Logstail

Beyond Defense: Crafting Resilient SOCs for Tomorrow's Cyber Frontiers

Major (Ret) Christos NTRIGKOGIAS,
FOUNDER AND CEO

Contributing in Cyber Defense..

Business Overview

Logstail

3 offices

Users in **17** countries worldwide

4.500 SaaS platform users

Logstail Participation in EU Cyber Defense

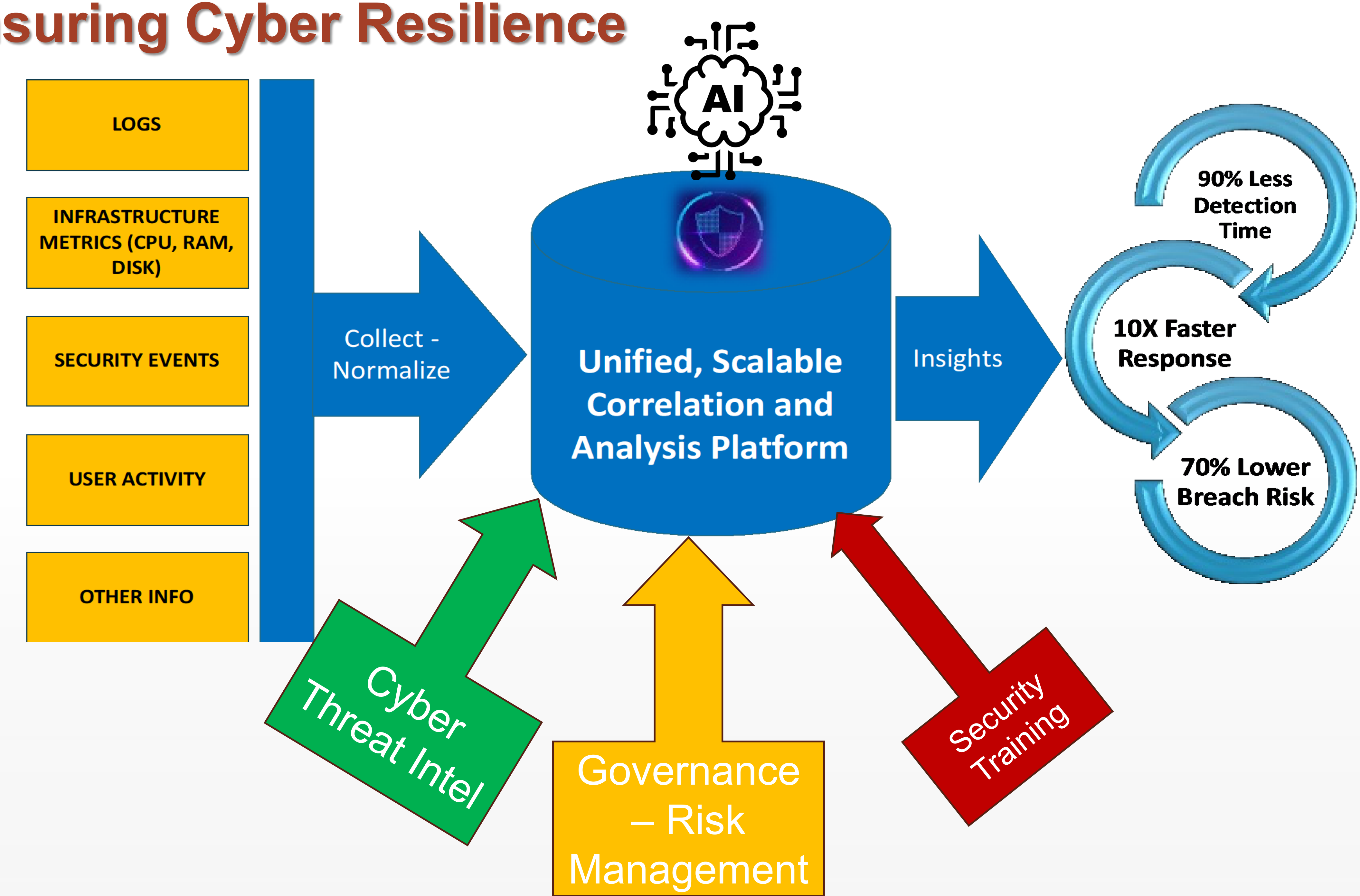
- Pandora (EDIDP) – Completed
- AInception (EDF 21) – Ongoing
- Newsroom (EDF 22) – Ongoing

Cyber Solutions Portfolio

- AI-powered monitoring suite
- Next gen XDR
- Security Audit
- Red Team Operations
- Incident Response
- Zero-trust Architecture Design

› Real-time monitoring of interconnected military and space assets to detect and respond to cyber-threats.
› Actionable Threat Intelligence (CTI)
› Compliance monitoring and reporting
› Data driven decision making

Ensuring Cyber Resilience



LOGS

INFRASTRUCTURE METRICS (CPU, RAM, DISK)

SECURITY EVENTS

USER ACTIVITY

OTHER INFO

Collect - Normalize

AI

Unified, Scalable Correlation and Analysis Platform

Insights

90% Less Detection Time

10X Faster Response

70% Lower Breach Risk

Cyber Threat Intel

Governance – Risk Management

Security Training

Reference Use Case

Use Case: Governmental Organisation in Europe

Challenge:

Lack of unified visibility of Organisation’s IT / OT Ecosystem Security

250+ IT /OT Assets

40+ Different Technologies and Products

Air Gapped Environment

Users / External Contractors Activity Monitoring

After 1 month of using Logstail:

