected	91	disable offense in rule / CRE event only
Anomaly: Long Duration ICMP Flows	72	disable offense in rule / CRE event only
Exploit: All Exploits Become Offenses	70	ok
Exploit: Multiple Vector Attack Source	68	set host/network exception in BBs
Anomaly: Excessive Firewall Denies from Single Source	38	set host/network exception in BBs
Botnet: Potential Botnet Connection (DNS)	33	set NOT my DNS / remove BB FW Accept / change offense category / disable offense in rule / C
Anomaly: Excessive Firewall Accepts From Multiple Sources to a Single Destination	26	set host/network exception in rule / disable offense in rule / CRE event only
Exploit: Attack followed by Attack Response	12	check BBs for false alarms, e.g. system users, technical accounts
Anomaly: DMZ Jumping	11	rule modified: check BB:HostDefinition: Network Management Servers
Recon: Local L2L ICMP Scanner	9	disable offense in rule / CRE event only
Anomaly: Excessive Firewall Accepts Across Multiple Hosts	6	disable offense in rule / CRE event only
Exploit: Exploits Followed by Firewall Accepts	5	check BBs for false alarms, e.g. system users, technical accounts
Exploit: Exploits Events with High Magnitude Become Offenses	2	ok
Anomaly: Systems using many different protocols	1	check souce ip / set host/network exception in rule / disable offense in rule / CRE event only

Beispiel Finetuning

Maßnahme: identifiziere BB und nutze Refset für Ausnahmen (white list)

Exploit: Multiple Vector Attack Source	when at least 4 BB:BehaviorDefinition: Compromise Activities, BB:CategoryDefinition: Authentication Failures, BB:CategoryDefinition: Authentication to Disabled Account, BB:CategoryDefinition: Authentication to Expired Account, BB:CategoryDefinition: Countries/Regions with no Remote Access, BB:CategoryDefinition: DDoS Attack, BB:CategoryDefinition: Exploits Backdoors and Trojans, BB:CategoryDefinition: Firewall or ACL Denies, BB:CategoryDefinition: Key Loggers, BB:CategoryDefinition: Mail Policy Violation, BB:CategoryDefinition: Malware Annoyances, BB:CategoryDefinition: Network DoS Attack, BB:CategoryDefinition: Service DoS, BB:CategoryDefinition: Recon Events, BB:CategoryDefinition: Virus Detected, BB:CategoryDefinition: Worm Events, BB:CategoryDefinition: Database Access Denied, BB:Database: System Action Deny, BB:NetworkDefinition: Darknet Addresses, BB:NetworkDefinition: Honeypot like Addresses, BB:NetworkDefinition: Undefined IP Space, BB:NetworkDefinition: Watch list Addresses, BB:PortDefinition: Unauthorized L2R Ports, in any order, from the same source IP to any destination IP, over 1 days	
false false 100051 This rule detects when an source host tries multiple attack vectors	this may indicate the source host is specifically targeting an asset."	New Event

Metaevents (CRE 1h)

