



# 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

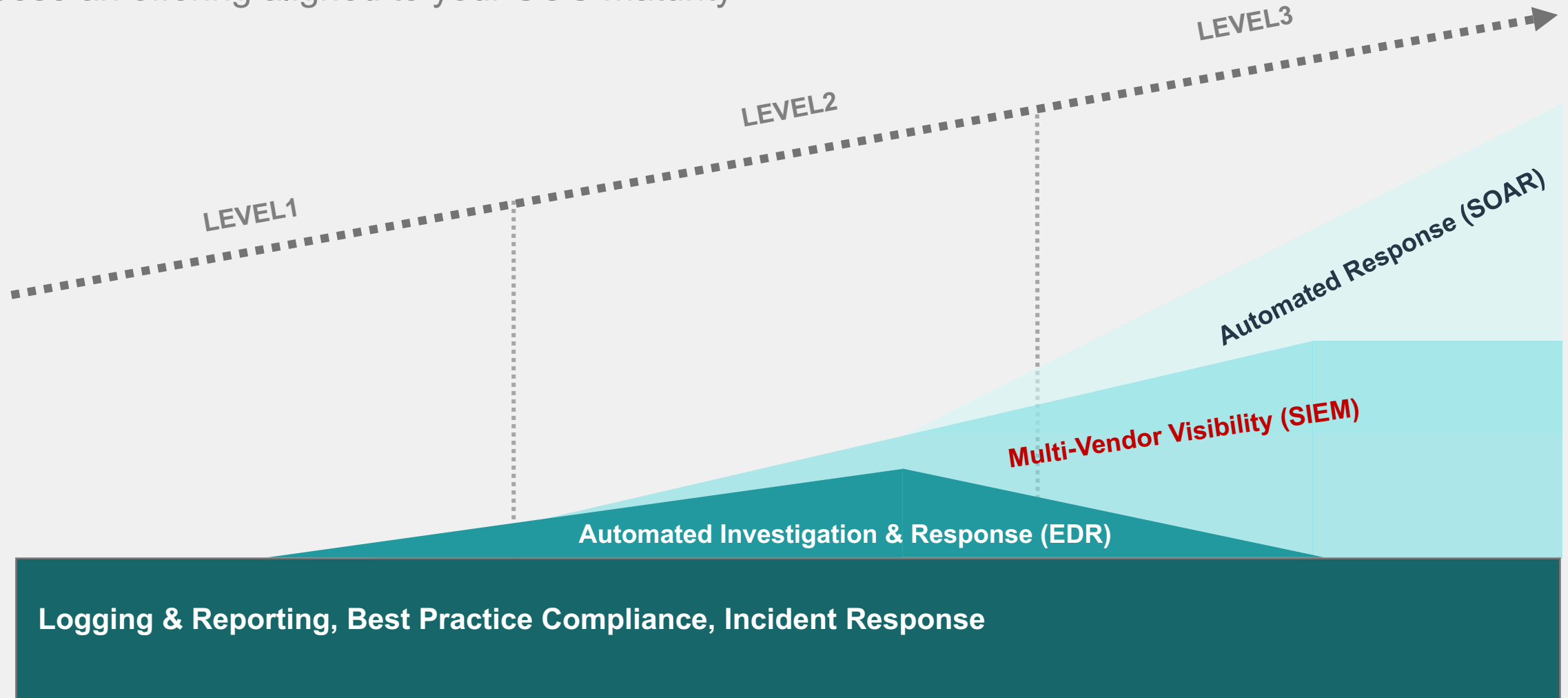
## Nick NG

- 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



# Gartner says:

A proactive approach to Cybersecurity

## Magic Quadrant for Security Information and Event Management

Published 29 June 2021 - ID G00467384 - 58 min read

By Kelly Kavanagh, Toby Busa, [and 1 more](#)

