Trustwave
a Singtel company

Review of Threat Monitoring Dashboards

Version: draft_0.2.1

06/07/2021

Confidentiality Notice: This document is confidential and contains proprietary information and intellectual property of Trustwave, a Singtel company, its parent company and its subsidiaries. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances. Please be aware that disclosure, copying, distribution or use of this document and the information contained therein is strictly prohibited.

Review of Threat Monitoring Dashboards

Introduction

In this document, we will do a short review of different threat monitoring dashboards used by several leading security vendors and summaries the key features, then we will compare them with the existing Trustwave Fusion Portal and identify what are the gaps. We will introduce the user interface features, threat detection and analytics features and main function/control features of Fusion portal, Anomali, BitSight, Exabeam, Extrahop, LogRhythm and Splunk in the first section. The key features comparison table will be show in the second section.

Section I. Individual Review of Venders' Dashboards

1. Trustwave Fusion Portal Threat Monitoring Dashboard

1.1 Dashboard Version: 1.0.60

1.2 Vendor Company: Trustwave Holdings, Inc.

1.3 Dashboard Key Features:

Dashboard User Interface Key Features:

- Customizable dashboard.
    - Fusion Portal allows the user to customize their dashboard UI view and create multiple tailored dashboards to summarize activity or check security status.
- Multiplatform UI optimization.
    - The dashboard UI was optimized for different kinds of web browsers, Android / IOS App for mobile devices and QR code one-time quick setup is also supported.
- Result display type:
    - Security orchestration, automation and response (SOAR)
    - Security information and event management (SIEM): Jumpstart, Information Security Advisor

Dashboard Function/Control Key Features:

- Search assets, data set finding and data searching.
    - Allow users to quickly get access to the data they need, this includes the ability to search log data received from various devices.
- Managed asset view.
    - Allow users to view the details about devices undermanagement including their current and history status.
- Combined findings.
    - Understand user's full security posture with combined threats and vulnerability findings. Also drill down into detail for individual findings.
- Support area with chart.

- Technical service team can support user via dashboard integrated chart and get increased visibility into the security incidents and device technology management related tickets.

- Security testing.
  - User can use Trustwave security SpiderLab's testing suite provided in the dashboard to test their IT environment.
- Access permission control.
  - Provide different access tickets based on user's data accessing permission.
- Task management and periodic report generation.
  - The user can plan the security action/activity/alert handling which they want to implement via the dashboard and generate the threat monitoring report periodically.

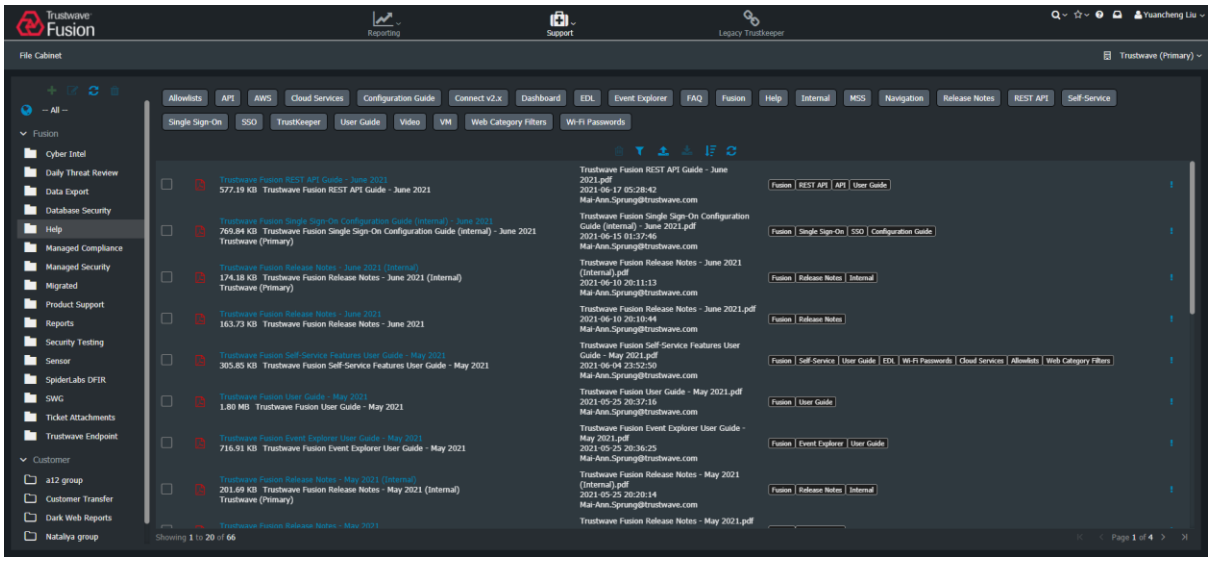
Threat Detection and Analytics Key Feature:

- Type of scoring
  - Rigorous scoring methodology based on both qualitative and quantitative criteria.
- Threat detection
  - Intelligence threat detection method research are provided by: Trustwave SpiderLabs, Microsoft (MAPP partners), Google/VirusTotal, the Anti-Phishing Working Group (APWG), Facebook, Malicious URL Threat Exchange (MUTE), and Team Cymru.
  - Malware, rogue code, behavioural anomalies and other indicators of malicious activity.
- Threat analytics
  - Trustwave's Global Threat Operations (GTO) team's three tiers analytics.
  - Machine learning and automation analytics have been incorporated to improve incident accuracy, response time and actions.
- Rule creation and tuning
  - Rule creation supported type: Managed assets, Event report, Threats findings, Incident aging, Incident distribution, Incident created, SLA Achieved.

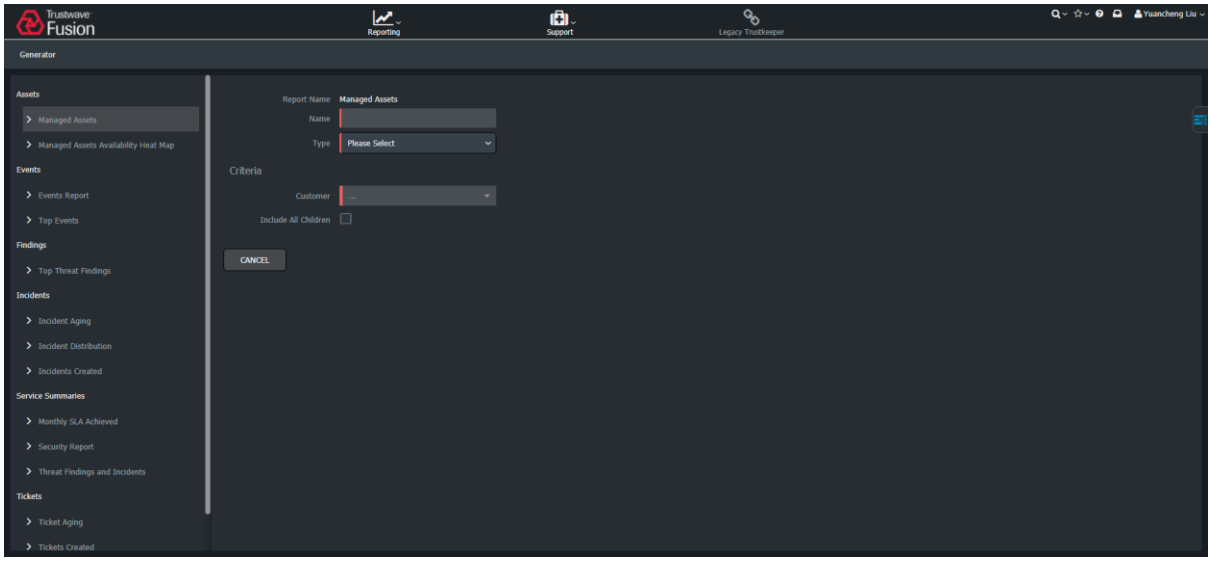
1.4 Dashboard Preview:

- Fusion Portal dashboard main ticket page

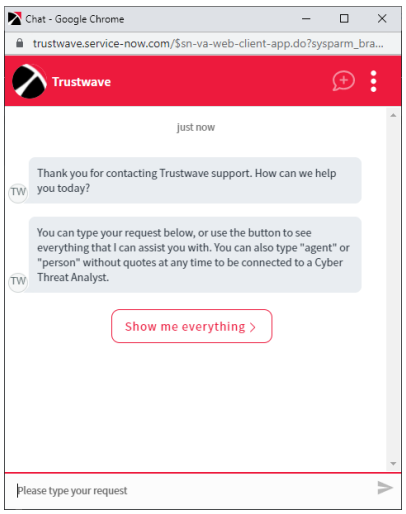
- Fusion Portal report source file cabinet page