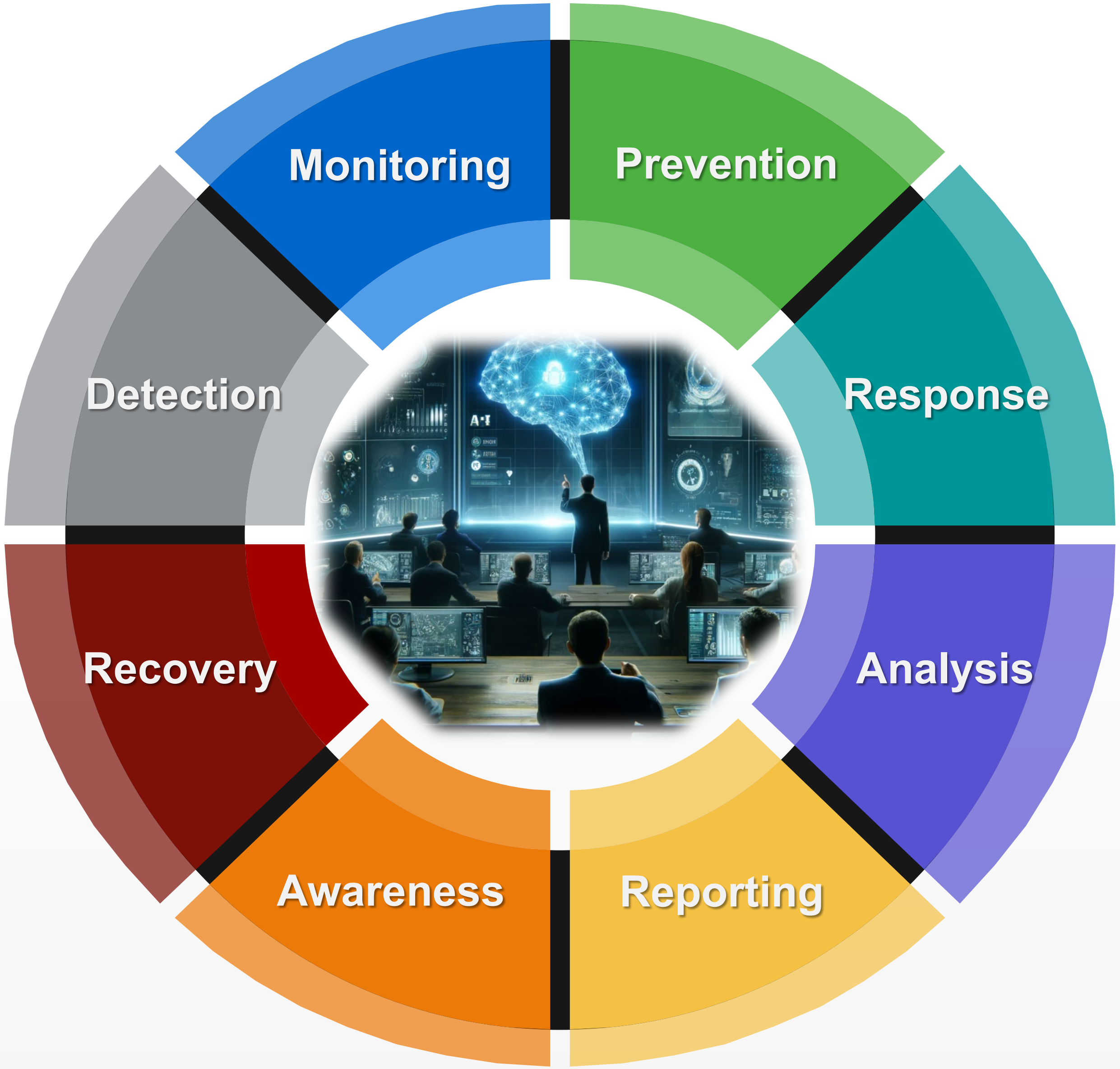
From > 5UIs → One unified UI

Response:
2 hours → 15 min

Detection:
30 days → 30min

No Risk Plan -> Unified Risk Management Plan

SOC Modules



Monitoring

Prevention

Detection

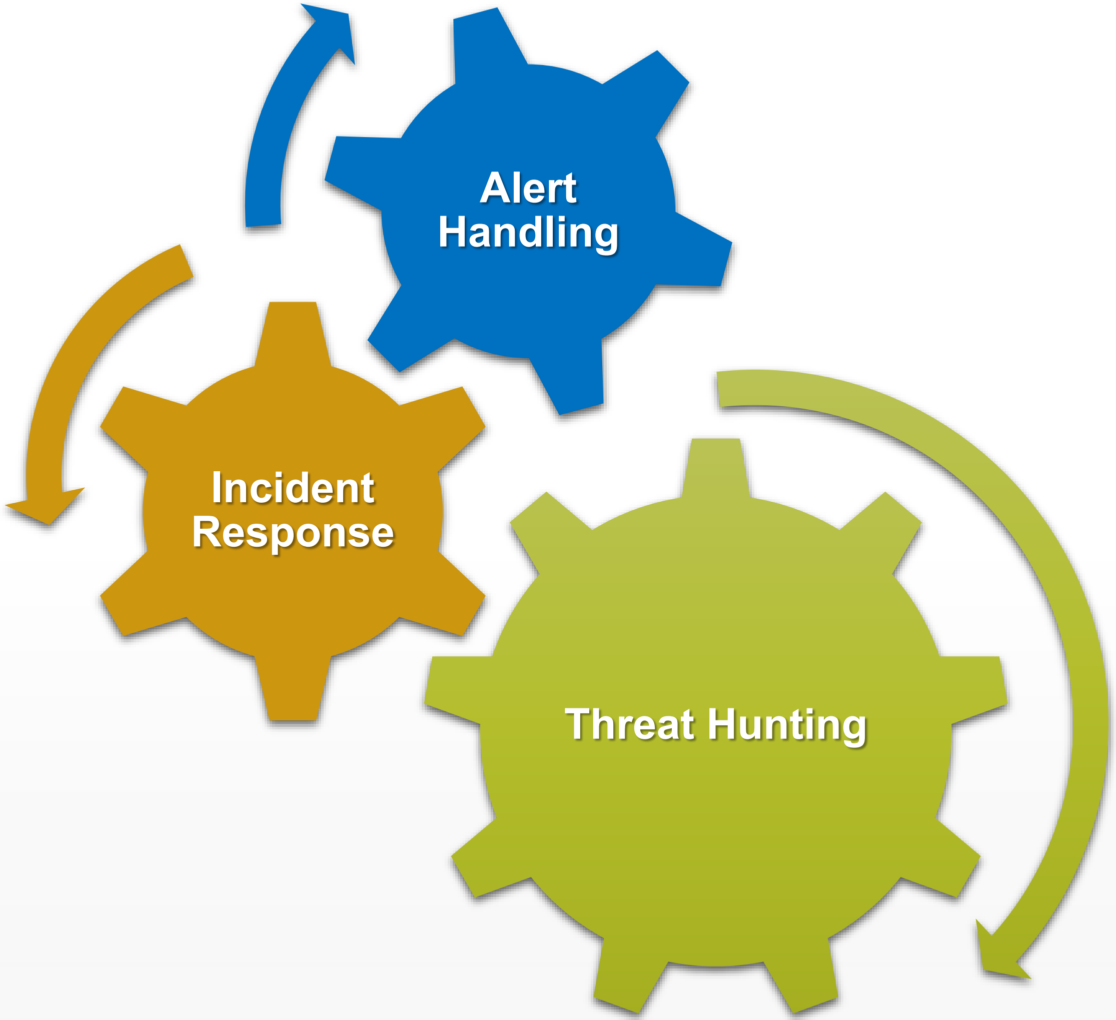
Response

Recovery

Analysis

Awareness

Reporting



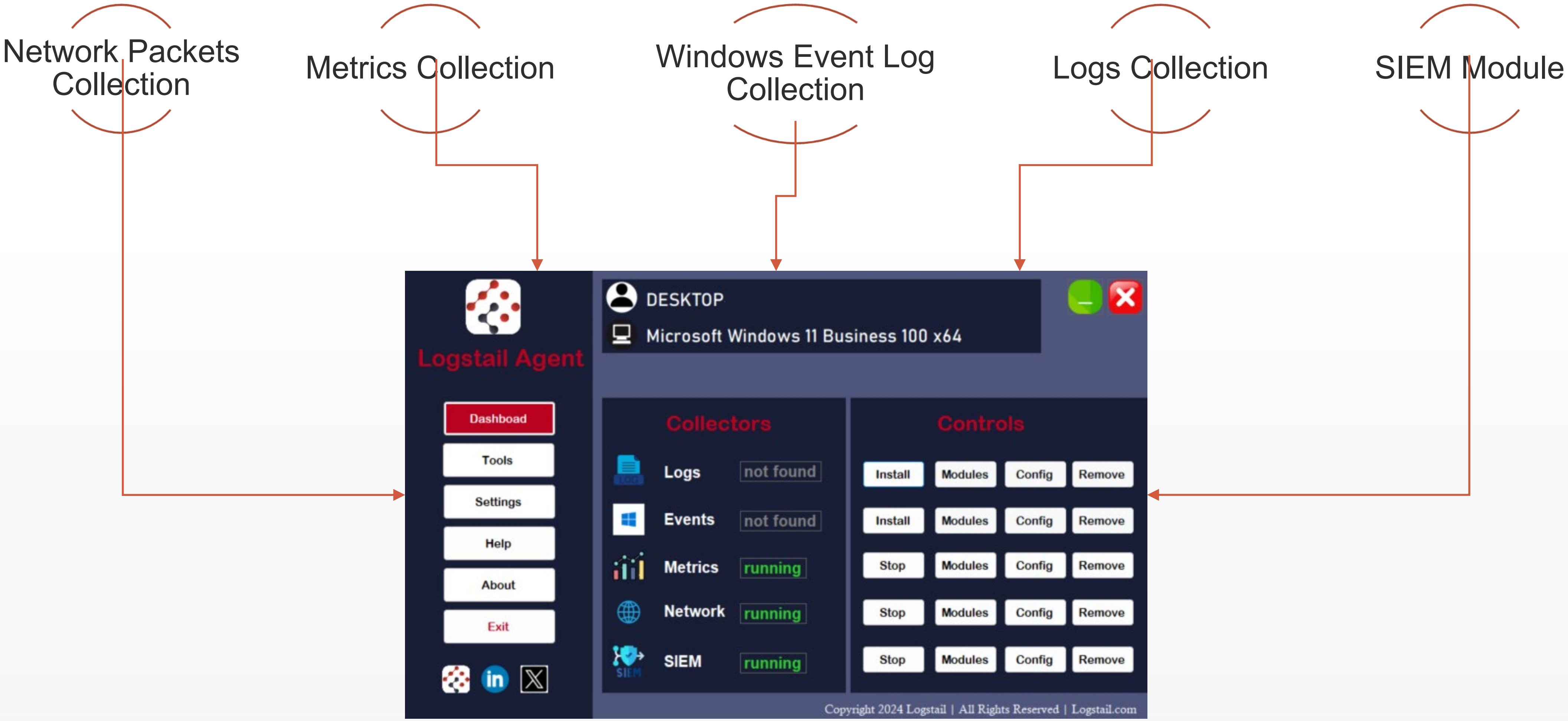
Alert Handling

Incident Response

Threat Hunting

Logstail Unified Agent

Lightweight software that runs on Windows hosts. It collects logs, metrics, network packets and security events from a variety of sources and sends them to Logstail Platform where you can analyse your monitoring and performance data.



Network Packets Collection

Metrics Collection

Windows Event Log Collection

Logs Collection

SIEM Module

Logstail Agent

DESKTOP

Microsoft Windows 11 Business 100 x64

Collectors		Controls			
Logs	not found	Install	Modules	Config	Remove
Events	not found	Install	Modules	Config	Remove
Metrics	running	Stop	Modules	Config	Remove
Network	running	Stop	Modules	Config	Remove
SIEM	running	Stop	Modules	Config	Remove

Copyright 2024 Logstail | All Rights Reserved | Logstail.com

Endpoint Security

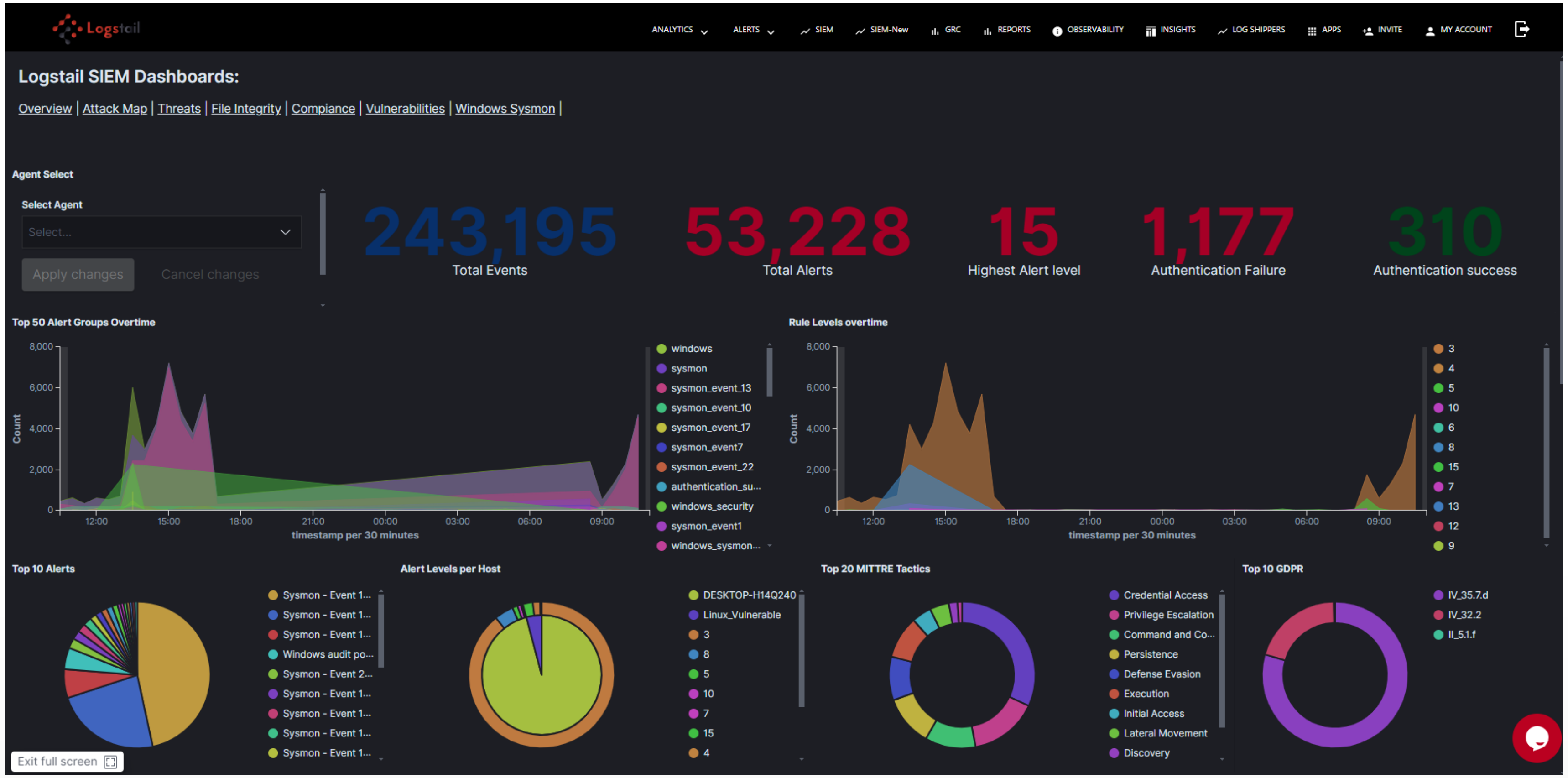
Data Sources: Logstail Unified Agent – OS native log collectors

➢ Detection Techniques:

- File Integrity Monitoring
- Security Configuration Assessment
- Software Vulnerabilities
- Malicious connections

➢ Capabilities & Skillset:

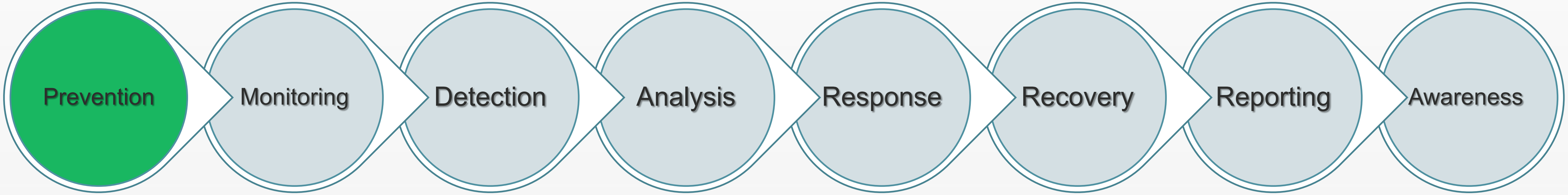
- Endpoint Attacks Detection
- Incident Response Skills
- Mitigation Actions based on MITRE ATT&CK



Logstail SIEM Dashboards:

Overview | Attack Map | Threats | File Integrity | Compiance | Vulnerabilities | Windows Sysmon |

243,195	53,228	15	1,177	310
Total Events	Total Alerts	Highest Alert level	Authentication Failure	Authentication success



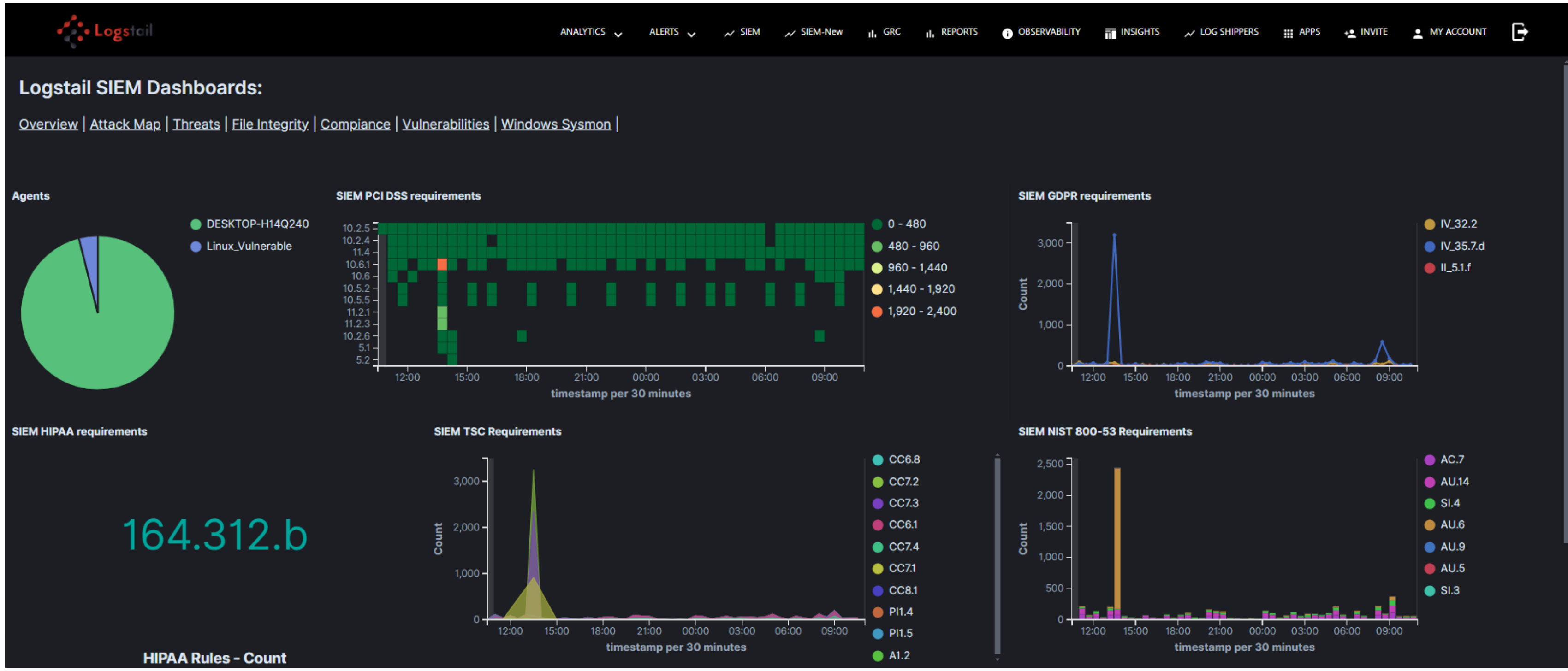
Prevention → Monitoring → Detection → Analysis → Response → Recovery → Reporting → Awareness