“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..”**

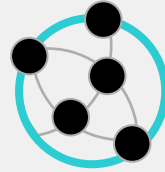


# SIEM solution Key Value to grow your business



## 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



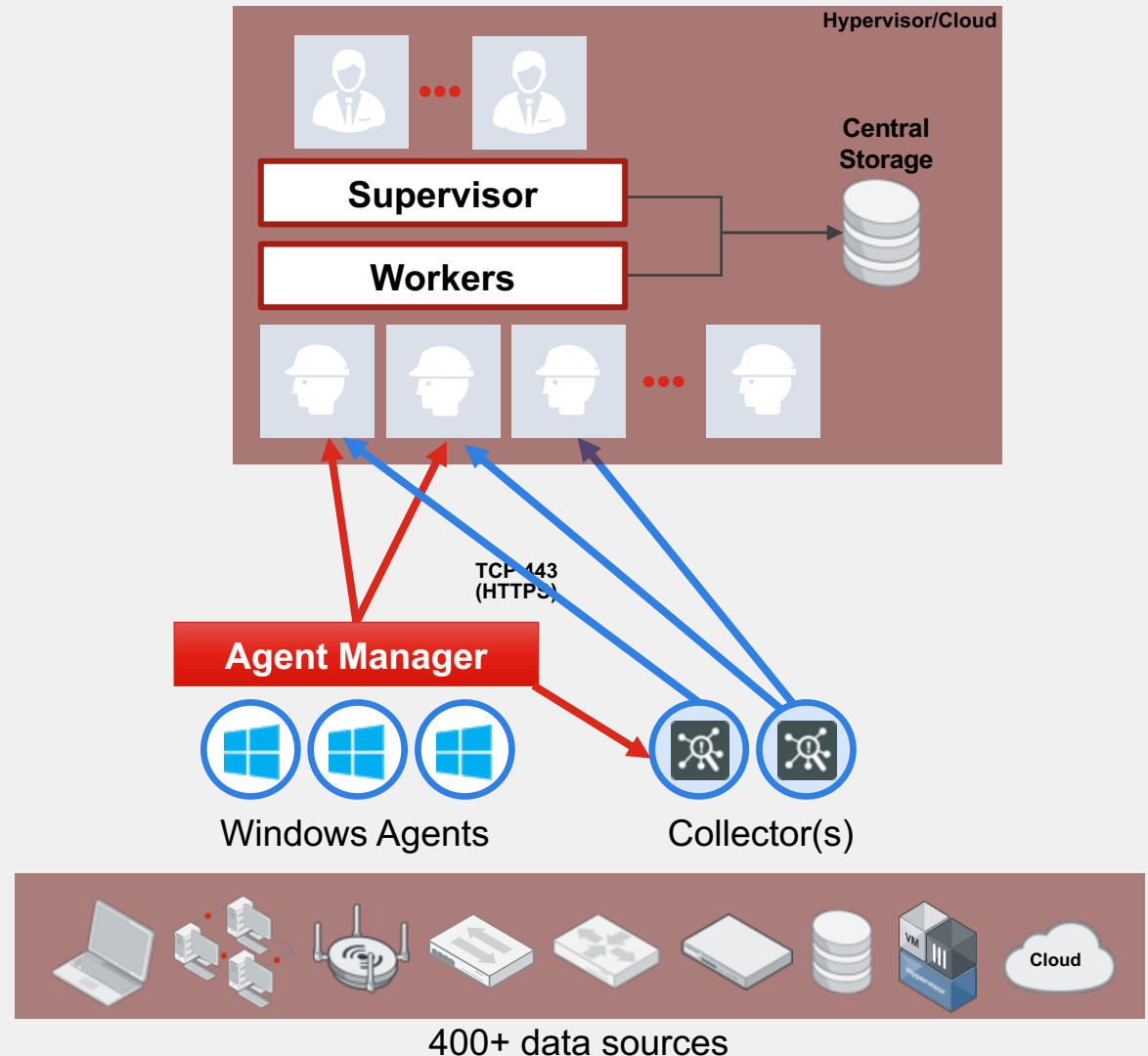
## Single Pane of Glass

- 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





# Combined SOC & NOC Analytics

## Solving the SOC Visibility Puzzle

### Security Events

Web Application  
AAA Server  
Database  
Cloud Application  
Firewall/ IPS/ VPN  
Router/ Switch/ WLAN  
Vulnerability Scanner

### Performance Metrics

CPU  
Memory  
Storage  
Uptime  
Services  
Interface Utilization



### Combined SOC & NOC

Integrated CMDB | Threat Intelligence  
Increased Functionality | Increased Visibility | Reduced Time to Respond





# 1. CMDB (Configuration Management Database)

The screenshot displays the Fortinet CMDB interface. At the top, a summary bar shows counts for various device types: 7 Routers, 11 Firewalls (highlighted), 10 Windows, 3 Unix, 0 ESX, 0 AWS, and 0 Azure. The left sidebar shows a navigation tree with 'Firewall' selected under 'Network Device'. The main area shows a table of firewalls with columns for Name, IP, Type, Status, Discovered, Method, Agent Policy, Agent Status, Monitor Status, Event Status, AWS Account, and AWS Instance. The 'FortiGate90D' device is highlighted in orange. Below the table, the 'Summary' tab is active, showing details for the selected device. The 'Health Overview' section shows 'Availability Health: Up' and 'Performance Health: Critical'. The 'Statistics' section shows creation and discovery dates and methods.

Name	IP	Type	Status	Discovered	Method	Agent Policy	Agent Status	Monitor Status	Event Status	AWS Account	AWS Instance
FG240D	192.168.3.1	Fortinet FortiOS	Pending	Sep 10 2019, 02:49:49 PM	SNMP				Normal		
FG240D	10.10.240.1	Fortinet FortiOS	Pending	Sep 10 2019, 02:48:49 PM	SNMP						
FGT90D	10.10.100.1	Fortinet FortiOS	Pending	Aug 22 2019, 10:10:16 PM	LOG						
FGVM04	10.77.1.3	Fortinet FortiOS	Pending	Aug 22 2019, 10:17:48 PM	LOG						
FortiGate50B	172.16.255.82	Fortinet FortiOS	Pending	Sep 10 2019, 02:48:50 PM	SNMP				Normal		
<b>FortiGate90D</b>	<b>10.1.1.1</b>	<b>Fortinet FortiOS</b>	<b>Pending</b>	<b>Sep 10 2019, 02:48:50 PM</b>	<b>SNMP</b>				<b>Critical</b>		
HOST-10	10.10.240.6	Cisco ASA	Pending	Jul 24 2019, 01:14:38 PM	LOG						
PA-500	172.16.1.2	Palo Alto PAN-OS	Pending	Sep 10 2019, 02:48:50 PM	SNMP				Critical		
FW-01	172.16.3.10	Juniper SSG ScreenOS	Pending	Jul 24 2019, 01:10:51 PM	LOG				Critical		
SJ-Main	192.168.19.65	Cisco ASA	Pending	Oct 10 2016, 10:30:05 AM	SNMP, PING				Normal		

