

When you are Cybersafe We are **Cyberhappy**

Copyright © NSC42 Ltd 2019



Protect our clients against modern threats leaving them able to fend by themselves

To make the digital world safer by securing one digital company at a time.

To deliver to you world-class cybersecurity consultancy services to help protect your **business from modern-day** threats.

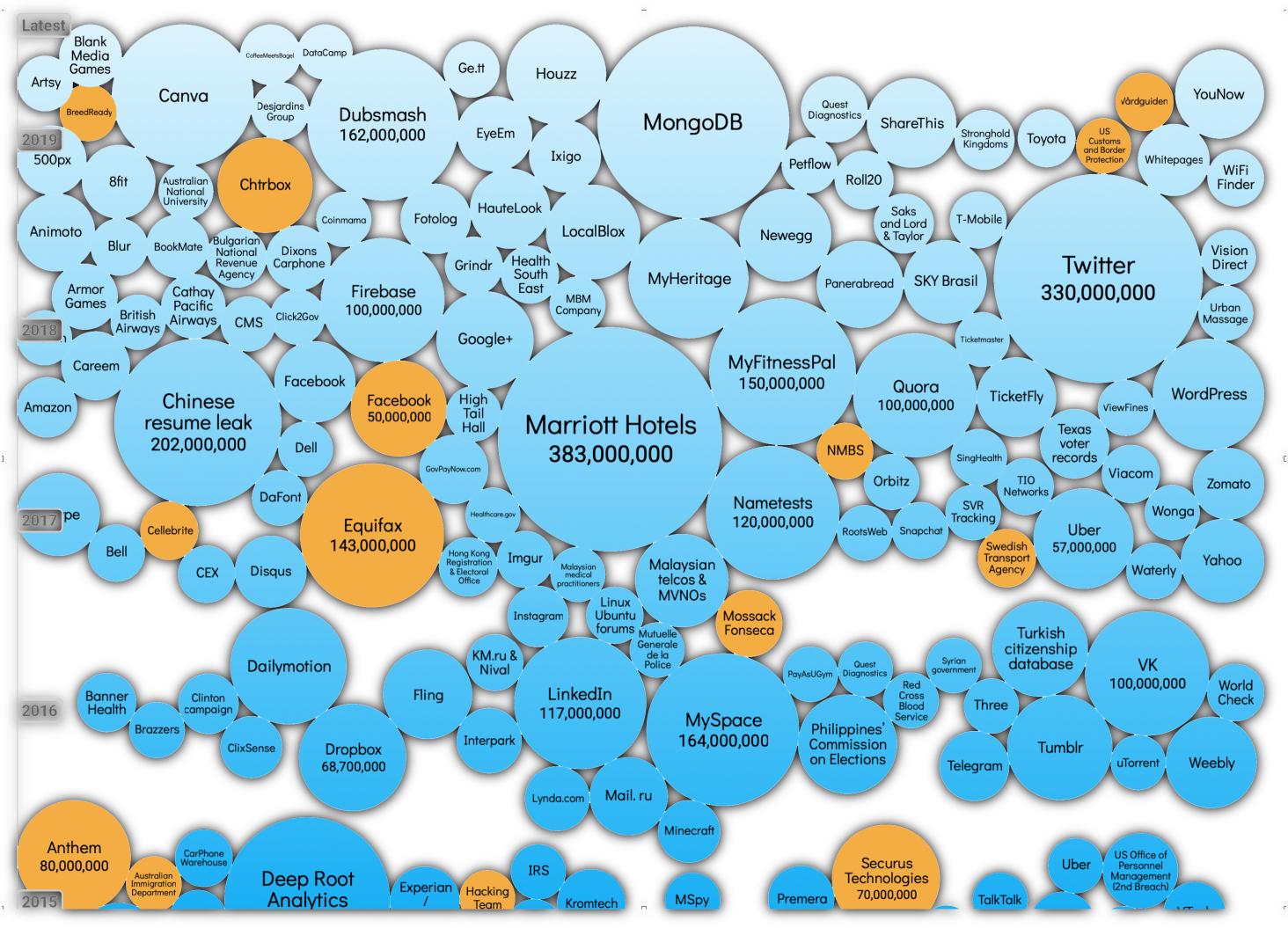


Why security?

Data breaches exposed 4.1 billion records in the first half of 2019.

Data breaches are the new norm. They threaten the viability of every business as they're now larger in number and impact.

it takes only one vulnerability exploit to get a data breach



Source: www.informationisbeautiful.net



The Cloud security numbers

Adversaries don't need many misconfiguration ONE is all it takes.

Is your business equipped with the right tool and trusted partner to address it?

Every min

62K record disclosed

Record per minute disclosed

Data breaches 80% due to misconfiguration Cloud misconfiguration is dominat

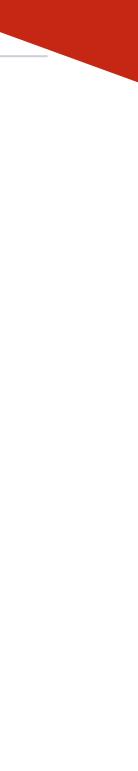
Total cost of cloud breaches 5 trillion \$ / 4 trillion GBP