CSV Analysedaten unterstützen Finetuning

Custom Rule	Source IP (Unique	Destination IP (Unic	Destination Port (U	Low Level Categor	Event Name (Un	Log Source (Unique Count)	Protocol (Uniqu	Usernar	Event Coun	Count
System: Load Building Blocks	Multiple (1,542)	Multiple (1,045)	Multiple (108)	Multiple (14)	Multiple (19)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	844,989	844,989
Magnitude Adjustment: Source Network Weight is Low	Multiple (1,542)	Multiple (1,045)	Multiple (108)	Multiple (14)	Multiple (19)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	844,989	844,989
BB:CategoryDefinition: Regular Office Hours	Multiple (1,542)	Multiple (1,045)	Multiple (108)	Multiple (14)	Multiple (19)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	844,989	844,989
Magnitude Adjustment: Destination Network Weight is Low	Multiple (1,542)	Multiple (1,045)	Multiple (108)	Multiple (14)	Multiple (19)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	844,989	844,989
BB:PortDefinition: Web Ports	Multiple (1,462)	Multiple (163)	Multiple (3)	Multiple (7)	Multiple (9)	Custom Rule Engine-8 :: UX00-000-120	tcp_ip	None	829,875	829,875
BB:NetworkDefinition: Client Networks	Multiple (1,531)	Multiple (990)	Multiple (93)	Multiple (13)	Multiple (16)	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	823,098	823,098
Compliance:Load ISO 27001 Building Blocks	Multiple (1,509)	Multiple (275)	Multiple (65)	Multiple (9)	Multiple (12)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	821,198	821,198
BB:Local To Remote	Multiple (1,504)	Multiple (193)	Multiple (64)	Multiple (6)	Multiple (7)	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	820,506	820,506
Magnitude Adjustment: Context is Local to Remote	Multiple (1,504)	Multiple (193)	Multiple (64)	Multiple (6)	Multiple (7)	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	820,506	820,506
Magnitude Adjustment: Source Asset Exists	Multiple (1,423)	Multiple (387)	Multiple (93)	Multiple (7)	Multiple (10)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	815,37	815,37
Recon: Local L2R Suspicious Probe Events Detected	Multiple (1,417)	Multiple (132)	Multiple (17)	Multiple (6)	Multiple (6)	Custom Rule Engine-8 :: UX00-000-120	Multiple (2)	None	814,36	814,36
BB:PortDefinition: Authorized L2R Ports	Multiple (1,500)	Multiple (253)	Multiple (6)	Multiple (8)	Multiple (11)	Custom Rule Engine-8 :: UX00-000-120	Multiple (2)	None	812,485	812,485
BB:CategoryDefinition: Countries/Regions with no Remote Access	Multiple (1,053)	Multiple (856)	Multiple (91)	Multiple (11)	Multiple (15)	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	580,315	580,315
BB:BehaviorDefinition: Post Compromise Activities	Multiple (1,463)	Multiple (793)	Multiple (33)	Multiple (11)	Multiple (15)	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	485,306	485,306
BB:ReconDetected: All Recon Rules	Multiple (1,447)	Multiple (784)	Multiple (33)	Multiple (9)	Multiple (13)	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	485,277	485,277
BB:CategoryDefinition: Recon Events	Multiple (1,439)	Multiple (810)	Multiple (32)	Multiple (8)	Multiple (11)	Custom Rule Engine-8 :: UX00-000-120	Multiple (2)	None	425,735	425,735
BB:CategoryDefinition: Recon Event Categories	Multiple (1,439)	Multiple (810)	Multiple (32)	Multiple (8)	Multiple (11)	Custom Rule Engine-8 :: UX00-000-120	Multiple (2)	None	425,735	425,735
BB:CategoryDefinition: Firewall or ACL Accept	Multiple (1,426)	Multiple (323)	Multiple (40)	Multiple (2)	Multiple (2)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	286,374	286,374
Recon: Recon Followed by Accept	Multiple (1,426)	Multiple (323)	Multiple (40)	Multiple (2)	Multiple (2)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	286,373	286,373
Anomaly: Excessive Firewall Accepts From Multiple Sources to a Single Destinatio	Multiple (1,413)	Multiple (18)	443	Multiple (2)	Multiple (2)	Custom Rule Engine-8 :: UX00-000-120	tcp_ip	None	255,06	255,06
BB:CategoryDefinition: Suspicious Events	Multiple (1,460)	Multiple (139)	Multiple (62)	Suspicious Activity	Multiple (3)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	131,506	131,506
BB:CategoryDefinition: Suspicious Event Categories	Multiple (1,460)	Multiple (139)	Multiple (62)	Suspicious Activity	Multiple (3)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	131,506	131,506
Anomaly: Long Duration Flow Involving a Remote Host	Multiple (1,454)	Multiple (132)	Multiple (60)	Suspicious Activity	Anomaly: Long D	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	131,497	131,497
Magnitude Adjustment: Context is Local to Local	Multiple (814)	Multiple (199)	Multiple (42)	Multiple (4)	Multiple (5)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	23,383	23,383
BB:NetworkDefinition: DMZ Addresses	Multiple (815)	Multiple (66)	Multiple (28)	Multiple (6)	Multiple (8)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	21,891	21,891
BB:NetworkDefinition: Server Networks	Multiple (815)	Multiple (66)	Multiple (28)	Multiple (6)	Multiple (8)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	21,891	21,891
BB:CategoryDefinition: Post DMZ Jump	Multiple (810)	Multiple (60)	Multiple (26)	Multiple (4)	Multiple (5)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	21,703	21,703
BB:NetworkDefinition: Darknet Addresses	Multiple (85)	Multiple (43)	Multiple (59)	Multiple (5)	Multiple (7)	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	9,196	9,196
BB:NetworkDefinition: Honeypot like Addresses	Multiple (83)	Multiple (40)	Multiple (58)	Multiple (5)	Multiple (7)	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	9,133	9,133
Exploit: Multiple Vector Attack Source	Multiple (9)	Multiple (88)	Multiple (7)	Multiple (8)	Multiple (9)	Custom Rule Engine-8 :: UX00-000-120	Multiple (2)	None	2,961	2,961
BB:ProtocolDefinition: Windows Protocols	Multiple (71)	Multiple (460)	Multiple (15)	Multiple (7)	Multiple (12)	Custom Rule Engine-8 :: UX00-000-120	Multiple (2)	None	2,202	2,202
Magnitude Adjustment: Destination Asset Exists	Multiple (19)	Multiple (180)	Multiple (36)	Multiple (4)	Multiple (5)	Custom Rule Engine-8 :: UX00-000-120	Multiple (4)	None	1,969	1,969
BB:HostDefinition: Servers	Multiple (20)	Multiple (170)	Multiple (20)	Multiple (3)	Multiple (3)	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	1,544	1,544
BB:CategoryDefinition: Policy Events	Multiple (1,395)	Multiple (74)	Multiple (14)	Misc Policy Violati	Long Duration Fl	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	1,395	1,395
Policy: Remote: Long Duration Flow Detected	Multiple (1,395)	Multiple (74)	Multiple (14)	Misc Policy Violati	Long Duration Fl	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	1,395	1,395
Compliance:Load GPG13 Building Blocks	Multiple (61)	Multiple (126)	Multiple (6)	Multiple (8)	Multiple (10)	Custom Rule Engine-8 :: UX00-000-120	Multiple (3)	None	963	963
BB:NetworkServices	Multiple (60)	Multiple (126)	Multiple (5)	Multiple (7)	Multiple (9)	Custom Rule Engine-8 :: UX00-000-120	Multiple (2)	None	961	961
BB:HostDefinition: Host with Port Open	Multiple (12)	Multiple (124)	Multiple (23)	Multiple (3)	Multiple (3)	Custom Rule Engine-8 :: UX00-000-120	Multiple (2)	None	945	945
Magnitude Adjustment: Destination Asset Port is Open	Multiple (12)	Multiple (124)	Multiple (23)	Multiple (3)	Multiple (3)	Custom Rule Engine-8 :: UX00-000-120	Multiple (2)	None	945	945
Recon: Remote Suspicious Probe Events Detected: NOWEDA	Multiple (26)	Multiple (620)	Multiple (18)	Multiple (3)	Multiple (3)	Custom Rule Engine-8 :: UX00-000-120	Multiple (2)	None	930	930
BB:PortDefinition: DNS Ports	Multiple (43)	Multiple (45)	53	Multiple (5)	Multiple (6)	Custom Rule Engine-8 :: UX00-000-120	Multiple (2)	None	881	881

