How to Streamline your SOC and Bridge Security Gap with SIEM

Nick Ng

Head of Systems Engineering

Fortinet, HK | Macau | Mongolia

- 2018 Cyber Range

- 2019 Video channel of "1 min technology dictionary"

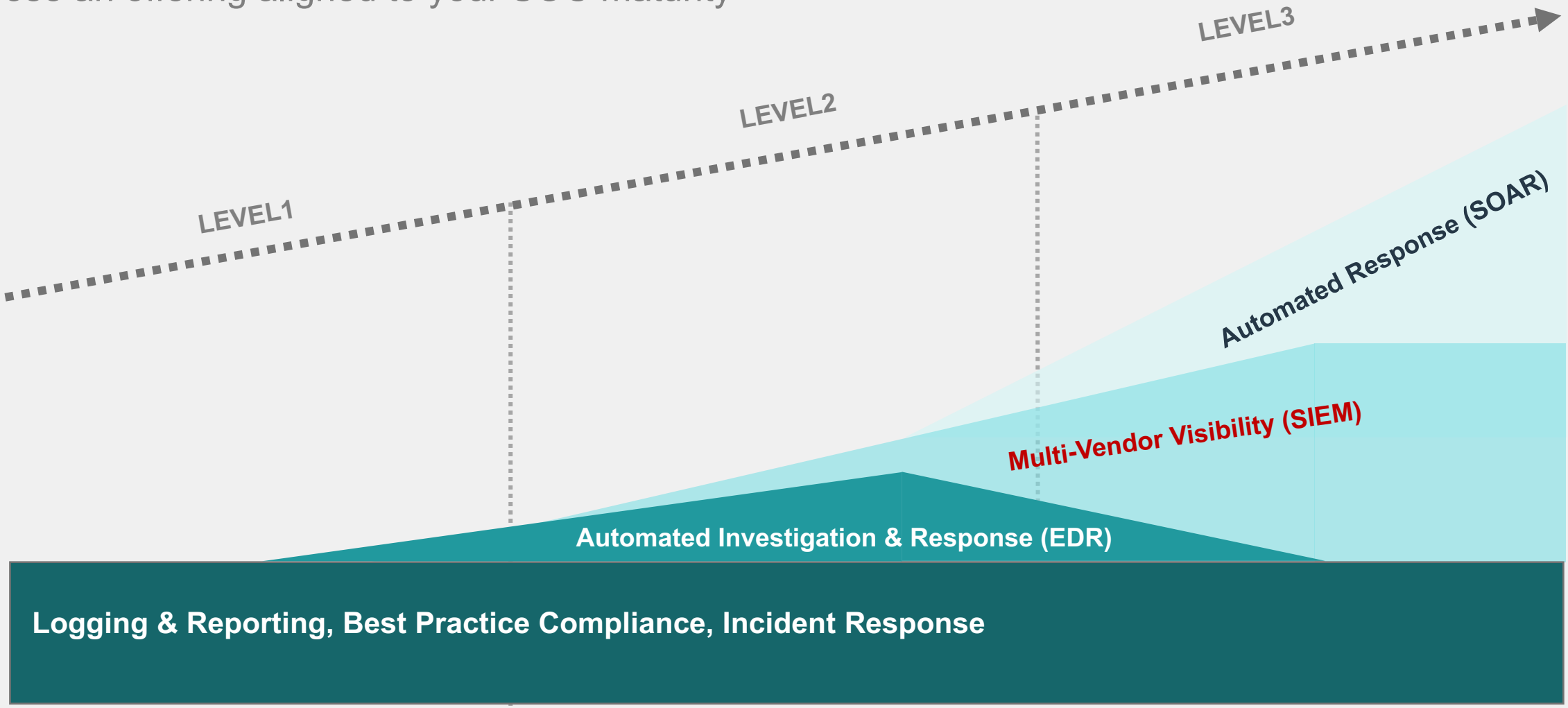
- 2021 CTF (capture the flag) competition

Nick NG

- Fortinet (NASDAQ:FTNT) Head of Systems Engineering
- CISA, CISSP, CEH, NSE8 (#003336) certified
- 15 years expertized Cyber Security

How to simplify Security Operations ?

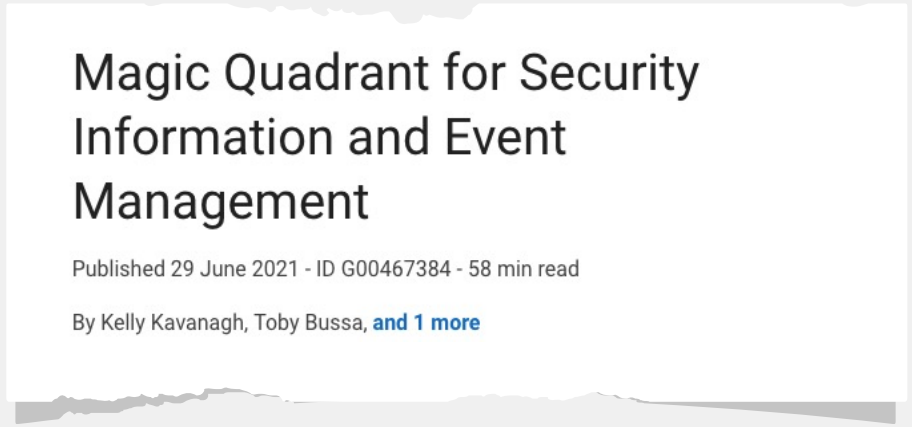
Choose an offering aligned to your SOC maturity



Ref: 2020 CISO Benchmark Study

Gartner says:

A proactive approach to Cybersecurity



"Security and risk management leaders increasingly want SIEM solutions with **attack detection, investigation, response and compliance capabilities**."

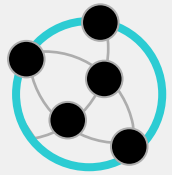
"Gartner defines this market as catering to customers' need to:

- **Collect security event logs and telemetry in real time for threat detection and compliance use cases.**
- **Analyze telemetry in real time and over time to detect attacks and other activities of interest.**
- **Investigate incidents to determine their potential severity and impact on a business..**"

SIEM solution Key Value to grow your business

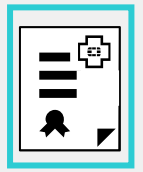
Scale-As-You-Grow

- Scale Out Architecture
- Scale Licensing



Unified Platform

- Reduce Complexity
- Virtual, HW and Cloud ready



Compliance Ready

- PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, SANS Critical Controls, COBIT, ITIL, ISO 27001, NERC, NIST800-53, NIST800-171, NESA