N. Of Vuln records 33 billion

Disclosed records over 1 year

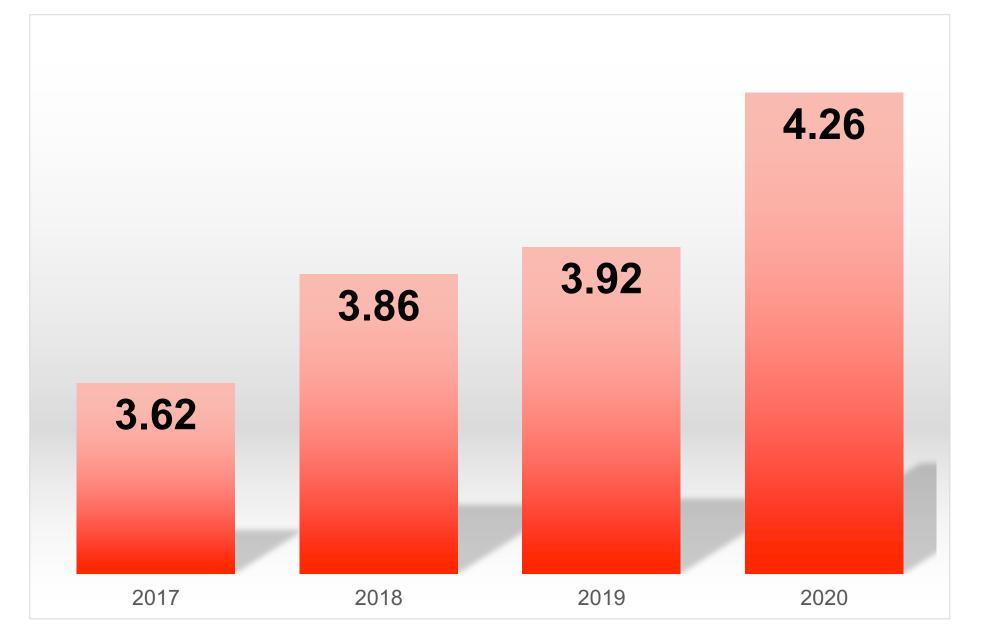
Av. Cost per record 150\$ per record

Average cost per loss record



The Cybersecurity Sector in Numbers

Av Cost of data Breach 3.03 m



Source Gartner Report 2018

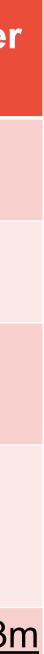
AVERAGE COST OF DATA BREACH IN MILLION OF DOLLARS

llion US dollars Spending in

The number of data breaches reported since 2017 to regulators has increased 480%.

71% of breaches in 2019 were financially motivated

Company	Net Loss (\$US)	Settlement/ Regulatory Fine	No. of Customer Affected
eBay	2.33 billion, \$1.82/share	\$650million	147million
Equifax	\$555.9 million	\$700million	147million
Capital One	\$150million	TBD	106million
Travelex	£4.6m ransom + 30 days inactivity	TBD	
Average	the average total c	ost of a breach nov	v stands at £3.03r