Abbildung Infrastruktur

False Positive BBs / Category Definitions / Host Definitions / Network Definitions

Rule Name ▲	Group	Rule Category	Rule Type	Event/Flo...	Offense Coun	Origin
BB:FalsePositive: All Default False Positive BBs	False...	Custom Rule	Common	0	0	Modified

Rule Name ▲	Group	Rule Category	Rule Type	Event/Flow Count	Offense Count	Origin
BB:BehaviorDefinition: Compromise Activities	Catego...	Custom Rule	Event	0	0	System
BB:CategoryDefinition: Exploits Backdoors and Trojans	Catego...	Custom Rule	Event	0	0	System
BB:CategoryDefinition: Policy Events	Catego...	Custom Rule	Event	0	0	System
BB:CategoryDefinition: Post Exploit Account Activity	Catego...	Custom Rule	Event	0	0	System
BB:CategoryDefinition: Privileged Activity : UBA		Custom Rule	Event	0	0	System
BB:CategoryDefinition: Recon Event Categories	Catego...	Custom Rule	Event	0	0	System
BB:CategoryDefinition: Recon Events	Catego...	Custom Rule	Common	0	0	System
BB:CategoryDefinition: Recon Flows	Catego...	Custom Rule	Flow	0	0	System
BB:CategoryDefinition: Suspicious Event Categories	Catego...	Custom Rule	Event	0	0	System
BB:CategoryDefinition: Suspicious Events	Catego...	Custom Rule	Common	0	0	System
BB:CategoryDefinition: Suspicious Flows	Catego...	Custom Rule	Flow	0	0	System