- Fusion Portal report generator configuration page



- Fusion Portal live support and troubleshooting chart page



2. Anomali Intelligence Platform Dashboard

2.1 Dashboard version: V4.4 May 2021

2.2 Vendor Company: Anomali Inc.

2.3 Key Features:

Dashboard User Interface Key Features:

- Threat analysis tools selection
    - User can select the tools used for threat analysis in the dashboard management page such as Authentic8, Cisco Umbrella, DomainTools, GreyNoise, HYAS, Joe Security, Maltego, Recorded Future, Silobreaker, Soltra, VirusTotal, VMray.
- Customizable dashboard
    - Customer can create their own widgets and layout for their dashboard.
- Research community website integrated.
- Result display type:
    - Security orchestration, automation, and response (SOAR)
    - Security information and event management (SIEM)

Dashboard Function/Control Key Features:

- Automate threat detection.
    - Provide Intelligence threat source selection and auto IOCs (indicators of compromise) matching configuration for auto detection.
- Activity/task management and periodic analysis report generation.
- Threat sandbox detonation.
    - Provide sandbox environment setup page for user to implement the threat testing.
- Browser-based management console.
- Data set finding and data searching function.
- Third party threat analysis tools integration.
    - Provide third party threat analysis tools/App plugin management page and allow user to import their customized threat observation rule as new observables to enhance the available intelligence analysis tool set.

Threat Detection and Analytics Key Feature:

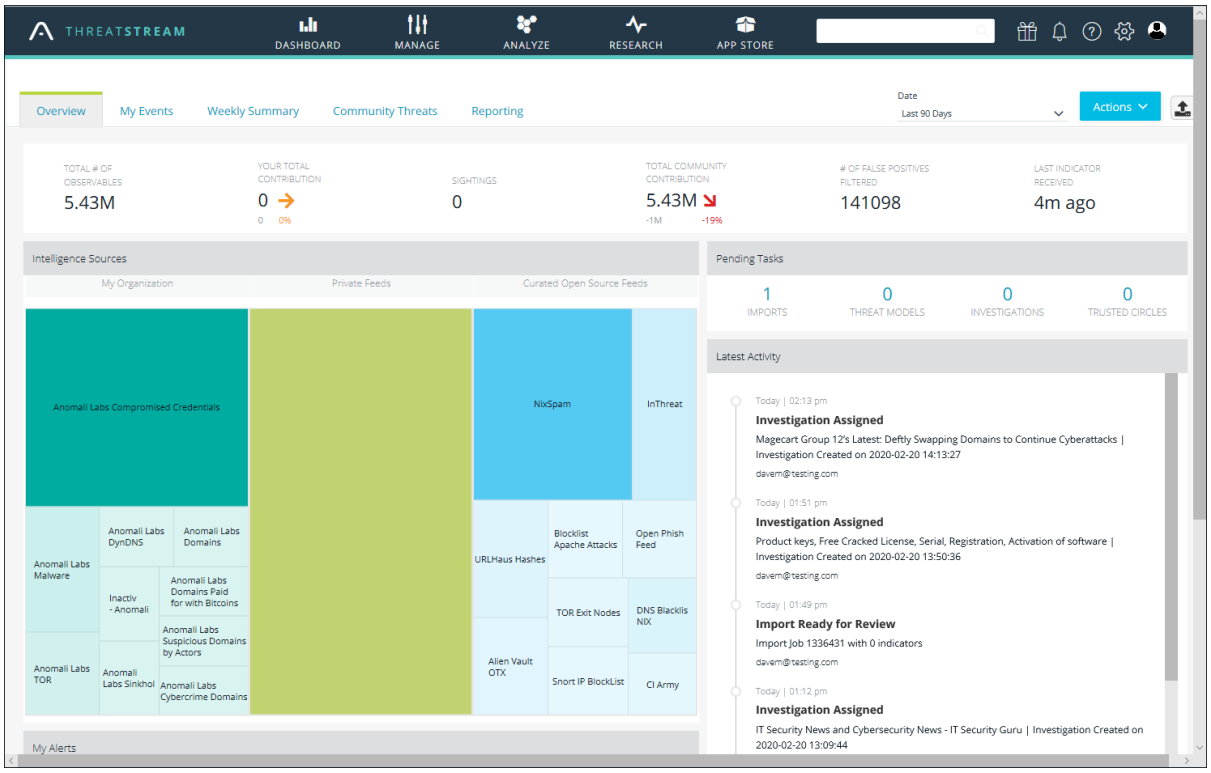
- Type of scoring: Risk scoring
- Threat detection
    - Threat categories: Adversary Monitoring, Brand Monitoring, Malware Intelligence, social media, DNS/URL/IP, Deep & Dark Web, Domain Monitoring, Phishing, Fraud Intelligence, Mobile Device, Physical Infrastructure, Vulnerability Prioritization.
    - Threat detection App/tools**:** Accenture DeepSight, Blueliv, Cicso AMP Threat Grid, Cofense, CrowdStrike, CSIS Security Group, Digital Shadows, Dragos, Emerging Threats, Facebook ThreatExchange, Farsight Security, FireEyem Flashpoint, Fox-IT, Georgia Tech Research Institute (GTRI), Group-IB, iDefene, Intel 471, ISight Partners, Kaspersky, Malware Patrol, PolySwarm, Proofpoint, Q6 Cyber, Red Sky Alliance, ReversingLabs, SecneurX, Silobreaker, Sixgill, TeamT5, The Media Trust, ThreatFabric, ZeroFOX.

