Note:

- Main FortiSIEM Documentation
- Open Ports and Protocols
- External Systems Configuration Guide
- Licensing

- we have `sizing` and `high availability` guide for 3 types of databases in FortiSIEM
  - ClickHouse - Fortinet guys was able to bring something in the middle - optimum performance and simple solution at the same time - `recommended option`, supported by Fortinet `100%`
  - EventDB - very simple solution, but its low performance
  - Elasticsearch - complex database solution, but it's very powerful - Supported partially by Fortinet

- FortiSIEM come in both hw & sw, only limitation is you can't install on your own hw.

- FortiSIEM was able to bring the NOC and SOC together because we don't need to contact as a SOC analyst, i don't need to contact the NOC to give me running configuration of a router or even if they are managing the firewall as from administration point of view, we don't need to contact the IT for that. because we already have `SSH` protocol used to discover my FortiGate.

- e.g., Fortinet FortiGate Firewall

What is Discovered and Monitored

Protocol	Information Discovered	Metrics collected	Used for
Netflow		Firewall traffic, application detection and application link usage metrics	Security monitoring and compliance, Firewall Link Usage and Application monitoring

Protocol	Information Discovered	Metrics collected	Used for
REST API	Host name, Model, Version, Interfaces, Serial Number, FortiAP and FortiSwitch managed by FortiGate.	Uptime, CPU, Memory and Disk utilization, Network Interface metrics, VPN metrics, Firewall Connection metrics FortiGate Security Fabric Discovery - Adjacent firewall Host name, Model, Version, Serial Number. Fortinet Security Fabric - Risk Rating Dashboard - Fabric root risk rating data FortiGate User Device Store Discovery - Discover FortiClient installed hosts passing through Firewalls.	Performance and Availability Monitoring
SNMP	Host name, Hardware model, Network interfaces, Operating system version	Uptime, CPU and Memory utilization, Network Interface metrics (utilization, bytes sent and received, packets sent and received, errors, discards and queue lengths). For 5xxx series firewalls, per CPU utilization (event PH_DEV_MON_FORTINET_PROCESSOR_USGE)	Availability and Performance Monitoring
Syslog	Device type	All traffic and system logs	Availability, Security and Compliance
SSH	Running configuration	Configuration Change	Performance Monitoring, Security and Compliance

- when an attack happening on some web server or on some asset, the attack will be either successful or unsuccessful
    - with classic SIEM solution, you only collect syslog about the events like from your IPS, for example, IPS triggered an attack against your apache server or ISS server. so you have only one side of story that the IPS tells you that there is a web attack against your web server. but you don't have other side of the story, whether the web server was impacted or not.
        - if you don't have the logs integrated of the web server, it will not tell the second part of the story, not have the logs about the CPU and memory usage, but if you have the metrics collected using `SNMP` about memory utilisation, so along side you can tell the full story. for example,
            - you get the attack against your web server and at the same time you see the sharp increase in the memory utilisation because you have `SNMP` discovery in

place. so both pieces of info can tell you that there is a successful attack. this is the beauty of bringing both SOC and NOC into FortiSIEM.