

CYBROTECH PRESENTS

“SACHET”

SOC/SIEM

“सचेत”

TAME THE BEAST, IN THE TRACKS

Exceptional, Unmatched & Best Features

 Address: 101, SIDDHARTHA CHAMBERS, AUROBINDO MARG, HAUZ KHAS, NEW DELHI 110016

 <https://Cybrotech.us>

 cxo@cybotech.in

 +91-11-43073750/+91-817082027



“

A security operations center (SOC) takes care of an organization's all cyber-security threats, detection, response and prevention by unifying and coordinating cybersecurity technologies and operations.

”

Introduction

SACHET is a full feature, all encompassing SOC/SIEM solution. It's scalability & integrations with most popular tools or frameworks and formats like MDM, DLP, or Anti-malware solutions makes it a great centralized SOC/SIEM tool with XDR capabilities. Modules on security events, auditing, threat detection and regulatory compliance modules enhance specific use cases. Industries like FinTech health-tech, game-tech, regulatory compliance is something which is of utmost importance. SACHET also helps with compliance completeness and readiness like GDPR, HIPPA, SOC2, DPDP, SEBI/RBI/IRDAI Cyber Security Framework. Finally, SACHET's ruleset and custom policymaking abilities help massively in Intrusion Detection in clusters, virtual machines and even mobile devices.

FEATURES SACHET



Key Features

- ❑ **24/7 Real-time Threat Monitoring:** Continuous surveillance of your IT environment using advanced analytics and threat intelligence to detect and respond to security incidents as they occur.
- ❑ **Proactive Threat Hunting:** Actively search for hidden threats within your network, leveraging the latest threat-hunting techniques and tools.
- ❑ **Comprehensive Incident Response:** Swift and effective response to security incidents, including containment, eradication, and recovery, minimizing the impact on your business operations.
- ❑ **Customized Security Dashboards:** Personalized dashboards that provide visibility into your security posture, with real-time updates and actionable insights.
- ❑ **Advanced Threat Intelligence Integration:** Incorporating global threat intelligence to enhance detection capabilities and stay ahead of emerging threats.
- ❑ **Compliance and Reporting:** Ensures your organization meets industry regulations and standards, with detailed reporting and audit support.

1. Configuration Assessment

Perform periodic scans for misconfigurations or gaps.

Customize checks to fit organizational needs.

Receive actionable security alerts with recommendations.

2. Malware Detection

Detect malware activity using built-in rulesets (e.g., SCA, Rootcheck, FIM).

Customize configurations for enhanced detection.

3. File Integrity Monitoring (FIM)

Monitor file changes (content, permissions, ownership).

Identify users/applications modifying files.

Integrate with threat intelligence for threat detection.

4. Threat Hunting

Use log retention, indexing, and queries for investigation.

Map detection rules to MITRE ATT&CK framework.

Integrate third-party threat intelligence feeds.

5. Log Data Analysis

Collect and analyze OS and application logs.

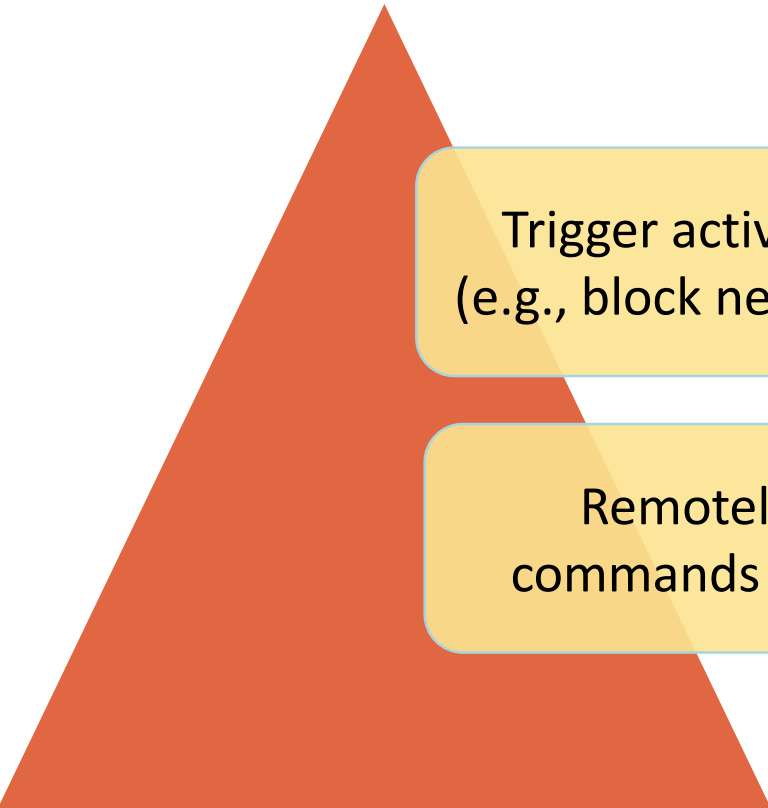
Detect errors, misconfigurations, and policy violations.

6. Vulnerability Detection

Correlate software inventory with CVE databases.

Identify vulnerable software for timely remediation.

7. Incident Response



Trigger active responses (e.g., block network access).