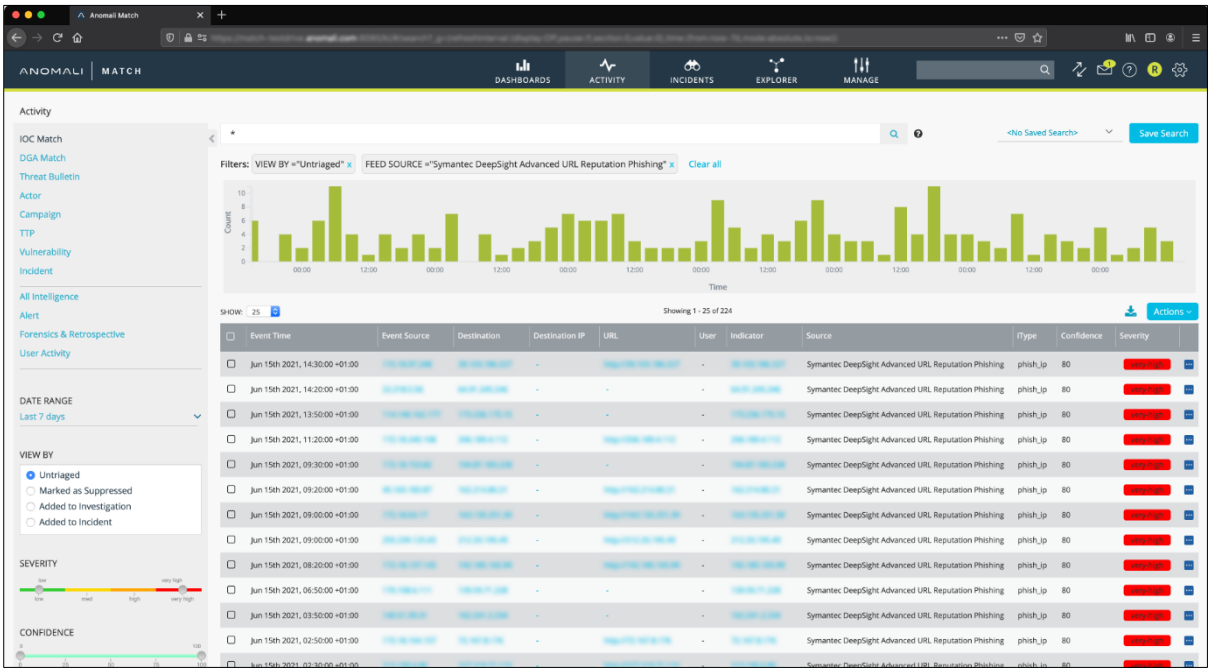
- Threat analytics

- Anomali provides 200+ advanced threat analysis services App plug in such as: Authentic8, Cisco Umbrella, DomainTools, GreyNoise, HYAS, Joe Security, Maltego, Recorded Future, Silobreaker, Soltra, VirusTotal, VMray.