**Device Summary**

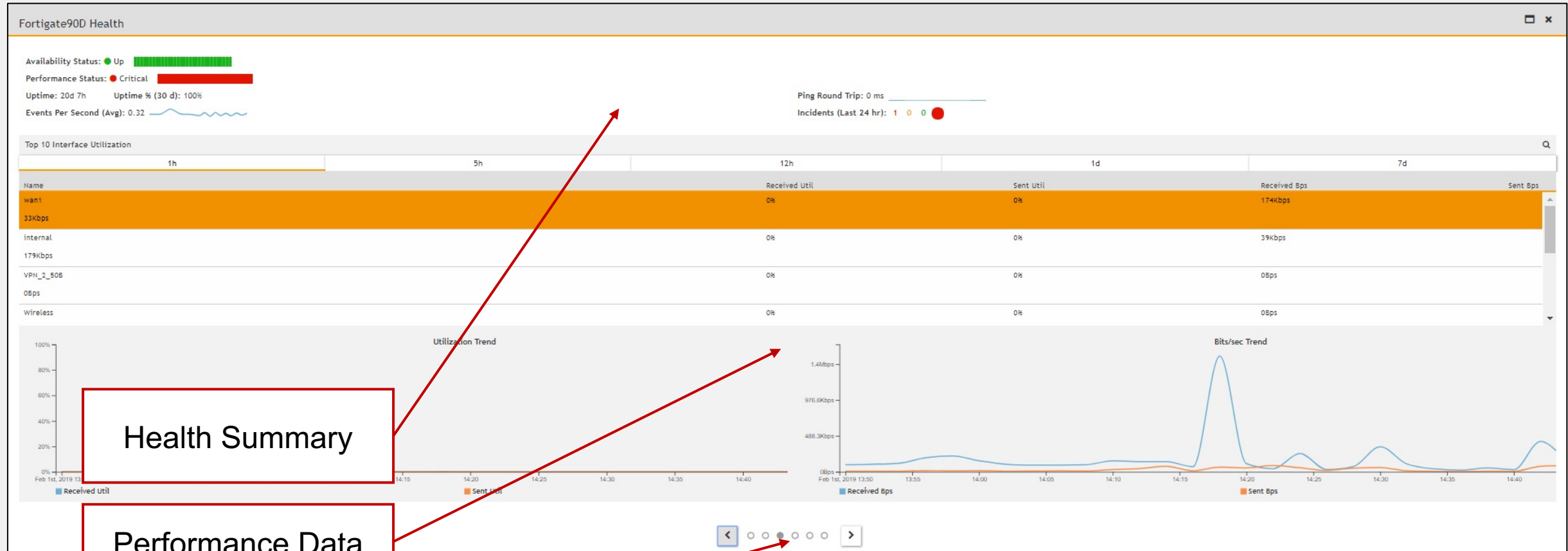
**Auto Asset Discovery & Auto Asset Categorization**

