
Auditoria de endpoints com Loqed

Neo Vedder



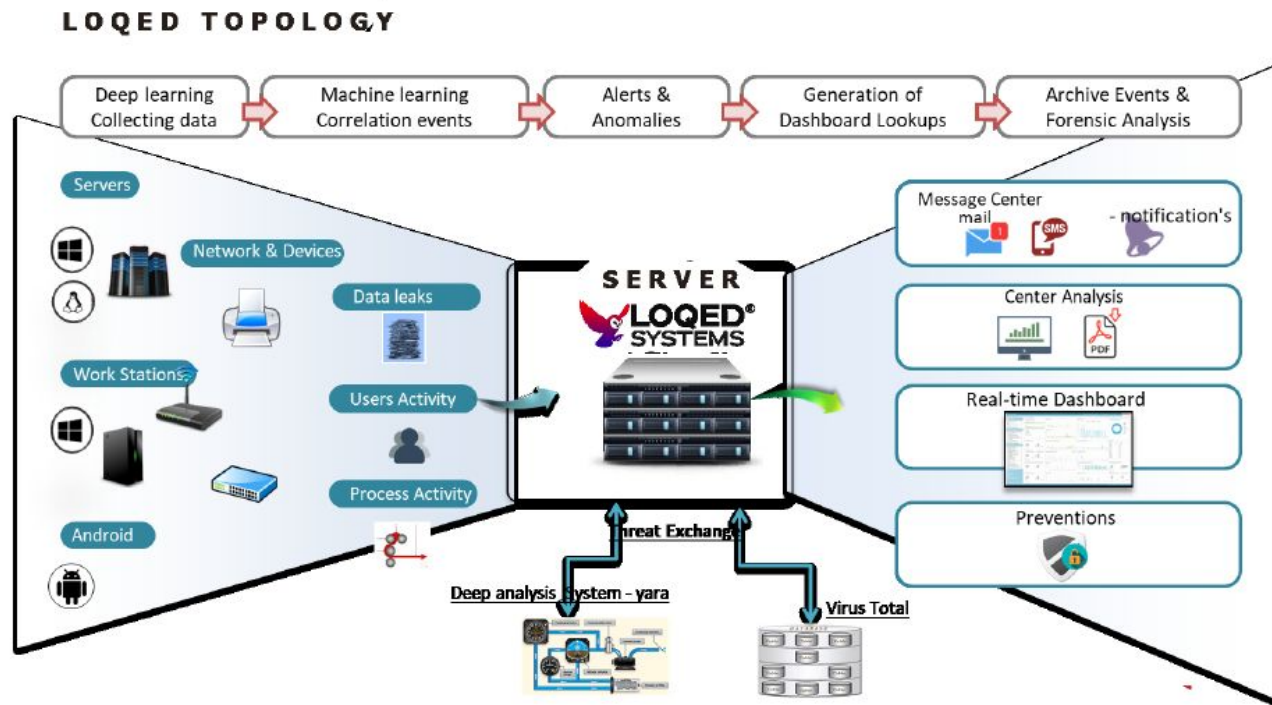
Topologia

Vigilância ininterrupta

Processamento de insights

Coleta de evidências em tempo real

Coleta de dados voláteis



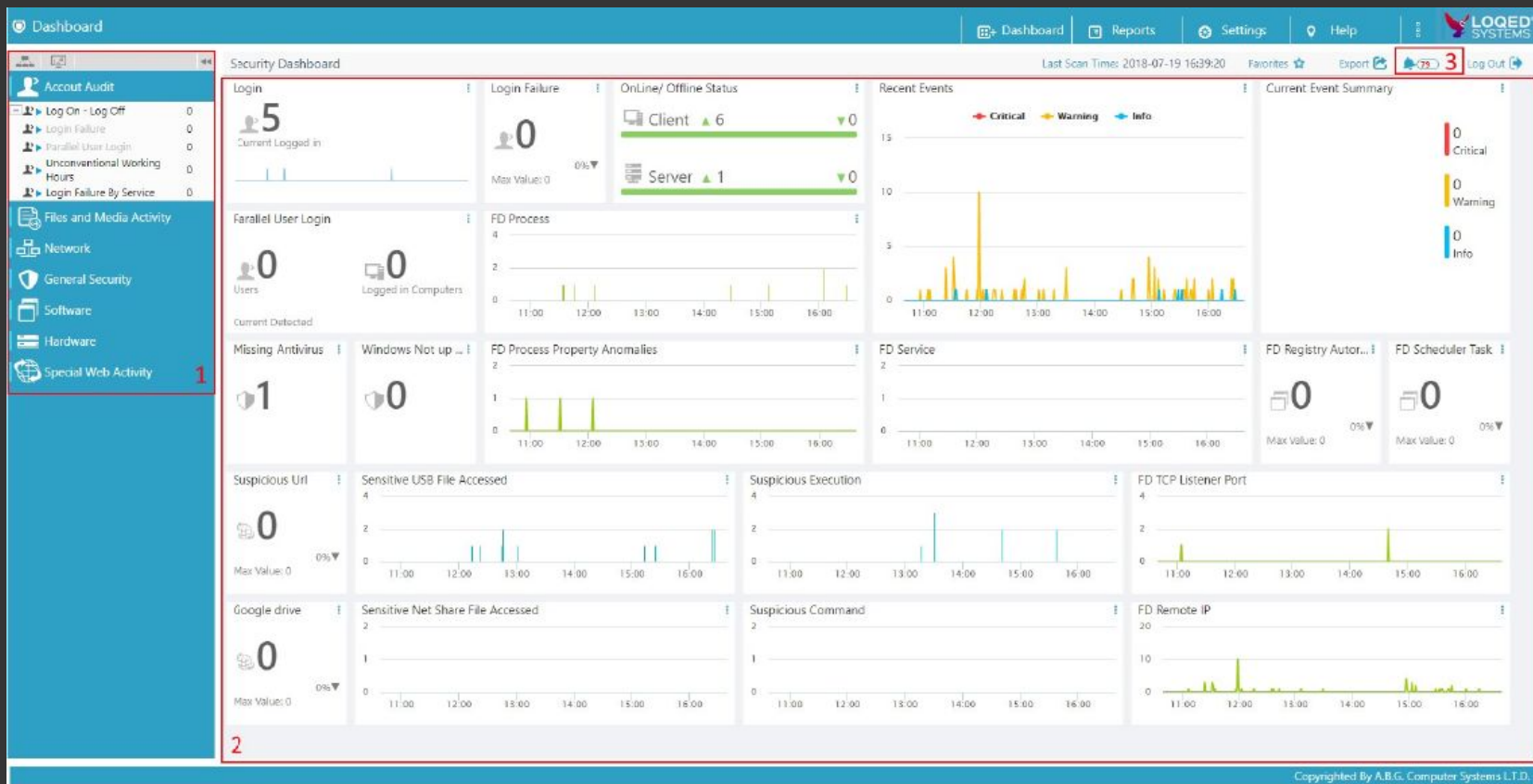
Motores

- **NÍVEL 1** Detecção instantânea de um evento em tempo real conforme capturado pelo agente de endpoint local e definido por ele.
- **NÍVEL 2** Determina se o evento é novo ou é um desvio de seu perfil, com base em um perfil estabelecido do endpoint específico e do Motor de Regras Dinâmicas.
- **NÍVEL 3** Determina se o evento específico foi detectado anteriormente em qualquer lugar da rede da organização.
- **NÍVEL 4** Correlaciona com outros eventos da rede, simultâneos ou anteriores. Gera insights sobre tendências de eventos, compreensão do comportamento do terminal, identificação de problemas de segurança e riscos potenciais, bem como previsão de ameaças futuras.
- **NÍVEL 5** É o corte transversal entre eventos passados e presentes em relação a um evento específico atual.

– Monitoramentos

- Inventário