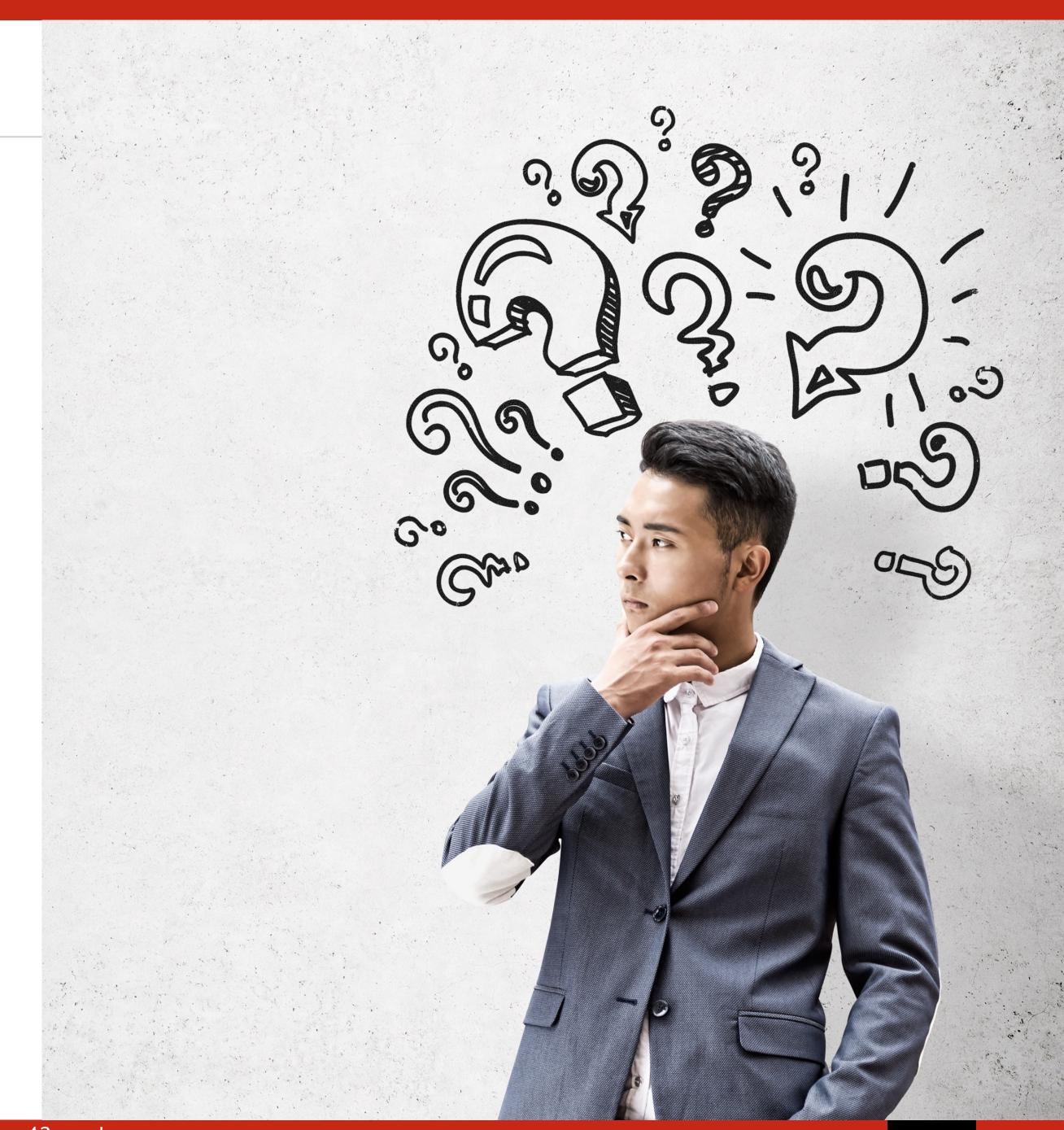


Problem with vendor only solution

Too many vendors Too many alerts & dashboards

Not enough skilled expertise

Not enough time



Fix the problem with technology

People – Process – Technology is the mantra of cybersecurity Why starting from the latter?

C Y B E R **s c a p e** Web Securit ICS + OT priver: aurionpro 🖗 a APERIO D BAYSHORE BELDEN CODV Check Poin EdgeWave PAS M.PFF FORCEPOINT F DOS arrest CYRE radifi W CRhebo ##SCADAfence iduss 🔊 Menio proofpoint. C Reblaze G SH-Pe SH HUAWEI O OPAG DEMONTO SANGFOR OSECUCIONAL SOPHOS STORMSHELD LUMETA NETSCOU SOPHOS SPI CyberTrap @Cymmetria Symantec 💋 TREND 🖄 SS8 utimaco AVECTRA TRAPX SMOKESCREEN inbotify Dwhiteops 🌏 avanced MSS & MDR boffle warrypter CipherCloud COVERTIX Ca clearswift 🔼 🐋 atat BAESYSTEMS BT C CenturyLink CSC Hewlett Packard IRM MogaPath CONTRACTOR STATEMENT ENVELL VFortanix FORMATICS TO Patter esentire Secureworks SELUTIONARY SELUTIONARY SECURE FILES Security TITALES DIREND (V) virtru Security Ratings BITSIGHT COTAX CyberCube cyther CB GRX Bolbix Bay Dynamics de cavirin C Coalition Cyber CORRELOG FICO S GUIDEWI FIRENON MOSEC Cenna DNIE ost24 🏟 PREVALENT 👹 REDSEAL 🗊 HanSight 🛦 Huntsman 🔼 🏗 🖽 logentries logpoint LogRhythm OLogscape Slogz.io CMCAfee curity Awareness & Trainin Barracuda CyberVista OR RONSCALES QPalantir RSA КложВе4 🛊 рызнаяв MetricStream neturix AZERCILT 🚺 NOPSEC 🠬 ds[♥] splunk > ∎sumologic TIBCØ Martustway RESOLVER RSA proofpoint. MMS AVERODIN M & R-sam 🚾 🔁 Autho (Baveron 🛞 BehavioSec BIOCATCH 🕻 Callsign: 🔊 Centrify RAPID 🖞 imprivata 🔅 INTRINS (a) iovation Nok Nok @ plant (A) saaspass of SaferPass & SECURE (RedLock PResilient SEC Servicenow 🚳 Siemplify splunk> SWIMLANE CUREPUSH 🍏 ShoCard 🕼 SILVERFORT tascent Threal Metrix. SYNCURITY SYGN/A VETHREATCONNECT THREATQUOTIENT UPLEVEL Centrify IBM Ilantus onelogin ORACLE RSA THALES Security Analytics AWAKE Bay Dynamics Varktrace AVECTO BeyondTrust BOMGAR C SCHUTTACHI 🕼 exabeam 🚯 Fluency 🚺 HanSight Hewlett Packard IEM ManageEngine DHOLDE ONE IDENTITY CRemediant Thycolic & WHEEL Reservoir Labs SECURONIX TERAMIND OTHETARAY Consumer Identity -Consumer Identity -D.me jonradius - Microsoft Pine TripleCyber VECTRA Veriato VERSIVE VINWARE YZoneFox 🖓 PIREAN 🎒 🏧 secure 🚳 Trulico 🗟 vchain verato 🖓 🕬



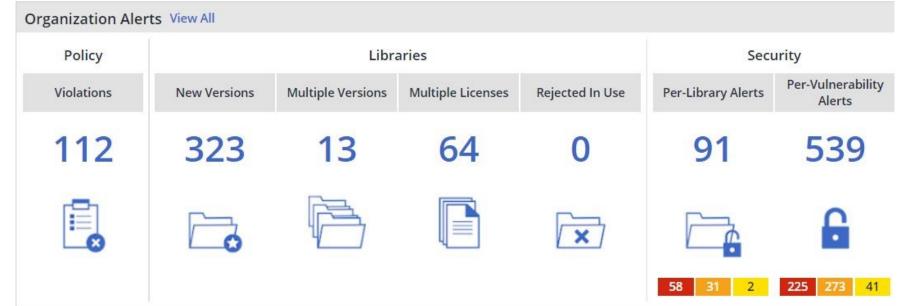
www.nsc42.co.uk

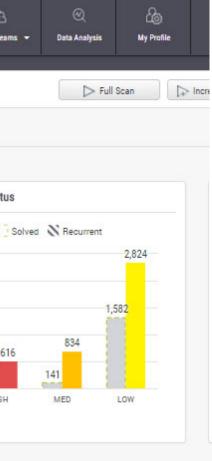


Fix the problem with technology

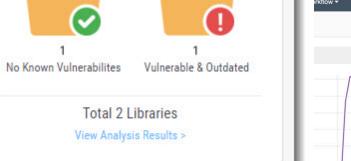
The More technologies the more dashboards