Improve Incident Detection

- Real-time Detection & UEBA
- Hunt Threats
- Compliance Monitoring

Reduce Incident Impact

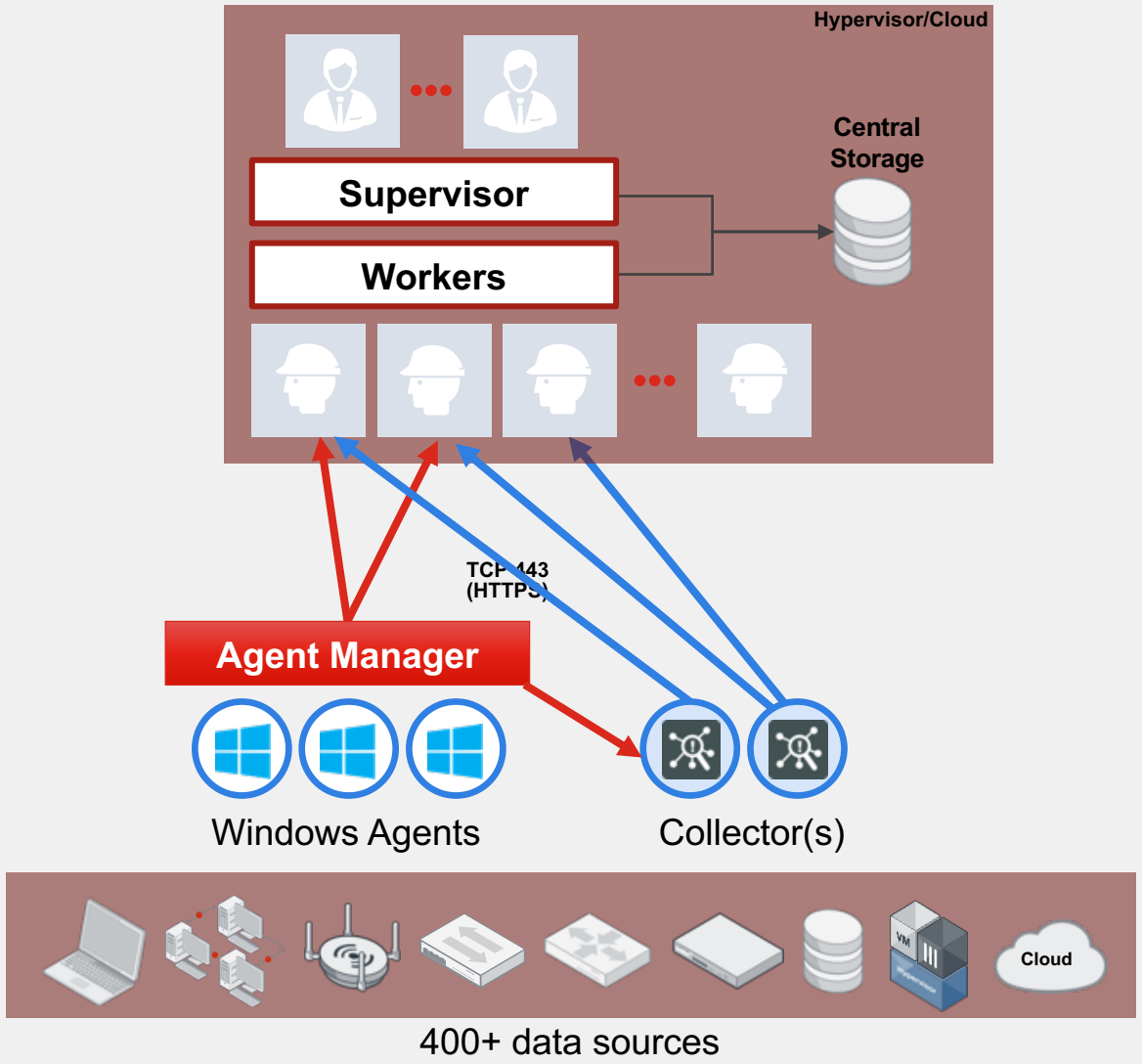
- Reduce MTTR
- Automate Responses
- Central Case management

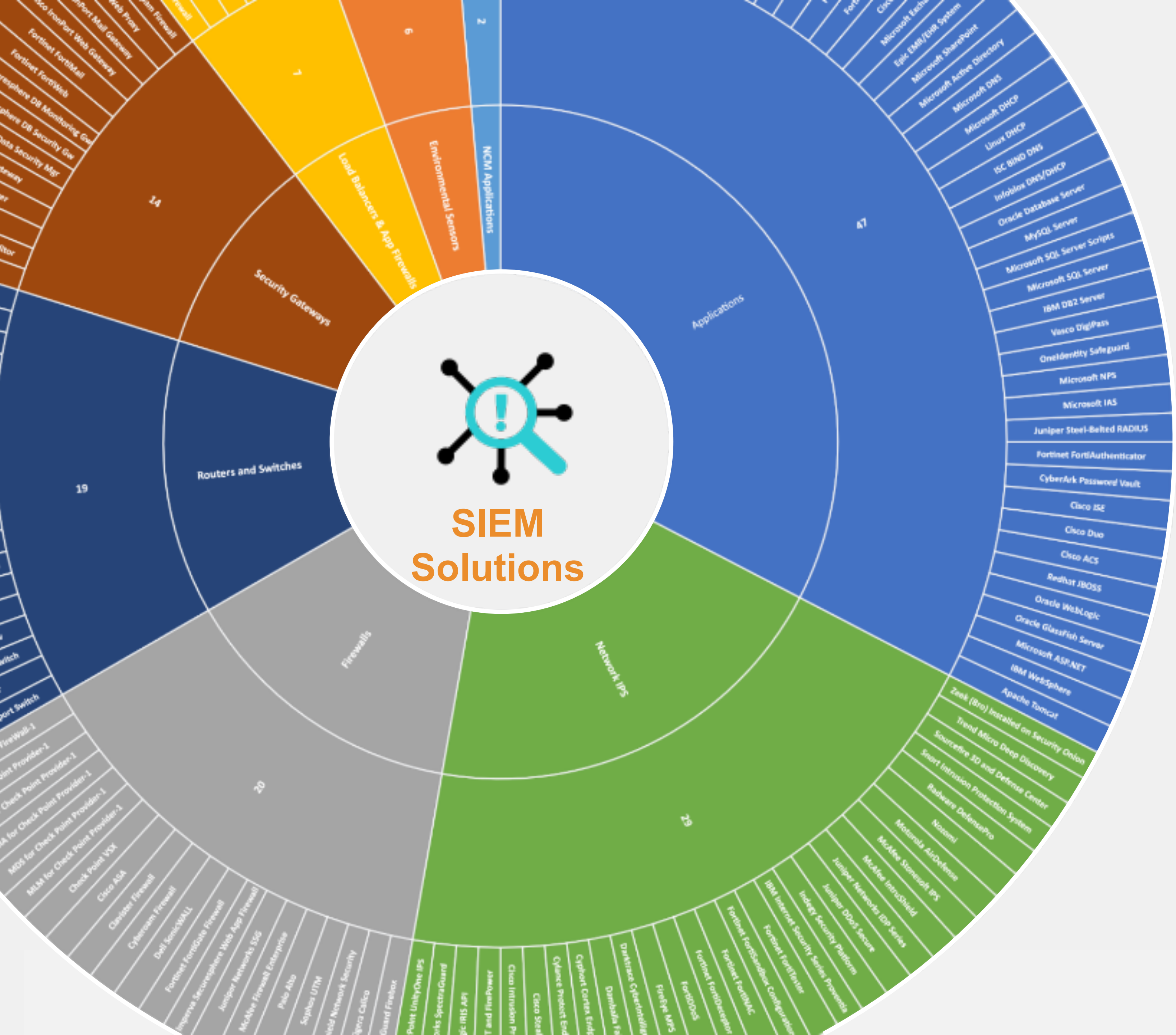
Single Pane of Glass

- Unify NOC & SOC functions
- Comprehensive CMDB
- Performance and Security Monitoring

Rapid Scale Architecture

- **Support Virtual Appliance (VA)**
  - Private hypervisor and public cloud
- **Architecture Components**
  - **Supervisors**
    - Web Server, Application Server and Database Server tiers and serving the GUI
  - **Workers**
    - Perform analytics on their view of the data.
    - Real-time search, Historical search, etc
  - **Collector(s)**
    - Parses the collected data
  - **Windows Agent(s) and Manager(s)**
    - More Granular monitoring





How to Streamline your SOC

- Unify your NOC & SOC
- Supports handful reporting & compliance.
- Custom parsers can be created to support even more.