- Processos maliciosos by Yara
- Dados confidenciais
- Compartilhamentos criados ou estabelecidos
- Portas em escuta
- Mudança de hash
- Comportamento de usuário
- Compliance

- Dashboard tempo real - 12h



IDENTIFICAÇÃO RESPOSTA

Suspicious Execution

Process Name	Computer Name	TCP Address	User Name	Process Path	Parent	Parent User	Command Line	Date&Time	Correlation
MpCmdRun.exe								2018-07-19 15:38	13
MpCmdRun.exe								2018-07-19 15:38	13

Suspicious details for [MpCmdRun.exe]

Description	Value
Computer Name	PC-MpCmd
TCP Address	192.192.192.192
User Name	NETWORK SERVICE
Date&Time	2018-07-19 15:38
Process Path	C:\ProgramData\Microsoft\Windows Defender\platform\
Parent	
Command Line	C:\ProgramData\Microsoft\Windows Defender\platform\
Checksum	97D5086C5407921A78F2CA365313A5F0
Original Name	MpCmdRun.exe
64 bit	1
Verified	1

USB Inserted/Detected

USB Details on [P192[192.192.192]]

USB Details	Device Type	Count Files	Action	Date&Time
Apple Inc. Apple iPhone	Mobile		INSERTED	2018-07-23 15:25:14

Right Click

USB Inserted/Detected Prevention, Immediate direct action.