Regulatory Compliance

Data Sources: Logstail Unified Agent

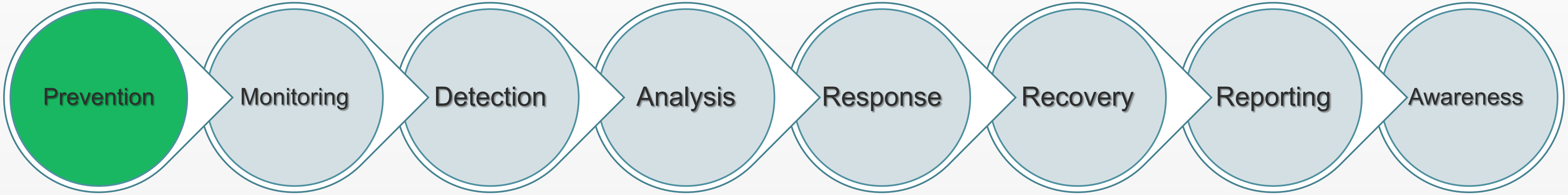
- **Monitor Regulatory Standards:**
  - GDPR
  - HIPAA
  - NIST
  - NIS2

- **Capabilities & Skillset developed**
  - Familiarise with Compliance Regulations Requirements
  - Self-Auditing skills
  - Self-training with the integrated controls



Logstail SIEM Dashboards:

Overview | Attack Map | Threats | File Integrity | Compiance | Vulnerabilities | Windows Sysmon |


Prevention

Monitoring

Detection

Analysis

Response

Recovery

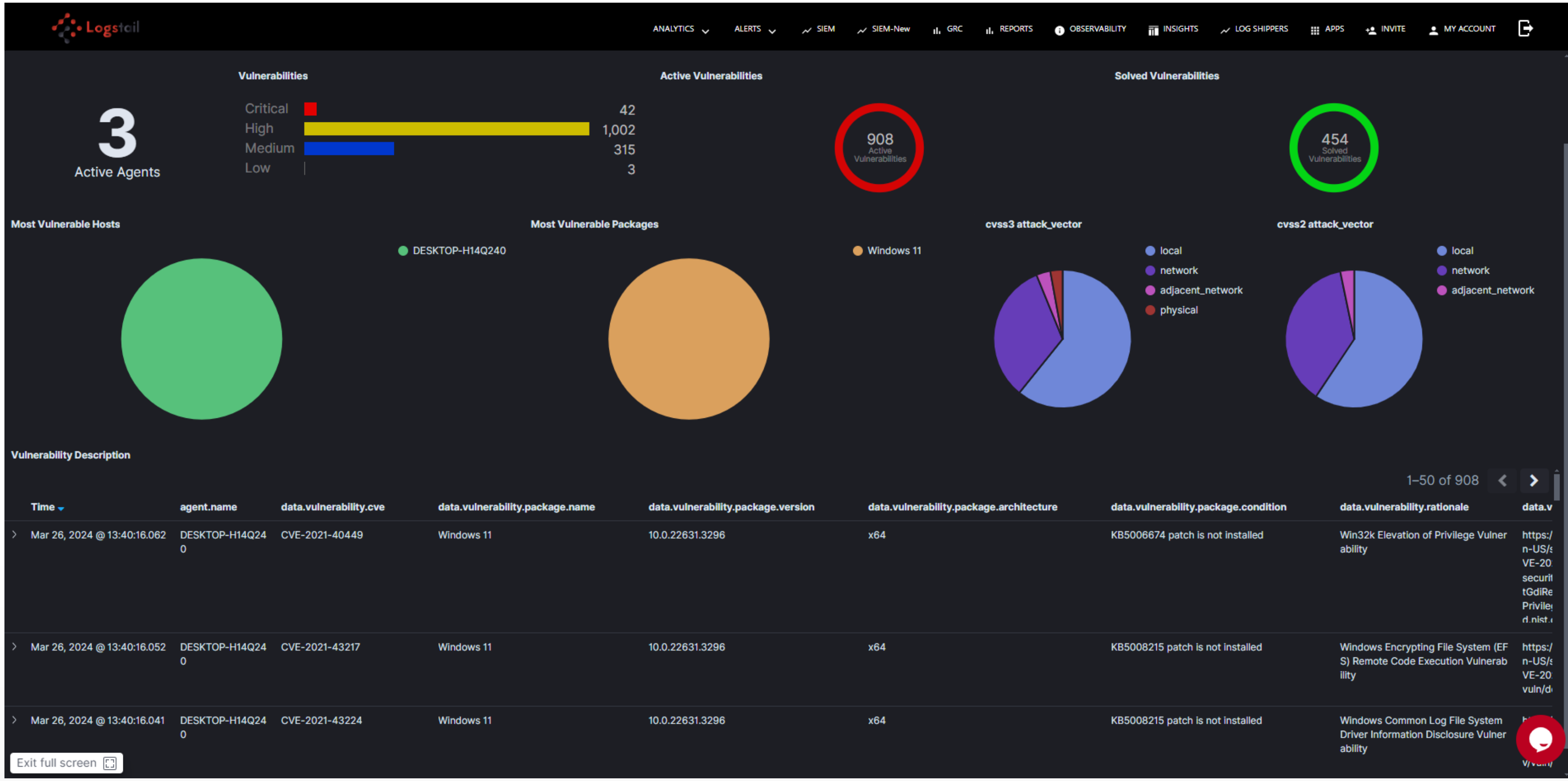
Reporting

Awareness

Vulnerability Scanning

Data Sources: Logstail Unified Agent – OS native SIEM collector

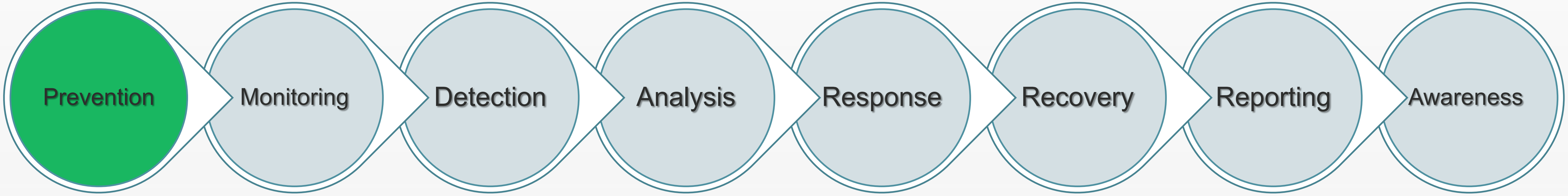
- **Detection Techniques:**
  - Vulnerability Detection
- **Capabilities & Skillset:**
  - Find outdated software
  - Prevent attacks



Vulnerability Description

1–50 of 908

Time	agent.name	data.vulnerability.cve	data.vulnerability.package.name	data.vulnerability.package.version	data.vulnerability.package.architecture	data.vulnerability.package.condition	data.vulnerability.rationale	data.v
Mar 26, 2024 @ 13:40:16.062	DESKTOP-H14Q240	CVE-2021-40449	Windows 11	10.0.22631.3296	x64	KB5006674 patch is not installed	Win32k Elevation of Privilege Vulnerability	https:/ n-US/s VE-20 securit tGdiRe Privile d.nist.c
Mar 26, 2024 @ 13:40:16.052	DESKTOP-H14Q240	CVE-2021-43217	Windows 11	10.0.22631.3296	x64	KB5008215 patch is not installed	Windows Encrypting File System (EFS) Remote Code Execution Vulnerability	https:/ n-US/s VE-20 vuln/d
Mar 26, 2024 @ 13:40:16.041	DESKTOP-H14Q240	CVE-2021-43224	Windows 11	10.0.22631.3296	x64	KB5008215 patch is not installed	Windows Common Log File System Driver Information Disclosure Vulnerability	v/vuln/

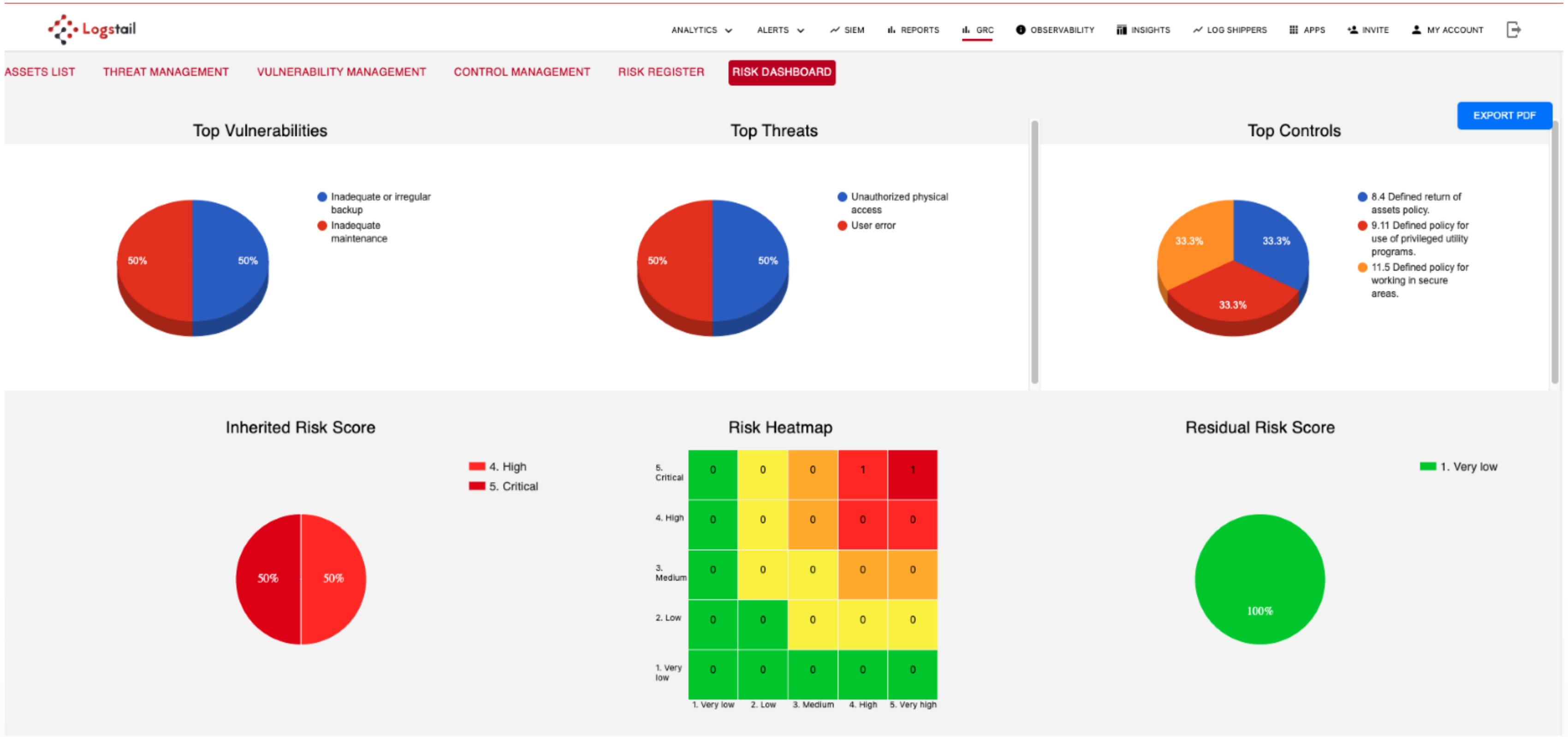


Security Risk Governance (GRC)