**Configuration Auditing**

**Device Detail**



# CMDB Performance and Availability Monitoring

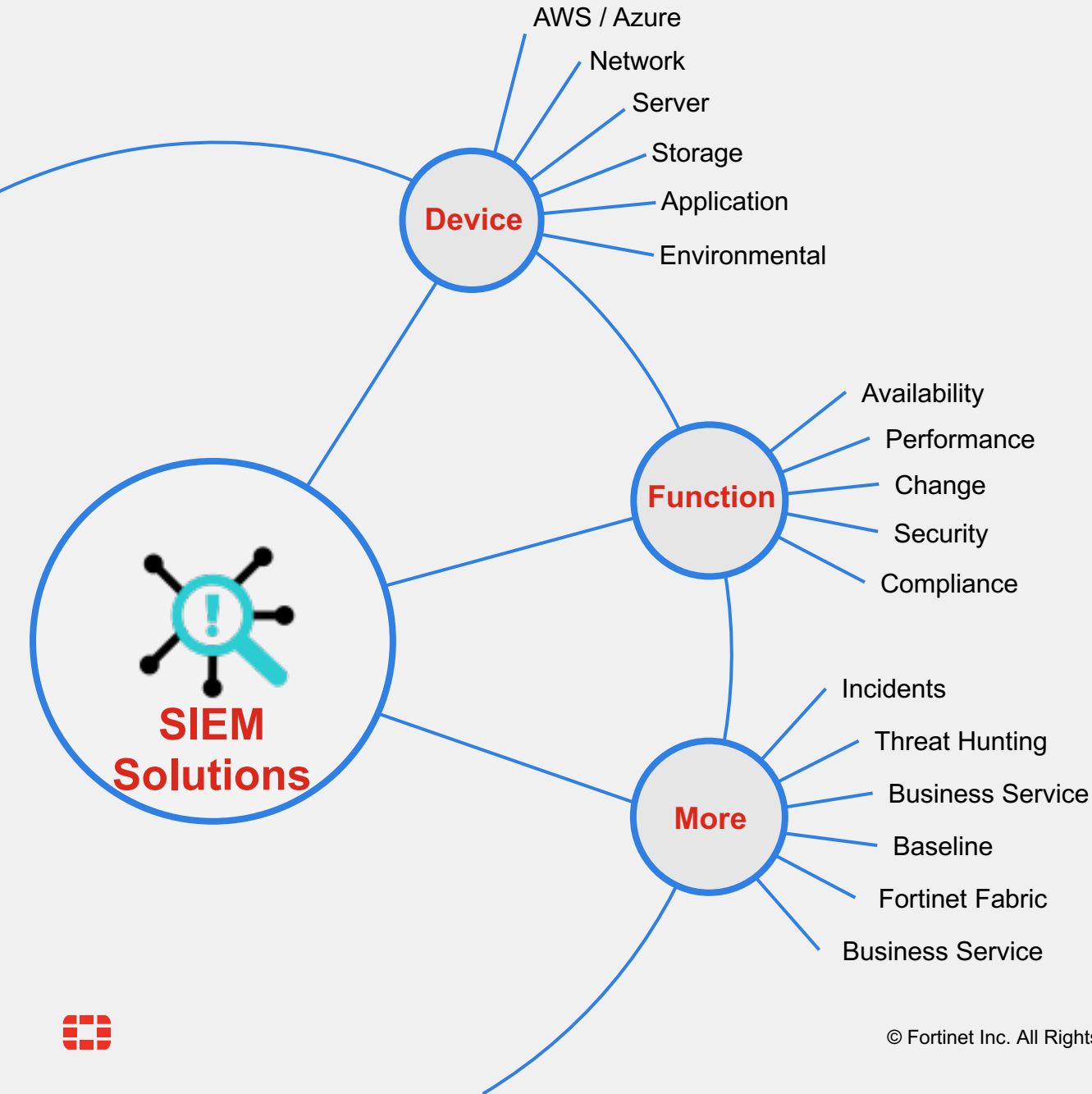


Health Summary

Performance Data

Additional Data





## 2. Reporting

Should come with built-in reports covering

- Security
- Performance
- Availability
- Compliance

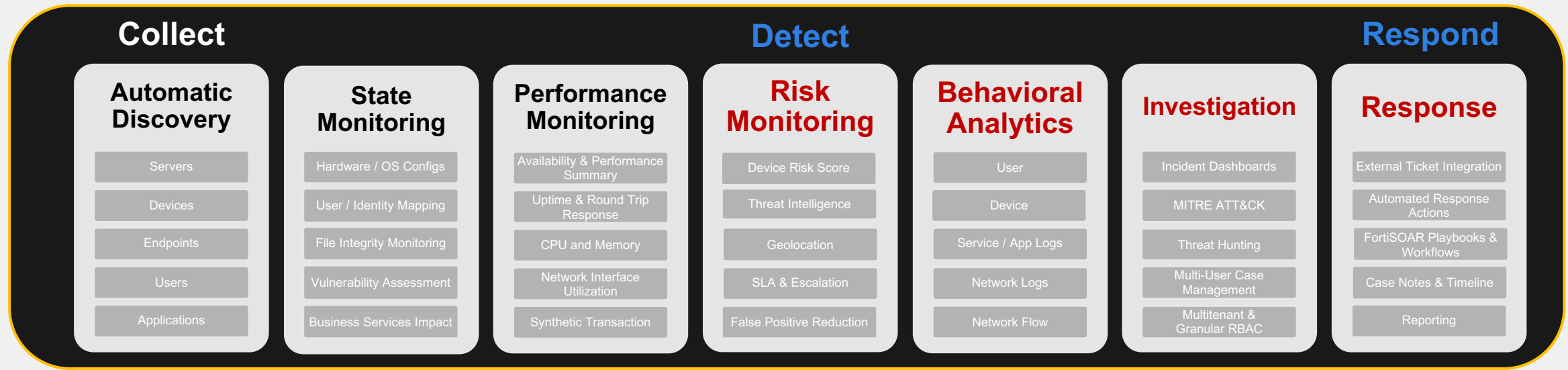
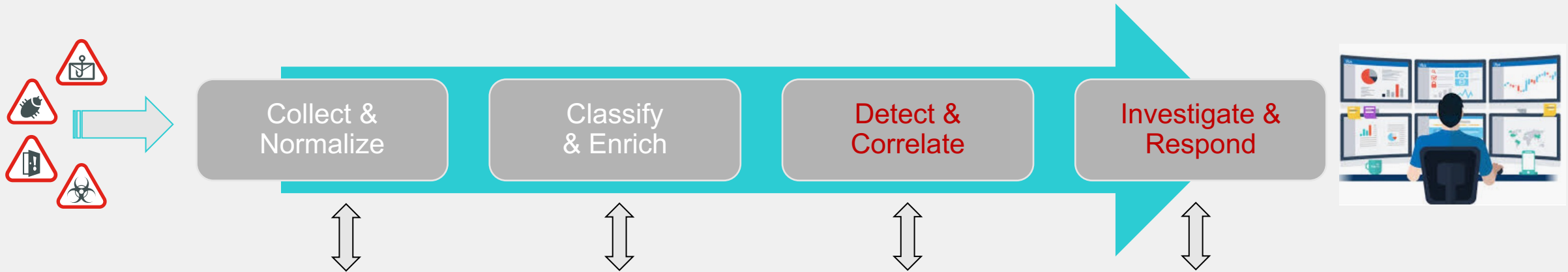
Require custom reports and features an inbuilt report designer

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





# 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

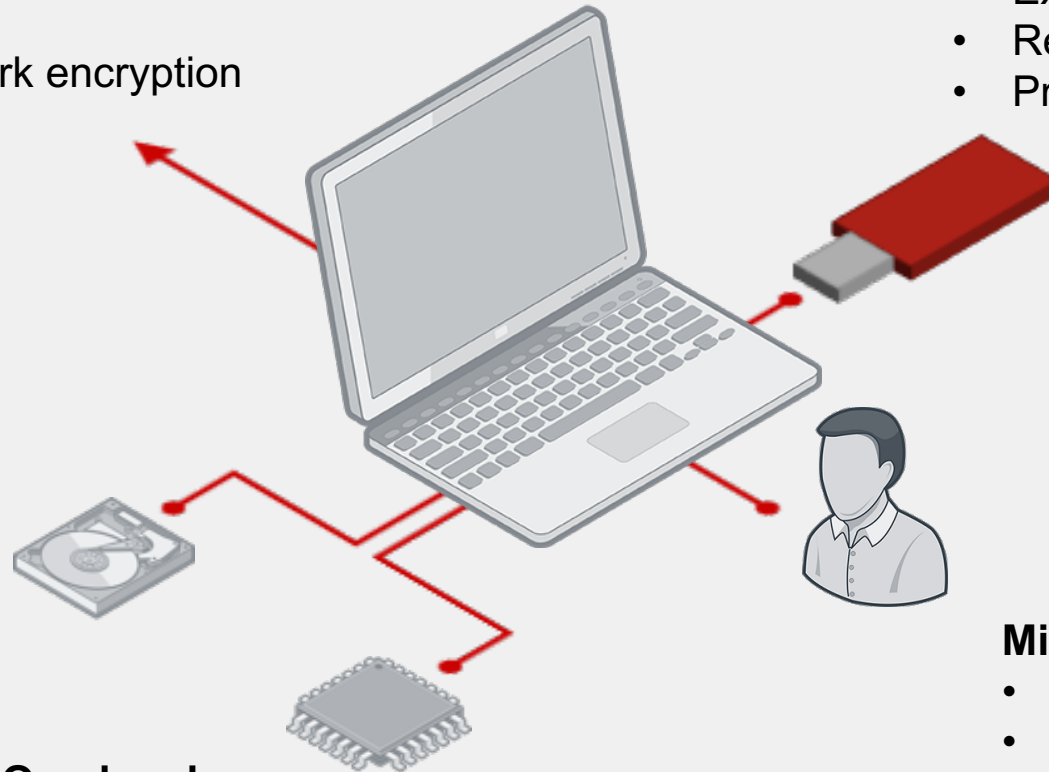
- Off-line data caching
- Upload to public collector