- USB - Apple Inc. Apple iPhone
- Disconnect USB from Machine
- Full Lock USB from Machine
- Machine - P192
- Shut down Machine
- User - P192
- Log Out from Machine

☒ Notify User when action is done

Execute Action Cancel

LIVE

- Abas no navegador
- Suspicious execution, Run cmd from browser
- Powershell (hidden, NonInteractive, police bypass)
-



Account Audit

Log On - Log Off	41
Login Failure	5
Parallel User Login	32
Unconventional Working Hours	4
Login Failure By Service	0



Files and Media Activity

Removable & Mobile Devices	146
Shared Access	47
Sensitive Data Accessed	968



Network

Adapter	1
Connectivity	15
Activity	164



General Security

Antivirus Issues	342
Windows Not up to date	73
Windows Network Firewall	32
Anti-Spyware Protection	61

Security Dashboard

Login

742

Current Logged in

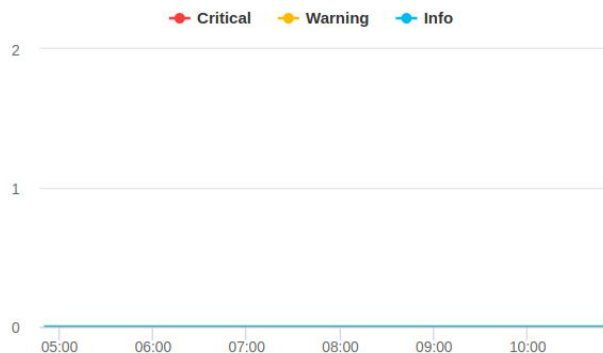


OnLine/ Offline Status

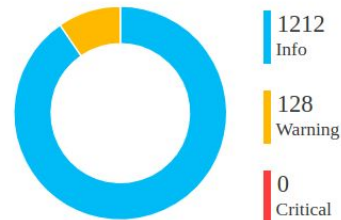
Client ▲ 374 ▼ 413

Server ▲ 50 ▼ 68

Recent Events



Current Event Summary

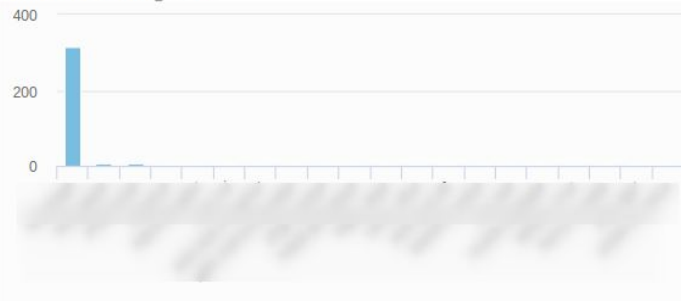


Parallel User Login

Filters :

Main Details

Name	 Parallel User Login
Org Units	 All
Event Date	 2023-08-03 10:51:00
Event Count	 31
Description	 Is the total amount of Users that each one of them is logged In to more than one computer simultaneously.

Parallel User Login 

Additional Related Counters Last 6 hours

Parallel User Login TOP 20 From 30  Zoom

User Name	Remote Hosts	Correlations
SIS	314	
aut	8	
jon	7	
ant	4	
Ad	4	
aut	4	
aut	4	
adr	4	
jon	3	
ma	3	
reg	3	
car	3	
aut	2	
lea	2	
anc	2	

History Graph

 31
Users 462
Logged in Computers



Software

	New Software	0
	New SW or Win Updates	0
	Driver	0
	Service	30
	Scheduler Task	98
	Registry Autorun	226



Process

	Process Property Anomalies	0
	New Process	1
	Process Behavior Anomalies	0
	Process Version Changed	0
	Suspicious Execution	28
	Suspicious Command	52
	Current Malicious Process	0



First Detection

	FD Process	0
	FD Driver	0
	FD Process Property Anomalies	0
	FD Process Version Changed	0
	FD Service	0
	FD Software	0
	FD Registry Autorun	0
	FD Service DLL	0
	FD Scheduler Task	0



Hardware

	Hardware Changed/Removed	0
	New Hardware Detection	0
	First Detection of Hardware	0
	High CPU	0
	Bios Changed	0



Special Web Activity

	Social Networking	5
	Cloud & P2P Networking	1
	Web Mail	15
	Suspicious Url	0

OBRIGADO