Remotely execute commands and queries.

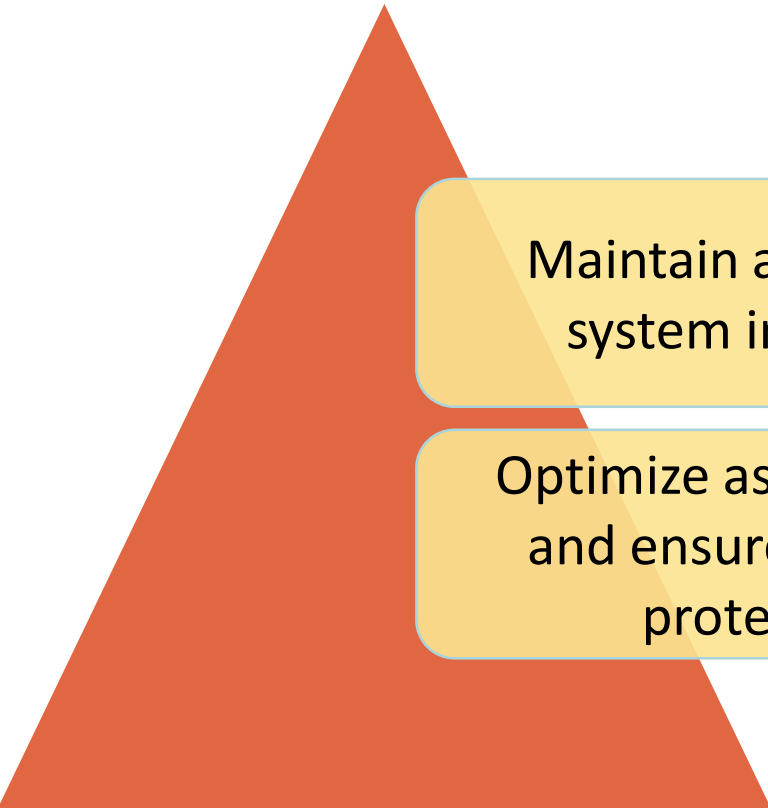
8. Regulatory Compliance



Meet compliance standards like PCI-DSS, NIST, HIPAA, GDPR, DPP Act-2000

Utilize dashboards and reports for adherence tracking.

9. IT Hygiene



Maintain an updated system inventory.

Optimize asset visibility and ensure endpoint protection.

10. Container Security



Monitor Docker hosts and containers for threats.

Alert on privileged mode, vulnerable apps, and anomalous behavior.

11. Workload Protection

Protect cloud and on-premises workloads.

Monitor platforms like AWS, Azure, GCP, and Microsoft 365.

Dashboard Overview

ENDPOINT SECURITY



Configuration Assessment

Scan your assets as part of a configuration assessment audit.



Malware Detection

Verify that your systems are configured according to your security policies baseline.



File Integrity Monitoring

Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE



Threat Hunting

Browse through your security alerts, identifying issues and threats in your environment.



Vulnerability Detection

Discover what applications in your environment are affected by well-known vulnerabilities.



MITRE ATT&CK

Security events from the knowledge base of adversary tactics and techniques based on real-world observations.



VirusTotal

Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

SECURITY OPERATIONS



PCI DSS

Global security standard for entities that process, store, or transmit payment cardholder data.



GDPR

General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.



HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.



NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

CLOUD SECURITY



Docker

Monitor and collect the activity from Docker containers such as creation, naming, starting, stopping or pausing events.



Amazon Web Services

Security events related to your Amazon AWS services, collected directly via AWS API.