## Low Client Overhead

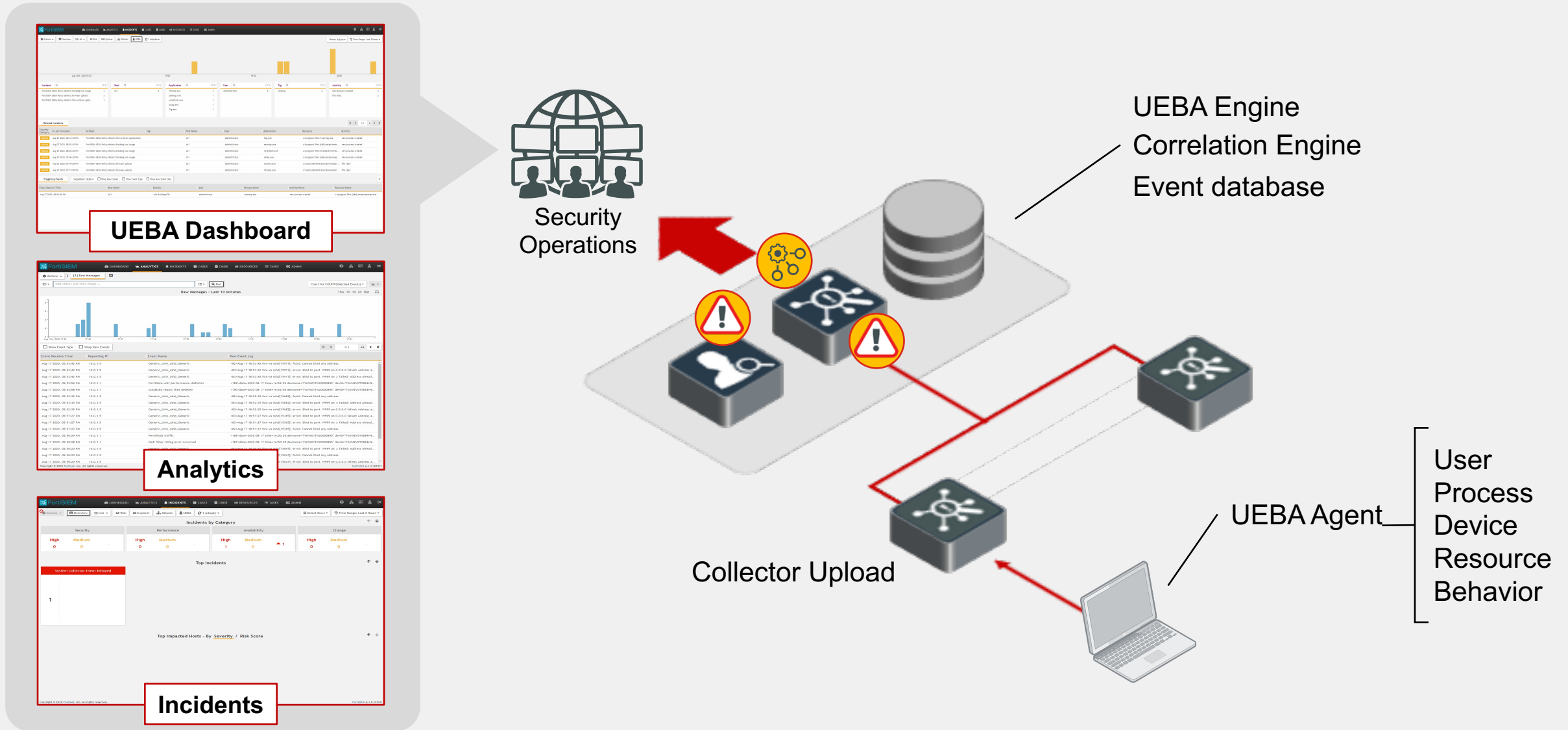
- Approx. 1% CPU use
- All analysis performed by FortiSIEM

## Minimally Invasive Solution

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



# UEBA: Log & Endpoint Visibility



## 2. MITRE ATT&CK® Data

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

The screenshot displays the FortiSIEM dashboard with a 'Valid Accounts Details' modal window open. The modal shows the following information:

- Tactics: Initial Access
- Technique: **Valid Accounts: Local Accounts** (ID: T1078.003)
- Platform: Linux, Windows, macOS
- Description: Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service. Local Accounts may also be abused to elevate privileges and harvest credentials through [OS Credential Dumping].

A red arrow points from the 'Valid Accounts: Local Accounts' link in the modal to the corresponding page on the MITRE ATT&CK website. The website page shows the breadcrumb 'Home > Techniques > Enterprise > Valid Accounts > Local Accounts' and the title 'Valid Accounts: Local Accounts'. It also lists 'Other sub-techniques of Valid Accounts (4)' and provides a detailed description of the technique.



# 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

The screenshot displays the FortiSIEM MITRE ATT&CK Incident Explorer dashboard. The top navigation bar includes 'DASHBOARD', 'ANALYTICS', 'INCIDENTS', 'CASES', 'CMDB', 'RESOURCES', 'TASKS', and 'ADMIN'. The main interface features a search bar for devices (168/168) and a table with columns for various MITRE ATT&CK tactics and techniques. Below the table is a 'Related Incidents' section with a table of incident details.

