UNIT 2
CYBER THREAT HUNTING

Tejas Mhaske

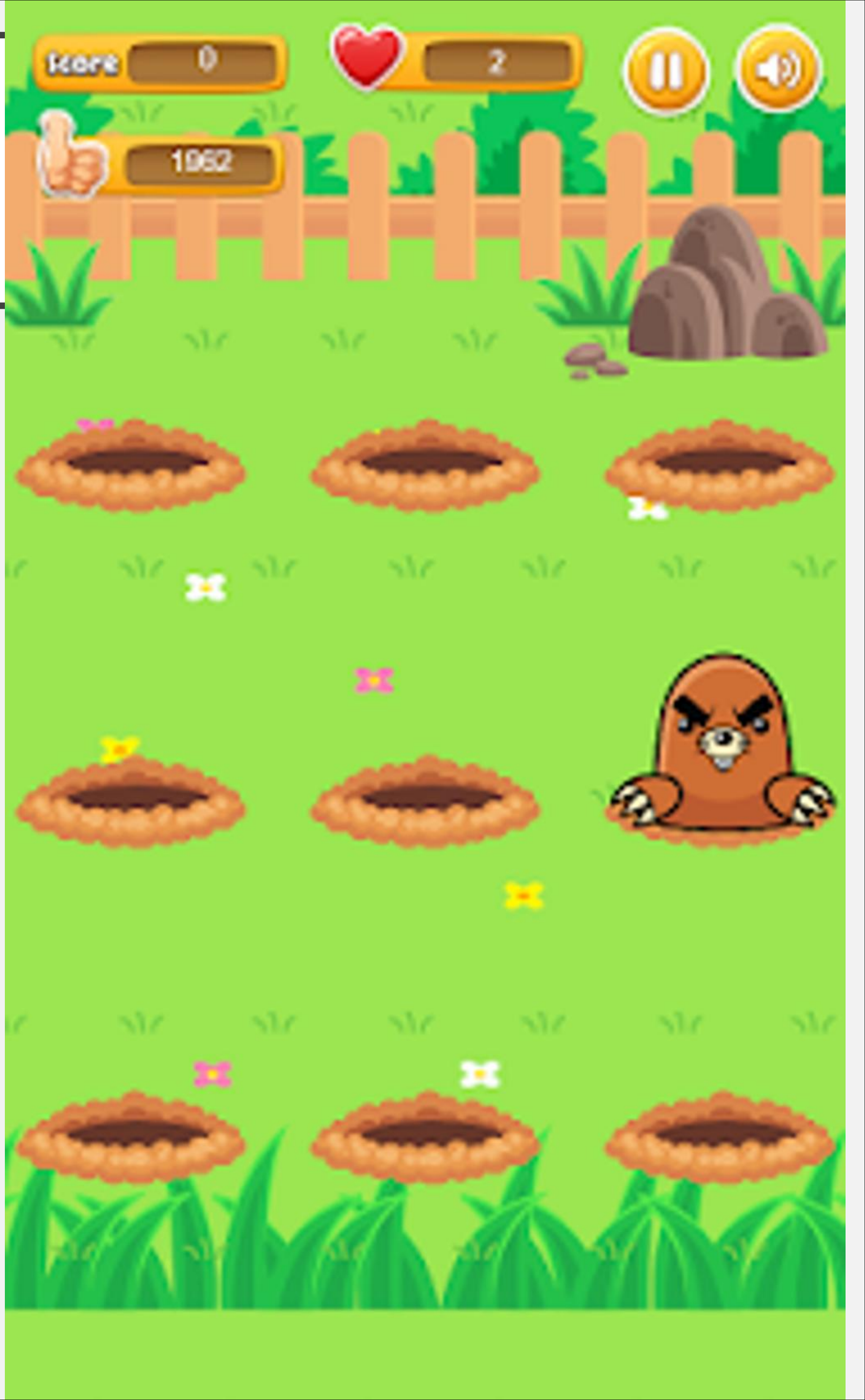
Cyber Security Trainer

INTRODUCTION TO CYBER THREAT HUNTING

- Cyber Threat Hunting is a **proactive approach** to identifying, investigating, and mitigating cyber threats that evade traditional security tools like firewalls and antivirus software. Unlike automated defenses, threat hunting involves human expertise and active exploration of potential risks.