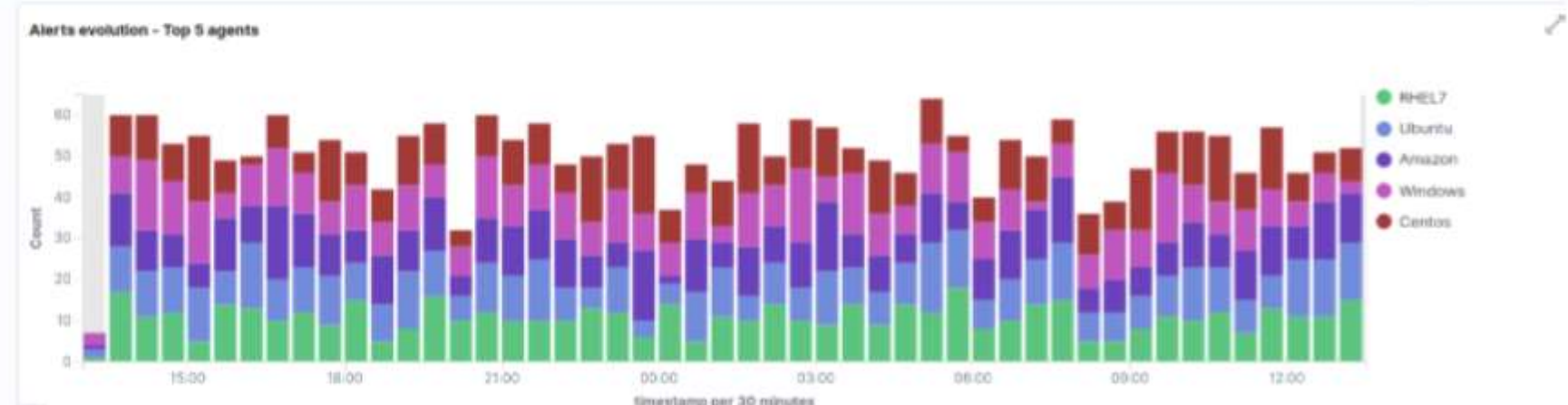
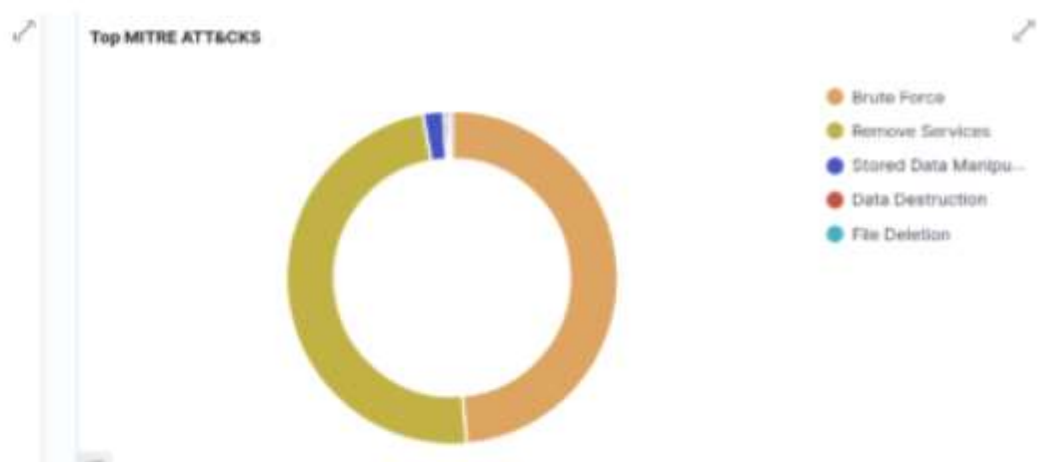
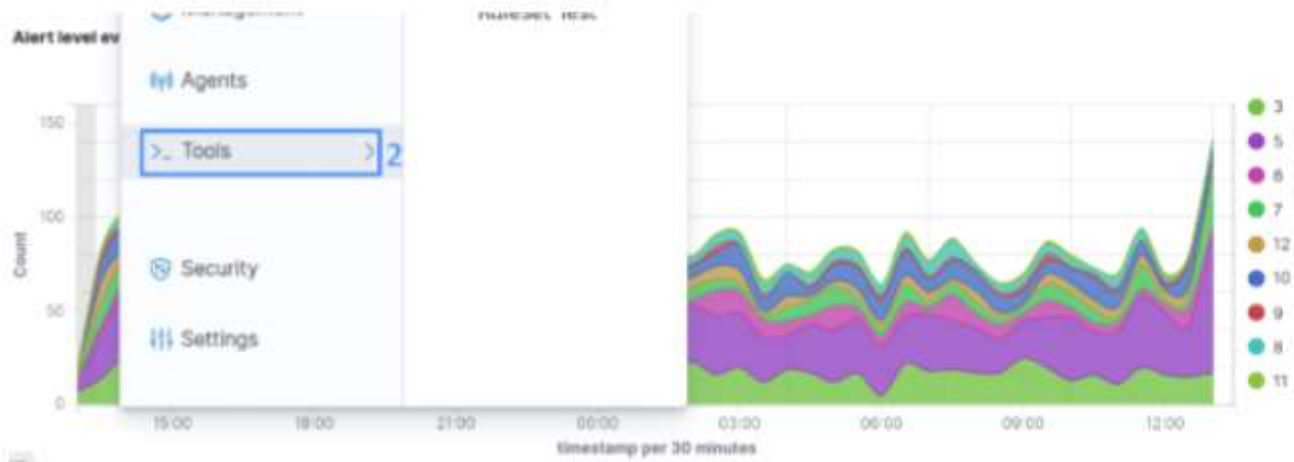
Google Cloud

Security events related to your Google Cloud Platform services, collected directly via GCP API.



GitHub

Monitoring events from audit logs of your GitHub organizations.



- Discover
- Visualize
- Dashboard
- Timeline
- Watch
- Dev Tools
- Management

Search...

184 Alerts

0 Level 12 or above alerts

181 Authentication failure

2 Authentication success



Collapse

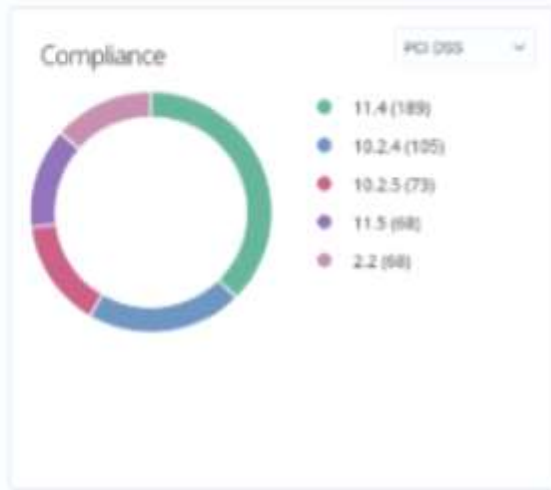
ID	Status	IP address	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
001	active	FE80:0034:0223:A000:0002:81FF:0000:8329	Wazuh v4.1.7	default debian	Debian GNU/Linux 9	master	Aug 25, 2022 @ 13:25:55.000	Sep 12, 2022 @ 05:48:40.000