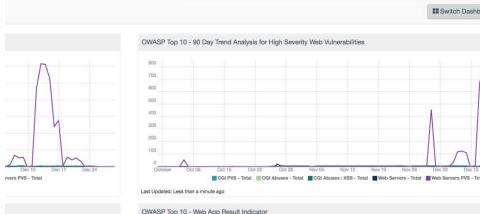
🙆 Das	shboard	/ Newest Risk	<						
Dash			x				Calculate Trends		
VIEWI	ING				NON-PROPRIETARY RESULTS	COMPONEN	IT MATCH	_	
DF 3 (67	ATIONS	POLIC OF 14	CIES	31 COMPONENTS	Exact Match 27 (87%)	Gimilar Match 3 (10	1%)		
RISK					Newest	By Component	By Application	ß	Ş
THREAT	T AGE	▲POLICY	APPLICATION	COMPONENT	BUI	LD STAGE RE	LEASE OPERATE	rojects & Scans 📼	5√ Management + L
7	7h	Security- Medium	A Pristine Application	tomcat : catalina : 5.5.15	5 7 h	0			
3	7h	Security- Low	A Pristine Application	tomcat : catalina : 5.5.15	5 7h	▲		Scans	History
9	1d	Security-	A Test Scan	org.mortbay.jetty:jetty	: 6.1.15 1d			5 1:49:05 PM)	
		High				SAST Vuinerad		0 1.10.001 m	SAST progre
						Full Scan Re	$) \bigcirc$	2994 laur	3000 - 2400 - 1800 -
ter Dashboard + atus		• Scans • Reporting •	Assets Workflow+ Users			616 New	834 Med 834 New	2824 Low 2824 New 0 Recurring	2400 - 1800 - 1200 -
atus		Par	Assets Workflow - Users	Failed	XenServer-Top 10 Events	G16 High	834 Med 834 New 9 0 Recurring		2400 - 1800 -
atus nerabilities by CoCS Catego Device Information Application Information Secure Configs		Par	ssed	Falled 11 0 11		616 New 0 Recurrin	834 Med 834 New g 0 Recurring	2824 New 0 Recurring	2400 - 1800 - 1200 - 600 -
atus nerabilities by CoCS Catego Device Information Application Information		Par	ssed	Failed 11 0	Count	616 New 0 Recurrin	834 Med 834 New g 0 Recurring	2824 New 0 Recurring	2400 - 1800 - 1200 - 600 -
atus Device Information Application Information Secure Configs Unertability Assessments Ports & Protocols Privileges Monitoring & Logs		Par	ssed	Failed 11 0 11 0 4	Count	616 New 0 Recurrin	834 Med 834 New g 0 Recurring	2824 New 0 Recurring	2400 - 1800 - 1200 - 600 -
atus Device Information Application Information Secure Configs Jinerability Assessments Ports & Protocols Privileges		Par	ssed	Failed 11 0 13 0 4 0 1	Count	616 New 0 Recurrin	834 Med 834 New g 0 Recurring	2824 New 0 Recurring	2400 - 1800 - 1200 - 600 -
atus Device Information Application Information Secure Configs Unertability Assessments Ports & Protocols Privileges Monitoring & Logs		Par	ssed	Faled 11 0 11 0 4 0 1		616 New 0 Recurrin	834 Med 834 New g 0 Recurring	2824 New 0 Recurring	2400 - 1800 - 1200 - 600 - 0 -
atus Device Information Application Information Secure Configs Unertability Assessments Ports & Protocols Privileges Monitoring & Logs		Par	ssed	Faled 11 0 13 0 4 0 1 1 0 1 0 1 0 1 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 0 1 0	KenServer- Vulnerability Summary Plugin ID Name 1000729 XenServer - List crash dumps 1000729 XenServer - List crash dumps	616 New 0 Recurrin 13 Solved (834 Med 834 New g 0 Recurring	2824 New O Recurring 1582 Solved ()	2400 - 1800 - 1200 - 600 - 0 -
atus Device Information Application Information Secure Configs Unertability Assessments Ports & Protocols Privileges Monitoring & Logs		Par	ssed	Faled 11 0 13 0 4 0 1 1 0 1 0 1 0 1 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 0 1 0	Vanishing Summary Pugn ID Name 1000729 XenServer - List crash dumps	4P5 kooks a access by default	834 Med 834 New g 0 Recurring	2824 New O Recurring 1582 Solved ()	2400 - 1800 - 1200 - 600 - 0 -
atus Device Information Application Information Secure Configs Unertability Assessments Ports & Protocols Privileges Monitoring & Logs		Par	ssed	Faled 11 0 13 0 4 0 1 1 Critical Figh Head Head Head Head Head Head Head Head	KanSarver- Vulnerability Summary Plugn ID Name 1000739 XenSarver - List creath dumps 1000738 XenSarver - The hosts.alow file I 1000739 XenSarver - The hosts.alow file I 1000740 XenSarver - List bridden Vice I	ups teocks access by default mits access to the local network enders to be used for storage access	834 Med 834 New g 0 Recurring	2824 New O Recurring 1582 Solved ()	2400 - 1800 - 1200 - 600 - 0 -
atus Device Information Secure Configs dinerabilities by CoCS Categor device Information Secure Configs dinerability Assessments Ports & Protocols Privileges Monitoring & Logs ces Summary	jory .	Par	ssed	Faled 11 0 13 0 4 0 1 1 Critical Figh Head Head Head Head Head Head Head Head	VerServer Vulnerability Summary Plugin ID Name 1000729 XerServer - List crash dumps 1000739 XerServer - The hosts.deny file II 1000739 XerServer - The hosts.deny file II 1000739 XerServer - List borded NIIC gro 1000739 XerServer - The hosts.deny file II 1000740 XerServer - List borded NIC gro 1000741 XerServer - List borded NIC gro	ups teocks access by default mits access to the local network enders to be used for storage access	834 Med 834 New g 0 Recurring	2824 New O Recurring 1582 Solved ()	2400 - 1800 - 1200 - 600 - 0 -