Key Features:

- Focuses on **unknown threats** or anomalies.
- Combines **human intelligence** and **automated tools**.
- Aims to identify advanced persistent threats (APTs) or stealthy attackers.



CYBER THREAT HUNTING METHODOLOGIES

A. Hypothesis-Driven Hunting

- Based on a **theory** or suspicion about potential threats.
- Uses intelligence from prior attacks or unusual system behaviors.
- **Example:** An analyst hypothesizes that attackers might exploit unpatched servers and searches logs for signs of exploitation.

CYBER THREAT HUNTING METHODOLOGIES

B. Indicator of Attack (IoA)-Driven Hunting

- Focuses on **attack patterns** rather than specific malware or signatures.
- Looks for suspicious activities like unusual file transfers or privilege escalations.
- **Example:** Identifying the use of tools like PowerShell scripts for lateral movement within the network.

CYBER THREAT HUNTING METHODOLOGIES

C. Analytics-Driven Hunting

- Leverages **machine learning** and advanced analytics to detect anomalies.
- Relies on analyzing large datasets to find deviations from normal behavio
- **Example:** Detecting abnormal traffic spikes to obscure regions using analytics tools.

THREAT HUNTING TOOLS AND TECHNIQUES

- **Key Tools Used in Threat Hunting**

1. **SIEM (Security Information and Event Management):**
    - Aggregates and analyzes logs from various systems.
    - **Example:** Splunk, IBM QRadar.
2. **Endpoint Detection and Response (EDR):**
    - Monitors endpoint activities for malicious behaviors.
    - **Example:** CrowdStrike Falcon, Carbon Black.

1. **Network Traffic Analysis (NTA):**
    - Monitors network traffic for anomalies.
    - **Example:** Darktrace, Cisco Stealthwatch.