Data Sources: External Sources – Logstail Unified Agents – Manual Input

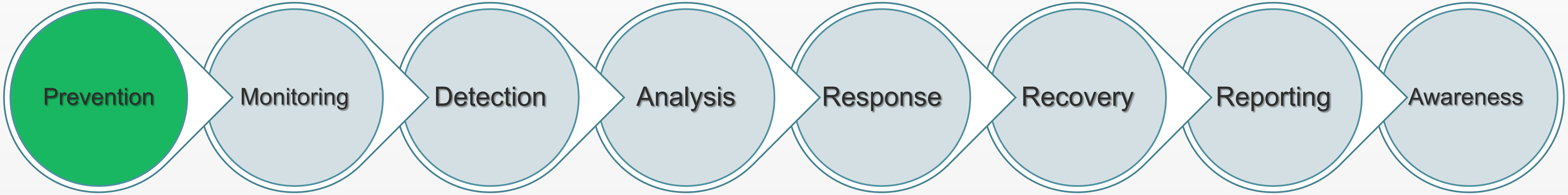
- **Indicative Risk Standards:**
  - ISO 27001 (2022)
  - NIST

- **Capabilities & Skillset developed**
  - Familiarise with Security Risk Governance (GRC)
  - Prepare for certification (Auditors, CISOs)
  - Self-training with integrated controls



Risk Heatmap

5. Critical	0	0	0	1	1
4. High	0	0	0	0	0
3. Medium	0	0	0	0	0
2. Low	0	0	0	0	0
1. Very low	0	0	0	0	0
	1. Very low	2. Low	3. Medium	4. High	5. Very high



Prevention → Monitoring → Detection → Analysis → Response → Recovery → Reporting → Awareness

Network Security

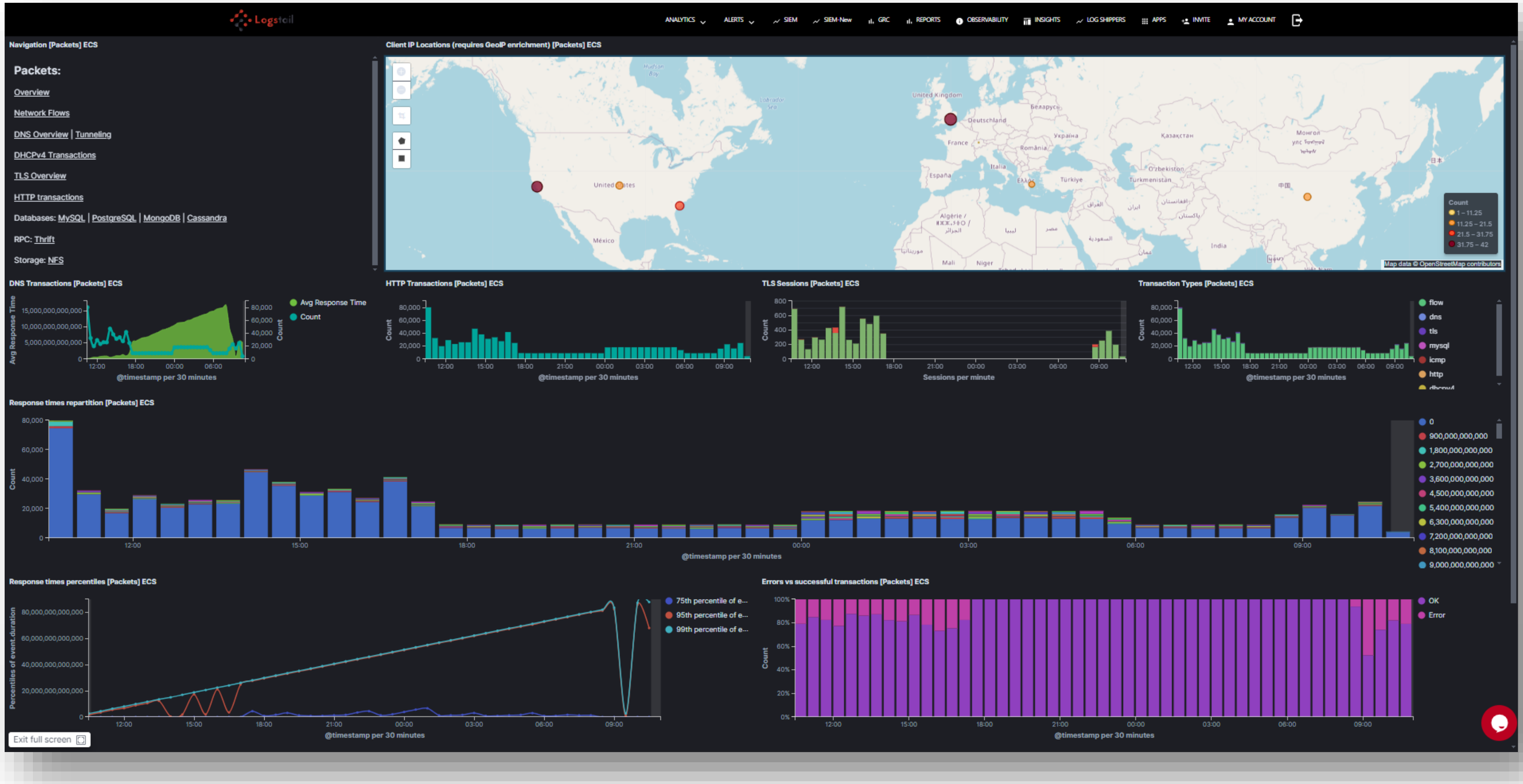
Data Sources: Network Devices (FWs, Routers, IDS, WAFs etc)

➢ Detection Techniques:

- Packets Inspection
- Network Protocols Analysis
- Malicious Traffic Detection
- Network Attack Map

➢ Capabilities & Skillset:

- Network Attacks Detection
- Incident Response Skills
- Mitigation Actions based on MITRE ATT&CK
- Rule-based - Autonomous alerts



Logstail
ANALYTICS
ALERTS
SIEM
SIEM-New
GRC
REPORTS
OBSERVABILITY
INSIGHTS
LOG SHIPPERS
APPS
INVITE
MY ACCOUNT

Navigation [Packets] ECS

Packets:

Overview

Network Flows

DNS Overview | Tunneling

DHCPv4 Transactions

TLS Overview

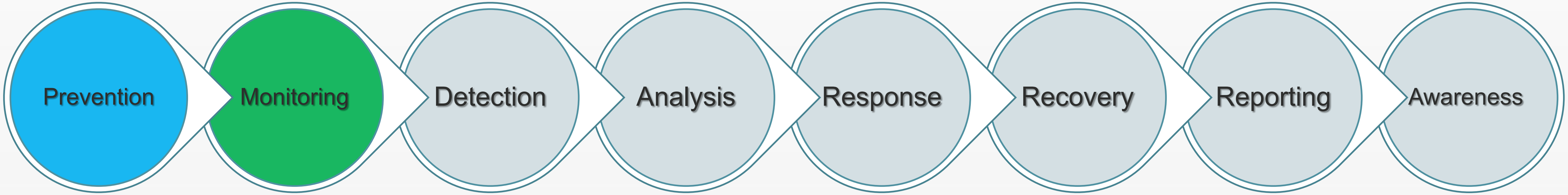
HTTP transactions

Databases: MySQL | PostgreSQL | MongoDB | Cassandra

RPC: Thrift

Storage: NFS

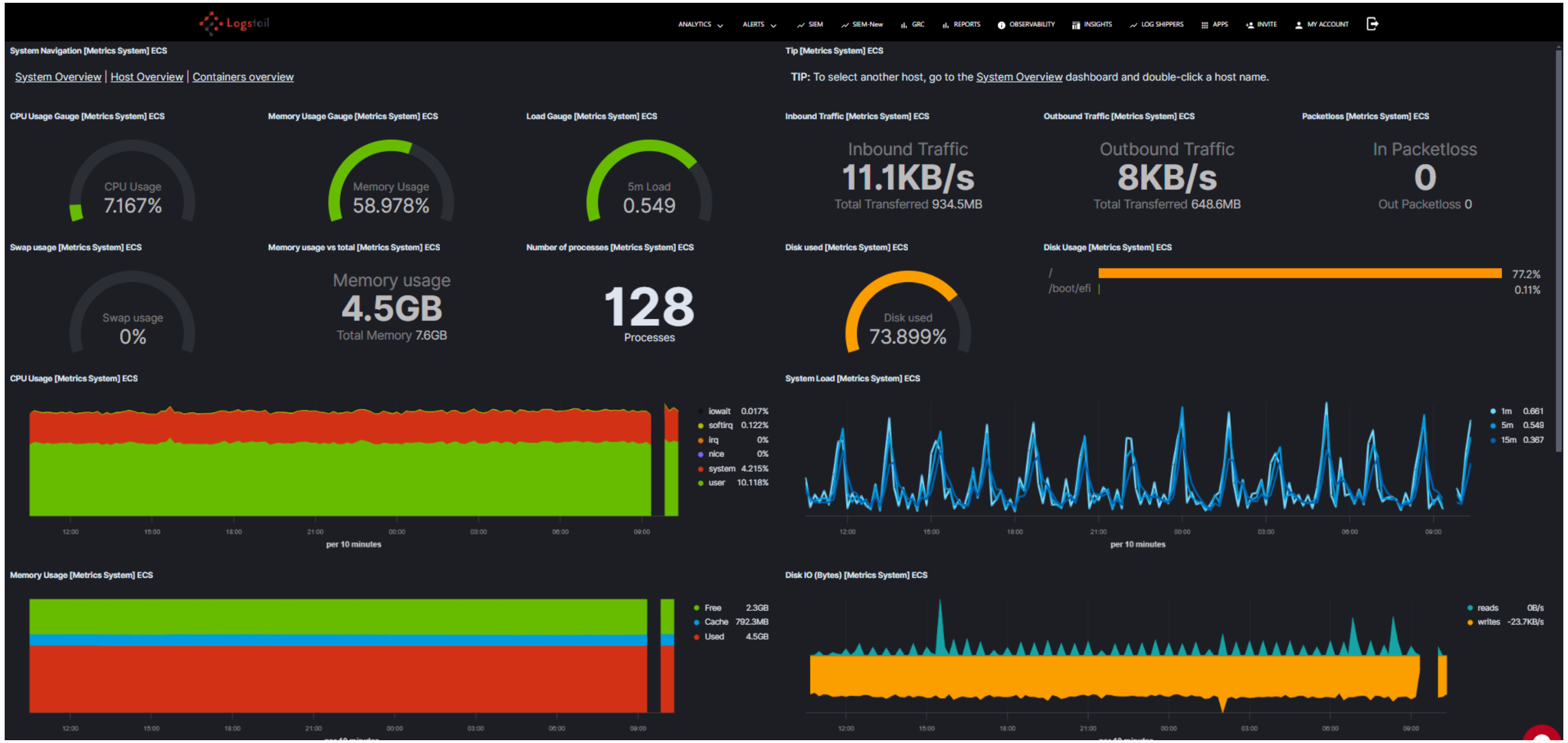
Client IP Locations (requires GeoIP enrichment) [Packets] ECS
Count
1 - 11.25
11.25 - 21.5
21.5 - 31.75
31.75 - 42
Map data © OpenStreetMap contributors
DNS Transactions [Packets] ECS
Avg Response Time
Count
@timestamp per 30 minutes
HTTP Transactions [Packets] ECS
Count
@timestamp per 30 minutes
TLS Sessions [Packets] ECS
Count
Sessions per minute
Transaction Types [Packets] ECS
flow
dns
tls
mysql
icmp
http
dhcpv4
@timestamp per 30 minutes
Response times repartition [Packets] ECS
Count
@timestamp per 30 minutes
Response times percentiles [Packets] ECS
Percentiles of event.duration
75th percentile of e...
95th percentile of e...
99th percentile of e...
@timestamp per 30 minutes
Errors vs successful transactions [Packets] ECS
OK
Error
@timestamp per 30 minutes
Exit full screen



Prevention → Monitoring → Detection → Analysis → Response → Recovery → Reporting → Awareness

Infrastructure Monitoring

Data Sources: Logstail Unified Agent – OS native metrics collectors



System Navigation [Metrics System] ECS

System Overview | Host Overview | Containers overview

Tip [Metrics System] ECS

TIP: To select another host, go to the System Overview dashboard and double-click a host name.