Last 24 hours

MITRE ATT&CK

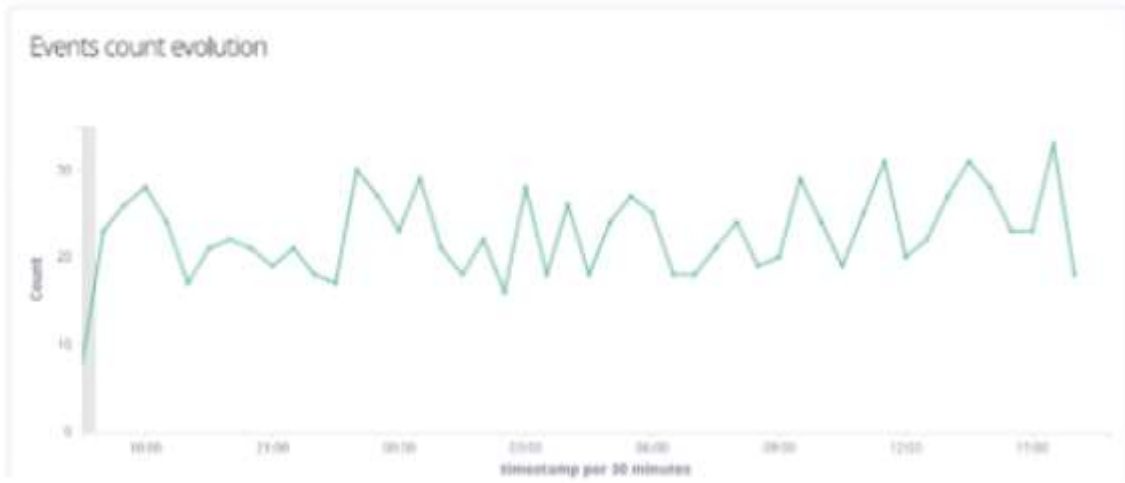
Top Tactics

- Lateral Movement: 71
- Collection: 33
- Credential Access: 30
- Impact: 18
- Initial Access: 18



FIM: Recent events

Time	Path	Action	Rule description	Rule Le...	Rule ID
May 1, 2024 @ 10:17:36.888	/var/wazuh/queue/fim/db/fim...	added	File added to the system.	5	554
May 1, 2024 @ 13:48:24.838	/tmp/wazuh-config	added	File added to the system.	5	554
May 1, 2024 @ 15:46:29.021	/var/wazuh/queue/fim/db/fim...	modified	Integrity checksum changed.	7	550
May 1, 2024 @ 15:43:07.996	/var/osquery/osquery.db/CURR...	deleted	File deleted.	7	553
May 1, 2024 @ 15:37:11.977	/var/wazuh/queue/fim/db/fim...	deleted	File deleted.	7	553



SCA: Lastest scans

CIS benchmark for Ubuntu Linux 20.04 LTS ck.ubuntu20-04

Policy	End scan	Passed	Failed	Not appli...	Score
CIS benchmark for Ubuntu Linux 20.04 LTS	Sep 27, 2022 @ 05:07:02.000	50	87	48	39%

< 1 >

Use Cases

- Create internal/operational efficiencies
- Improve compliance & risk management
- Improve business process agility
- Cost management

SACHET INTEGRATION



Endpoint Detection and Response (EDR)+Antivirus

- Defender +

SOAR (Security Orchestration Automation and Response)