Combined SOC & NOC Analytics

Solving the SOC Visibility Puzzle

Performance Metrics

CPU

Memory

Storage

Uptime

Services

Interface Utilization

Security Events

Web Application

AAA Server

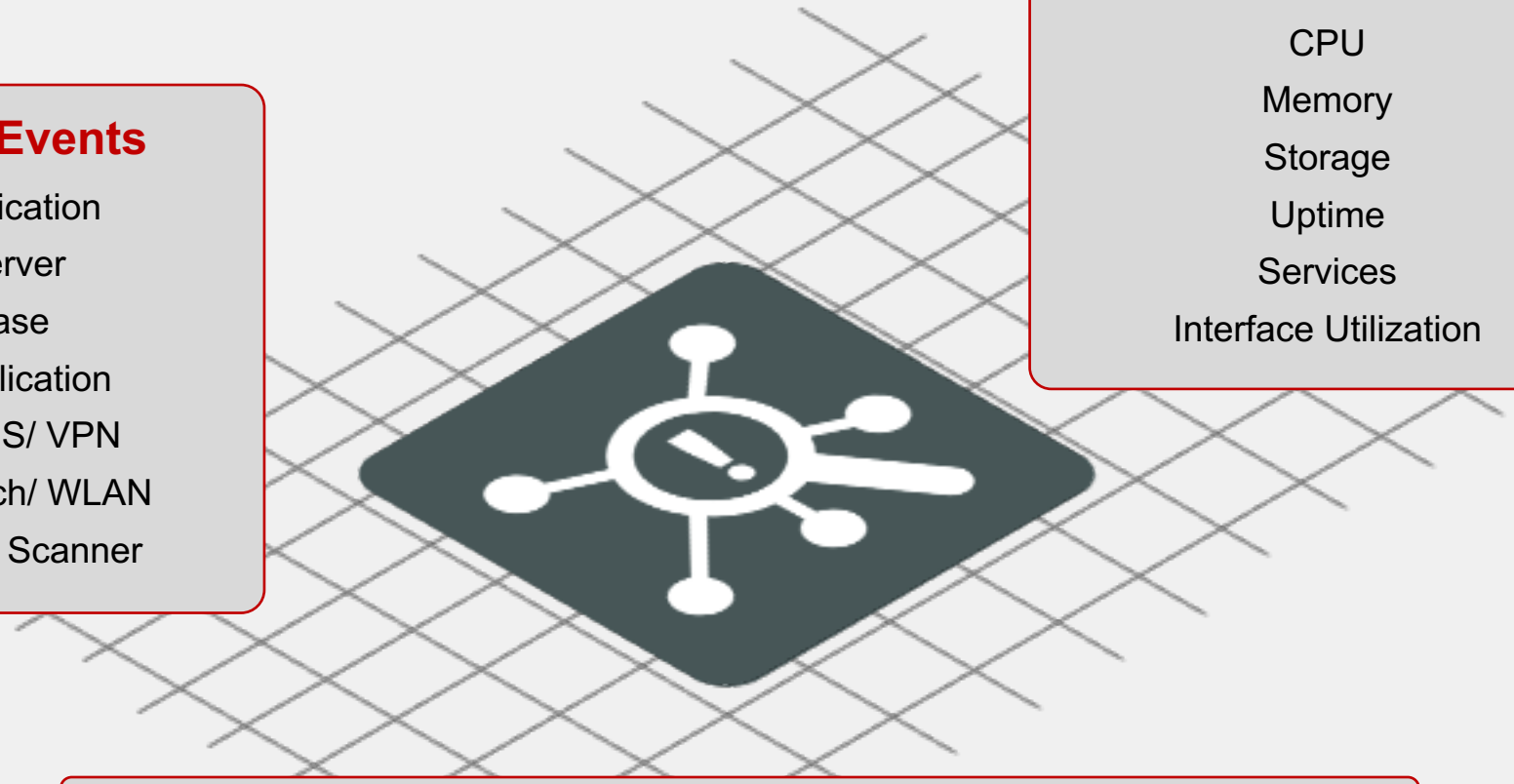
Database

Cloud Application

Firewall/ IPS/ VPN

Router/ Switch/ WLAN

Vulnerability Scanner

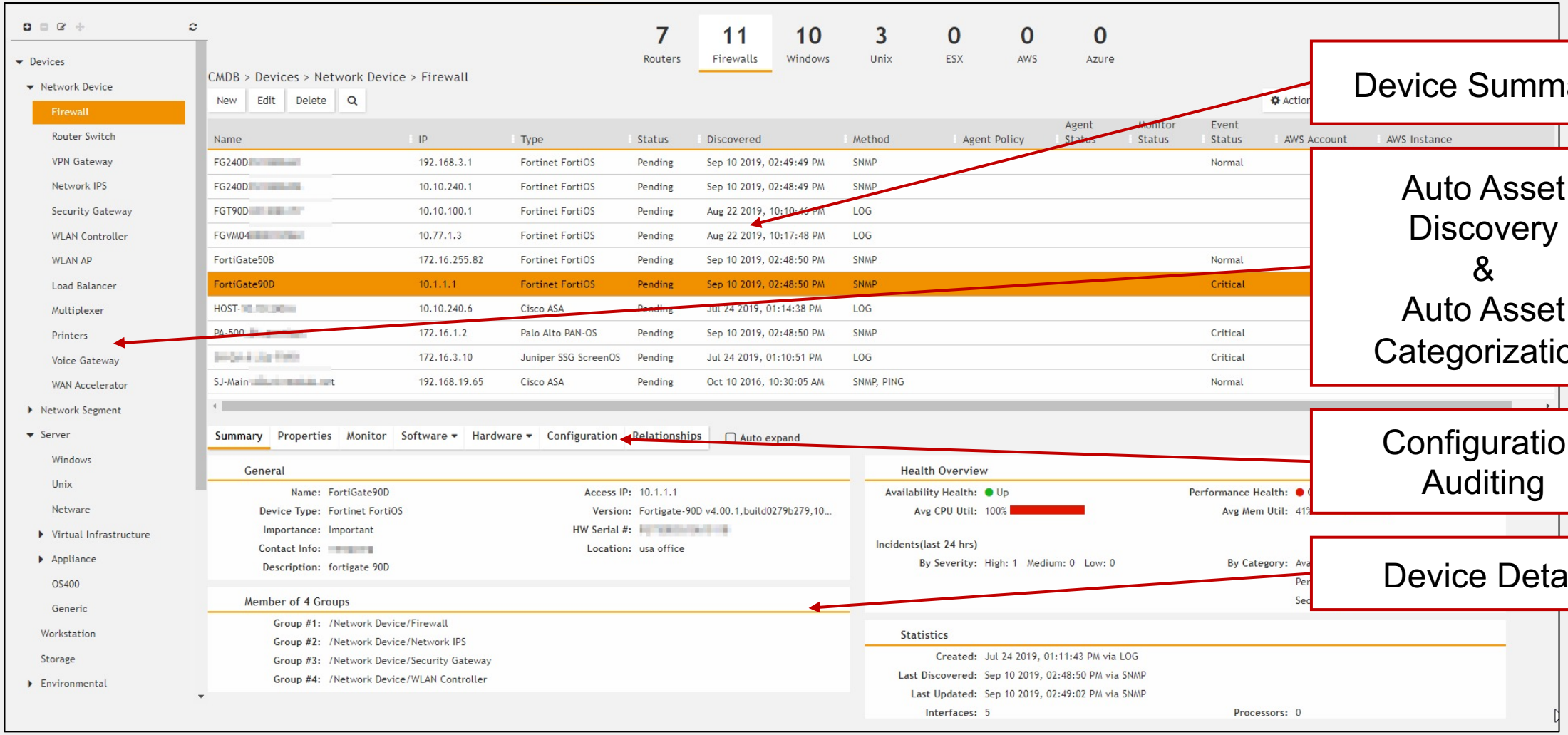


Combined SOC & NOC

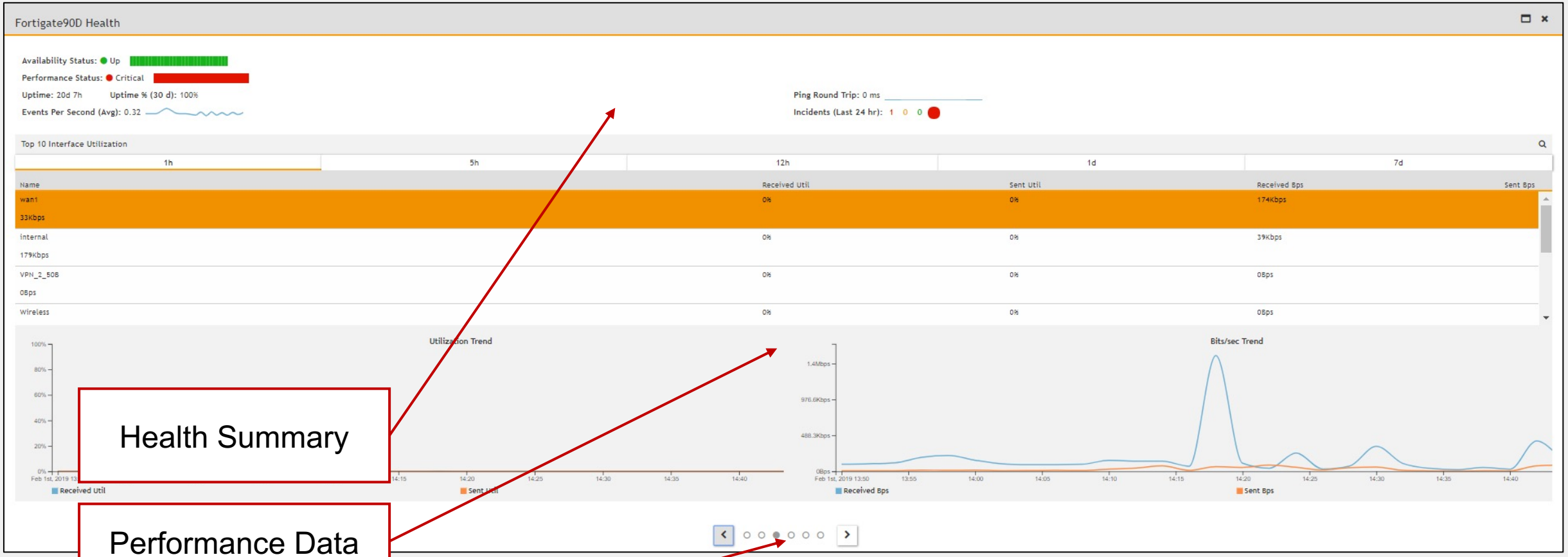
Integrated CMDB | Threat Intelligence

Increased Functionality | Increased Visibility | Reduced Time to Respond

1. CMDB (Configuration Management Database)



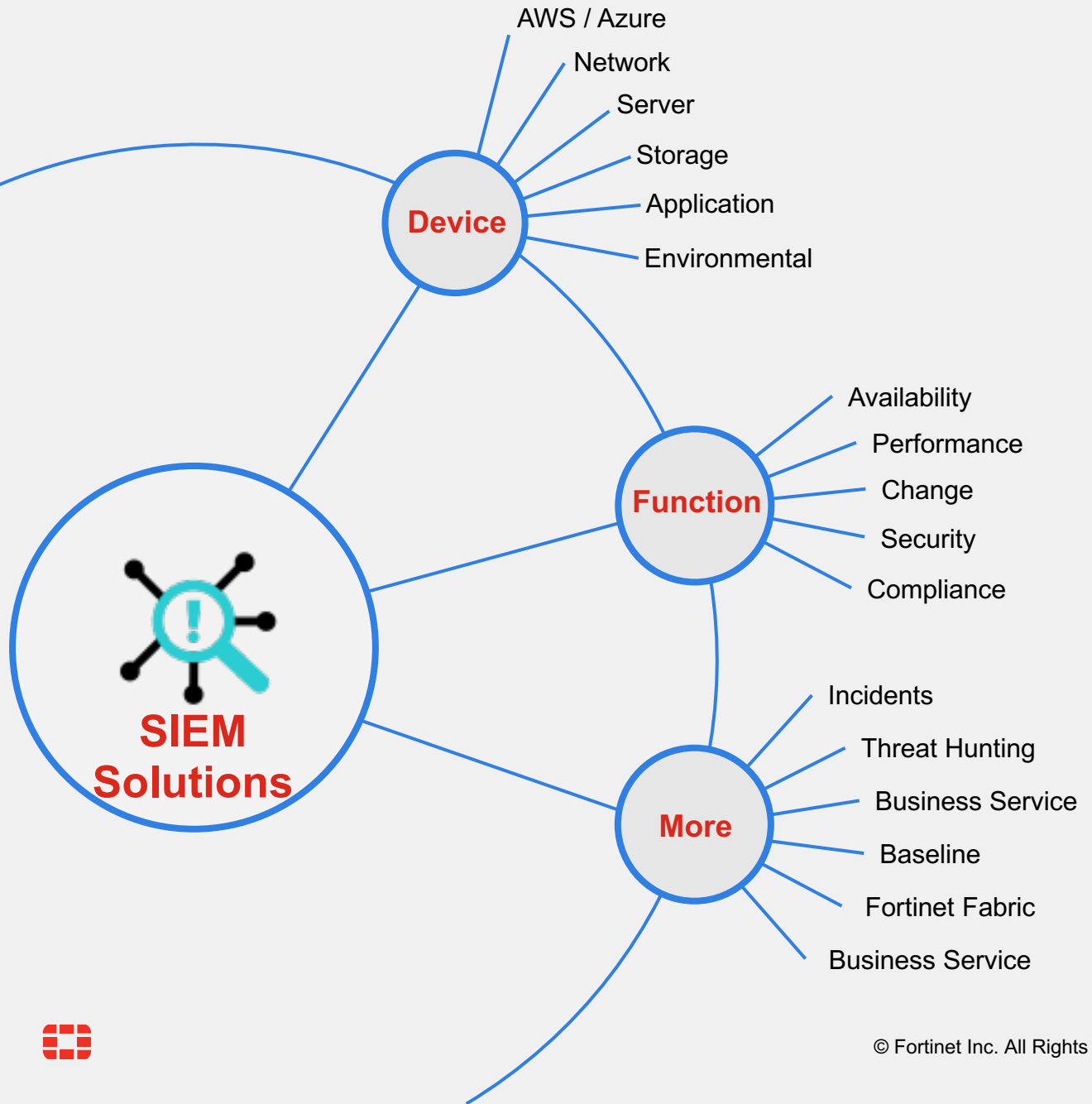
CMDB Performance and Availability Monitoring



Health Summary

Performance Data

Additional Data



2. Reporting

Should come with built-in reports covering

- Security
- Performance
- Availability
- Compliance

Require custom reports and features an inbuilt report designer

PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, SANS Critical Controls, COBIT, ITIL, ISO 27001, NERC, NIST800-53, NIST800-171, NESA

SIEM Security Analytics Platform

Accelerate Threat Detection and Incident Response

Collect & Normalize → Classify & Enrich → Detect & Correlate → Investigate & Respond

Collect

Automatic Discovery
- Servers
- Devices
- Endpoints
- Users
- Applications

State Monitoring
- Hardware / OS Configs
- User / Identity Mapping
- File Integrity Monitoring
- Vulnerability Assessment
- Business Services Impact

Detect

Performance Monitoring
- Availability & Performance Summary
- Uptime & Round Trip Response
- CPU and Memory
- Network Interface Utilization
- Synthetic Transaction

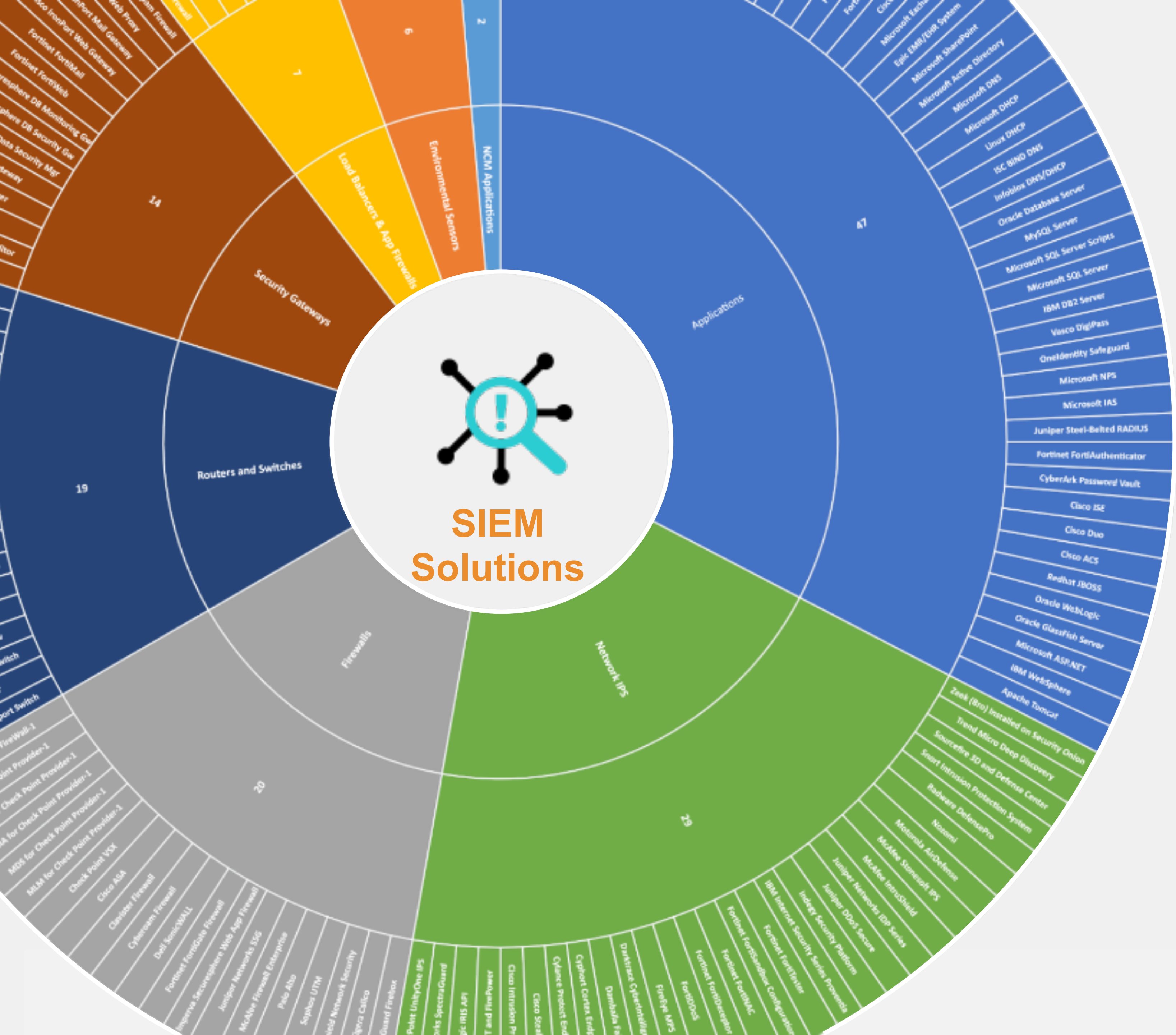
Risk Monitoring
- Device Risk Score
- Threat Intelligence
- Geolocation
- SLA & Escalation
- False Positive Reduction