CPU Usage Gauge [Metrics System] ECS

CPU Usage 7.167%

Memory Usage Gauge [Metrics System] ECS

Memory Usage 58.978%

Load Gauge [Metrics System] ECS

5m Load 0.549

Inbound Traffic [Metrics System] ECS

Inbound Traffic 11.1KB/s
Total Transferred 934.5MB

Outbound Traffic [Metrics System] ECS

Outbound Traffic 8KB/s
Total Transferred 648.6MB

Packetloss [Metrics System] ECS

In Packetloss 0
Out Packetloss 0

Swap usage [Metrics System] ECS

Swap usage 0%

Memory usage vs total [Metrics System] ECS

Memory usage 4.5GB
Total Memory 7.6GB

Number of processes [Metrics System] ECS

128 Processes

Disk used [Metrics System] ECS

Disk used 73.899%

Disk Usage [Metrics System] ECS

/	77.2%
/boot/efi	0.11%

CPU Usage [Metrics System] ECS

iowait	0.017%
softirq	0.122%
irq	0%
nice	0%
system	4.215%
user	10.118%

System Load [Metrics System] ECS

1m	0.661
5m	0.549
15m	0.367

Memory Usage [Metrics System] ECS

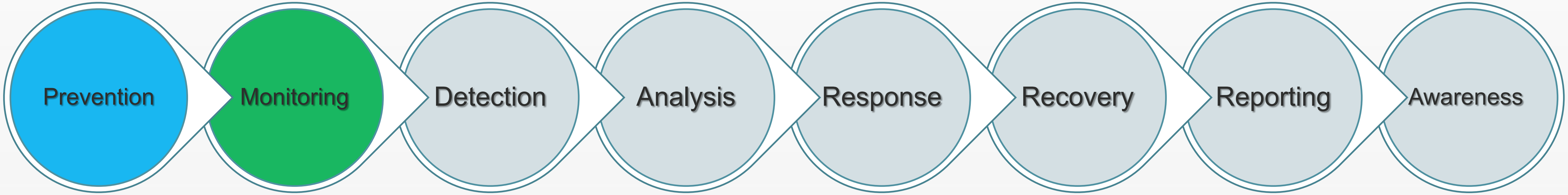
Free	2.3GB
Cache	792.3MB
Used	4.5GB

Disk IO (Bytes) [Metrics System] ECS

reads	0B/s
writes	-23.7KB/s

- **Capabilities & Skillset:**

- Spot unusual activities that might be threats.
- Catch hidden, ongoing attacks.
- Find and fix potential security risks due to device issues.
- Keep systems running smoothly to avoid security gaps.
- Know what normal looks like to spot when something's off.
- Look at data over time to spot trends and foresee threats.
- Find and fix overused or underused security resources.



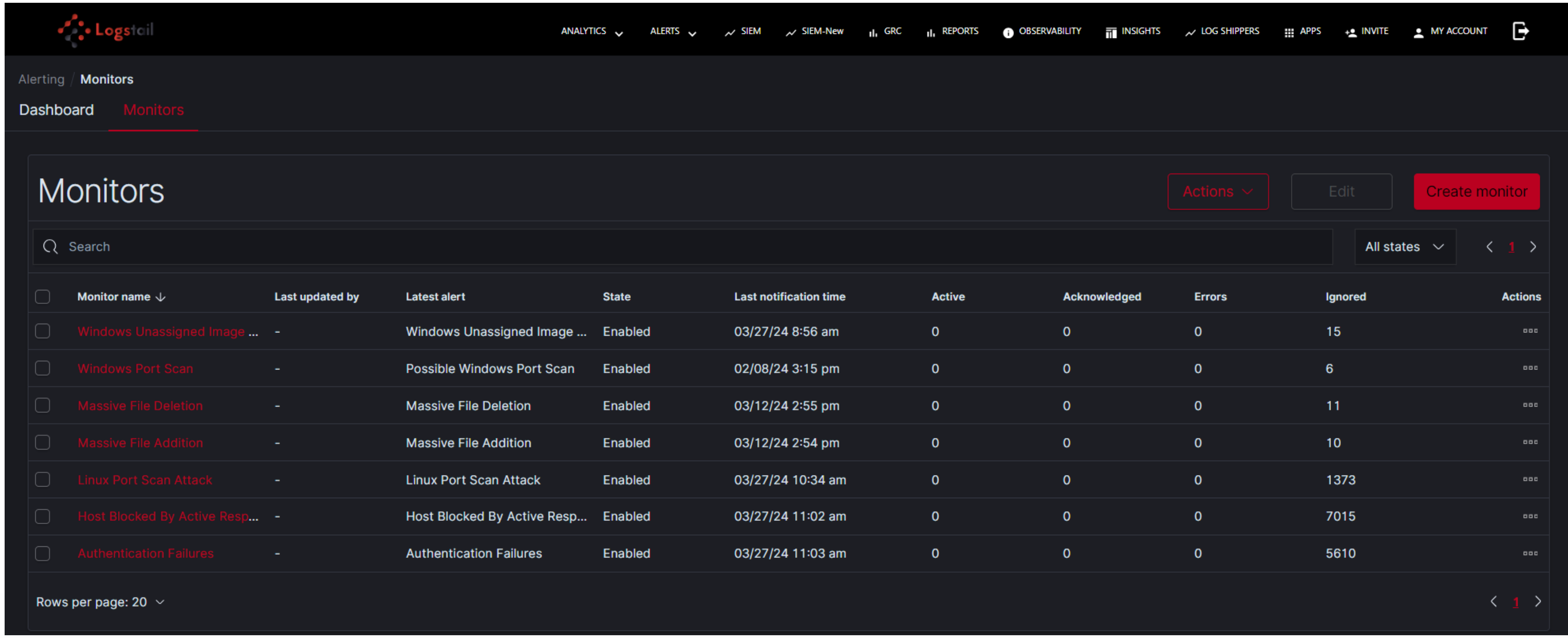
Prevention
Monitoring
Detection
Analysis
Response
Recovery
Reporting
Awareness

Rule Based Alerting

Create Custom Alerts

- **Alerting Capabilities**
  - Create Custom Alerting Rules
  - Get the Alerts to Email or to a Custom Platform

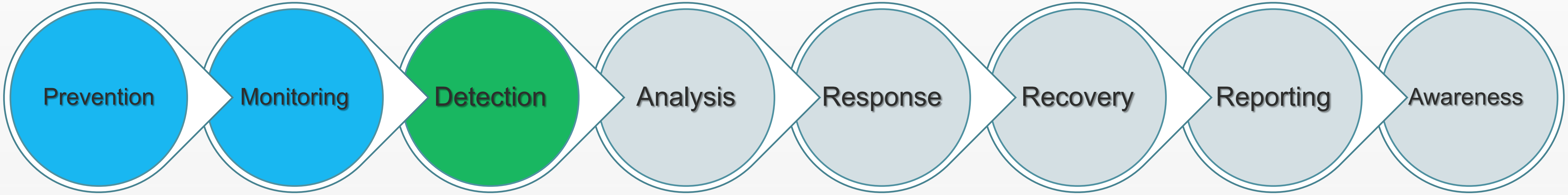
- **Capabilities & Skillset developed**
  - Quick awareness of potential security threats, allowing for rapid response.
  - Prioritize security tasks by distinguishing between critical issues and false alarms.
  - Constant watch on the security environment, nothing slips through unnoticed!



Monitors

□	Monitor name ↓	Last updated by	Latest alert	State	Last notification time	Active	Acknowledged	Errors	Ignored	Actions
□	Windows Unassigned Image ...	-	Windows Unassigned Image ...	Enabled	03/27/24 8:56 am	0	0	0	15	⋯
□	Windows Port Scan	-	Possible Windows Port Scan	Enabled	02/08/24 3:15 pm	0	0	0	6	⋯
□	Massive File Deletion	-	Massive File Deletion	Enabled	03/12/24 2:55 pm	0	0	0	11	⋯
□	Massive File Addition	-	Massive File Addition	Enabled	03/12/24 2:54 pm	0	0	0	10	⋯
□	Linux Port Scan Attack	-	Linux Port Scan Attack	Enabled	03/27/24 10:34 am	0	0	0	1373	⋯
□	Host Blocked By Active Resp...	-	Host Blocked By Active Resp...	Enabled	03/27/24 11:02 am	0	0	0	7015	⋯
□	Authentication Failures	-	Authentication Failures	Enabled	03/27/24 11:03 am	0	0	0	5610	⋯

Rows per page: 20



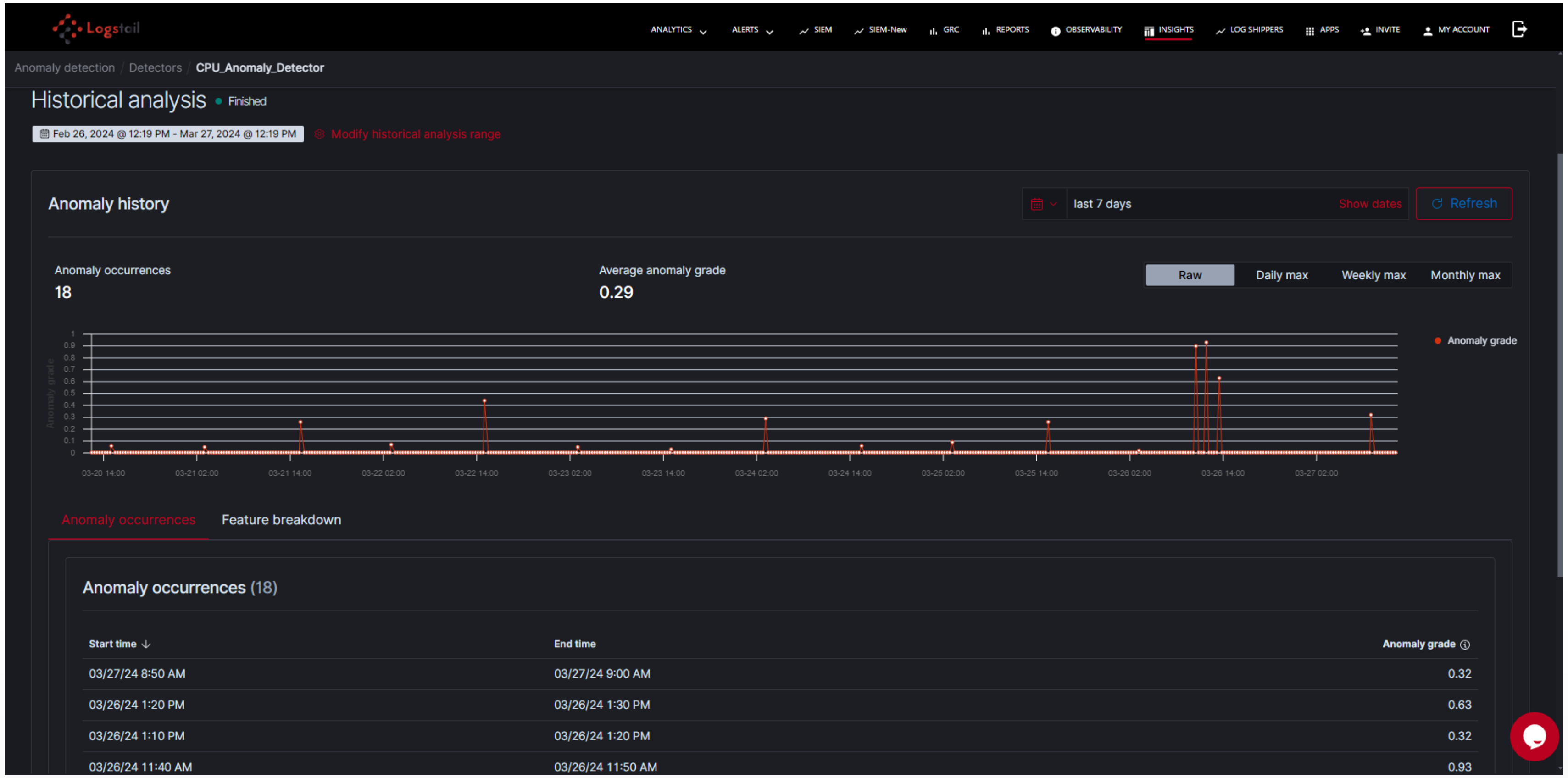
Prevention → Monitoring → Detection → Analysis → Response → Recovery → Reporting → Awareness

Anomaly Based Alerting

Create Custom Detectors

- **Alerting Capabilities**
  - Create Custom Anomaly Detectors
  - Integrate with Alerting feature.