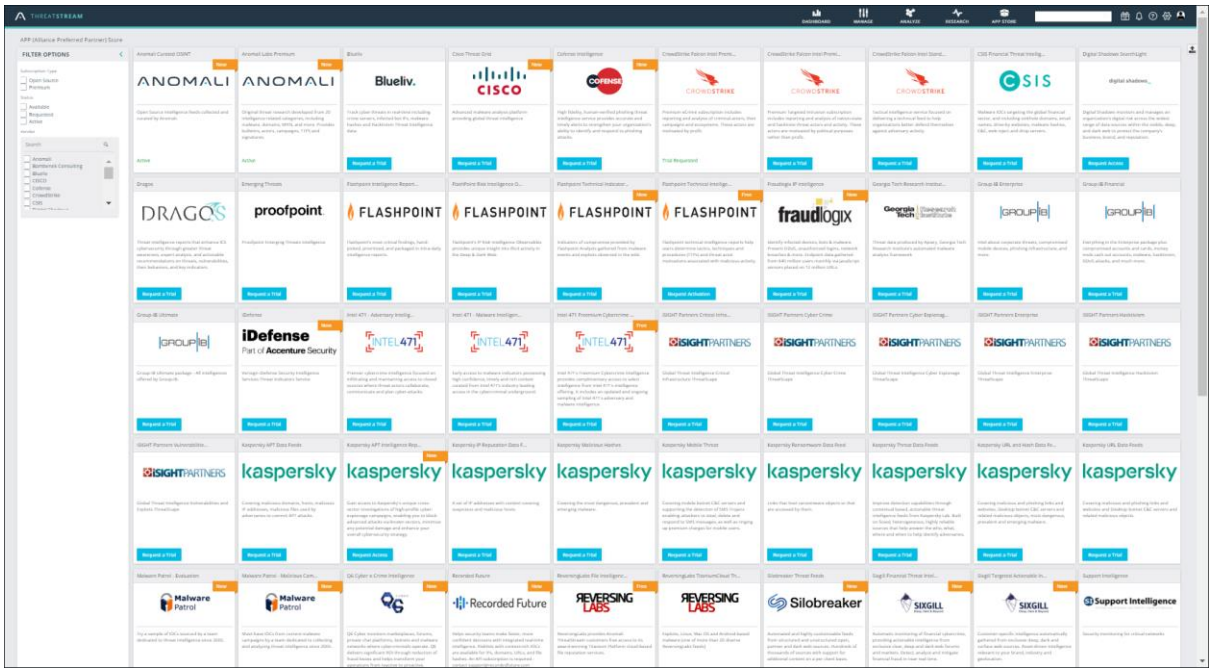
- Rule creation and tuning
  - Customized rules by rules engine: The Anomali Rules Engine is a powerful tool used by customers to define threat filtering rule that are relevant to their organization, and automatically assign research and investigation tasks.