Behavioral Analytics
- User
- Device
- Service / App Logs
- Network Logs
- Network Flow

Respond

Investigation
- Incident Dashboards
- MITRE ATT&CK
- Threat Hunting
- Multi-User Case Management
- Multitenant & Granular RBAC

Response
- External Ticket Integration
- Automated Response Actions
- FortiSOAR Playbooks & Workflows
- Case Notes & Timeline
- Reporting



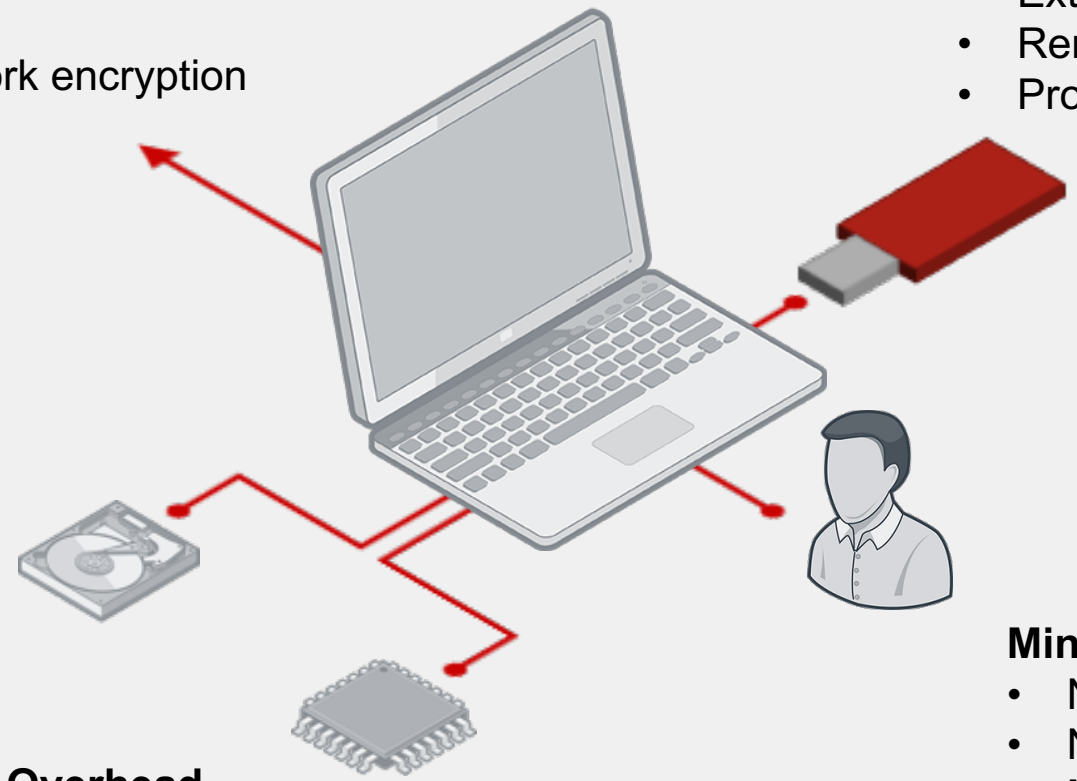
Bridge the security gap with end user existing devices

1. UEBA
2. MITRE ATT&CK
3. Threat Intelligence

1. UEBA (User and entity behavior analytics)

Activity logged on the host
- Increases visibility
- Logged before network encryption
- See file name details

Detailed Endpoint Visibility
- Extensive file access logging
- Removable media use
- Program and process use

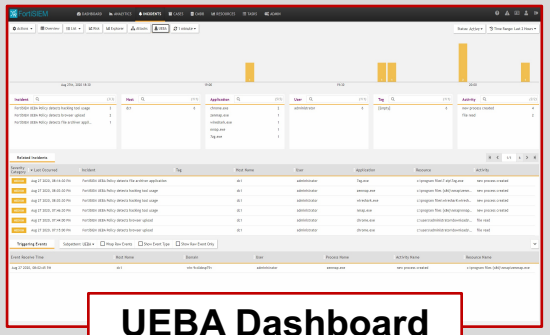


Off-net Client Visibility
- Off-line data caching
- Upload to public collector

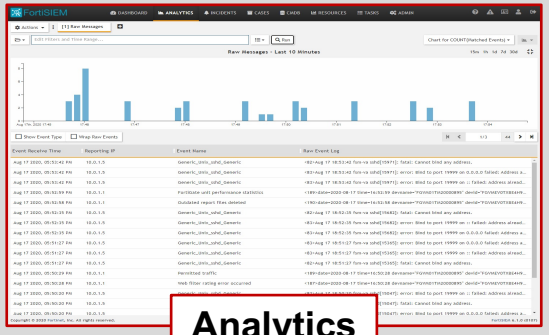
Minimally Invasive Solution
- No screen or keystroke logging
- No detailed web activity logging
- Minimal performance impact