Device	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
192.168.22.16	4		4			27		4		4		
win2008-ads			34			4						
[Empty]	2		3	2	2	1					8	5
192.168.15.1	5		5	4	4	1		1				
orders-erp									4		1	14
10.95.7.10	4		4	4	4							
10.95.7.151	4		4	4	4							
10.95.7.154	4		4	4	4							

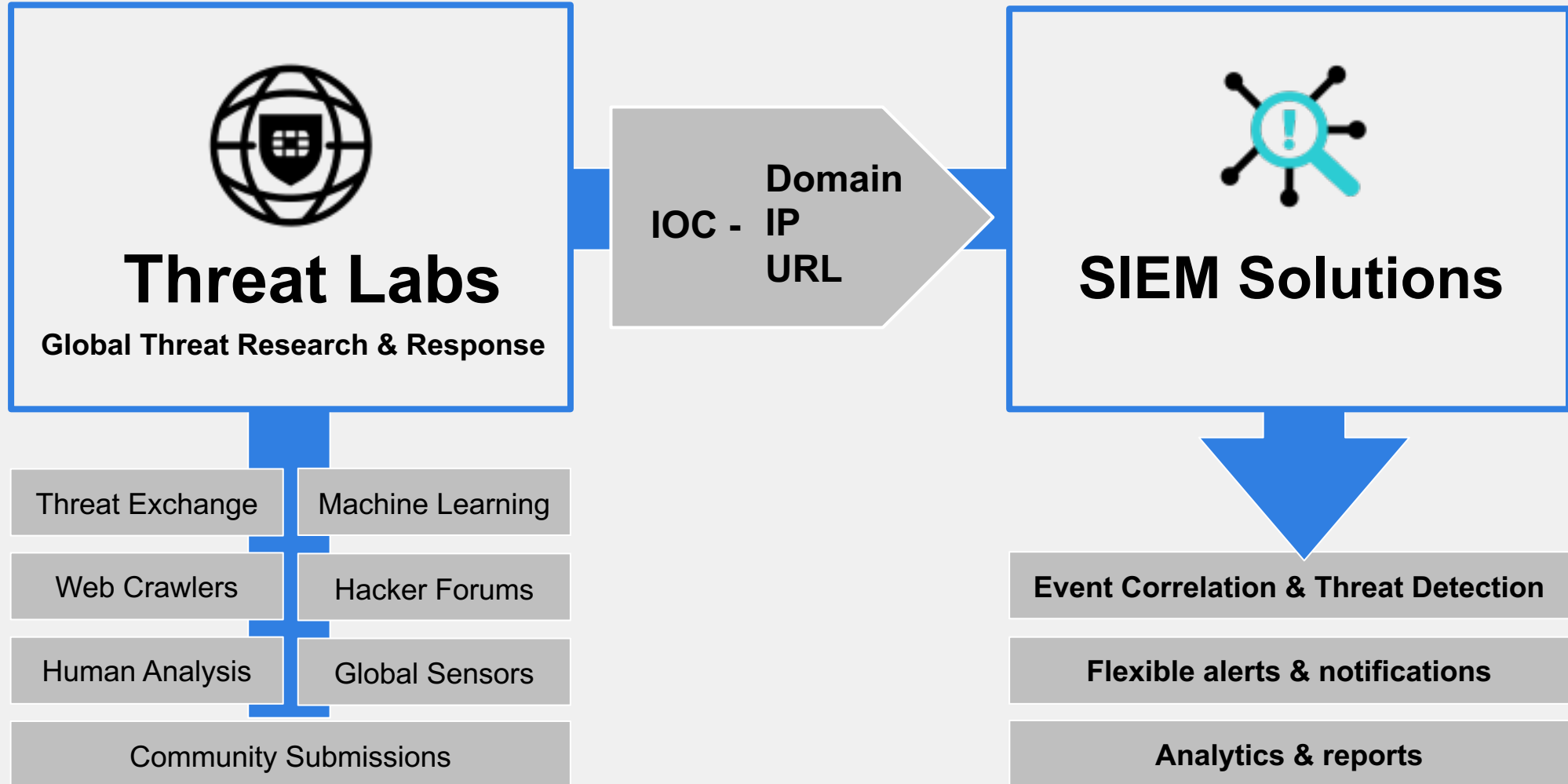
  

Severity Category	Last Occurred	Incident	Tactics	Technique	Source	Target	Detail	Incident Status
MEDIUM	Apr 08 2021, 03:48:00 PM	Excessive End User DNS Qu...	Command And Co...	Dynamic Resoluti...	192.168.22.11		Triggered Event Count: 532	Active
HIGH	Apr 08 2021, 03:48:00 PM	FortiSandbox detects malic...	Exfiltration	Exfiltration Over ...			Malware Name: W32/Agent.ZIMtr Risk Name: Malicious Informational URL: trilog.exe	Active
HIGH	Apr 08 2021, 03:48:00 PM	FortiSandbox detects malic...	Exfiltration	Exfiltration Over ...			Malware Name: W32/Patched.SAPtr Risk Name: Malicious Informational URL: wrar591.exe	Active
HIGH	Apr 08 2021, 03:48:00 PM	FortiSandbox detects malic...	Exfiltration	Exfiltration Over ...			Malware Name: VBA/Agent.DDV!tr.dldr Risk Name: Malicious Informational URL: Untitled-59129-160946...	Active
LOW	Apr 08 2021, 03:48:00 PM	Multiple Logon Failures: Do...	Credential Access	Brute Force: Pass...	192.168.26.120	WIN2008-ADS 192.168.0.10 Domain: random.org ... Show More	Triggered Event Count: 7	Active