- Shuffle SOAR
- Cortex XSOAR
- Simplify
- Swimlane

Threat Intelligence

- Virus Total

Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) / Incident Response

- Suricata

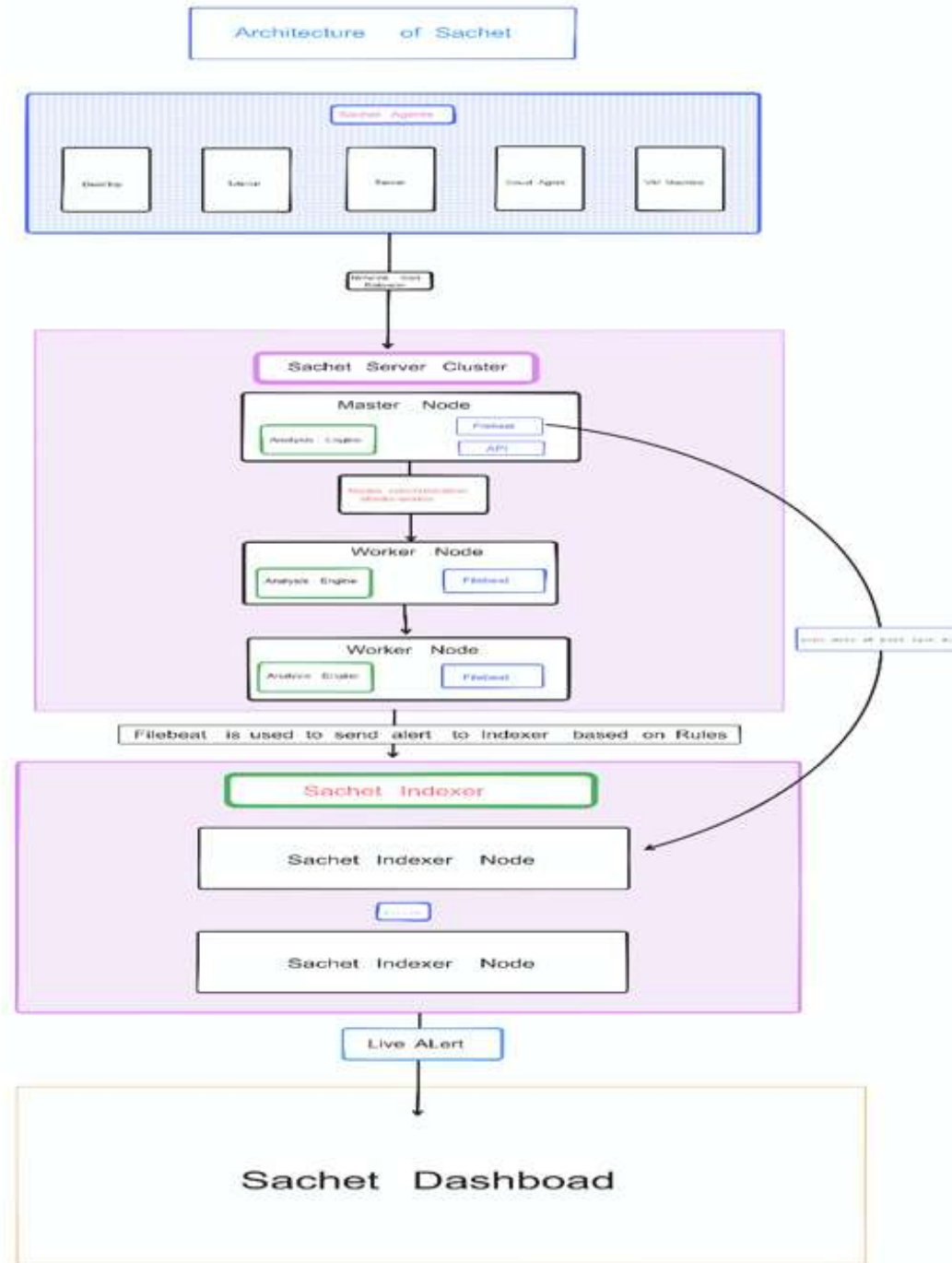
Log Management

- Elastic Stack

Cloud Security

- Cloudflare

Architecture of Sachet



Premium Features Checklist

Blocking Known Malicious Actors

Block malicious IPs accessing web resources (e.g., using IP reputation databases).

Detecting Brute-Force Attacks

Identify and block brute-force attempts on SSH/RDP.

Monitoring Docker Events

Detect security incidents across containers in real-time.

Monitoring AWS Infrastructure

Enable log data collection from AWS services using `aws-s3`.

Premium Features Checklist (Linux)

Detecting Unauthorized Processes

Identify unauthorized tools (e.g., Netcat) via command monitoring.

Network IDS Integration

Integrate with NIDS (e.g., Suricata) for enhanced network traffic inspection.

Detecting SQL Injection Attacks

Analyze web server logs for SQL injection patterns.

Detecting Suspicious Binaries

Use Root-Check to identify hidden processes and trojans.

Premium Features Checklist (Linux)

YARA Integration for Malware Detection

Scan files on modification and enrich alerts with AI-based insights

Detecting Hidden Processes

Detect processes hidden by rootkits.

Monitoring Malicious Commands

Detect security incidents across containers in real-time.

Leveraging LLMs for Alert Enrichment

Integrate with ChatGPT for detailed YARA alert insights.

