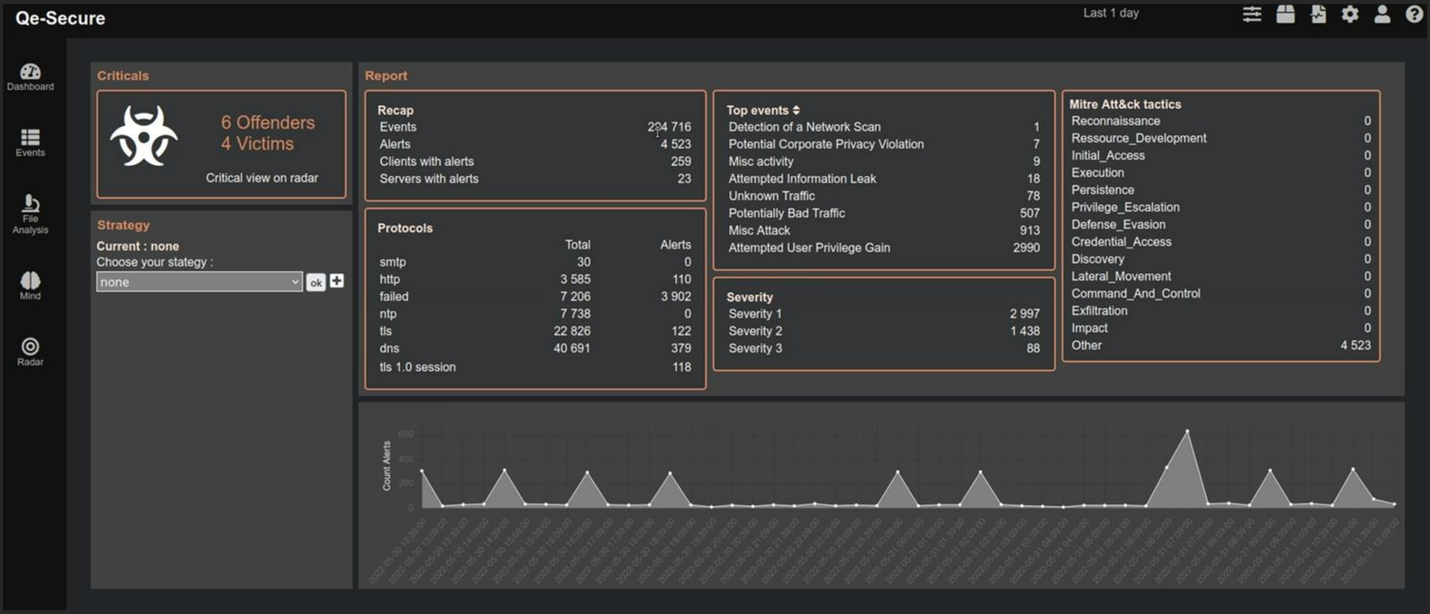
allentis

Qe-Secure

Security event management made easy

Qe-Secure is a threat detection system developed in France by allentis to meet the needs expressed by the Military Programming Law (LPM) as well as the expectations of companies and organizations wishing to protect themselves in a simple and efficient way from attacks.
The solution benefits from the experience of Allentis in the design of analysis probes. It is distinguished in particular by optimal ergonomics, an intuitive user interface allowing significant time savings in understanding security events.



Criticals

6 Offenders
4 Victims
Critical view on radar

Strategy

Current : none
Choose your stategy :
none ok

Report

Recap	
Events	294 716
Alerts	4 523
Clients with alerts	259
Servers with alerts	23

Protocols	Total	Alerts
smtp	30	0
http	3 585	110
failed	7 206	3 902
ntp	7 738	0
tls	22 826	122
dns	40 691	379
tls 1.0 session		118

Top events ⬍	
Detection of a Network Scan	1
Potential Corporate Privacy Violation	7
Misc activity	9
Attempted Information Leak	18
Unknown Traffic	78
Potentially Bad Traffic	507
Misc Attack	913
Attempted User Privilege Gain	2990

Severity	
Severity 1	2 997
Severity 2	1 438
Severity 3	88

Mitre Att&ck tactics	
Reconnaissance	0
Ressource_Development	0
Initial_Access	0
Execution	0
Persistence	0
Privilege_Escalation	0
Defense_Evasion	0
Credential_Access	0
Discovery	0
Lateral_Movement	0
Command_And_Control	0
Exfiltration	0
Impact	0
Other	4 523

Scalable solution

Qe-Secure includes one or more QESEC probes in communication with a QEMAN-NG server. This architecture makes it possible to centralize in one point the management of security events generated by several probes distributed over the infrastructure, and to adapt the monitoring configuration according to changes in the network.

Track down threats on their usual paths

QESEC probes are connected via traffic replication systems to critical arteries of the network infrastructure. They see and decode the traffic in which the threats hide, then they generate security events resulting from the application of analysis rules. They selectively extract files for analysis by the QEMAN-NG manager..

Accelerate research and understanding

The QEMAN-NG manager has a detection strategy management mechanism. This process makes it possible to concentrate the analytical work according to particular needs and contexts. With QEMAN-NG, the identification of the most critical events is instantaneous and their understanding is just as fast. The Qe-Mind artificial intelligence module makes it possible to generate security events even in the event of weak signals not detected by the rule engines. The graphical presentation of attack patterns saves significant time in analyzing situations.

Native SIEM support

Qe-Secure interfaces with IBM QRadar or Splunk in just a few clicks, as well as most third-party tools on the market. The events filtered or not by Qe-Secure are transmitted to the SIEM thus allowing a differentiated post-processing. However, the ergonomics and search resources offered by QEMAN-NG allow security teams to achieve a high level of efficiency even in the absence of SIEM..

France Cyber Security Label

The Qe-Secure solution has obtained the basic qualification of ANSSI for version 2.1.X, as well as the France Cyber Security label, in order to allow in particular Operators of Vital Importance to equip themselves as part of their implementation. compliance with the LPM. It can thus be implemented in particular with the replication products (TAP) of allentis already qualified as elementary by the ANSSI and with the traffic aggregators offered by allentis.

Long-term support

Allentis' unique experience in the deployment and support of large probe configurations allows it to benefit from comprehensive project support. From the study and architecture phase, then deployment, configuration and optimization to 24/7 maintenance and support, allentis provides its customers with the highest level of service. Every Qe-Secure user has direct access to allentis support.

MAIN FEATURES OF QE-SECURESECURE

Modular and scalable architecture Manager and Probes	√
Manager and Probes delivered turnkey hardware + integrated software + detection rules	√
Intuitive HMI - Display filtering by drilling on all the data presented (avoids the use of menus)	√
Securing roles (operator, remote administrator, local administrator)	√
Complete ruleset and source management from GUI	√
Management of rules by authorized operator from GUI	√
Up to 10 Gbps	√
Strategy detection management	√
Qe-Mind IA module	√
Graphical presentation of attack patterns	√
Intelligent event processing avoiding the use of a SIEM	√

ABOUT ALLENTIS

allentis is a French SME specializing in systems for monitoring the performance and security of data flow network exchanges. It has designed and manufactures QE flow analysis systems (Qe-Secure for threat detection, Qe-Streams and Qe-Flows for performance analysis and mapping of WAN, SD-WAN and LAN flows, Qe -Packets for massive data capture, Qualevent for business hypervision), and the TAPICS range of network components for traffic replication and isolation.

allentis
info@allentis.eu
www.allentis.eu