Low Client Overhead
- Approx. 1% CPU use
- All analysis performed by FortiSIEM

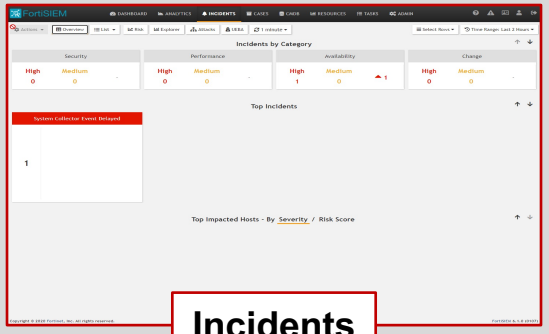
UEBA: Log & Endpoint Visibility



UEBA Dashboard

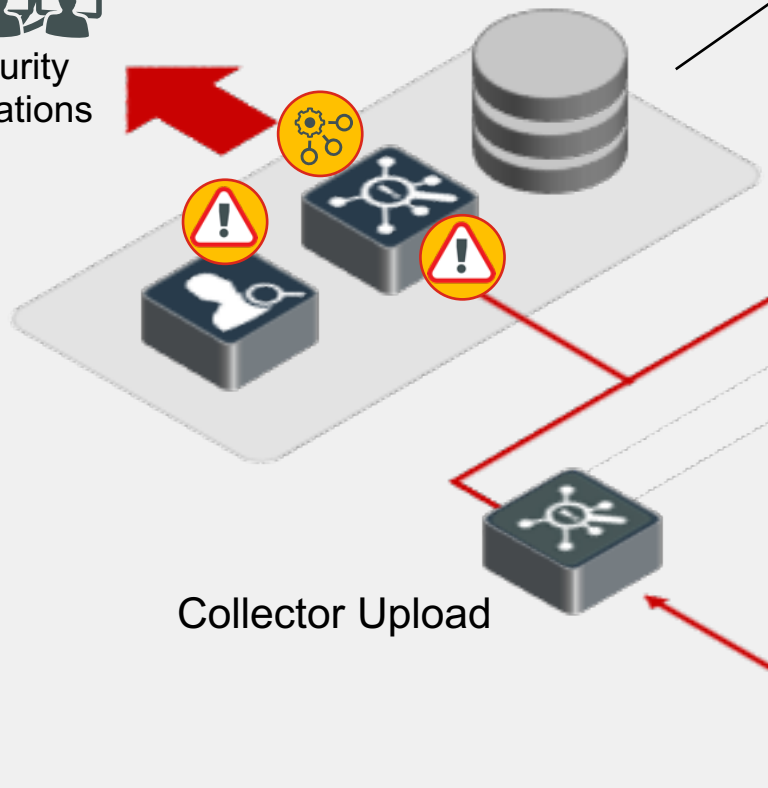


Analytics



Incidents

Security Operations



UEBA Engine
Correlation Engine
Event database

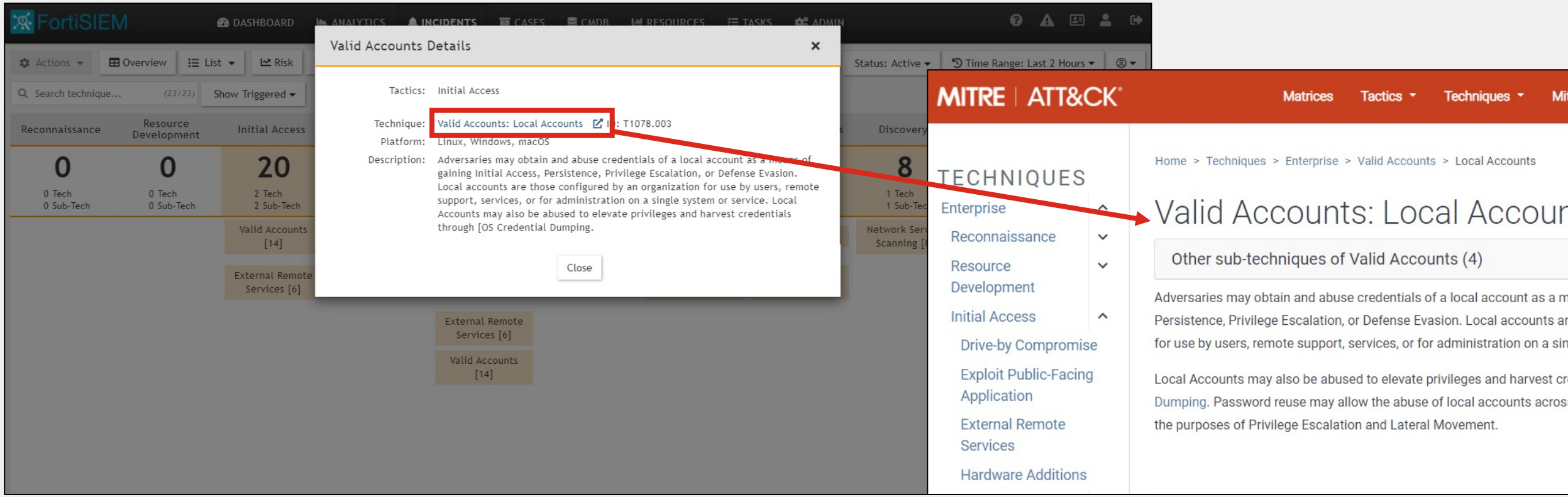
Collector Upload

UEBA Agent

User
Process
Device
Resource
Behavior

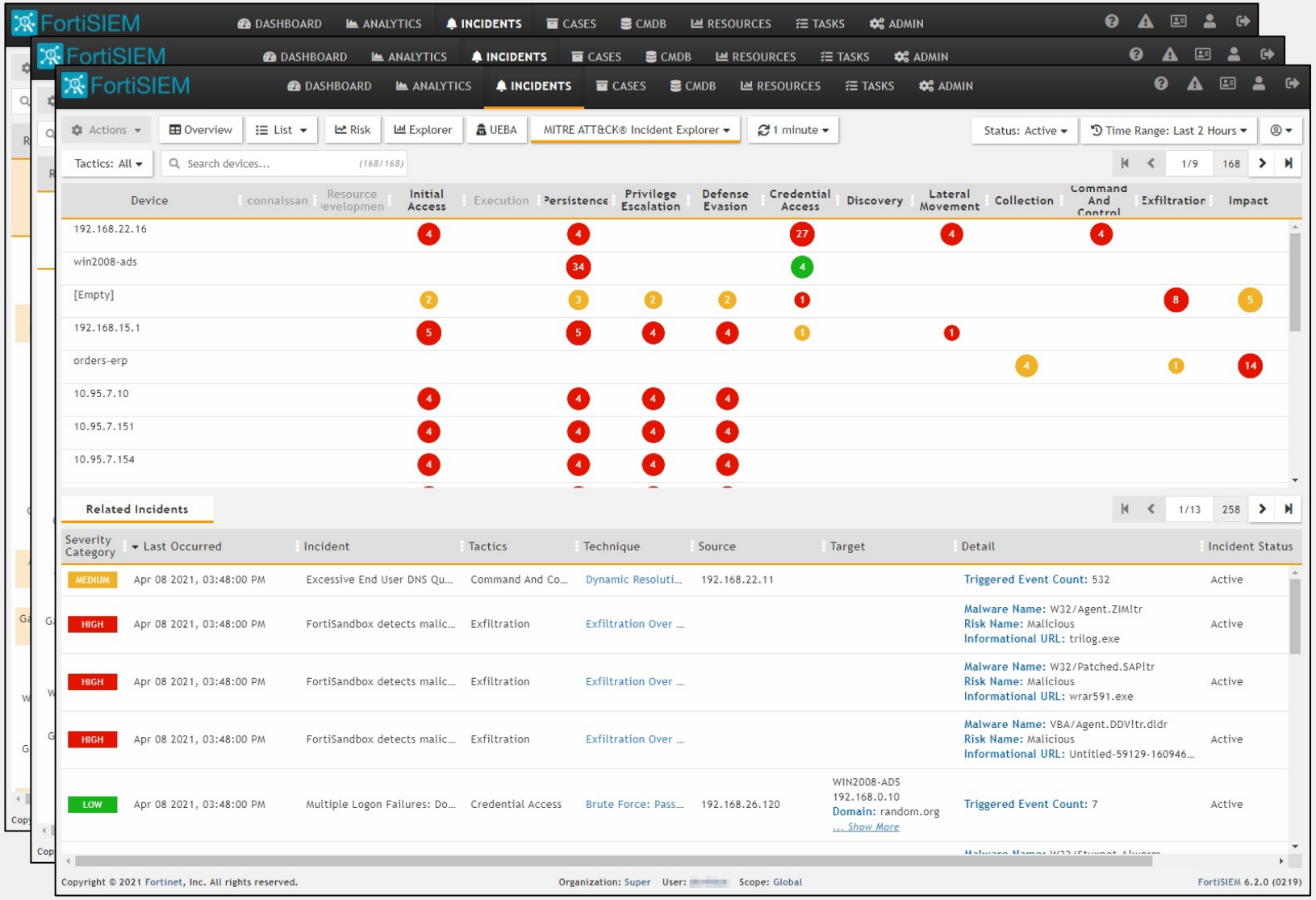
2. MITRE ATT&CK® Data

- Access top level ATT&CK data from within SIEM solution
- Pivot directly to MITRE ATT&CK® for additional information