Rule

Apply BB:CategoryDefinition: Suspicious Event Categories on events which are detected by the Local system
and when the event category for the event is one of the following Suspicious Activity, Potential Exploit, Access.ACL Deny, Access.Firewall Deny, Access.IPS Deny, Access.No Translation Gro
Flow.High number of Empty Packet Flows, Flow.High number of Unidirectional Flows, Flow.High number of Unidirectional ICMP Flows, Flow.High number of Unidirectional TCP Flows, Flow
Flow.Low number of Unidirectional Flows, Flow.Low number of Unidirectional ICMP Flows, Flow.Low number of Unidirectional TCP Flows, Flow.Medium number of Empty Packet Flows, Fl
Flows, Flow.Medium number of Unidirectional ICMP Flows, Flow.Medium number of Unidirectional TCP Flows, Flow.Suspicious Flow, Flow.Suspicious ICMP Flow, Flow.Suspicious TCP Fl
Flow.Unidirectional Flow, Flow.Unidirectional ICMP Flow, Flow.Unidirectional TCP Flow, Authentication.Admin Login Failure, Authentication.Auth Server Login Failed, Authentication.FTP Log
Authentication Failed, Authentication.Host Login Failed, Authentication.Login with username/password defaults failed, Authentication.Mail Service Login Failed, Authentication.Misc Login F
Escalation Failed, Authentication.Remote Access Login Failed, Authentication.Samba Login Failed, Authentication.SSH Login Failed, Authentication.Suspicious Password, Authentication.
Authentication.Telnet Login Failed, Authentication.Web Service Login Failed

Notes

Edit this BB to include all events that indicate suspicious activity.