THREAT HUNTING TOOLS AND TECHNIQUES

1. Security Information and Event Management (SIEM)

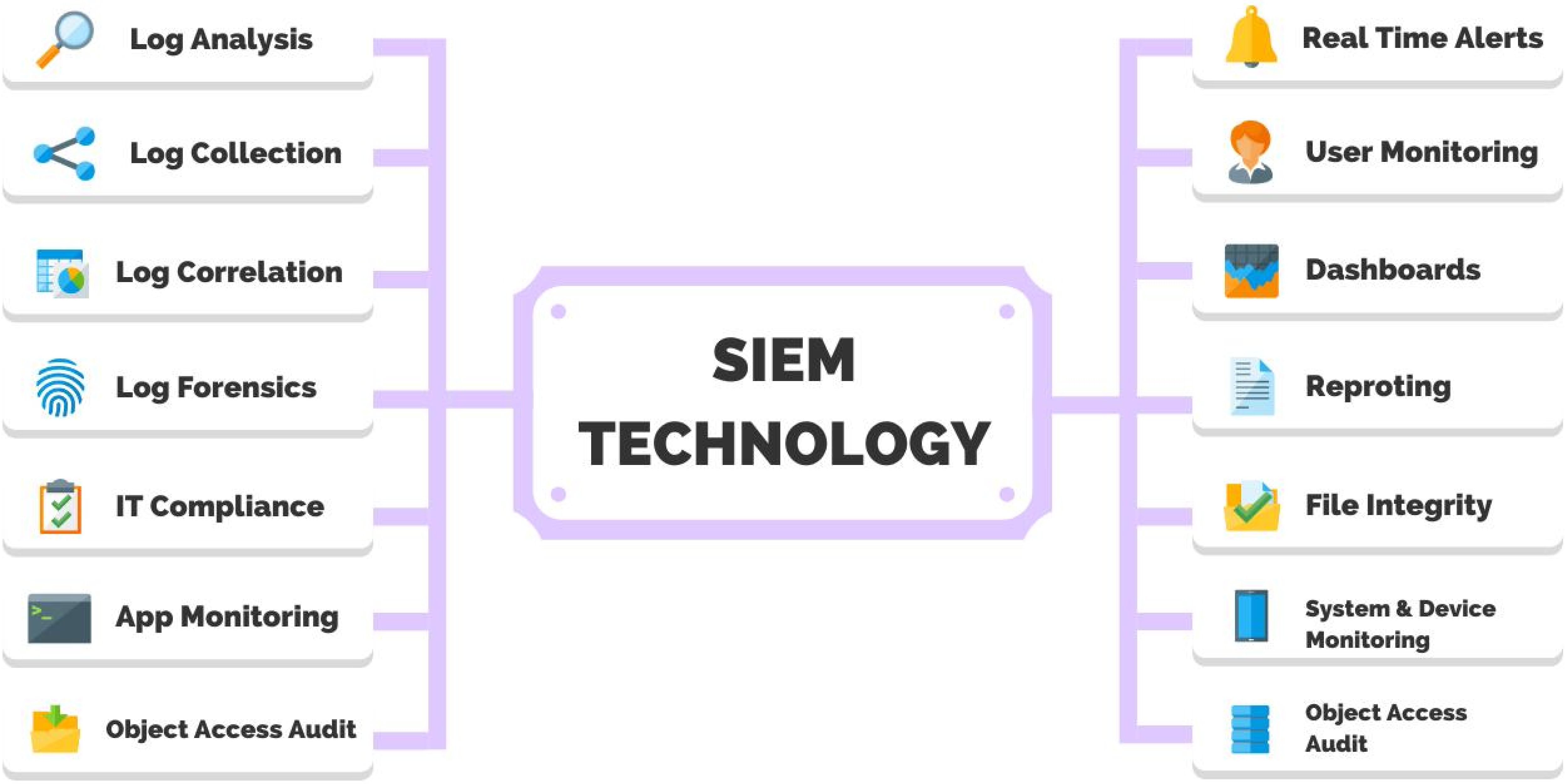
- **Purpose:** SIEM tools aggregate and analyze logs from various systems to detect security threats and compliance issues in real-time.

Functions:

- Collects data from diverse sources like servers, applications, and security devices.
- Correlates events to identify patterns indicating potential threats.
- Provides real-time alerts on suspicious activities.
- Facilitates incident response and investigation by offering detailed log analysis.

Examples:

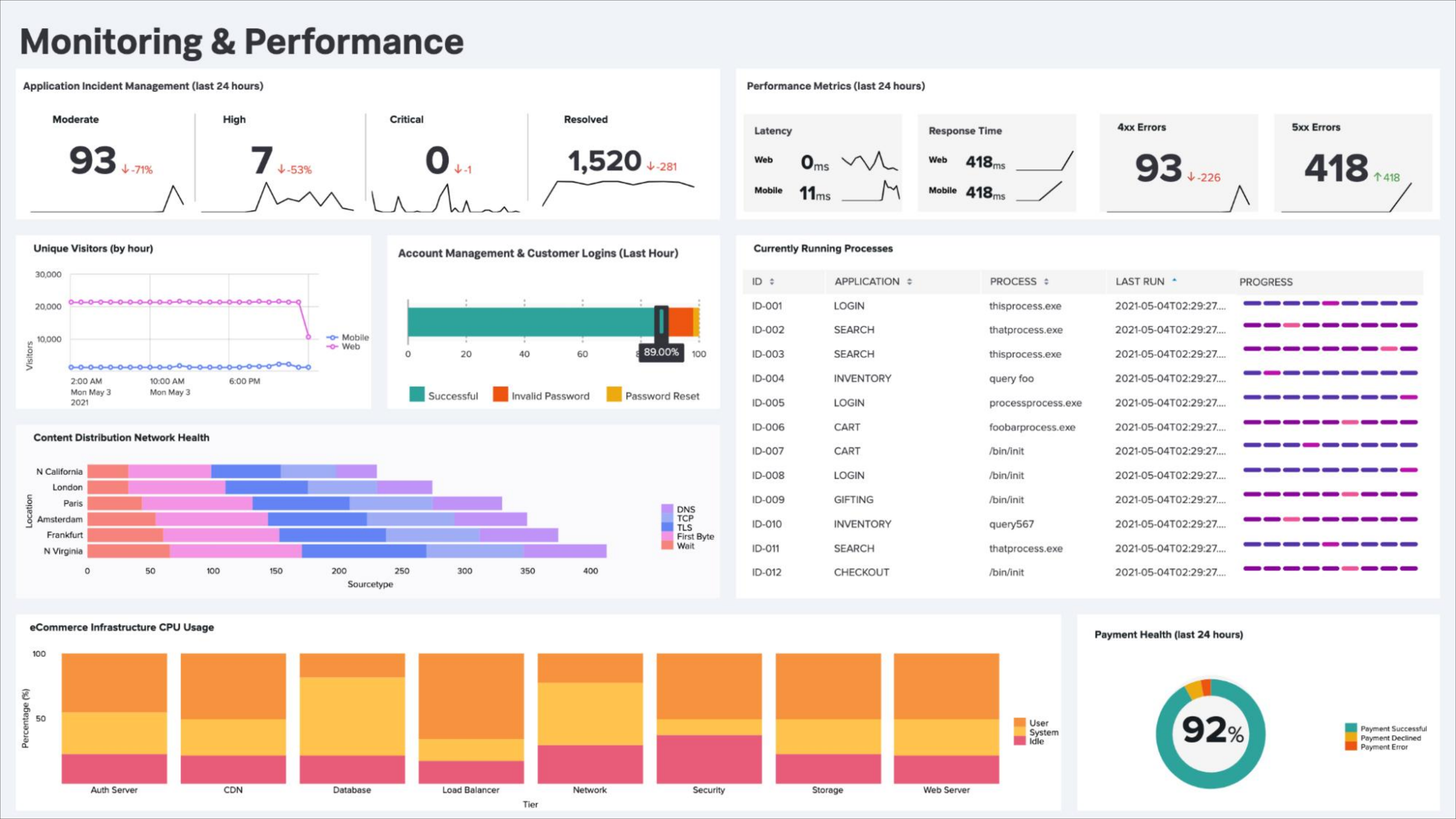
- **Splunk:** Known for its powerful search capabilities and user-friendly interface. It provides advanced analytics and visualization features.
- **IBM QRadar:** Highly efficient in threat detection through automated response



SIEM TECHNOLOGY

- Log Analysis
- Log Collection
- Log Correlation
- Log Forensics
- IT Compliance
- App Monitoring
- Object Access Audit

- Real Time Alerts
- User Monitoring
- Dashboards
- Reproting
- File Integrity
- System & Device Monitoring
- Object Access Audit



Monitoring & Performance

Application Incident Management (last 24 hours)

Moderate 93 ↓-71%

High 7 ↓-53%

Critical 0 ↓-1

Resolved 1,520 ↓-281

Performance Metrics (last 24 hours)

Latency

Web 0ms

Mobile 11ms

Response Time

Web 418ms

Mobile 418ms

4xx Errors 93 ↓-226

5xx Errors 418 ↑418

Unique Visitors (by hour)

Account Management & Customer Logins (Last Hour)

Currently Running Processes

ID	APPLICATION	PROCESS	LAST RUN	PROGRESS
ID-001	LOGIN	thisprocess.exe	2021-05-04T02:29:27....	
ID-002	SEARCH	thatprocess.exe	2021-05-04T02:29:27....	
ID-003	SEARCH	thisprocess.exe	2021-05-04T02:29:27....	
ID-004	INVENTORY	query foo	2021-05-04T02:29:27....	
ID-005	LOGIN	processprocess.exe	2021-05-04T02:29:27....	
ID-006	CART	foobarprocess.exe	2021-05-04T02:29:27....	
ID-007	CART	/bin/init	2021-05-04T02:29:27....	
ID-008	LOGIN	/bin/init	2021-05-04T02:29:27....	
ID-009	GIFTING	/bin/init	2021-05-04T02:29:27....	
ID-010	INVENTORY	query567	2021-05-04T02:29:27....	
ID-011	SEARCH	thatprocess.exe	2021-05-04T02:29:27....	
ID-012	CHECKOUT	/bin/init	2021-05-04T02:29:27....	