# 3. Global Threat Intelligence

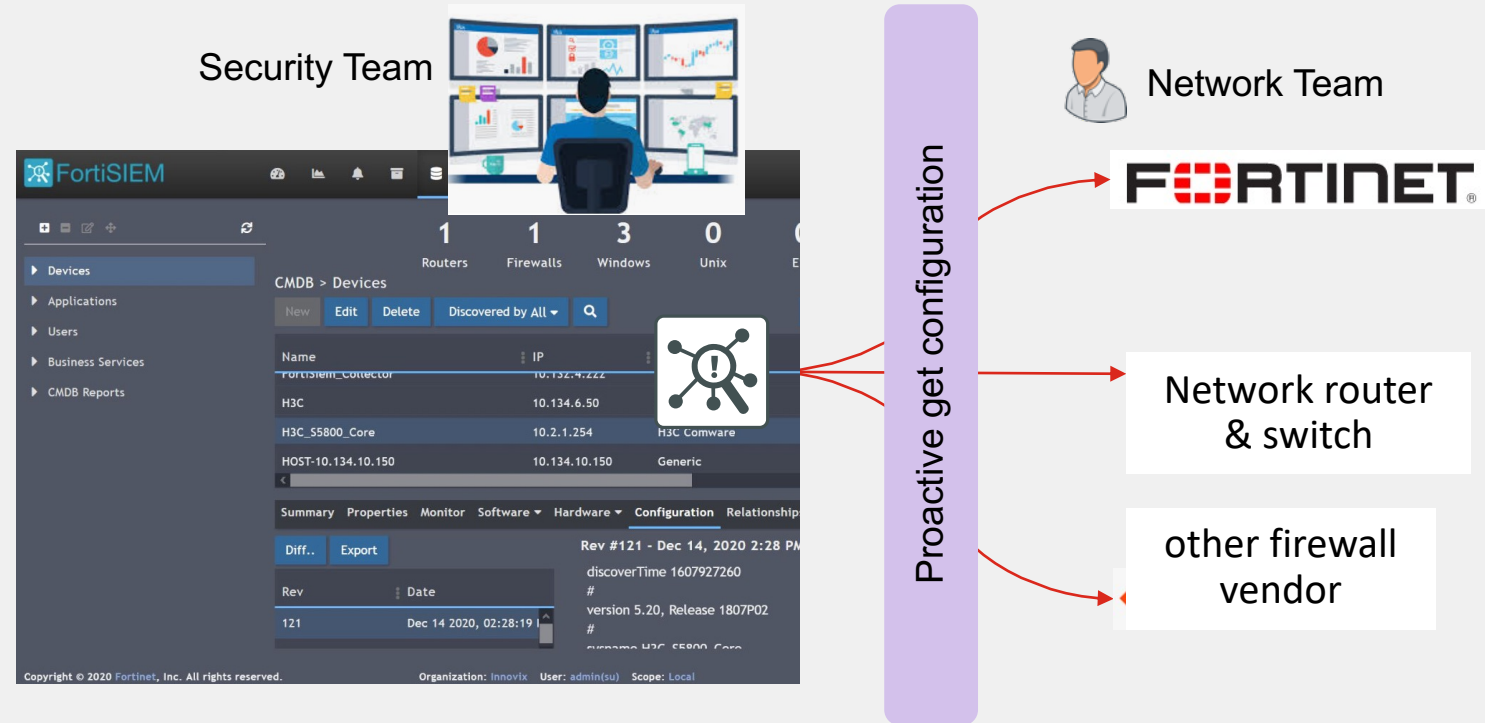
Build intelligence on dummy systems



# Use Case sharing: An Insurance Company

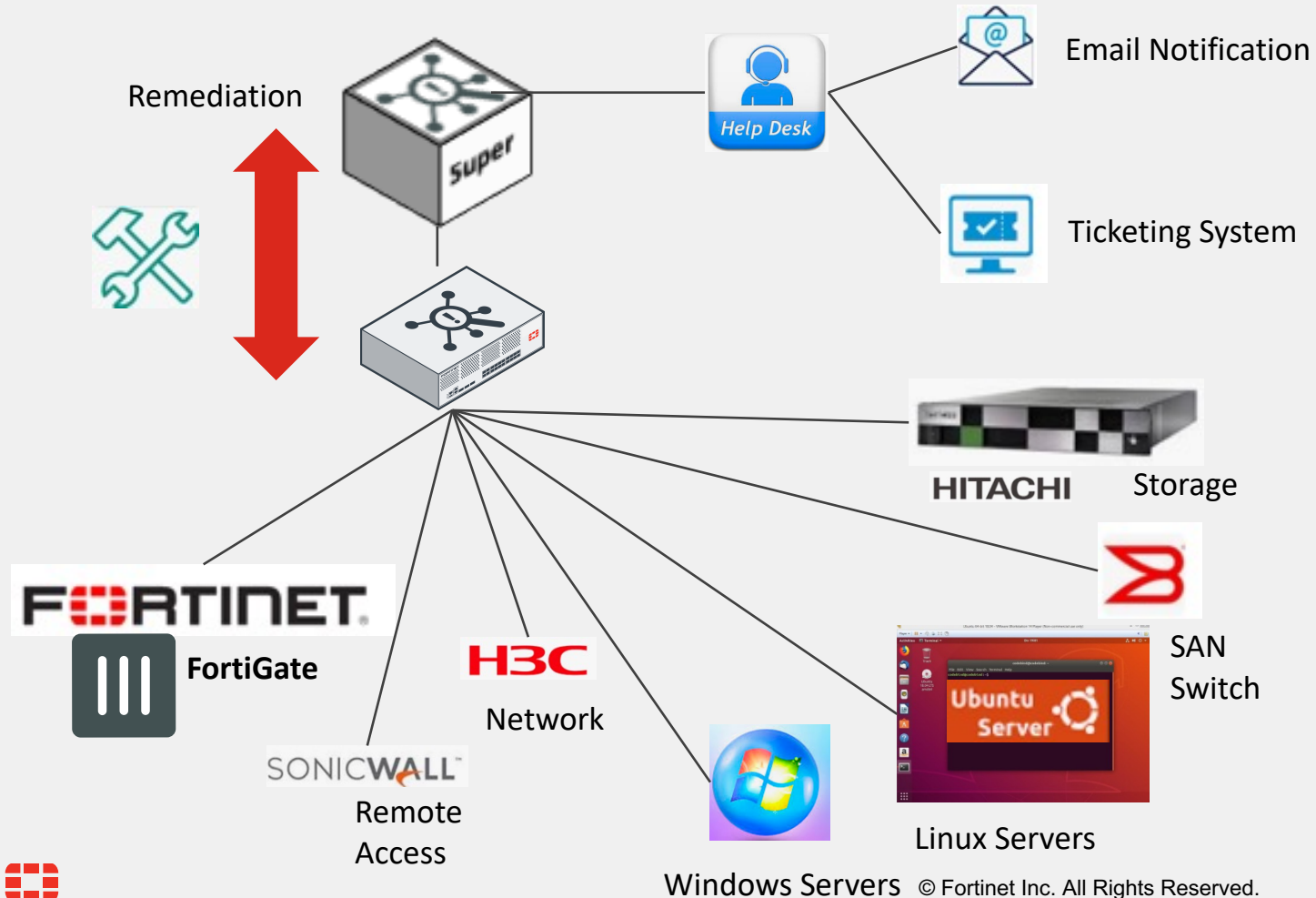
## Use Case: Compliance, configuration audit