- **Capabilities & Skillset developed**
  - Catches suspicious activities that could lead to data theft or loss.
  - Continuously learns from normal behaviour, refining the detection of future anomalies.
  - Identifies unusual behaviour early, often before specific threats are recognized.

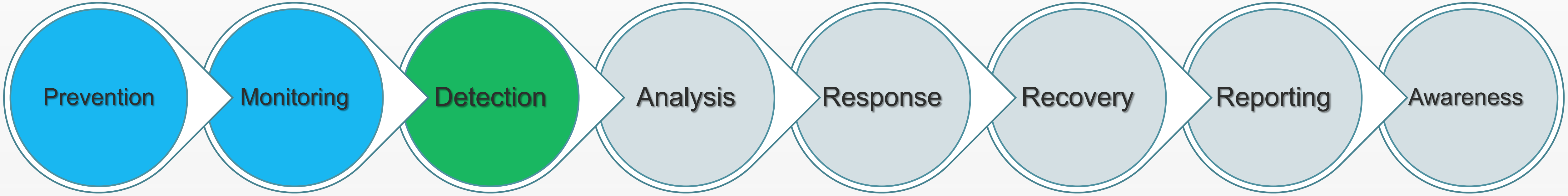


Anomaly occurrences
18

Average anomaly grade
0.29

Anomaly occurrences (18)

Start time ↓	End time	Anomaly grade ⓘ
03/27/24 8:50 AM	03/27/24 9:00 AM	0.32
03/26/24 1:20 PM	03/26/24 1:30 PM	0.63
03/26/24 1:10 PM	03/26/24 1:20 PM	0.32
03/26/24 11:40 AM	03/26/24 11:50 AM	0.93

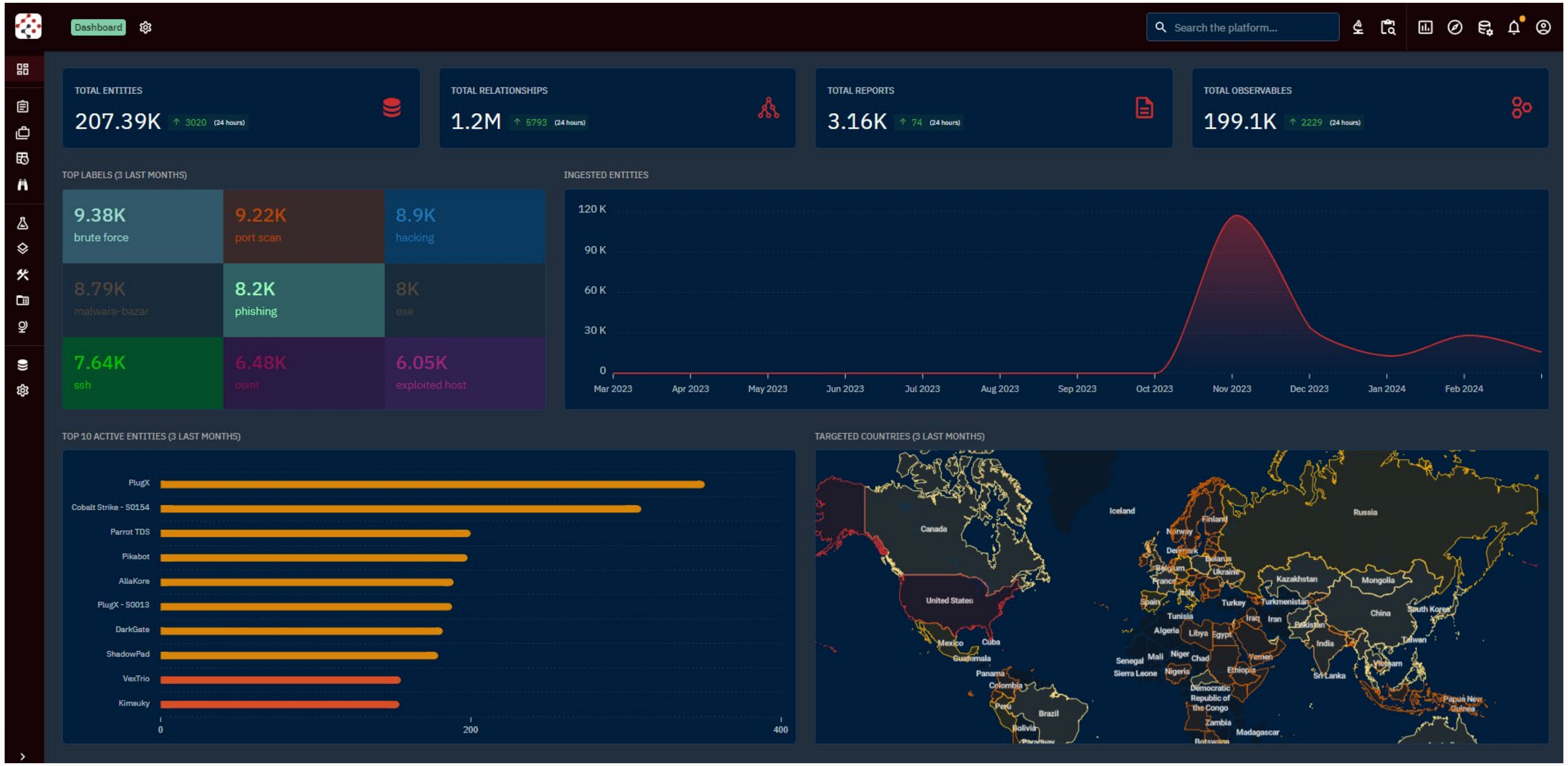


Prevention → Monitoring → Detection → Analysis → Response → Recovery → Reporting → Awareness

Cyber Threat Intelligence

Data Sources: Logstail CTI Module - MITRE ATT&CK

- **Capabilities & Skillset developed:**
  - Leverage Threat Intelligence
  - Incident Response Skills
  - Mitigation Actions based on MITRE ATT&CK
  - Mitigation Actions based on Logstail CTI Module



Dashboard

Search the platform...

TOTAL ENTITIES
207.39K ↑ 3020 (24 hours)

TOTAL RELATIONSHIPS
1.2M ↑ 5793 (24 hours)

TOTAL REPORTS
3.16K ↑ 74 (24 hours)

TOTAL OBSERVABLES
199.1K ↑ 2229 (24 hours)

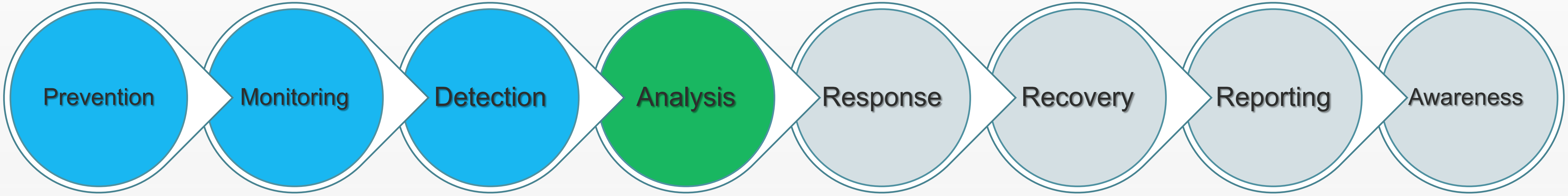
TOP LABELS (3 LAST MONTHS)

9.38K brute force	9.22K port scan	8.9K hacking
8.79K malware-bazar	8.2K phishing	8K exe
7.64K ssh	6.48K osint	6.05K exploited host

INGESTED ENTITIES

TOP 10 ACTIVE ENTITIES (3 LAST MONTHS)

TARGETED COUNTRIES (3 LAST MONTHS)

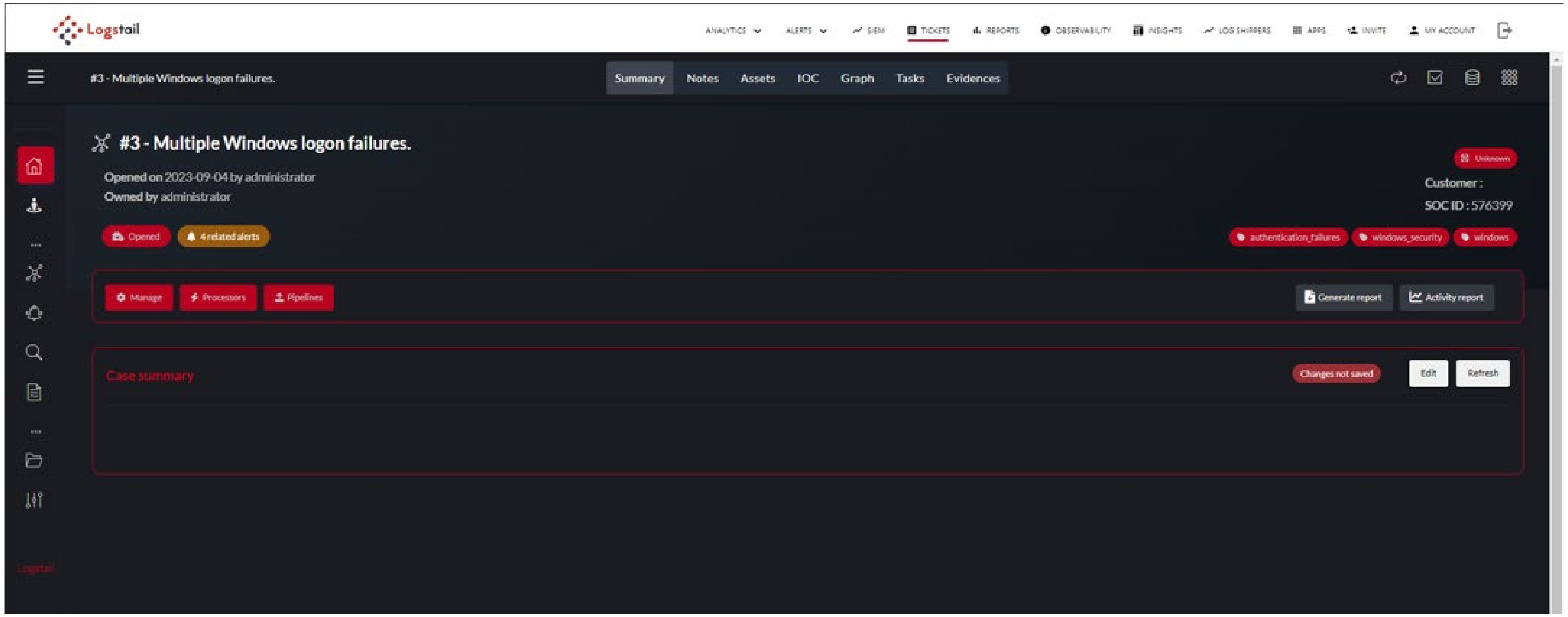


Ticketing

Integration with Ticketing Systems

➢ **Skillset developed:**

- Structured Response Workflow.
- Accountability and Tracking.
- Documentation for Analysis.
- Efficiency and Prioritization.
- Communication Channel.



#3 - Multiple Windows logon failures.