Content Distribution Network Health

eCommerce Infrastructure CPU Usage

Payment Health (last 24 hours)

THREAT HUNTING TOOLS AND TECHNIQUES

2. Endpoint Detection and Response (EDR)

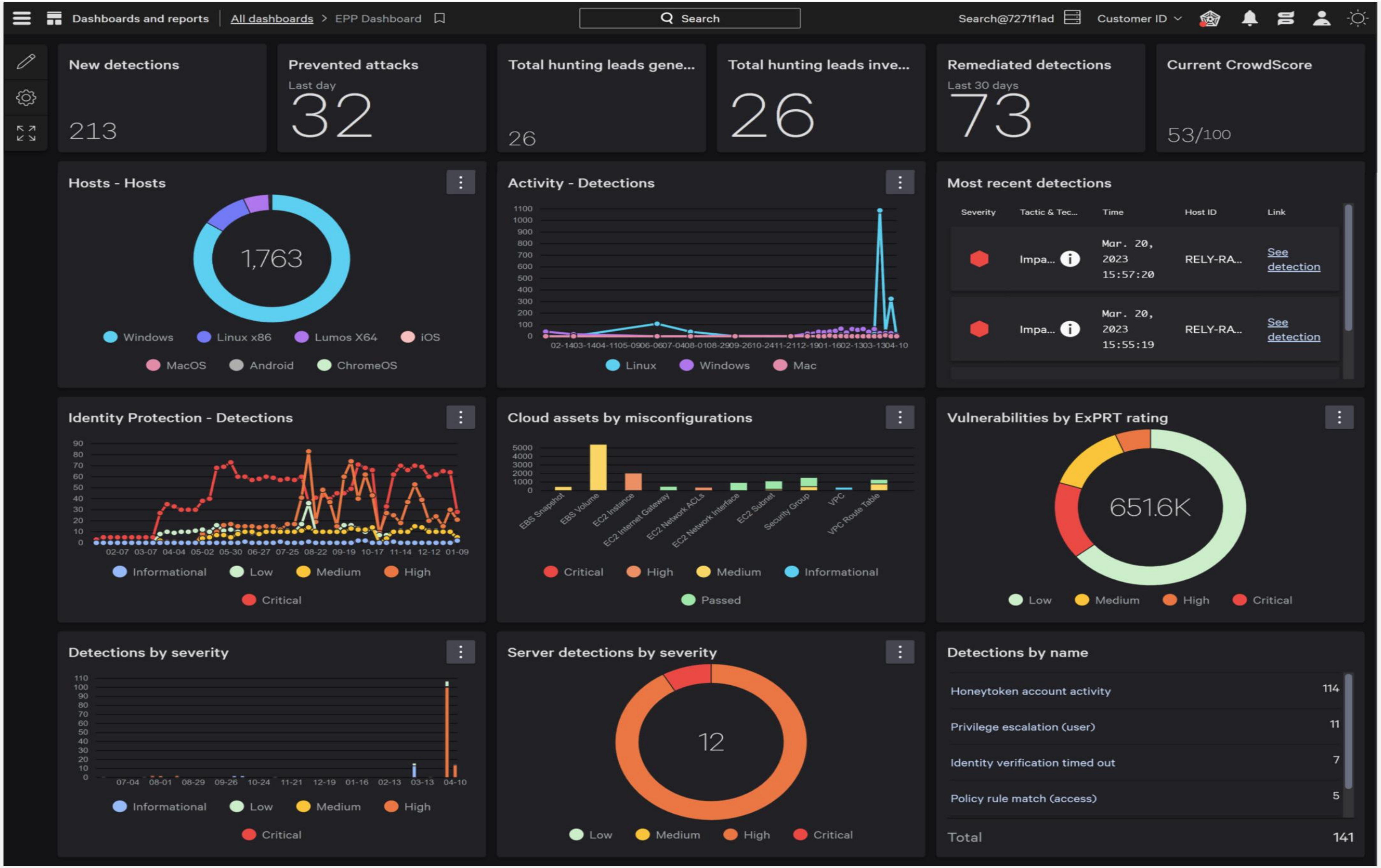
- **Purpose:** EDR tools monitor and respond to endpoint activities to detect malicious behaviors, providing insights into threats targeting endpoints like computers, mobile devices, and servers.