asset DB

um Kontextinformation ergänzen / Infrastruktur aufnehmen

IBM Security QRadar SIEM

admin ▼ Prefere

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Vulnerabilities | Admin

Assets

Asset Profiles

Server Discovery

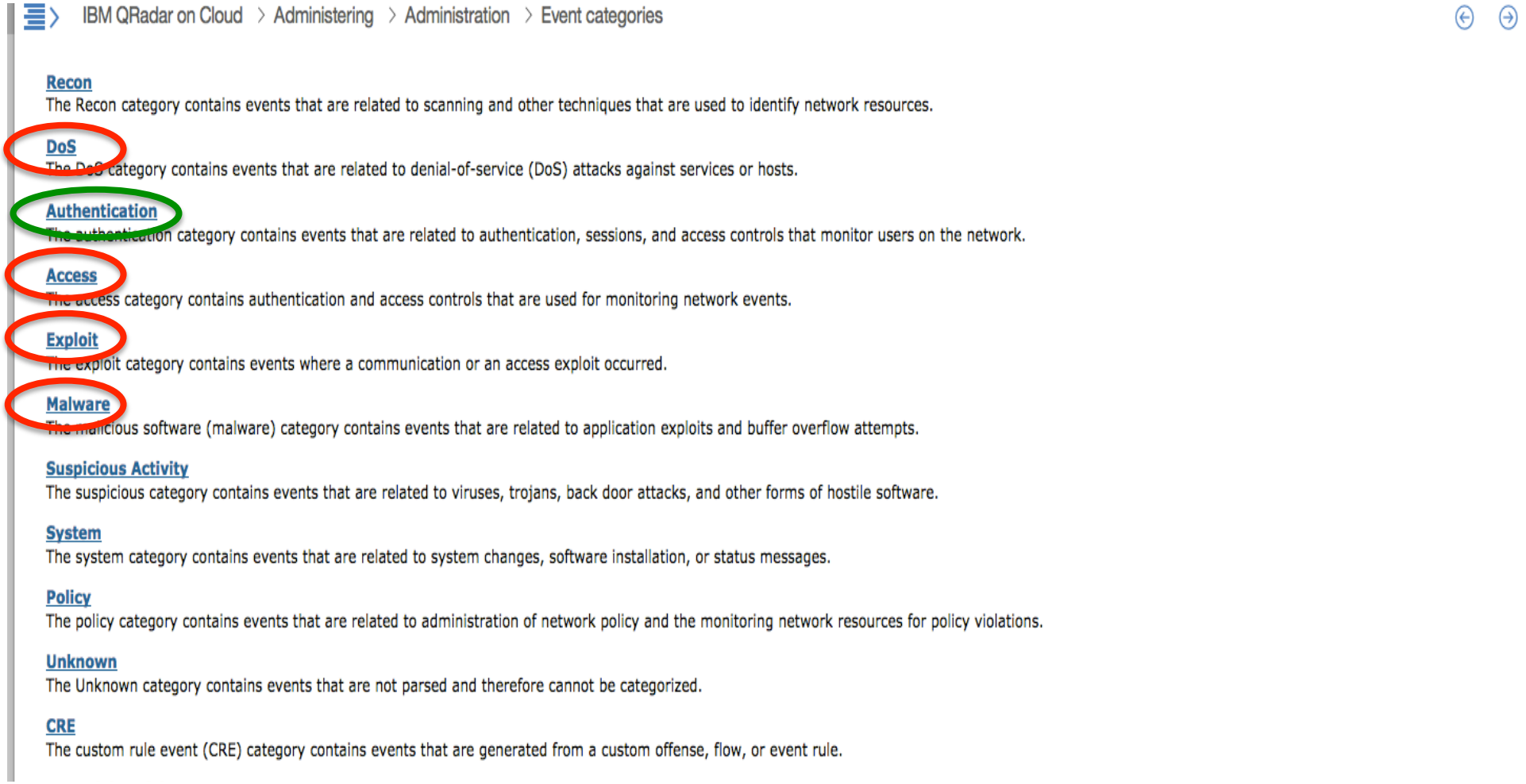
VA Scan

Search ▼ Quick Searches ▼ Save Criteria Add Filter Add Asset Edit Asset Actions ▼

Assets

Id	IP Address	Asset Name	Risk Score	Vulnerabil	Services	Last User	
1073	10.10.1.1	10.10.1.1	0.0	0	1		
1020	10.10.1.10	10.10.1.10	24.3	5	4		
1045	10.10.1.109	10.10.1.109	16.4	4	4		
1017	10.10.1.110	10.10.1.110	6.4	1	4		
1018	10.10.1.111	WIN2008MGMT	8.5	5	10	Administrator	2014-01-06 12:03:45.068
1021	10.10.1.117	DC1	31.2	11	12		
1023	10.10.1.12	10.10.1.12	35.1	9	9		
1085	10.10.1.120	PDC	52.1	15	28		
1003	10.10.1.121	SQL-SERVER	23.4	7	14		
1041	10.10.1.126	AD	35.5	11	21		
1008	10.10.1.127	TESTXP	16.5	4	7	Administrator	2014-01-08 11:47:07.955
1046	10.10.1.14	10.10.1.14	94.8	23	1		
1087	10.10.1.146	10.10.1.146	0.0	0	0		
1002	10.10.1.148	ISS2	34.6	9	17	ANONYMOUS LOGON	2013-09-23 13:22:18.227
1001	10.10.1.149	10.10.1.149	0.0	0	0		

Security Policy und Use Cases



IBM QRadar on Cloud > Administering > Administration > Event categories

Recon
The Recon category contains events that are related to scanning and other techniques that are used to identify network resources.

DoS
The DoS category contains events that are related to denial-of-service (DoS) attacks against services or hosts.

Authentication
The authentication category contains events that are related to authentication, sessions, and access controls that monitor users on the network.

Access
The access category contains authentication and access controls that are used for monitoring network events.

Exploit
The exploit category contains events where a communication or an access exploit occurred.

Malware
The malicious software (malware) category contains events that are related to application exploits and buffer overflow attempts.

Suspicious Activity
The suspicious category contains events that are related to viruses, trojans, back door attacks, and other forms of hostile software.

System
The system category contains events that are related to system changes, software installation, or status messages.

Policy
The policy category contains events that are related to administration of network policy and the monitoring network resources for policy violations.

Unknown
The Unknown category contains events that are not parsed and therefore cannot be categorized.

CRE
The custom rule event (CRE) category contains events that are generated from a custom offense, flow, or event rule.

Beispiel: Use Case IAM

IBM QRadar on Cloud > Administering > Administration > Event categories > Authentication

Authentication

Version IBM QRadar on Cloud

The authentication category contains events that are related to authentication, sessions, and access controls that monitor users on the network.

The following table describes the low-level event categories and associated severity levels for the authentication category.