Opened on 2023-09-04 by administrator
Owned by administrator

Opened · 4 related alerts

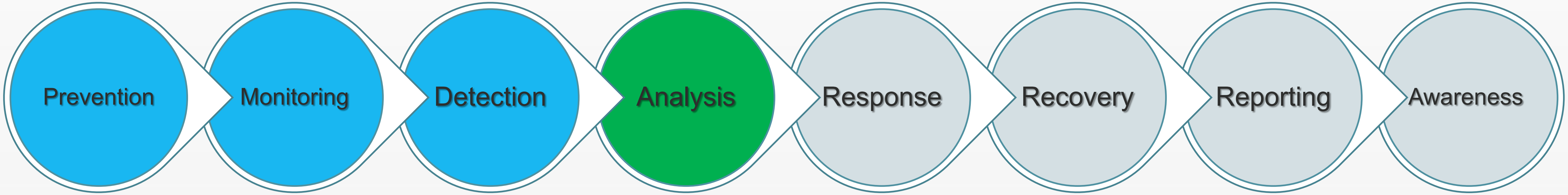
Unknown

Customer :
SOC ID : 576399

authentication_failures · windows_security · windows

Case summary

Changes not saved



Prevention → Monitoring → Detection → Analysis → Response → Recovery → Reporting → Awareness

Active Response

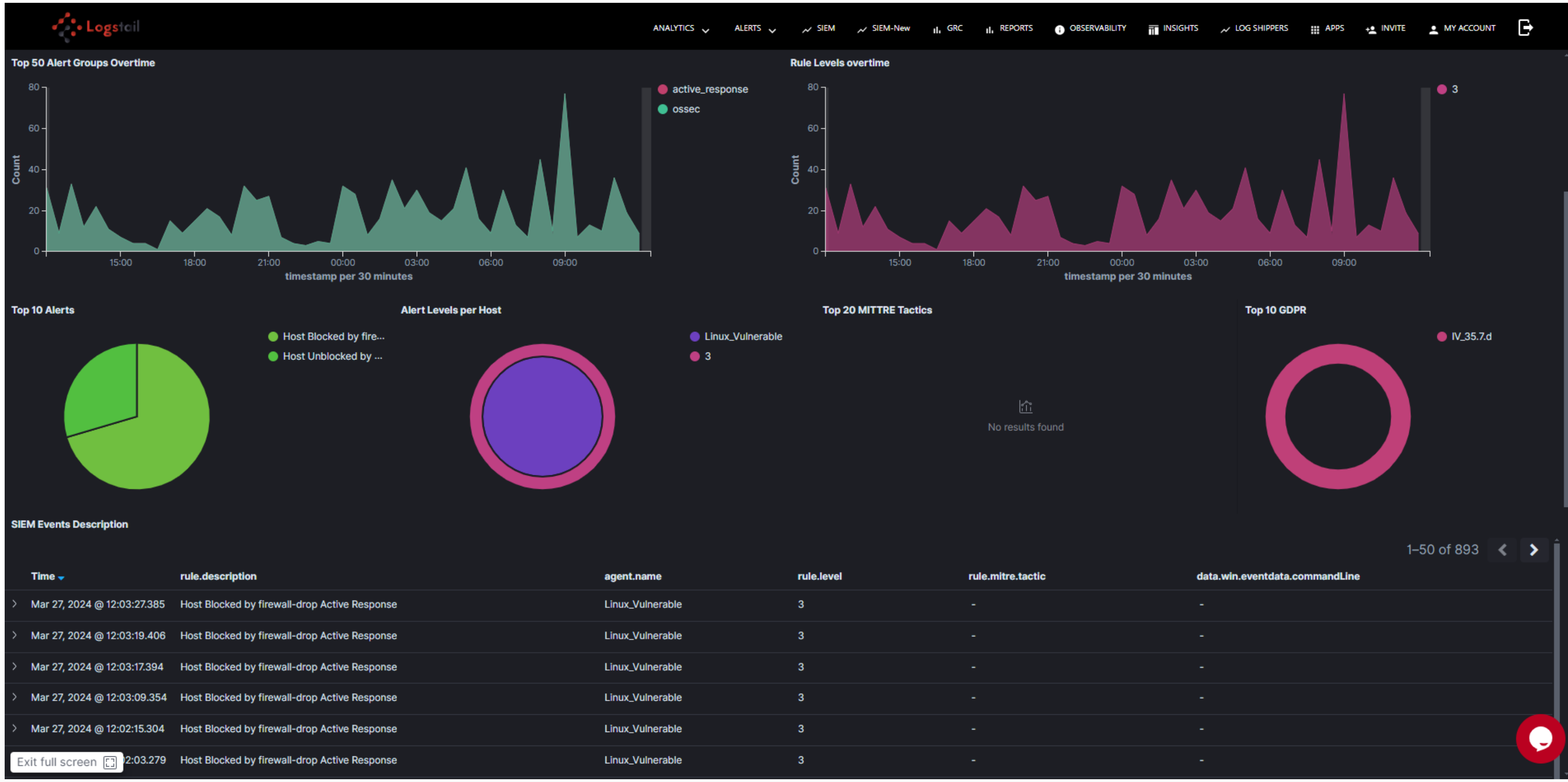
Response Scripts & Actions tailored to Environment

AR Capabilities:

- Control Endpoints
- Develop Custom Responses
- Adapt security measures based on current threat landscape and incident feedback.
- Automatic Response based on Rules

➢ **Capabilities & Skillset developed:**

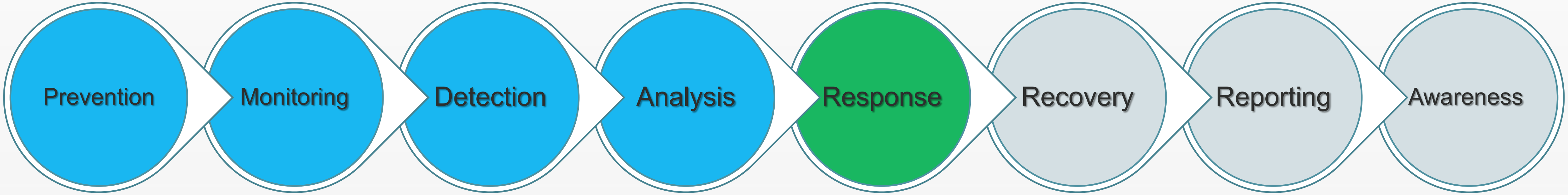
- Neutralize detected threats, reducing potential damage.
- Cut down the time between threat detection and response.
- Free up security teams by handling routine responses.
- Strengthen defenses by learning from attacks and improving responses over time.



SIEM Events Description

1–50 of 893

Time	rule.description	agent.name	rule.level	rule.mitre.tactic	data.win.eventdata.commandLine
Mar 27, 2024 @ 12:03:27.385	Host Blocked by firewall-drop Active Response	Linux_Vulnerable	3	-	-
Mar 27, 2024 @ 12:03:19.406	Host Blocked by firewall-drop Active Response	Linux_Vulnerable	3	-	-
Mar 27, 2024 @ 12:03:17.394	Host Blocked by firewall-drop Active Response	Linux_Vulnerable	3	-	-
Mar 27, 2024 @ 12:03:09.354	Host Blocked by firewall-drop Active Response	Linux_Vulnerable	3	-	-
Mar 27, 2024 @ 12:02:15.304	Host Blocked by firewall-drop Active Response	Linux_Vulnerable	3	-	-
2:03.279	Host Blocked by firewall-drop Active Response	Linux_Vulnerable	3	-	-



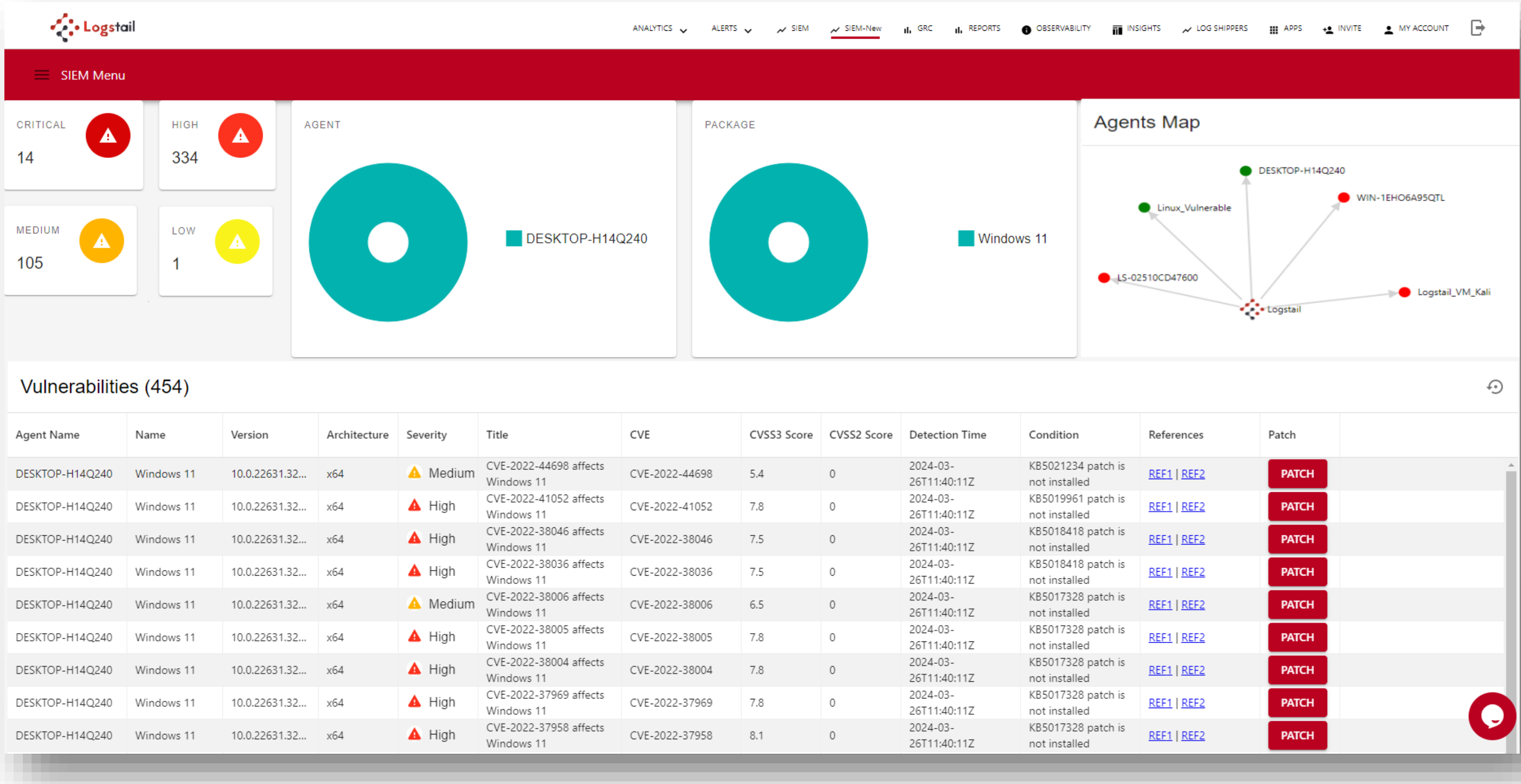
Prevention → Monitoring → Detection → Analysis → Response → Recovery → Reporting → Awareness

Vulnerability Patching

Patch Detected Software Vulnerabilities

➢ **Capabilities & Skillset:**

- Prevents Exploits
- Maintains Compliance
- Ensures System Stability



CRITICAL 14

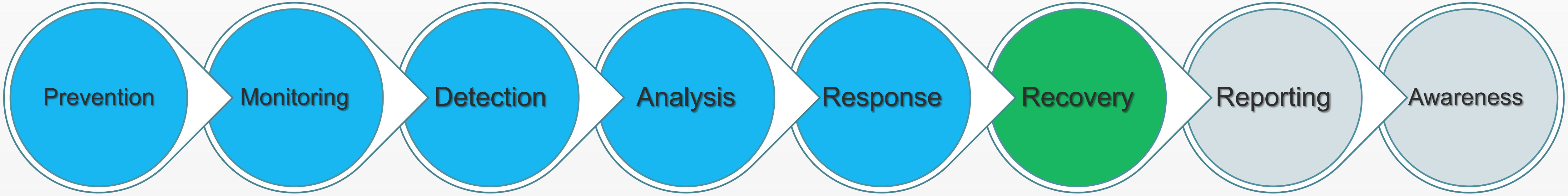
HIGH 334

MEDIUM 105

LOW 1

Vulnerabilities (454)

Agent Name	Name	Version	Architecture	Severity	Title	CVE	CVSS3 Score	CVSS2 Score	Detection Time	Condition	References	Patch
DESKTOP-H14Q240	Windows 11	10.0.22631.32...	x64	⚠ Medium	CVE-2022-44698 affects Windows 11	CVE-2022-44698	5.4	0	2024-03-26T11:40:11Z	KB5021234 patch is not installed	REF1 | REF2	PATCH
DESKTOP-H14Q240	Windows 11	10.0.22631.32...	x64	⚠ High	CVE-2022-41052 affects Windows 11	CVE-2022-41052	7.8	0	2024-03-26T11:40:11Z	KB5019961 patch is not installed	REF1 | REF2	PATCH
DESKTOP-H14Q240	Windows 11	10.0.22631.32...	x64	⚠ High	CVE-2022-38046 affects Windows 11	CVE-2022-38046	7.5	0	2024-03-26T11:40:11Z	KB5018418 patch is not installed	REF1 | REF2	PATCH
DESKTOP-H14Q240	Windows 11	10.0.22631.32...	x64	⚠ High	CVE-2022-38036 affects Windows 11	CVE-2022-38036	7.5	0	2024-03-26T11:40:11Z	KB5018418 patch is not installed	REF1 | REF2	PATCH
DESKTOP-H14Q240	Windows 11	10.0.22631.32...	x64	⚠ Medium	CVE-2022-38006 affects Windows 11	CVE-2022-38006	6.5	0	2024-03-26T11:40:11Z	KB5017328 patch is not installed	REF1 | REF2	PATCH
DESKTOP-H14Q240	Windows 11	10.0.22631.32...	x64	⚠ High	CVE-2022-38005 affects Windows 11	CVE-2022-38005	7.8	0	2024-03-26T11:40:11Z	KB5017328 patch is not installed	REF1 | REF2	PATCH
DESKTOP-H14Q240	Windows 11	10.0.22631.32...	x64	⚠ High	CVE-2022-38004 affects Windows 11	CVE-2022-38004	7.8	0	2024-03-26T11:40:11Z	KB5017328 patch is not installed	REF1 | REF2	PATCH
DESKTOP-H14Q240	Windows 11	10.0.22631.32...	x64	⚠ High	CVE-2022-37969 affects Windows 11	CVE-2022-37969	7.8	0	2024-03-26T11:40:11Z	KB5017328 patch is not installed	REF1 | REF2	PATCH
DESKTOP-H14Q240	Windows 11	10.0.22631.32...	x64	⚠ High	CVE-2022-37958 affects Windows 11	CVE-2022-37958	8.1	0	2024-03-26T11:40:11Z	KB5017328 patch is not installed	REF1 | REF2	PATCH