atus Pervice Information Secure Configs Unerabilities by CoCS Categor Automation Secure Configs Unerability Assessments Ports & Protocols Provileges Monitoring & Logs Res Summary ary	jory .	Par	ssed	Faled 11 0 13 0 4 0 1 1 Critical Figh Head Head Head Head Head Head Head Head	Court C	ups totoka access by defaut mits access to the local network entances to be used for storage access a storage network interface ction on the storage network interface an anagement network interface	834 Med 834 New g 0 Recurring	2824 New O Recurring 1582 Solved ()	2400 - 1800 - 1200 - 600 - 0 -
atus Pervice Information Pervice Information Secure Configs Information Pervices Pervices Pervices Pervices Nontoring & Logs Pervices Pe	jory .	Par	sed 15 1 2 2	Faled 11 0 13 0 4 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Court C	Apple access by default mits access to the local network interface as are operating in full-duplex mode	834 Med 834 New g 0 Recurring	2824 New O Recurring 1582 Solved ()	2400 - 1800 - 1200 - 600 - 0 -
atus Pervice Information Pervice Information Secure Configs Information Pervices Pervices Pervices Pervices Nontoring & Logs Pervices Pe	jory .	Par	sed 15 1 2 2	Faled 11 0 13 0 4 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	KenServer- Vulnerability Summary Plugin ID Name 1000739 XenServer - List crash dumps 1000743 XenServer - List crash dumps 1000744 XenServer - List crash dumps 1000743 XenServer - List crash dumps 1000744 XenServer - List crash dumps 1000743 XenServer - List crash dumps 1000744 XenServer - List crash dumps 1000743 XenServer - List crash dumps 1000744 XenServer - List crash dumps 1000744 XenServer - List crash dumps	ups toots access by default mits access to the local network interface a rearperating in full-duplex mode a rearperating in full-duplex mode	834 Med 834 New g 0 Recurring	2824 New O Recurring 1582 Solved ()	2400 - 1800 - 1200 - 600 - 0 -
atus Pervice Information Pervice Information Secure Configs Information Pervices Pervices Pervices Pervices Nontoring & Logs Pervices Pe	jory .	Par	sed 15 1 2 2	Faled 11 0 13 0 4 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	VerServer Vulnerability Summary Plugn ID Name 1000739 XenServer - List crash dumps 1000739 XenServer - List crash dumps 1000739 XenServer - The hosts.alow file List control 1000739 XenServer - The hosts.alow file List control 1000740 XenServer - The hosts.alow file List control 1000741 XenServer - Identify a network in the top of top of the top of top of top of top of the top of top	ups tooks access by defaut mits access to the local network enfaces to be used for storage access is storage network interface a management network interface a rear operating in full-duplex mode is roods on all network interfaces d guests.	834 Med 834 New g 0 Recurring	2824 New O Recurring 1582 Solved () High High High High High High High High	2400 - 1800 - 1200 - 600 - 0 - 0 -
atus Pervice Information Pervice Information Secure Configs Information Pervices Pervices Pervices Pervices Nontoring & Logs Pervices Pe	jory .	Par	sed 15 1 2 2	Faled 11 0 13 0 4 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	V KanSarver- Vulnerability Summary Plugn ID Name 1000739 XenSarver - List creath dumps 1000739 XenSarver - List creath dumps 1000739 XenSarver - The hosts.allow file II 1000740 XenSarver - Identify a nativori in 1000741 XenSarver - Disallow unplug desc 1000745 XenSarver - All network interface 1000745 XenSarver - Disable promiscuou 1000746 XenSarver - Enable OoS on all VI	ups locks access to the local network instancess to the local network instancess is torage network interface is an experiating in full-duplex mode in mode on all network interfaces is diguests is diguests is biological diguests	834 Med 834 New g 0 Recurring	2824 New O Recurring 1582 Solved ()	2400 - 1800 - 1200 - 600 - 0 - 0 -
atus Pervice Information Pervice Information Secure Configs Information Pervices Pervices Pervices Pervices Nontoring & Logs Pervices Pe	jory .	Par	sed 15 1 2 2	Faled 11 0 13 0 4 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Court Court <td< td=""><td>ups aps torcis a coeses by default mits access to the local network interface to ranagement network interface a ranageme</td><td>834 Med 834 New g 0 Recurring</td><td>2824 New O Recurring 1582 Solved ()</td><td>2400 - 1800 - 1200 - 600 - 0 - 0 -</td></td<>	ups aps torcis a coeses by default mits access to the local network interface to ranagement network interface a ranageme	834 Med 834 New g 0 Recurring	2824 New O Recurring 1582 Solved ()	2400 - 1800 - 1200 - 600 - 0 - 0 -