Table 1. Low-level categories and severity levels for the authentication events category

Low-level event category	Description	Severity level (0 - 10)
Unknown Authentication	Indicates unknown authentication.	1
Host Login Succeeded	Indicates a successful host login.	1
Host Login Failed	Indicates that the host login failed.	3
Misc Login Succeeded	Indicates that the login sequence succeeded.	1
Misc Login Failed	Indicates that login sequence failed.	3
Privilege Escalation Failed	Indicates that the privileged escalation failed.	3
Privilege Escalation Succeeded	Indicates that the privilege escalation succeeded.	1
Mail Service Login Succeeded	Indicates that the mail service login succeeded.	1
Mail Service Login Failed	Indicates that the mail service login failed.	3
Auth Server Login Failed	Indicates that the authentication server login failed.	3
Auth Server Login Succeeded	Indicates that the authentication server login succeeded.	1
Web Service Login Succeeded	Indicates that the web service login succeeded.	1

Finetuning mit Reference Sets

watchlists / black lists / white lists

Name	Type	Number of Elements	Associated Rules
Asset Reconciliation IPv4 Blacklist	IP	2	3
Asset Reconciliation MAC Blacklist	AlphaNumeric (Ignore Case)	1	3
Asset Reconciliation NetBIOS Blacklist	AlphaNumeric (Ignore Case)	1	3
Asset Reconciliation MAC Whitelist	AlphaNumeric (Ignore Case)	0	0
Asset Reconciliation DNS Blacklist	AlphaNumeric (Ignore Case)	0	3
External Contractor	AlphaNumeric	0	0
Mobile Worker	AlphaNumeric	0	0
Teleworker	AlphaNumeric	0	0
HR Data	AlphaNumeric	0	0
Financial Data	AlphaNumeric	0	0
General Data	AlphaNumeric	0	0
Sensitive Data	AlphaNumeric	0	0
User Sensitive Data	AlphaNumeric	0	0
Proprietary Data	AlphaNumeric	0	0
Publicly Published Data	AlphaNumeric	0	0
IT Admins	AlphaNumeric	0	0
System Test Data	AlphaNumeric	0	0
Source Code	AlphaNumeric	0	0
Asset Reconciliation IPv4 Whitelist	IP	0	0
Audit Tools	AlphaNumeric	0	0
Asset Reconciliation NetBIOS Whitelist	AlphaNumeric (Ignore Case)	0	0
Asset Reconciliation DNS Whitelist	AlphaNumeric (Ignore Case)	0	0

Network Security Policy – Applications used

Category Name	Offense Count ▼	Local Destination Count	Source Count	Event/Flow Count
Application	**1,995**	**5,491**	**1,995**	**37,950,070**
Web	1,755	1,536	1,755	36,401,828
Misc	1,189	139	1,189	708,451
[illegible]	124	3,291	124	314,544
Remote Access	68	1,052	68	147,998
[illegible]	40	56	40	7,114
Inner System	28	53	28	27,333
Mail	24	6	24	10,929
Data Warehousing	23	78	23	176,299
File Transfer	12	10	12	2,446
Mail Opened	6	6	6	1,238
Network Management	5	12	5	89
Chat	3	7	3	62
Authentication (Appl...	2	7	2	56
[illegible]	2	7	2	43
P2P	2	9	2	92
[illegible]	2	2	2	609
Security Protocol	1	1	1	1
Streaming	1	6	1	22
Mail Denied	1	1	1	7,550
Mail In Progress	1	1	1	143,361
HTTP In Progress	1	0	1	2
VPN Closed	1	0	1	1
Web In Progress	1	2	1	2
▶ Suspicious Activity	1,893	129	1,893	5,740,069
▶ Policy	1,883	21	1,883	14,116
▶ Access	1,785	4,252	1,759	103,525,089
▶ Recon	1,715	934	1,715	7,925,803
▶ Exploit	70	25	70	124
▶ Malware	33	0	33	555
▶ System	14	4	14	1,213
▶ VIS Host Discovery	8	8	8	8
▶ Asset Profiler	5	0	5	5
▶ Authentication	2	2	2	15
▶ SIM Audit	2	2	2	8
▶ DOS	2	2	2	7
▶ Potential Exploit	1	0	1	1
▶ Risk	1	0	1	4

Projektplanung

- QRadar Health Check (one day)
- Maßnahmenkatalog erarbeiten (free)
- Präsentation der Ergebnisse (free)

- Regelwerk anpassen – Finetuning aktive Regeln
- False Positive BBs überprüfen
- Database Setup anpassen
- Asset DB checkup
- Host und Network Definitions
- Custom Dashboard
- Quick Searches und Timelines
- Reports
- Security Policy Use Cases
- Workflow Integration
- Trouble Shooting
- Release Upgrade