- 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



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	Security Incidents	
	FortiGate90D	Fortinet FortiOS	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	20 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: red;">●</span>	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<div style="width: 41%;"><div style="width: 41%;"></div></div> 41%			<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%				<span style="color: red;">■</span>	
	THREATSOCDC	Microsoft Windows Server 2008	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	2 hours	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: red;">●</span>	<span style="color: green;">●</span>	<div style="width: 2%;"><div style="width: 2%;"></div></div> 2%	<div style="width: 61%;"><div style="width: 61%;"></div></div> 61%	<div style="width: 71%;"><div style="width: 71%;"></div></div> 71%	11 GB	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	4				
	WIN2K8	Microsoft Windows Server 2008	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	1728 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: red;">●</span>	<span style="color: red;">●</span>	<div style="width: 10%;"><div style="width: 10%;"></div></div> 10%	<div style="width: 45%;"><div style="width: 45%;"></div></div> 45%	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	58 MB	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	21		<span style="color: red;">■</span>	<span style="color: orange;">■</span>	
	ORDERS-ERP	Microsoft Windows Server 2008	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	1 hour	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: red;">●</span>	<span style="color: red;">●</span>	<div style="width: 4%;"><div style="width: 4%;"></div></div> 4%	<div style="width: 61%;"><div style="width: 61%;"></div></div> 61%	<div style="width: 71%;"><div style="width: 71%;"></div></div> 71%	11 GB	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	1		<span style="color: orange;">■</span>	<span style="color: red;">■</span>	
	juniperfw	Juniper SRX JunOS	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	227 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: orange;">●</span>	<span style="color: green;">●</span>	<div style="width: 10%;"><div style="width: 10%;"></div></div> 10%	<div style="width: 79%;"><div style="width: 79%;"></div></div> 79%			<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%		<span style="color: orange;">■</span>	<span style="color: orange;">■</span>		
	ibmaix	IBM AIX	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	1797 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: orange;">●</span>	<span style="color: green;">●</span>	<div style="width: 4%;"><div style="width: 4%;"></div></div> 4%	<div style="width: 96%;"><div style="width: 96%;"></div></div> 96%	<div style="width: 93%;"><div style="width: 93%;"></div></div> 93%	31 MB			1		<span style="color: orange;">■</span>		
	SJ-QA-F-Lnx-CHK	Fortinet FortiOS	demopack			1737 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: green;">●</span>	<span style="color: green;">●</span>											
	FG240D3913800456	Fortinet FortiOS	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	365 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: green;">●</span>	<span style="color: orange;">●</span>	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 49%;"><div style="width: 49%;"></div></div> 49%			<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	11	<span style="color: orange;">■</span>		<span style="color: orange;">■</span>	
	HOST-10.10.240.2	Security Onion BRO	demopack					<span style="color: green;">●</span>	<span style="color: green;">●</span>											
	THREATCTR	Microsoft Windows Server 2003	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	1308 days	<div style="width: 99%;"><div style="width: 99%;"></div></div> 99%	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 12%;"><div style="width: 12%;"></div></div> 12%	<div style="width: 1%;"><div style="width: 1%;"></div></div> 1%	460 GB	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%					
	HOST-10.10.240.6	Cisco ASA	demopack					<span style="color: green;">●</span>	<span style="color: green;">●</span>											
	521collectoriso	Generic Unix	demopack					<span style="color: green;">●</span>	<span style="color: green;">●</span>							16				
	HOST-127.0.0.1	Generic	demopack					<span style="color: green;">●</span>	<span style="color: green;">●</span>							30				
	SJ-Dev-A-Fdy-FastIron	Foundry Ironware	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	1783 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<div style="width: 4%;"><div style="width: 4%;"></div></div> 4%	<div style="width: 49%;"><div style="width: 49%;"></div></div> 49%			<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	1				
	PA-500_01_accelops	Palo Alto PAN-OS	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	228 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: green;">●</span>	<span style="color: green;">●</span>					<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%					
	QA-EXCHG	Microsoft Windows Server 2003	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	1735 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<div style="width: 3%;"><div style="width: 3%;"></div></div> 3%	<div style="width: 71%;"><div style="width: 71%;"></div></div> 71%	<div style="width: 78%;"><div style="width: 78%;"></div></div> 78%	51 GB	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	8				
	SJ-QA-S-Sun-Spc01	Sun SunOS	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	1760 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: green;">●</span>	<span style="color: green;">●</span>					<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%					
	WIN-RAQBSNW8OVY	Microsoft Windows Server 2008	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	227 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<div style="width: 16%;"><div style="width: 16%;"></div></div> 16%	<div style="width: 31%;"><div style="width: 31%;"></div></div> 31%	<div style="width: 34%;"><div style="width: 34%;"></div></div> 34%	26 GB	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	<div style="width: 0%;"><div style="width: 0%;"></div></div> 0%	13				
	HP-ProCurve-2910al	HP ProCurve	demopack	<span style="color: green;">●</span>	<div style="width: 100%;"><div style="width: 100%;"></div></div> 0%	1744 days	<div style="width: 100%;"><div style="width: 100%;"></div></div> 100%	<span style="color: green;">●</span>	<span style="color: green;">●</span>	<div style="width: 25%;"><div style="width: 25%;"></div></div> 25%	<div style="width: 22%;"><div style="width: 22%;"></div></div> 22%			<div style="width: 21%;"><div style="width: 21%;"></div></div> 21%	<div style="width: 21%;"><div style="width: 21%;"></div></div> 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®**