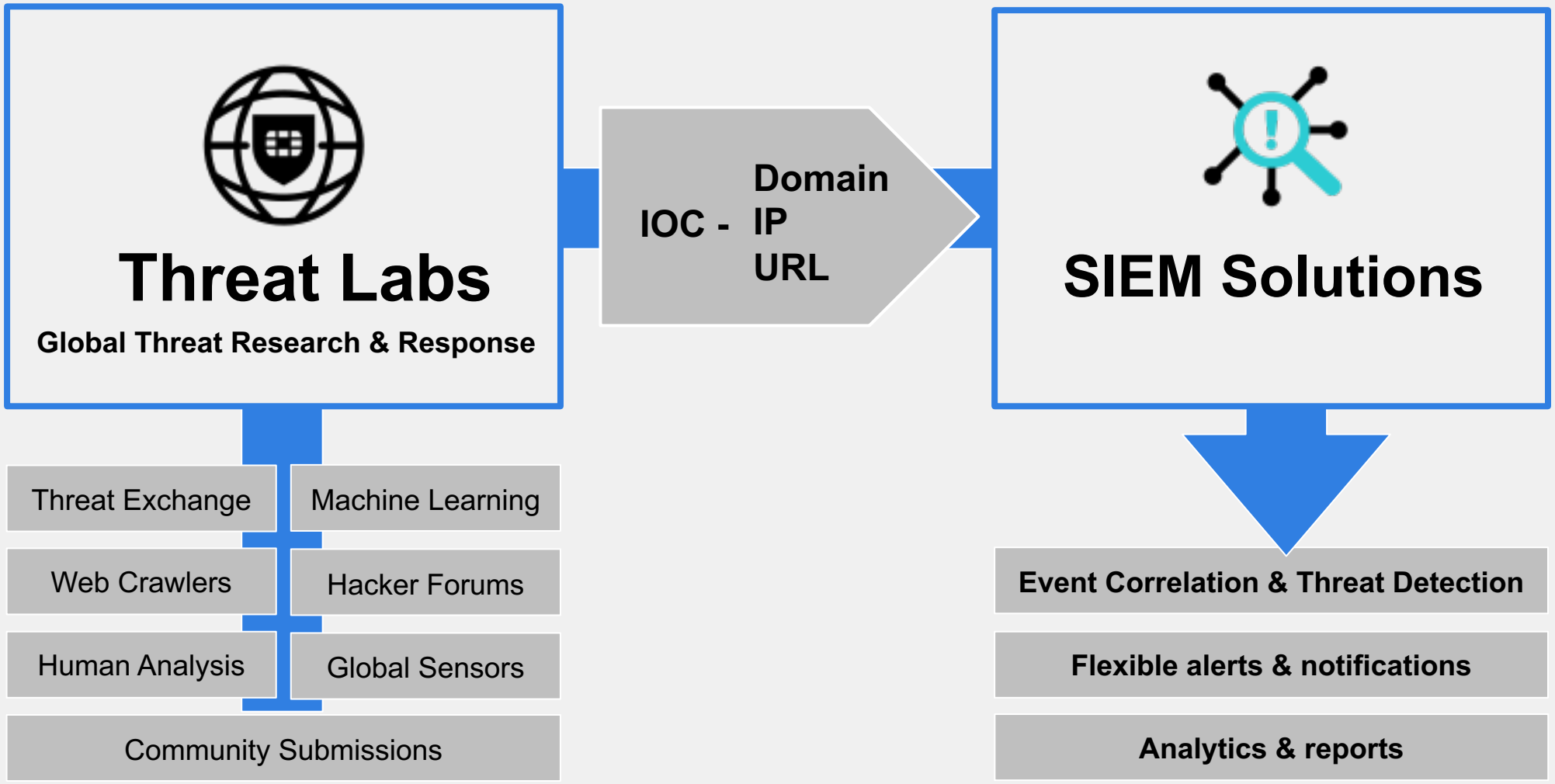
MITRE ATT&CK Dashboards

- Rule Coverage dashboard shows MITRE ATT&CK coverage
- Incident Coverage Dashboard shows corresponding incidents
- Incident Explorer shows host centric, interactive ATT&CK view



3. Global Threat Intelligence

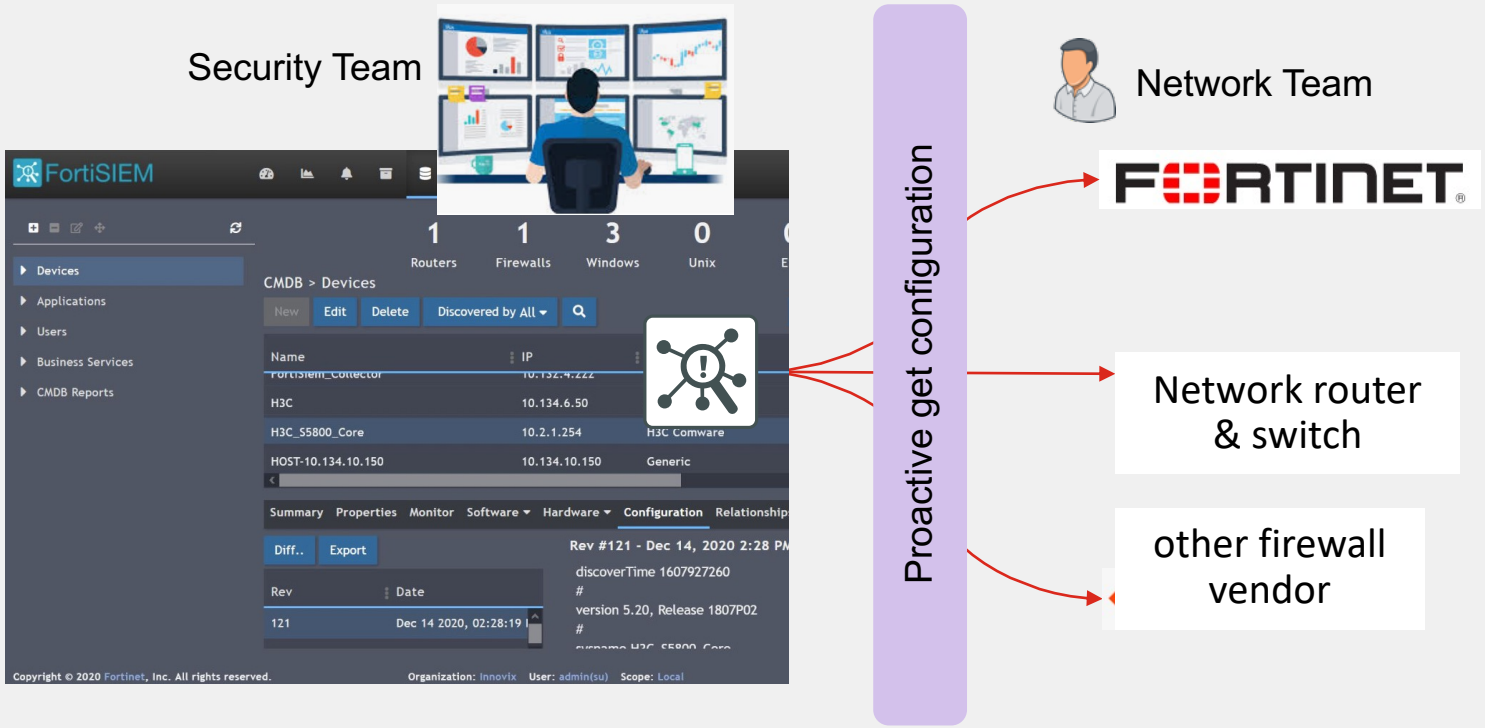
Build intelligence on dummy systems



Use Case sharing: An Insurance Company

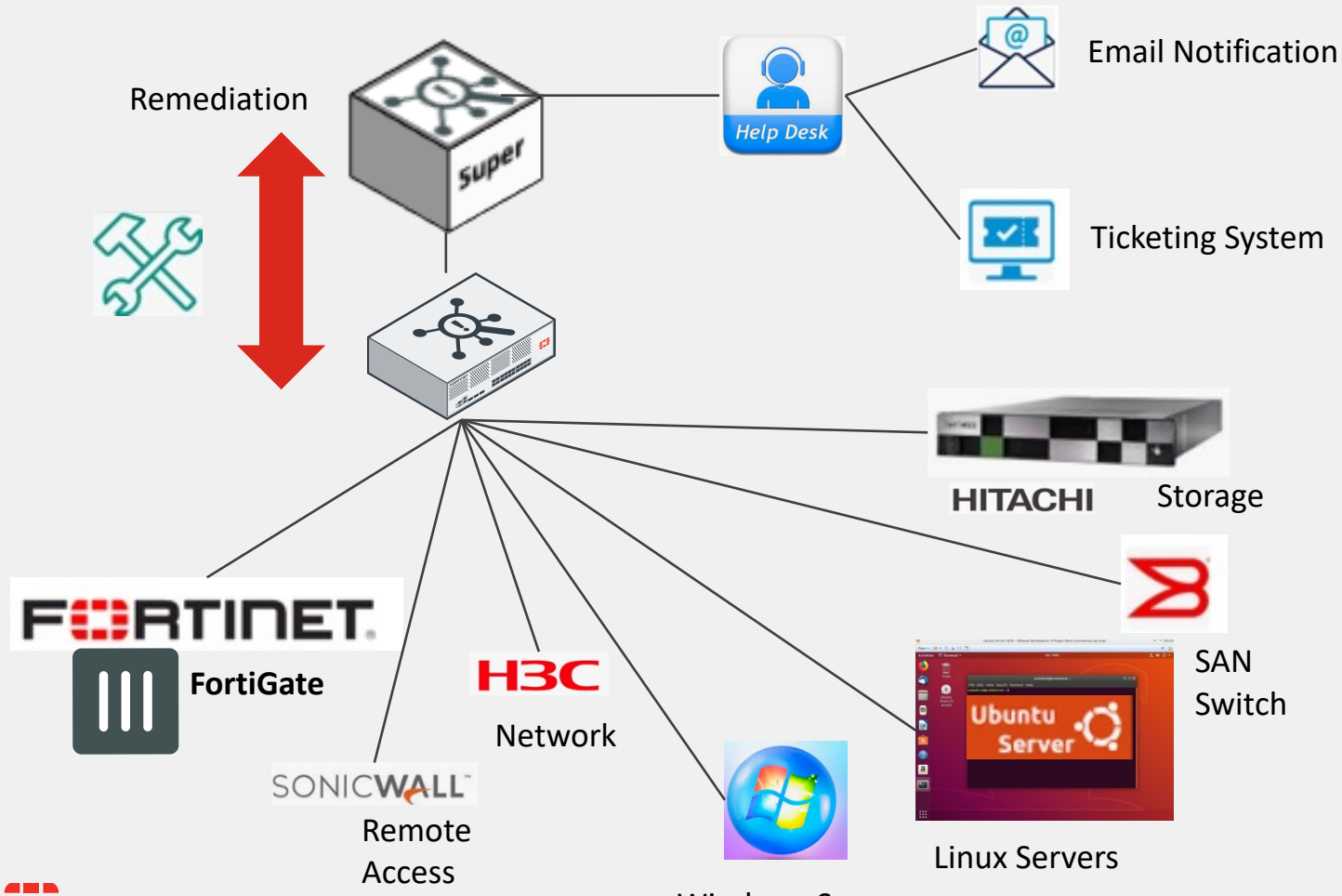
Use Case: Compliance, configuration audit

