

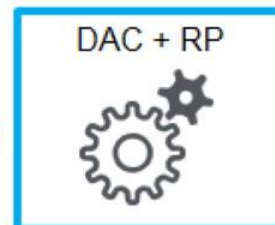
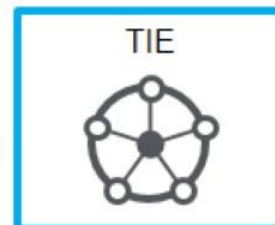
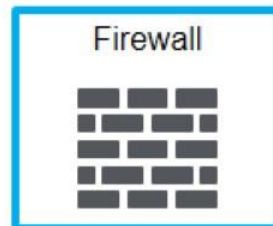


Jak skutecznie wykrywać i usuwać złośliwe oprogramowanie?

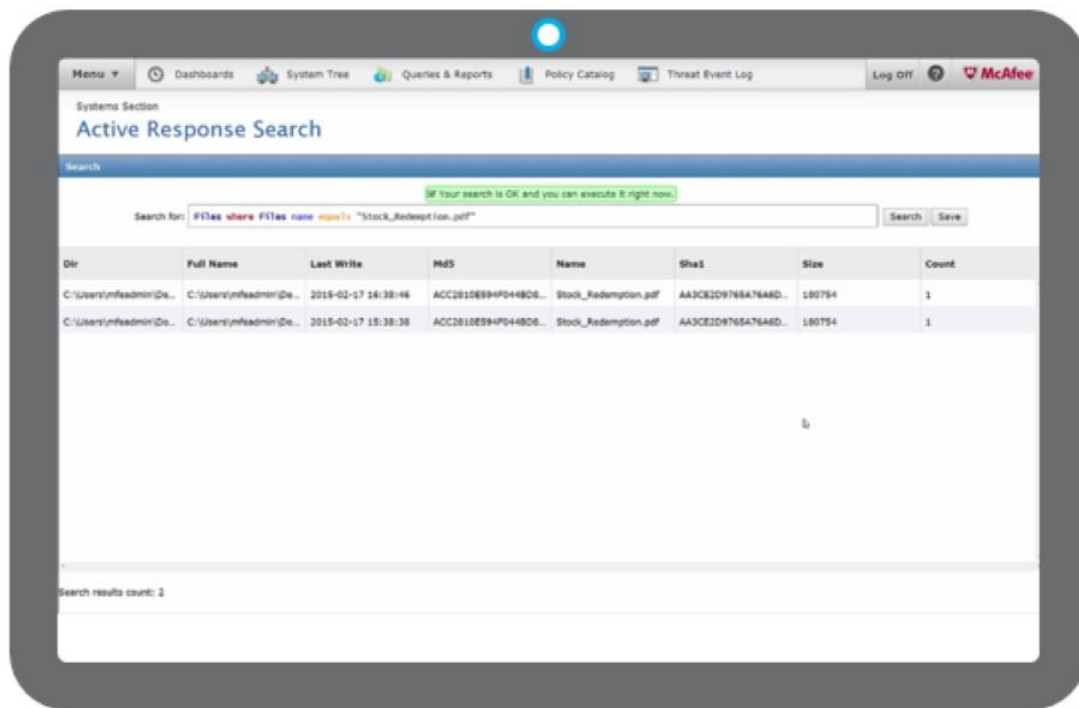
Bartosz Chmielewski | Presales Engineer CEE



Mechanizmy ochrony przez złośliwym kodem



A co jak już ktoś wejdzie?

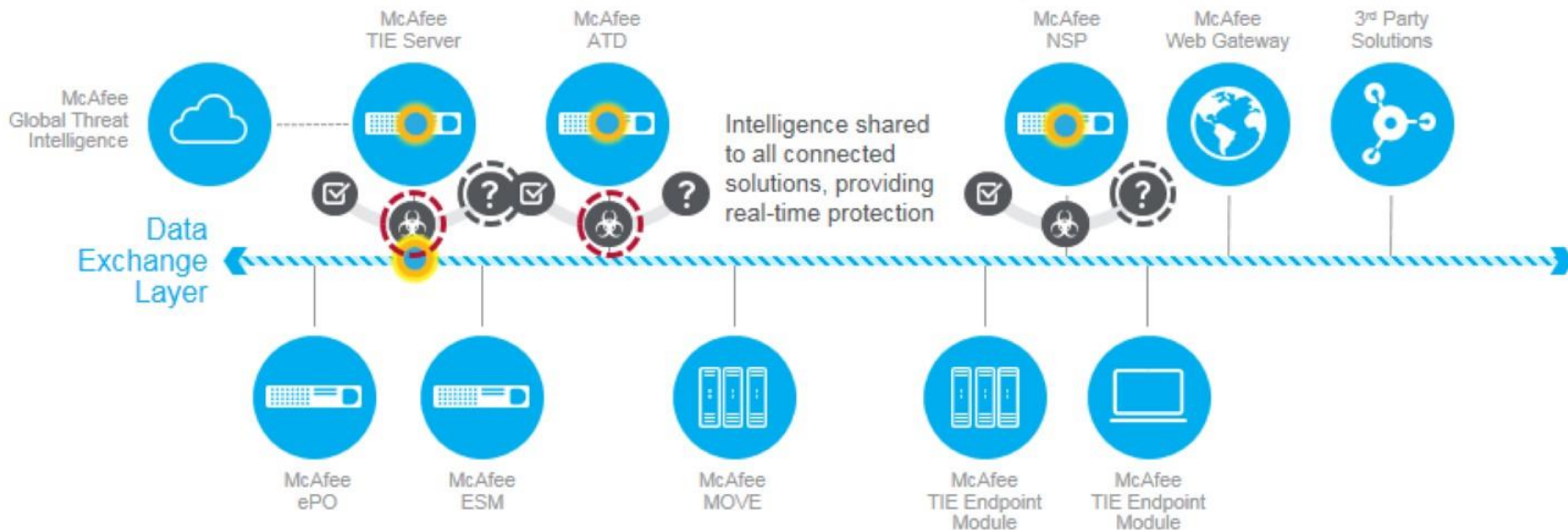


The screenshot displays the McAfee Active Response Search interface. The search bar contains the query: `Files where Files name equals "Stock_Redemption.pdf"`. The search results are as follows:

Dir	Full Name	Last Write	Md5	Name	Sha1	Size	Count
C:\Users\mfeadmin\De...	C:\Users\mfeadmin\De...	2015-02-17 14:38:46	ACC2810E594F0448D6...	Stock_Redemption.pdf	AA3CE2D9765A76A6D...	180754	1
C:\Users\mfeadmin\De...	C:\Users\mfeadmin\De...	2015-02-17 15:38:38	ACC2810E594F0448D6...	Stock_Redemption.pdf	AA3CE2D9765A76A6D...	180754	1

Search results count: 2

Ekosystem bezpieczeństwa



Adaptacyjna ochrona i wczesne wykrywanie

Urządzenia sieciowe

Inne

NSP (IPS)

Web Gateway

Endpoint



Komunikacja urządzeń sieciowych i stacji roboczych

TIE/Sandbox

ATD



- IOC 1
- IOC 2
- IOC 3
- IOC 4

Zawartość jest analizowana.

AR/SIEM

AR/SIEM



Informacja IoC jest analizowana wśród informacji historycznych

Ekosystem DxL

Ekosystem DxL

Stacje robocze



Endpoint

Endpoint

Endpoint

Endpoint

Systemy skompromitowane są izolowane oraz naprawiane.