Prevention

Monitoring

Detection

Analysis

Response

Recovery

Reporting

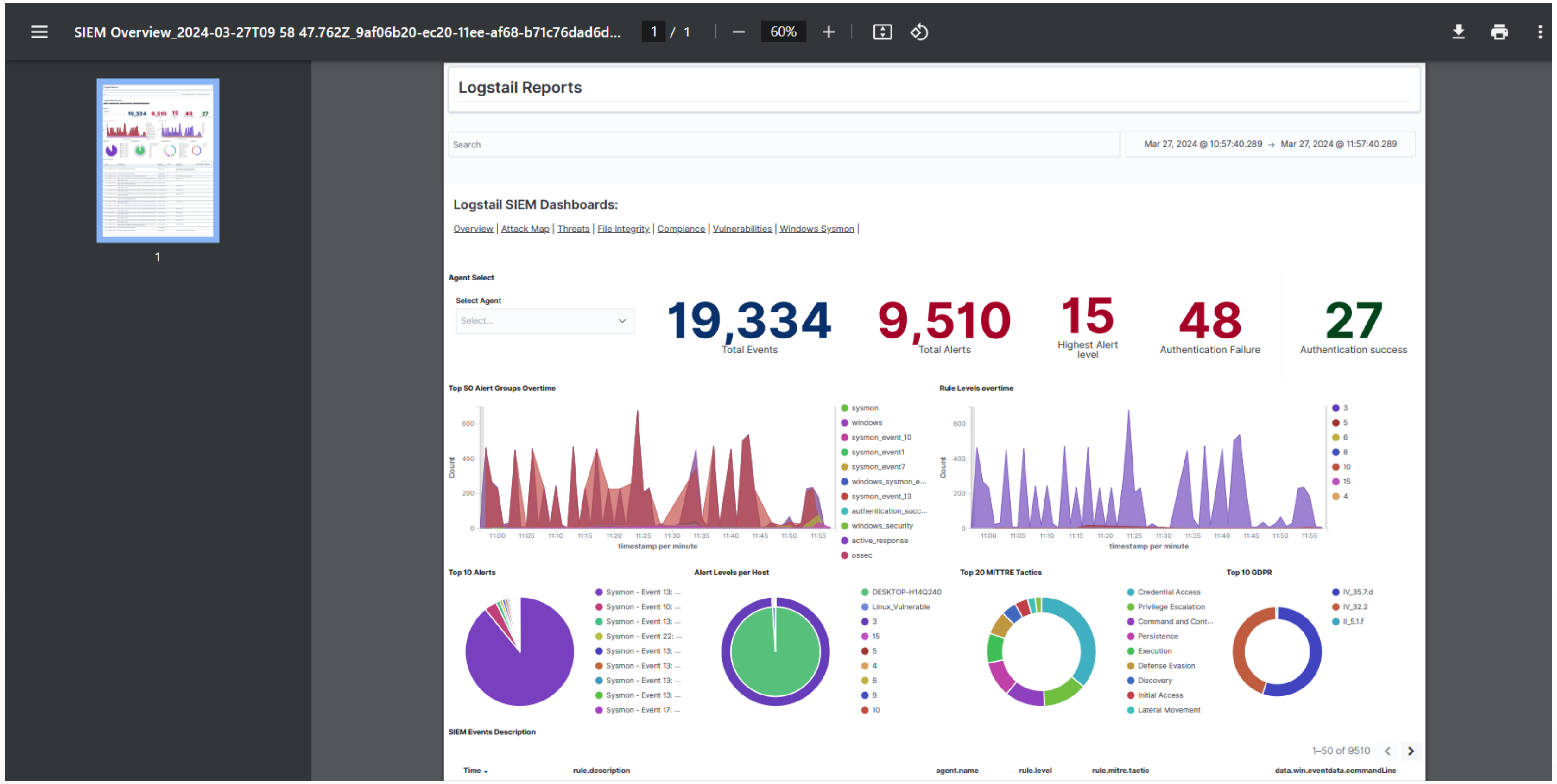
Awareness

Reporting

Create Custom Reports

- **Reporting Capabilities**
  - Create Custom Reports
  - Schedule the Reports

- **Capabilities & Skillset developed**
  - Data-driven insights for making strategic security decisions.
  - Clear communication about security posture and incidents to stakeholders.
  - Documentation and evidence are in place for compliance with security regulations.


SIEM Overview_2024-03-27T09 58 47.762Z_9af06b20-ec20-11ee-af68-b71c76dad6d... 1 / 1 60%

Logstail Reports

Search

Mar 27, 2024 @ 10:57:40.289 → Mar 27, 2024 @ 11:57:40.289

Logstail SIEM Dashboards:

Overview | Attack Map | Threats | File Integrity | Compiance | Vulnerabilities | Windows Sysmon |

Agent Select

Select Agent: Select...

19,334 Total Events

9,510 Total Alerts

15 Highest Alert level

48 Authentication Failure

27 Authentication success

Top 50 Alert Groups Overtime

Rule Levels overtime

Top 10 Alerts

Alert Levels per Host

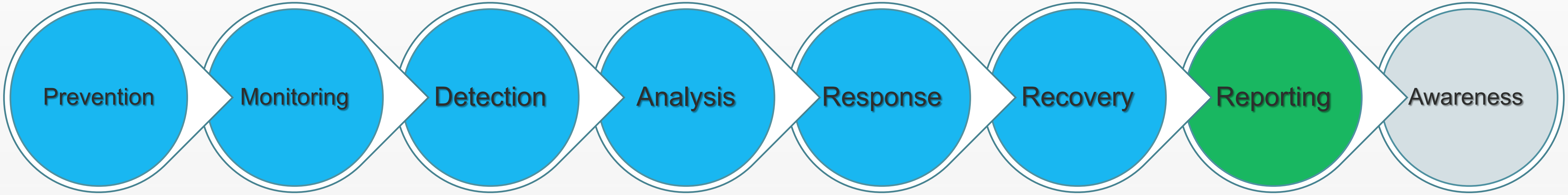
Top 20 MITTRE Tactics

Top 10 GDPR

SIEM Events Description

1–50 of 9510

Time	rule.description	agent.name	rule.level	rule.mitre.tactic	data.win.eventdata.commandLine


Prevention

Monitoring

Detection

Analysis

Response

Recovery

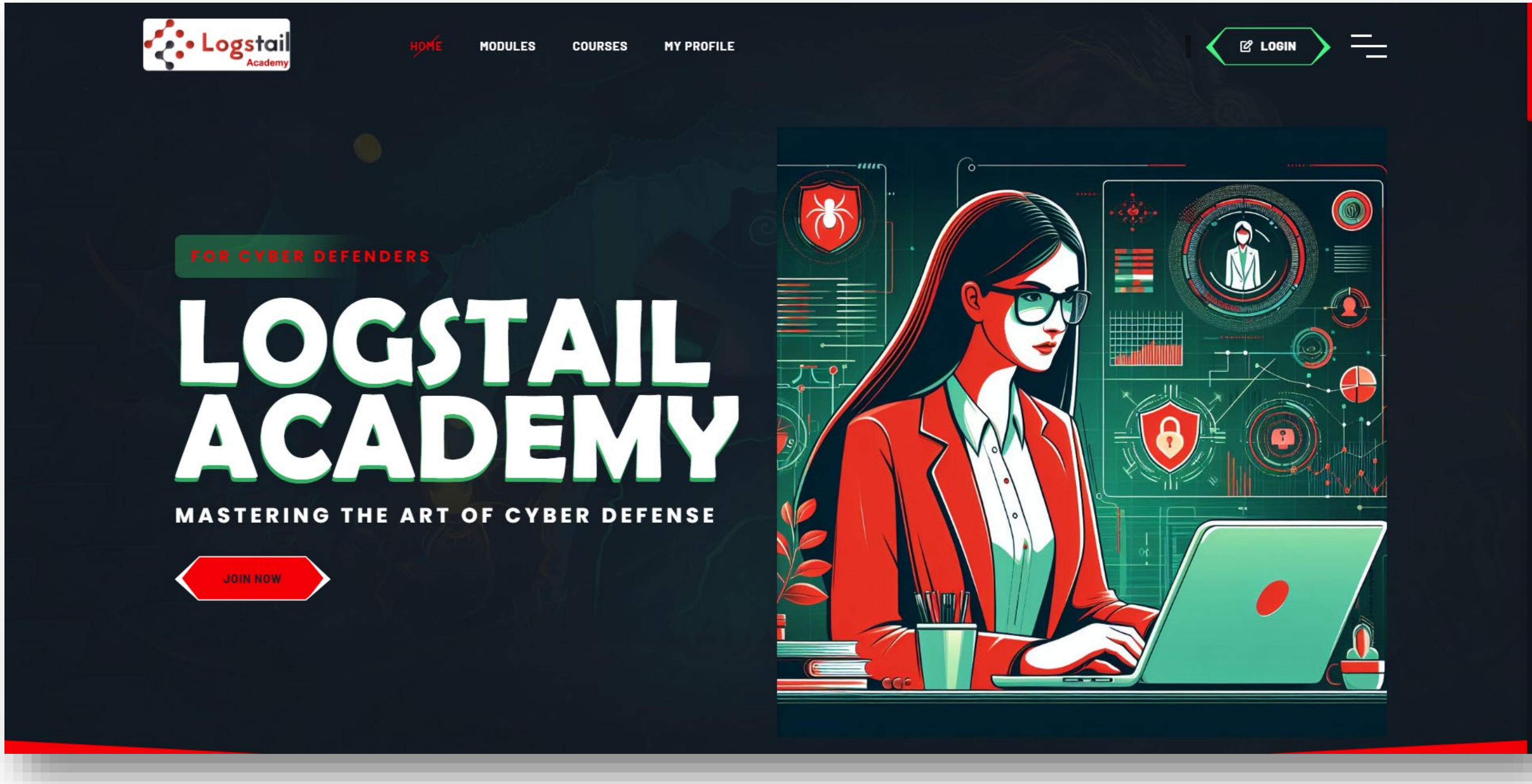
Reporting

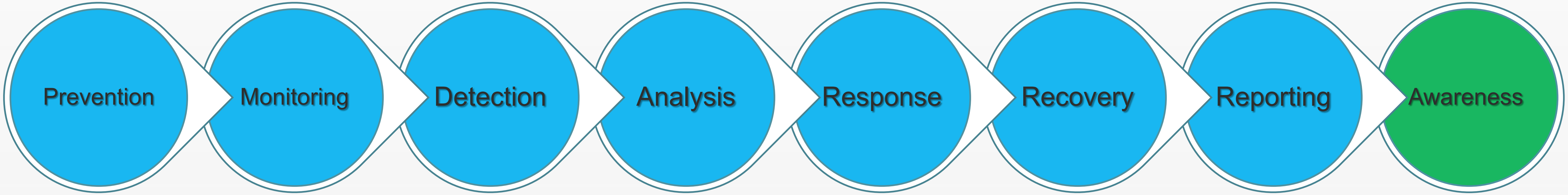
Awareness

Academy

Train your SOC Team

- **Skillset developed:**
  - Courses and materials that cover a wide range of topics within log management, cybersecurity, and data analysis.
  - Practical skills that are highly relevant to current industry needs and trends in IT security and data management.





Thank you!

Logstail

Contact Us

HQ: Theofanous 12, Athens 11523

☎ +30 216 0037838

sales@logstail.com

https://logstail.com