Top 10 Products (22) View All				
Product	Projects	Libraries	Vulnerable Libraries	Licenses
Struts	29	127	High: 8 Medium: 2	18
NewProj	5	24	High: 5 Medium: 4	14
CRM_Prod	4	81	High: 10 Medium: 1	19
KSA	3	42	High: 8 Medium: 1	8
Demo Product	2	328	High: 13 Medium: 13	31
My Product	2	36	High: 2 Medium: 3	9
Jenkins Test	2	10	No Vulnerabilities	1
ERP-1.0_Repo	1	318	High: 12 Medium: 13	29
ERP-1.0_Build	1	318	High: 12 Medium: 13	29
EUA_2019	1	39	High: 8 Medium: 1	9





Injection	Overflow
SSL	Error Handling
CGI Generic	XSS
High Web Vulns	Critical Web Vulns

Switch Dashboard - Options -

OWASP Top 10 - Web Events

Web Intrusion	Web Threatlist	
Web Stats	Long Term Web Error Activity	
NNM Detected Web Error	NNM Detected Web Access	
Apache Web Error	Apache Web Access	
IIS Web Error	IIS Web Access	

OWASP Top 10 - SQL Events and Vulnerabilities

Suspicious SQL User Database Dump	Suspicious SQL Command Detection
SQL Injection Vulnerability Detected	Suspicious SQL Query Detected
SQL Intrusion	Database Stats
SQL Error	SQL Login Failure

© 2016 Checkmarx

	System	Vulnerabilities	Exploitable
A1 – Injection	23	142	65%
A2 - Broken Authentication and Sess	6	6	0%
A3 - Cross-Site Scripting (XSS)	11	47	62%
A4 - Insecure Direct Object Reference	7	19	63%
A5 – Security Misconfiguration	136	209	25%
A6 – Sensitive Data Exposure	101	154	75%
A7 – Missing Function Level Access	7	16	56%
A8 - Cross-Site Request Forgery (CS	1	1	100%
A9 – Using Known Vulnerable Comp	0	0	0%
A10 - Unvalidated Redirects and For	0	0	0%
ast Updated: 3 minutes ago			

 \bigcirc

Plugin ID	Name	Family	Severity	Total
1442	Web Server Detection	Web Servers [Passive]	Info	3711
1724	Microsoft IIS Server Detection	Web Servers [Passive]	Info	406
10107	HTTP Server Type and Version	Web Servers	Info	238
24260	HyperText Transfer Protocol (HTTP) Information	Web Servers	Info	234
4667	Persistent Cookie Utilization	Web Servers [Passive]	Info	214

ww.nsc ²	42.cc	b.uk



Fix the problem with technology

Too many alert Too little time Who can you trust?

Total cost of cloud breaches 5 trillion \$ 4 trillion GBP

		2			
Over	rlay: None	1			
	_time \$	sourcetype \$	source \$	host \$	_raw ≑
1	7/25/12 11:00:34.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725230034.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=70
2	7/25/12 11:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725230027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700
3	7/25/12 11:00:15.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725230015.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700
4	7/25/12 11:00:15.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725230015.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=70
5	7/25/12 10:16:57.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725221657.000000 Category=7 CategoryString=Core EventCode=10000 EventIdentifier=10000 EventType=3
6	7/25/12 10:00:43.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725220043.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=70
7	7/25/12 10:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725220027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700
8	7/25/12 10:00:18:000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725220018.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=70
9	7/25/12 10:00:15.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725220015.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700
10	7/25/12 9:09:11.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725210911.000000 Category=0 CategoryString=NULL EventCode=1704 EventIdentifier=1073743528 EventTy
11	7/25/12 9:00:41.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725210041.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=70
12	7/25/12 9:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725210027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700
13	7/25/12 9:00:17.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725210017.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=70
14	7/25/12 9:00:16.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725210016.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700
15	7/25/12 8:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725200027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700

	System	Vulnerabilities	Exploitable	
A1 – Injection	23	142	65%	
A2 - Broken Authentication and Sess	6	6	0%	
A3 - Cross-Site Scripting (XSS)	11	47	62%	
A4 - Insecure Direct Object Reference	7	19	63%	Last
A5 – Security Misconfiguration	136	209	25%	
A6 - Sensitive Data Exposure	101	154	75%	OW
A7 - Missing Function Level Access	7	16	56%	
A8 - Cross-Site Request Forgery (CS	1	1	100%	
A9 – Using Known Vulnerable Comp	0	0	0%	
A10 - Unvalidated Redirects and For	0	0	0%	

ASP Top 10 - Web App Result Indicator

Updated: 3 minutes ago

VASP Top 10 - Web Events

Web Intrusion Web Stats NNM Detected Web Error Apache Web Error IIS Web Error

Last Updated: 3 minutes ago

701 EventType=3 Logfile=Application RecordNumber=84580 700 EventType=3 Logfile=Application RecordNumber=84579 700 EventType=3 Logfile=Application RecordNumber=84577 701 EventType=3 Logfile=Application RecordNumber=84578 =3 Logfile=Application RecordNumber=84576 SourceName= 701 EventType=3 Logfile=Application RecordNumber=84575 700 EventType=3 Logfile=Application RecordNumber=84574 701 EventType=3 Logfile=Application RecordNumber=84573 700 EventType=3 Logfile=Application RecordNumber=84572 Type=3 Logfile=Application RecordNumber=84571 SourceN 701 EventType=3 Logfile=Application RecordNumber=84570 700 EventType=3 Logfile=Application RecordNumber=84569 701 EventType=3 Logfile=Application RecordNumber=84568 700 EventType=3 Logfile=Application RecordNumber=84567 700 EventType=3 Logfile=Application RecordNumber=84565