Functions:

- Continuously monitors endpoint activity for signs of malicious behavior.
- Provides deep visibility into endpoint processes, network activities, and file changes.
- Facilitates threat hunting by enabling security teams to detect, investigate, and respond to advanced threats.
- Offers remediation capabilities to contain and eliminate detected threats.

Examples:

- **CrowdStrike Falcon:** Renowned for its cloud-based architecture, real-time monitoring, and comprehensive threat intelligence.
- **Carbon Black:** Offers extensive visibility into endpoint activities and



New detections
213

Prevented attacks
Last day
32

Total hunting leads gene...
26

Total hunting leads inve...
26

Remediated detections
Last 30 days
73

Current CrowdScore
53/100

Hosts - Hosts

Activity - Detections

Most recent detections

Severity	Tactic & Tec...	Time	Host ID	Link
⬢	Impa... ⓘ	Mar. 20, 2023 15:57:20	RELY-RA...	See detection
⬢	Impa... ⓘ	Mar. 20, 2023 15:55:19	RELY-RA...	See detection

Identity Protection - Detections

Cloud assets by misconfigurations

Vulnerabilities by ExPRT rating

Detections by severity

Server detections by severity

Detections by name

Honeytoken account activity	114
Privilege escalation (user)	11
Identity verification timed out	7
Policy rule match (access)	5
Total	141

DIFFERENCE BETWEEN SIEM & EDR

Category	SIEM (Security Information and Event Management)	EDR (Endpoint Detection and Response)
Primary Function	Aggregates and analyzes logs from various systems to detect and respond to security incidents.	Monitors and responds to endpoint activities for signs of malicious behavior.
Data Sources	Collects data from servers, applications, network devices, security appliances, and more.	Monitors endpoint devices such as computers, mobile devices, and servers.
Threat Detection	Detects threats by correlating events across multiple systems and logs.	Identifies threats based on endpoint behaviors and activities.
Incident Response	Provides real-time alerts and detailed log analysis to assist in incident response.	Offers remediation capabilities to contain and eliminate threats on endpoints.
Visibility	Provides a centralized view of security events across the entire organization.	Offers deep visibility into endpoint processes, network activities, and file changes.

DIFFERENCE BETWEEN SIEM & EDR

Category	SIEM (Security Information and Event Management)	EDR (Endpoint Detection and Response)
Use Cases	Ideal for detecting broad security issues and ensuring compliance.	Best for identifying and responding to endpoint-specific threats.
Examples	Splunk, IBM QRadar	CrowdStrike Falcon, Carbon Black
Deployment	Typically deployed in a centralized manner to cover the entire IT infrastructure.	Deployed on individual endpoints to monitor activities and behaviors.
Analytics	Utilizes advanced correlation and analytics to identify patterns and anomalies.	Employs behavioral analysis and machine learning to detect sophisticated threats.
Integration	Integrates with a wide range of other security tools and systems for comprehensive coverage.	Often integrates with SIEM and other security solutions for enhanced threat visibility.

TECHNIQUES USED IN THREAT HUNTING

1. **Log Analysis:**
    - Reviewing system logs to identify unauthorized access or unusual patterns.
    - **Example:** Analyzing login failures followed by a successful login from the same IP.
2. **Behavioral Analysis:**
    - Studying user and system behaviors to identify anomalies.
    - **Example:** Detecting a user downloading large files at unusual hours.
3. **Forensic Analysis:**
    - Investigating systems and files for traces of compromise.
    - **Example:** Recovering deleted files to trace malware origins.
4. **Lateral Movement Detection:**
    - Tracking how attackers move within the network after gaining access.
    - **Example:** Monitoring for unexpected connections between internal systems.