- Insurance authority customized dashboard & report
- Security team require proactive configuration monitor and backup
- Diff the changes in certain period
- Fast deploy within half month time frame

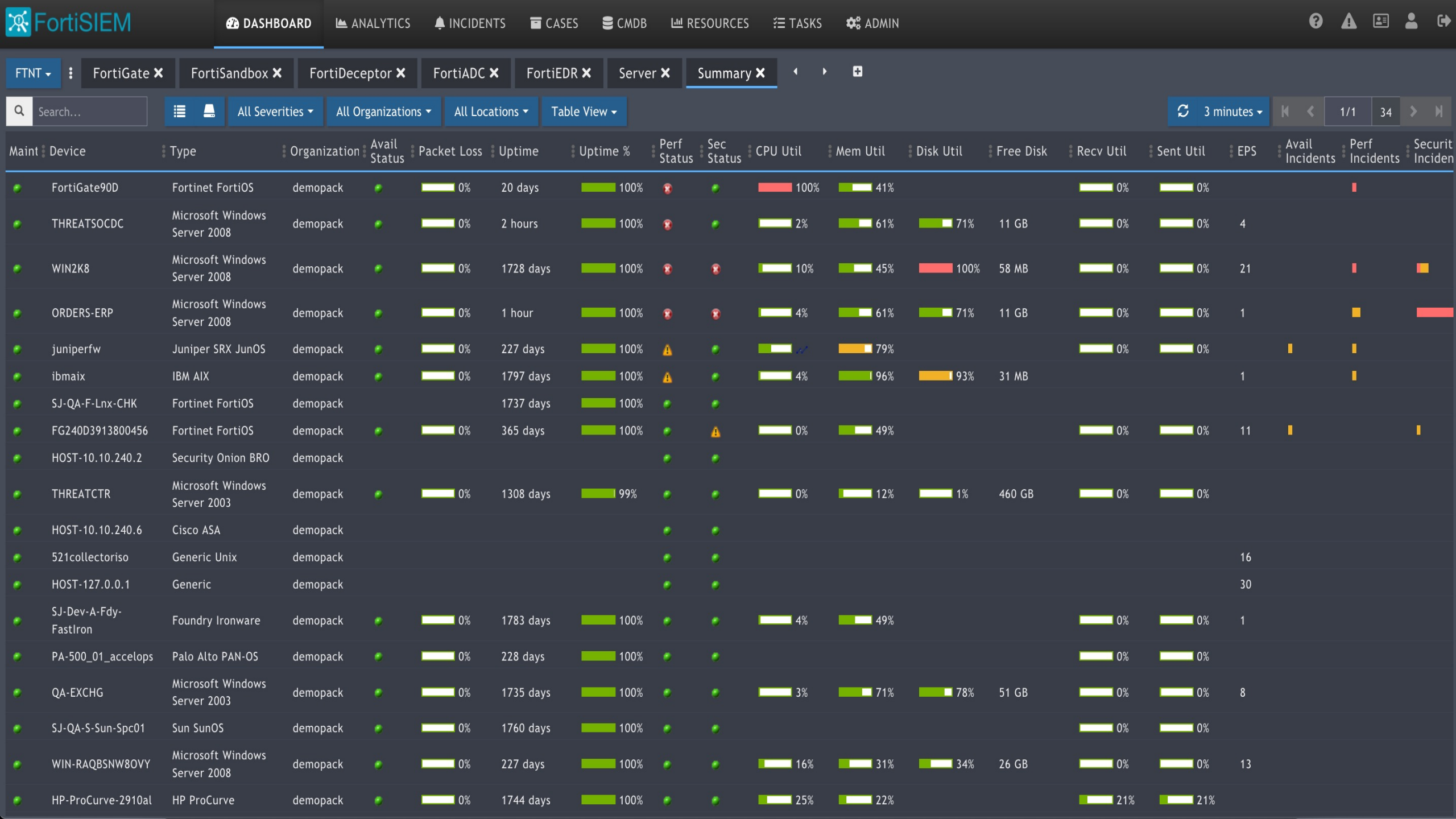


Use Case sharing: A government department

Use Case: Government regulation, threat intelligence, reporting



- Customizable dashboard for compliance
- Support custom parser extension eg. Hitachi storage
- Enrich network security FortiGuard threat intelligence
- Utilize ticketing system as helpdesk


FortiSIEM
DASHBOARD
ANALYTICS
INCIDENTS
CASES
CMDB
RESOURCES
TASKS
ADMIN
FTNT
FortiGate
FortiSandbox
FortiDeceptor
FortiADC
FortiEDR
Server
Summary
Search...
All Severities
All Organizations
All Locations
Table View
3 minutes
1/1
34
Maint
Device
Type
Organization
Avail Status
Packet Loss
Uptime
Uptime %
Perf Status
Sec Status
CPU Util
Mem Util
Disk Util
Free Disk
Recv Util
Sent Util
EPS
Avail Incidents
Perf Incidents
Securit Inciden
FortiGate90D
Fortinet FortiOS
demopack
0%
20 days
100%
100%
41%
0%
0%
THREATSOCDC
Microsoft Windows Server 2008
demopack
0%
2 hours
100%
2%
61%
71%
11 GB
0%
0%
4
WIN2K8
Microsoft Windows Server 2008
demopack
0%
1728 days
100%
10%
45%
100%
58 MB
0%
0%
21
ORDERS-ERP
Microsoft Windows Server 2008
demopack
0%
1 hour
100%
4%
61%
71%
11 GB
0%
0%
1
juniperfw
Juniper SRX JunOS
demopack
0%
227 days
100%
79%
0%
0%
ibmaix
IBM AIX
demopack
0%
1797 days
100%
4%
96%
93%
31 MB
1
SJ-QA-F-Lnx-CHK
Fortinet FortiOS
demopack
1737 days
100%
FG240D3913800456
Fortinet FortiOS
demopack
0%
365 days
100%
0%
49%
0%
0%
11
HOST-10.10.240.2
Security Onion BRO
demopack
THREATCTR
Microsoft Windows Server 2003
demopack
0%
1308 days
99%
0%
12%
1%
460 GB
0%
0%
HOST-10.10.240.6
Cisco ASA
demopack
521collectoriso
Generic Unix
demopack
16
HOST-127.0.0.1
Generic
demopack
30
SJ-Dev-A-Fdy-FastIron
Foundry Ironware
demopack
0%
1783 days
100%
4%
49%
0%
0%
1
PA-500_01_accelops
Palo Alto PAN-OS
demopack
0%
228 days
100%
0%
0%
QA-EXCHG
Microsoft Windows Server 2003
demopack
0%
1735 days
100%
3%
71%
78%
51 GB
0%
0%
8
SJ-QA-S-Sun-Spc01
Sun SunOS
demopack
0%
1760 days
100%
0%
0%
WIN-RAQBSNW8OVY
Microsoft Windows Server 2008
demopack
0%
227 days
100%
16%
31%
34%
26 GB
0%
0%
13
HP-ProCurve-2910al
HP ProCurve
demopack
0%
1744 days
100%
25%
22%
21%
21%

Key Tips to Better use your SIEM

Predictable License
(Not Storage size)

Threat Enrichment
Powered-by word-class FortiGuard AI threat intel.

Single Visibility Platform
Security + configuration
+ performance
+ business availability

Unifying UBEA
Combining factor of network, flow, agent info


FORTINET