« prev 1 2 3 4 5 6 next » 50 per

Overflow	
Error Handling	
XSS	
Critical Web Vulns	
Web Threatlist	
Long Term Web Error Activity	
NNM Detected Web Access	
Apache Web Access	
IIS Web Access	

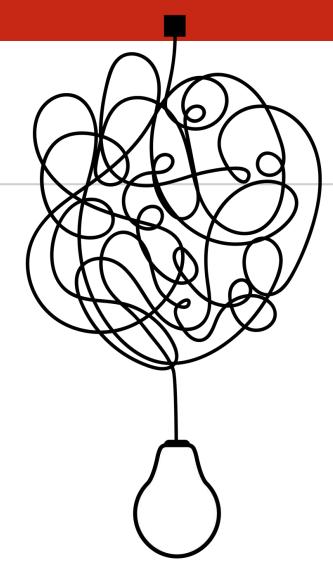
Every min 62K record disclosed Record per minute disclosed

Plugin ID	Name	Severity	Total
1000729	XenServer - List crash dumps	High	1
1000733	XenServer - List bonded NIC groups	High	1
1000738	XenServer - The hosts.deny file blocks access by default	High	1
1000739	XenServer - The hosts allow file limits access to the local network	High	1
1000740	XenServer - Identify a network interface to be used for storage access	High	1
1000741	XenServer - Use a static IP on the storage network interface	High	1
1000742	XenServer - Disallow unplug detection on the storage network interface	High	1
1000743	XenServer - Use a static IP on the management network interface	High	1
1000744	XenServer - All network interfaces are operating in full-duplex mode	High	1
000745	XenServer - Disable promiscuous mode on all network interfaces	High	1
1000746	XenServer - Enable QoS on all VM guests	High	1
1000752	XenServer - Host is enabled	High	1
1000753	XenServer - High availability is enabled	High	1
000755	XenServer - Snapshots are not present	High	,
1Server - Be	ast Practice Indicators		

Promiscuous	Crash Dumps	Disabled Hosts
Configure NTP	Certificate	NTP
Services	Snapshots	High Availability

Top 10 Products (22) View All				
Product	Projects	Libraries	Vulnerable Libraries	Licenses
Struts	29	127	High: 8 Medium: 2	18
NewProj	5	24	High: 5 Medium: 4	14
CRM_Prod	4	81	High: 10 Medium: 1	19
KSA	3	42	High: 8 Medium: 1	8
Demo Product	2	328	High: 13 Medium: 13	31
My Product	2	36	High: 2 Medium: 3	9
Jenkins Test	2	10	No Vulnerabilities	1
ERP-1.0_Repo	1	318	High: 12 Medium: 13	29
ERP-1.0_Build	1	318	High: 12 Medium: 13	29
EUA_2019	1	39	High: 8 Medium: 1	9

www.nsc42.co.uk



Trust & Clarity

Too many vendors Too many alerts & dashboards Too much confusion & overwhelm Not enough skilled expertise

Our Solution

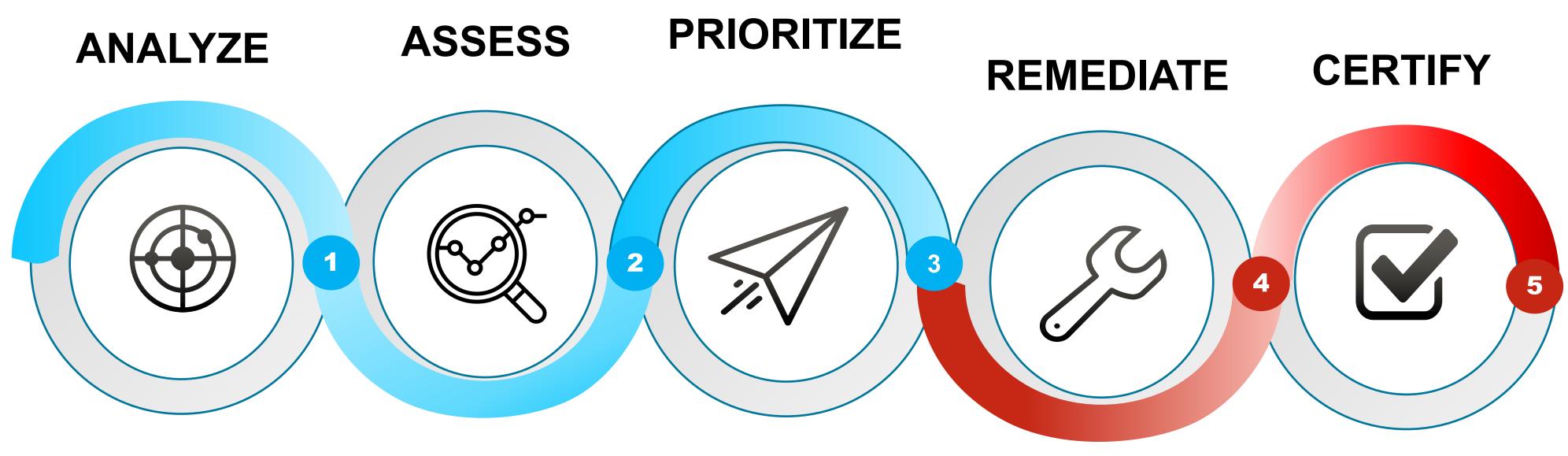
Single view and report Report and vulnerabilities explained by experts Consultancy from recognized