ADVERSARY EMULATION AND SIMULATION

- Adversary emulation and simulation are proactive cybersecurity techniques that help organizations evaluate and enhance their defenses by mimicking real-world attack scenarios. These methods are essential for identifying vulnerabilities and improving the overall security posture.
- **Adversary Emulation**
- **Purpose:** Adversary emulation focuses on replicating the tactics, techniques, and procedures (TTPs) used by known attackers. This approach is highly detailed and specific, aiming to test how well an organization's defenses can detect and respond to actual attack methods used by cyber adversaries.
- **Key Points:**
- **Tactics, Techniques, and Procedures (TTPs):** Emulation uses the exact methods that real attackers would employ, based on intelligence gathered from previous attacks.
- **Frameworks:** Often informed by frameworks like MITRE ATT&CK, which provides a comprehensive knowledge base of adversary behaviors.

ADVERSARY EMULATION AND SIMULATION

- **Purpose:** Adversary simulation is broader than emulation and encompasses a wider range of attack scenarios. It aims to test the resilience of an organization's systems, processes, and response plans against various types of attacks, not limited to specific TTPs.
- **Key Points:**
- **Broader Scope:** Includes various attack scenarios, such as phishing campaigns, social engineering, and other tactics beyond specific TTPs.
- **Testing Resilience:** Focuses on assessing the effectiveness of an organization's overall security strategy, including employee awareness and incident response procedures.
- **Example:** Conducting a simulated phishing campaign targeting employees to assess their ability to recognize and report phishing attempts. This helps in evaluating and improving the organization's security awareness training programs.

ADVERSARY EMULATION VS ADVERSARY SIMULATION

Aspect	Adversary Emulation	Adversary Simulation
Focus	Replicates specific TTPs of known attackers.	Includes a broader range of attack scenarios.
Frameworks	Often uses frameworks like MITRE ATT&CK.	May or may not use specific frameworks.
Purpose	Tests the effectiveness of security controls against known attack methods.	Tests the resilience of systems, processes, and response plans.
Example	Simulating a ransomware attack based on specific TTPs used by a ransomware group.	Conducting a phishing campaign to assess employee awareness and detection.
Tools	CALDERA, Red Team Operations.	Phishing Simulation Tools, Incident Response Drills.

THREAT HUNTING IN CLOUD ENVIRONMENTS

- Threat hunting in cloud environments refers to the proactive process of actively searching for potential cyber threats within a cloud infrastructure by analyzing various data sources like logs, network traffic, and user activity, aiming to identify malicious activity that might have evaded standard security controls, allowing for early detection and response before significant damage occurs.

KEY TECHNIQUES FOR CLOUD THREAT HUNTING

1. Log Monitoring:

- Analyze cloud-specific logs like AWS CloudTrail or Azure Monitor for suspicious activities.
- **Example:** Detecting unauthorized API calls in AWS CloudTrail logs.

2. Access Control Monitoring:

- Regularly audit identity and access management (IAM) policies.
- **Example:** Identifying overprivileged accounts with access to sensitive cloud resources.

3. Network Traffic Analysis:

- Monitor data flows between on-premises systems and the cloud.
- **Example:** Detecting unusual traffic to external IPs from cloud servers.

4. Behavioral Analysis:

- Use machine learning to detect anomalies in user behaviors.
- **Example:** Spotting login attempts from untrusted locations using Azure Security Center.

TOOLS FOR CLOUD THREAT HUNTING

- **AWS GuardDuty:** Detects threats in Amazon Web Services environments.
- **Azure Sentinel:** Cloud-native SIEM for advanced hunting and analytics.
- **Google Chronicle:** Cloud-based threat intelligence and hunting platform

धन्यवाद

ASSIGNMENT

1. What is cyber threat hunting, and how does it differ from traditional threat detection methods?
2. Compare different cyber threat hunting methodologies.
3. Identify key tools and techniques used in cyber threat hunting.
4. Describe the roles of adversary emulation and simulation in cyber threat hunting.
5. Discuss the challenges and strategies of threat hunting in cloud environments.