SACHET

BluSapphire

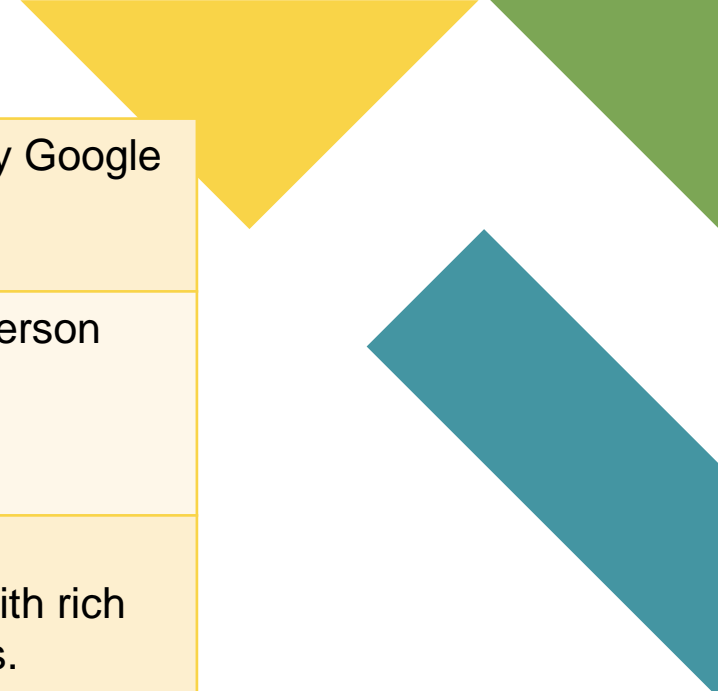
<ul style="list-style-type: none">• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&CK Matrix mapping and highly customizable dashboards through simple configuration.	<ul style="list-style-type: none">• Predictive, Powerful & Scalable Analytics, MITRE ATT&CK Matrix mapping and Rich Customizable Dashboards using simple configurations.
<ul style="list-style-type: none">• Utilizes Big Data Analytics to proactively detect and prioritize threats.	<ul style="list-style-type: none">• Leverages technologies like Advanced AI, ML & Big Data Analytics to detect and prioritize threats.
<ul style="list-style-type: none">• Risk Scoring based on contextual vulnerability and business impact.	<ul style="list-style-type: none">• Real time Correlation of Events, Log Management & Scalable and Flexible Log Collection.
<ul style="list-style-type: none">• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.	<ul style="list-style-type: none">• Support for Integration with third-party cloud APIs to facilitate ingestion of logs.
<ul style="list-style-type: none">• Third-Party Cloud API Integration to streamline log ingestion from external sources.	<ul style="list-style-type: none">• Flexible for Threat Intelligence & other third-party application integrations(Cloud Services, SaaS Apps).

<ul style="list-style-type: none"> Instant IOC Correlation against up to one full year of security telemetry. 	<ul style="list-style-type: none"> Infrastructure, Standard/Custom Apps) with 3000+ built-in uses cases.
<ul style="list-style-type: none"> Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.). 	<ul style="list-style-type: none"> 24X7 Live Support is offering by Blusapphire.
<ul style="list-style-type: none"> 24/7 Live Support provided by a dedicated support team. 	<ul style="list-style-type: none"> Comprehensive threat detection, investigation and workflow along with rich reporting for compliance use cases.
<ul style="list-style-type: none"> Custom Log Parsing Framework, enabling fast and flexible parsing options. 	<ul style="list-style-type: none"> Large Enterprise and Managed Service Provider Ready — “Multi-Tenant Architecture”.
<ul style="list-style-type: none"> Efficient and Scalable Architecture designed for seamless expansion. 	<ul style="list-style-type: none"> Easy Scale Out Architecture.
<ul style="list-style-type: none"> Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS. 	<ul style="list-style-type: none"> Out-of-the-Box Compliance Ready & Automated Reporting.

SACHET

Google Chronicle

<ul style="list-style-type: none">• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&CK Matrix mapping and highly customizable dashboards through simple configuration.	<ul style="list-style-type: none">• Predefined rules mapped to specific threats, suspicious activity, and security frameworks like MITRE ATT&CK.
<ul style="list-style-type: none">• Utilizes Big Data Analytics to proactively detect and prioritize threats.	<ul style="list-style-type: none">• Risk scoring based on contextual vulnerability, and business risk.
<ul style="list-style-type: none">• Risk Scoring based on contextual vulnerability and business impact.	<ul style="list-style-type: none">• Custom use case building functionality.
<ul style="list-style-type: none">• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.	<ul style="list-style-type: none">• Instant correlation IOCs against one full year of security telemetry.
<ul style="list-style-type: none">• Third-Party Cloud API Integration to streamline log ingestion from external sources.	<ul style="list-style-type: none">• Support for Integration with third-party cloud APIs to facilitate ingestion of logs.



<ul style="list-style-type: none">• Instant IOC Correlation against up to one full year of security telemetry.	<ul style="list-style-type: none">• 24X7 Live support is not offering by Google Chronicle .
<ul style="list-style-type: none">• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).	<ul style="list-style-type: none">• No Option for Live Online and In Person Training.
<ul style="list-style-type: none">• 24/7 Live Support provided by a dedicated support team.	<ul style="list-style-type: none">• Comprehensive threat detection, investigation and workflow along with rich reporting for compliance use cases.
<ul style="list-style-type: none">• Custom Log Parsing Framework, enabling fast and flexible parsing options.	<ul style="list-style-type: none">• Rapidly normalize data with pre-built parsers into a unified data model.
<ul style="list-style-type: none">• Efficient and Scalable Architecture designed for seamless expansion.	
<ul style="list-style-type: none">• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.	

SACHET

Fortinet

- Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&CK Matrix mapping and highly customizable dashboards through simple configuration.

- Utilizes Big Data Analytics to proactively detect and prioritize threats.

- Risk Scoring based on contextual vulnerability and business impact.

- Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.

- Third-Party Cloud API Integration to streamline log ingestion from external sources.

- Passive & active discovery methods, use of agents, **FortiGates**, & OT asset management systems.

- Correlation, UEBA ML engine, and over 1600 rules provide robust threat detection.

- FortiAI uses GenAI to guide, simplify, and automate security analyst activities.