cyber experts Training and consultancy



A validated methodology across our services

ASSESS



Analyze the posture & highlight the problems

Recommend remediation path

Your Protection is Our Success OUR METHOD: AAP-RC

Agree Scope, Prioritize

Execute the agreed remediation steps

Review & Certify



12

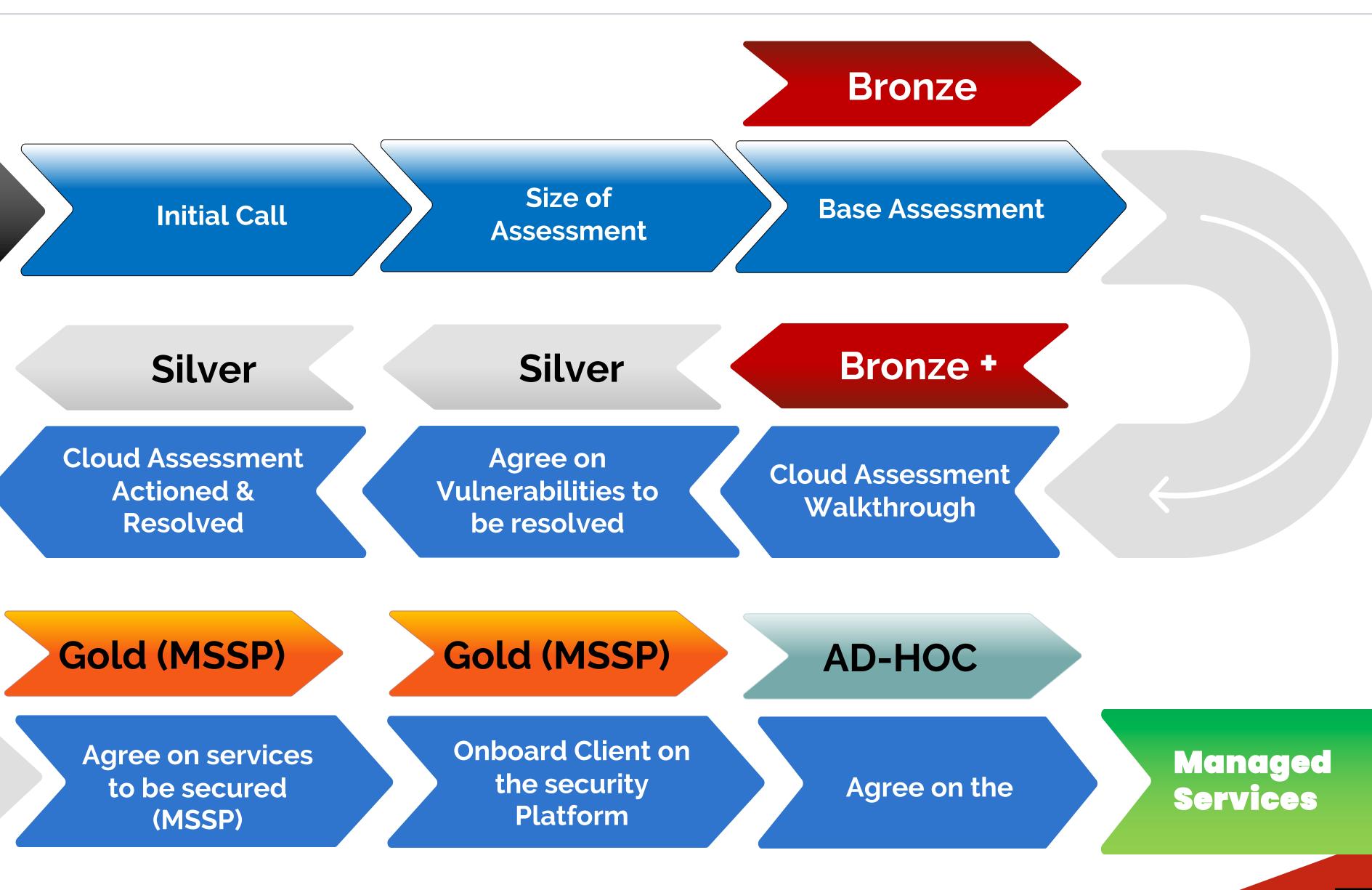
Customer Journey – Cloud Security Assessments

Initial Assessment

Service Tier

Unknown Security Posture

Actioned & Resolved







Our Other Services

We believe in an all rounded set of services built on the need of our clients over the years and recognized by the Cloud Security Alliance.

What differentiates our company from other consultancies is that we do what we love and are customer focused.

Our company goes the extra mile in order to deliver solutions that are fit for purpose, effective and costeffective for your organization's risks appetite. We offer a range of products within cybersecurity.



VCISO/INTERIM CISO



CYBER SECURITY STRATEGY



CYBER SECURITY CONSULTANCY











NSC42

Thank you Get in touch:



https://www.linkedin.com/company/n sc42-limited



Communications@nsc42.co.uk



www.nsc42.co.uk

WHEN YOU ARE CYBERSAFE WE ARE CYBERHAPPY