- Seamless integration provides extended endpoint investigation and forensic monitoring.

- Security Fabric integration across the Fortinet portfolio, and third-party solutions via robust APIs.

<ul style="list-style-type: none">• Instant IOC Correlation against up to one full year of security telemetry.	<ul style="list-style-type: none">• FortiSIEM as SaaS lets Fortinet take on the burden of deployment and software administration.
<ul style="list-style-type: none">• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).	<ul style="list-style-type: none">• FortiSIEM offers hardware and highly scalable virtual machines for those who prefer these solutions.
<ul style="list-style-type: none">• 24/7 Live Support provided by a dedicated support team.	<ul style="list-style-type: none">• Easy-to-manage automation in a single pane of glass integrates public and private cloud protections.
<ul style="list-style-type: none">• Custom Log Parsing Framework, enabling fast and flexible parsing options.	<ul style="list-style-type: none">• Hybrid approach enables combining SaaS, cloud, VM, and HW in whatever combination you need.
<ul style="list-style-type: none">• Efficient and Scalable Architecture designed for seamless expansion.	<ul style="list-style-type: none">• FortiSIEM's inbuilt CMDB synchs to OT asset systems and uses passive techniques for no-impact discovery, plus Purdue classification context.
<ul style="list-style-type: none">• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.	<ul style="list-style-type: none">• FortiSIEM's lightweight agent is perfect for collecting telemetry to track user behavior anomalies—even when disconnected and working remotely.

SACHET

splunk>

<ul style="list-style-type: none">• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&CK Matrix mapping and highly customizable dashboards through simple configuration.	<ul style="list-style-type: none">• Enhanced GUI with dashboards.
<ul style="list-style-type: none">• Utilizes Big Data Analytics to proactively detect and prioritize threats.	<ul style="list-style-type: none">• Faster troubleshooting with instant results.
<ul style="list-style-type: none">• Risk Scoring based on contextual vulnerability and business impact.	<ul style="list-style-type: none">• Best suited for root cause analysis.
<ul style="list-style-type: none">• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.	<ul style="list-style-type: none">• Get access to create dashboards, graphs, and alerts.
<ul style="list-style-type: none">• Third-Party Cloud API Integration to streamline log ingestion from external sources.	<ul style="list-style-type: none">• Enhanced GUI with dashboards.

<ul style="list-style-type: none">• Instant IOC Correlation against up to one full year of security telemetry.	<ul style="list-style-type: none">• Monitor business metrics for informed decision making.
<ul style="list-style-type: none">• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).	<ul style="list-style-type: none">• Log management from multiple sources.
<ul style="list-style-type: none">• 24/7 Live Support provided by a dedicated support team.	<ul style="list-style-type: none">• Accepts data in multiple formats.
<ul style="list-style-type: none">• Custom Log Parsing Framework, enabling fast and flexible parsing options.	<ul style="list-style-type: none">• Can create one central repository for Splunk data collected from multiple sources.
<ul style="list-style-type: none">• Efficient and Scalable Architecture designed for seamless expansion.	
<ul style="list-style-type: none">• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.	

SACHET

IBM QRADAR

<ul style="list-style-type: none">• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&CK Matrix mapping and highly customizable dashboards through simple configuration.	<ul style="list-style-type: none">• Intelligent algorithms to apply multiple layers of risk scoring on each observable within a case.
<ul style="list-style-type: none">• Utilizes Big Data Analytics to proactively detect and prioritize threats.	<ul style="list-style-type: none">• All siloed data can be accessed to enrich threat investigations. Federated search provides cost-effective flexibility to choose between what mission- critical data is ingested into SIEM and searching data where it resides.
<ul style="list-style-type: none">• Risk Scoring based on contextual vulnerability and business impact.	<ul style="list-style-type: none">• native support for open source Sigma Rules, cloud- native QRadar SIEM creates a common shared language for security analysts to overcome the challenge of writing rules in proprietary SIEM platforms.
<ul style="list-style-type: none">• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.	<ul style="list-style-type: none">• Reduces analyst fatigue through automation that provides a summary of information and recommendations all in one place.
<ul style="list-style-type: none">• Third-Party Cloud API Integration to streamline log ingestion from external sources.	<ul style="list-style-type: none">• access to the latest evolving trends without having to spend hours on research.

<ul style="list-style-type: none">• Instant IOC Correlation against up to one full year of security telemetry.	<ul style="list-style-type: none">• Automatic enrichment from X-Force Threat Intelligence allows organisations to avoid emerging threats and exposure from the latest vulnerabilities.
<ul style="list-style-type: none">• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).	
<ul style="list-style-type: none">• 24/7 Live Support provided by a dedicated support team.	
<ul style="list-style-type: none">• Custom Log Parsing Framework, enabling fast and flexible parsing options.	
<ul style="list-style-type: none">• Efficient and Scalable Architecture designed for seamless expansion.	
<ul style="list-style-type: none">• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.	

SACHET

McAfee

<ul style="list-style-type: none">• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&CK Matrix mapping and highly customizable dashboards through simple configuration.	<ul style="list-style-type: none">• Advanced Correlation Engine supplements with two dedicated correlation engines.
<ul style="list-style-type: none">• Utilizes Big Data Analytics to proactively detect and prioritize threats.	<ul style="list-style-type: none">• Application Data Monitor decodes an entire application session to Layer 7 to detect fraud, data loss, and hidden threats.
<ul style="list-style-type: none">• Risk Scoring based on contextual vulnerability and business impact.	<ul style="list-style-type: none">• Enterprise Log Manager automates log management and analysis for all log types and integrates with Manager for analysis and incident management.
<ul style="list-style-type: none">• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.	<ul style="list-style-type: none">• Hunt faster by searching billions of events in seconds and get immediate access to raw logs for context.
<ul style="list-style-type: none">• Third-Party Cloud API Integration to streamline log ingestion from external sources.	<ul style="list-style-type: none">• Built for big security data.

<ul style="list-style-type: none">• Instant IOC Correlation against up to one full year of security telemetry.	<ul style="list-style-type: none">• Enterprise Security Manager delivers intelligent, fast, and accurate security information and event management (SIEM) and log management.
<ul style="list-style-type: none">• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).	
<ul style="list-style-type: none">• 24/7 Live Support provided by a dedicated support team.	
<ul style="list-style-type: none">• Custom Log Parsing Framework, enabling fast and flexible parsing options.	
<ul style="list-style-type: none">• Efficient and Scalable Architecture designed for seamless expansion.	
<ul style="list-style-type: none">• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.	

SACHET

AlienVault

<ul style="list-style-type: none">• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&CK Matrix mapping and highly customizable dashboards through simple configuration.	<ul style="list-style-type: none">• Central monitoring and configuration for Sensors, Agents, and Logger.
<ul style="list-style-type: none">• Utilizes Big Data Analytics to proactively detect and prioritize threats.	<ul style="list-style-type: none">• Over 100 Pre-Defined Compliance & Threat Reports.
<ul style="list-style-type: none">• Risk Scoring based on contextual vulnerability and business impact.	<ul style="list-style-type: none">• spent on creating custom reports by reusing modules of existing reports.
<ul style="list-style-type: none">• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.	<ul style="list-style-type: none">• 3D network and security applications like Geo-location and botnet maps.
<ul style="list-style-type: none">• Third-Party Cloud API Integration to streamline log ingestion from external sources.	<ul style="list-style-type: none">• Multi-Tenant Management.

<ul style="list-style-type: none">• Instant IOC Correlation against up to one full year of security telemetry.	<ul style="list-style-type: none">• Open Extension API.
<ul style="list-style-type: none">• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).	<ul style="list-style-type: none">• Reduces time required to automate security operations.
<ul style="list-style-type: none">• 24/7 Live Support provided by a dedicated support team.	<ul style="list-style-type: none">• Wizard to Create Custom Correlation Rules.
<ul style="list-style-type: none">• Custom Log Parsing Framework, enabling fast and flexible parsing options.	<ul style="list-style-type: none">• Contextual Behavior Analysis.
<ul style="list-style-type: none">• Efficient and Scalable Architecture designed for seamless expansion.	<ul style="list-style-type: none">• Pattern Recognition & Behavior Analysis.
<ul style="list-style-type: none">• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.	<ul style="list-style-type: none">• Interface to Open Threat Exchange.

SACHET

Securonix

<ul style="list-style-type: none">• Predictive, Scalable Analytics with powerful capabilities, leveraging MITRE ATT&CK Matrix mapping and highly customizable dashboards through simple configuration.	<ul style="list-style-type: none">• on-demand scaling and zero infrastructure to manage.
<ul style="list-style-type: none">• Utilizes Big Data Analytics to proactively detect and prioritize threats.	<ul style="list-style-type: none">• Threat Chain Analytics.
<ul style="list-style-type: none">• Risk Scoring based on contextual vulnerability and business impact.	<ul style="list-style-type: none">• More than 500 integrations allow seamless integration and easily ingest of data from a wide variety of sources across hybrid infrastructures.
<ul style="list-style-type: none">• Real-time Event Correlation, Log Management, and highly scalable, flexible log collection.	<ul style="list-style-type: none">• Uncover blind spots with built-in API-based integrations with cloud applications, infrastructure, and services.
<ul style="list-style-type: none">• Third-Party Cloud API Integration to streamline log ingestion from external sources.	<ul style="list-style-type: none">• Achieve a fast time to-value with pre-built analytics modules for common threat scenarios.

<ul style="list-style-type: none">• Instant IOC Correlation against up to one full year of security telemetry.	<ul style="list-style-type: none">• Long-Term Search.
<ul style="list-style-type: none">• Flexible Integration with Threat Intelligence platforms and third-party applications (Cloud, SaaS, etc.).	<ul style="list-style-type: none">• Built-In SOAR.
<ul style="list-style-type: none">• 24/7 Live Support provided by a dedicated support team.	
<ul style="list-style-type: none">• Custom Log Parsing Framework, enabling fast and flexible parsing options.	
<ul style="list-style-type: none">• Efficient and Scalable Architecture designed for seamless expansion.	
<ul style="list-style-type: none">• Security Operations with compliance features and automated reporting capabilities, supporting standards such as GDPR, HIPAA, NIST 800-50, TSC, and PCI DSS.	



Thank You