2.4 Dashboard Preview:

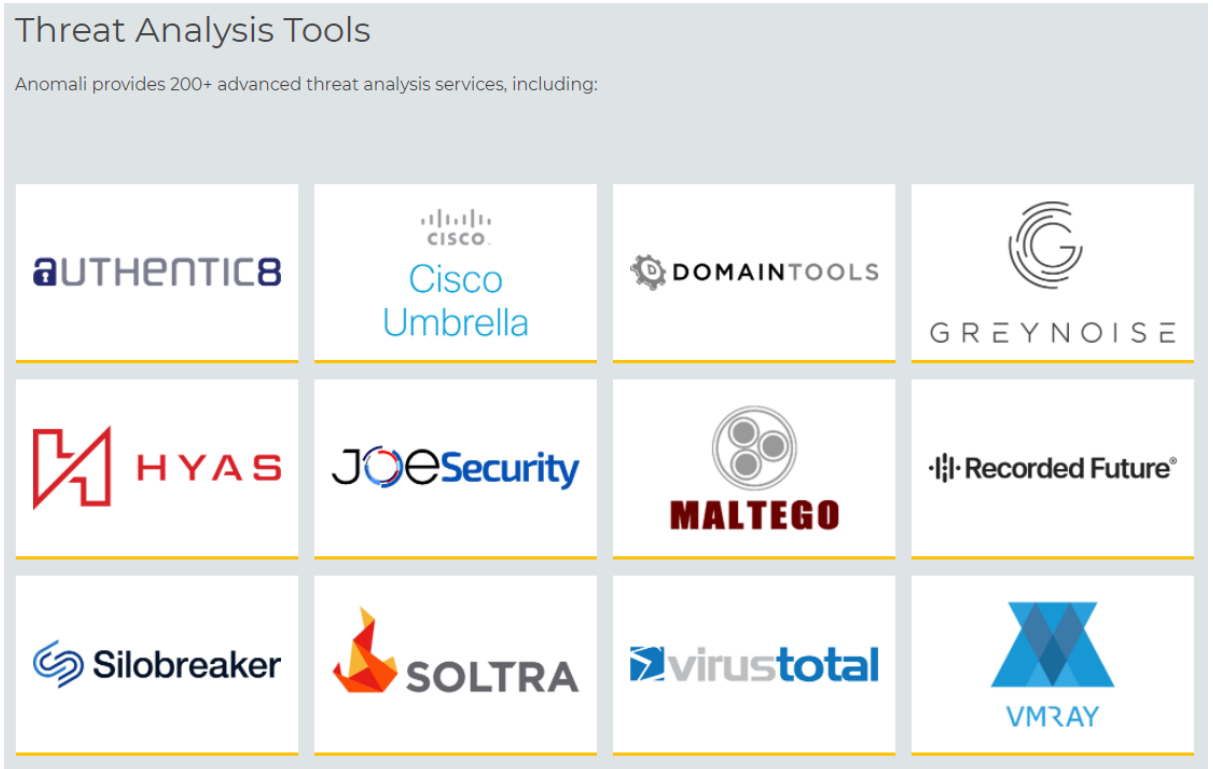




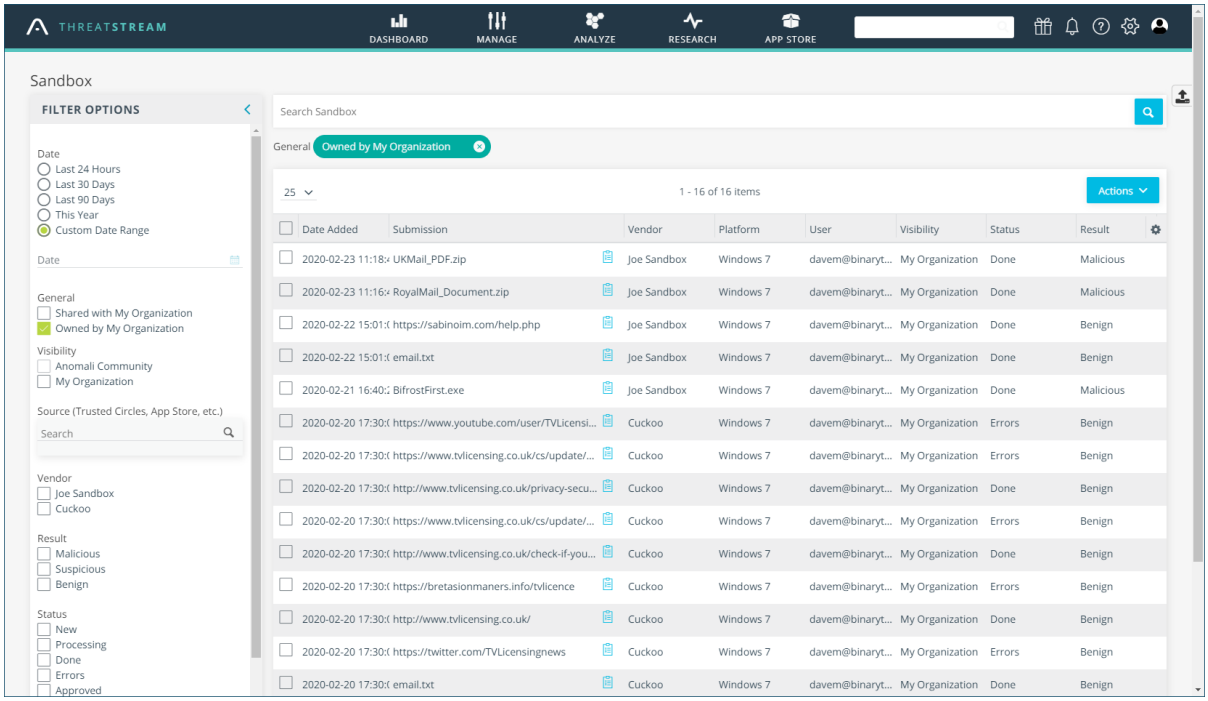
- Anomali threat detection tool config page:



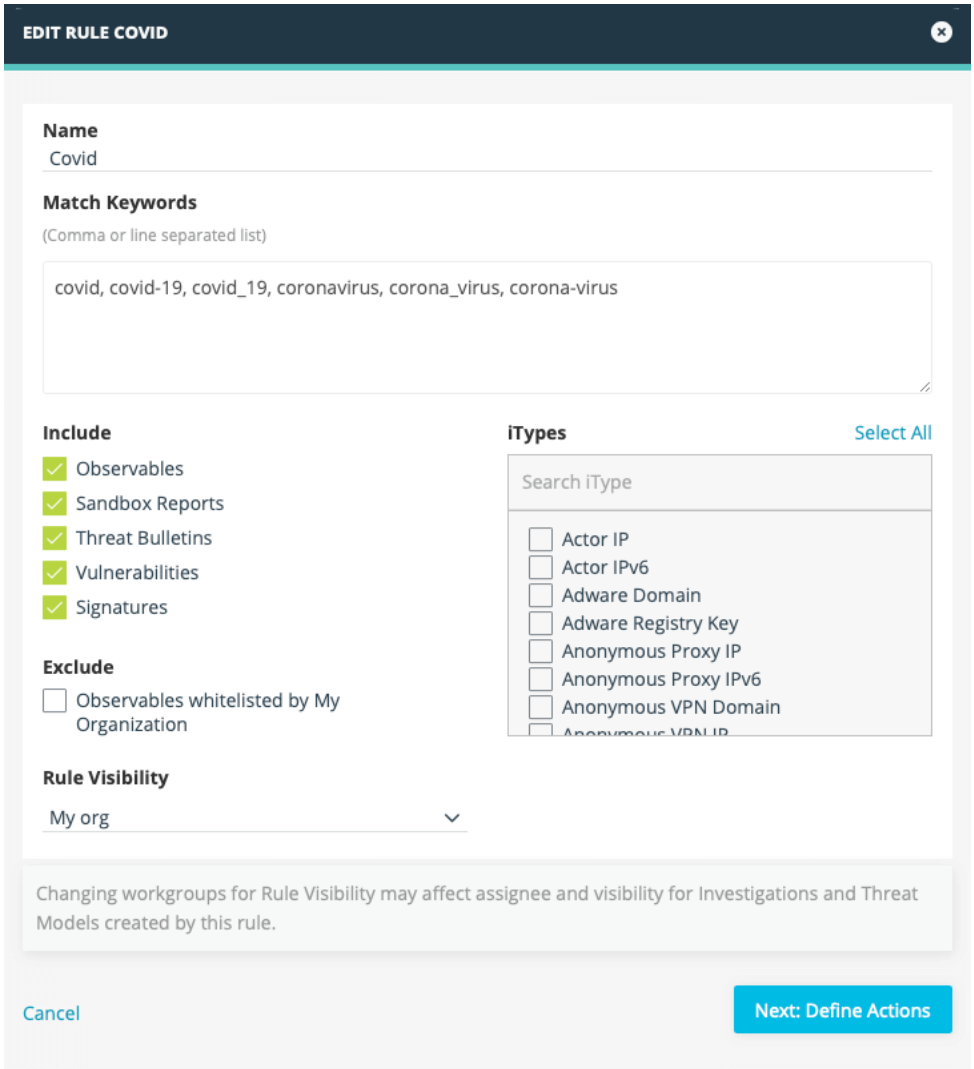
- Anomali threat analysis tool selection and config page:



- Sandbox detonation configuration page:



- Anomali rules engine customized rule configure page:



3. BitSight Security Monitoring Dashboard

3.1 Dashboard version: n.a

3.2 Vendor Company: BitSight Technologies

3.3 Key Features:

Dashboard User Interface Key Features:

- Security rating display panels/pages
    - Show security rating (250 - 900) for an organization in the security rating dashboard.
- Customizable dashboard with pre-build widgets and layout.
- Result display type:
    - Security ratings (kind of UEBA): BitSight Security Ratings provide a data-driven, dynamic measurement of an organization's cybersecurity performance.

Dashboard Function/Control Key Features:

- Display botnet infection grade (A-F) and unidentified devices on network.
- Peer to peer file sharing grade (A-F).
    - Provide panel to show how much P2P activity took place on a network within the last 60 days.
- Average vendor security rating over time and average industry security rating management.
- Phishing detection test success rating base on customer's input.
- Security awareness training completion rating platform.
- Data searching.
- Report generation and alert management function.

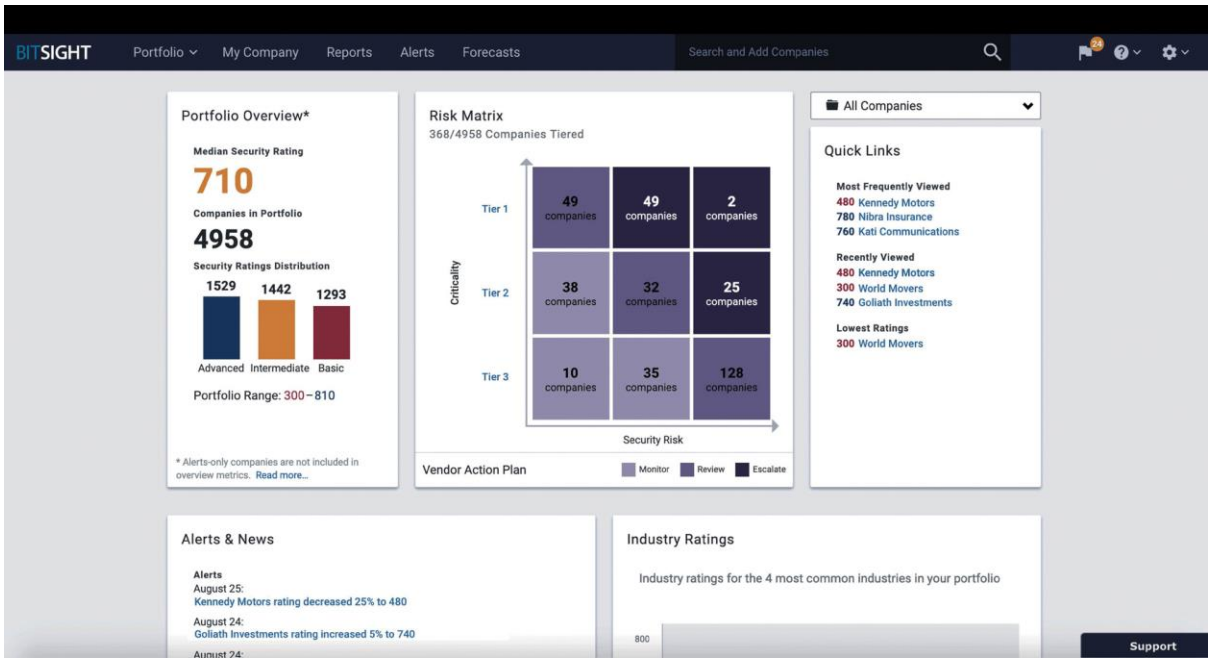
Threat Detection and Analytics Key Feature:

- Type of scoring: Risk and credit scoring
- Threat detection
    - Threat categories: botnet infections, spam propagation, malware servers, potentially exploited machines, and unsolicited communications.
- Threat analytics
    - BitSight analyzes security configurations and protocols associated with risk vectors such as open ports, patching cadence, and insecure systems.

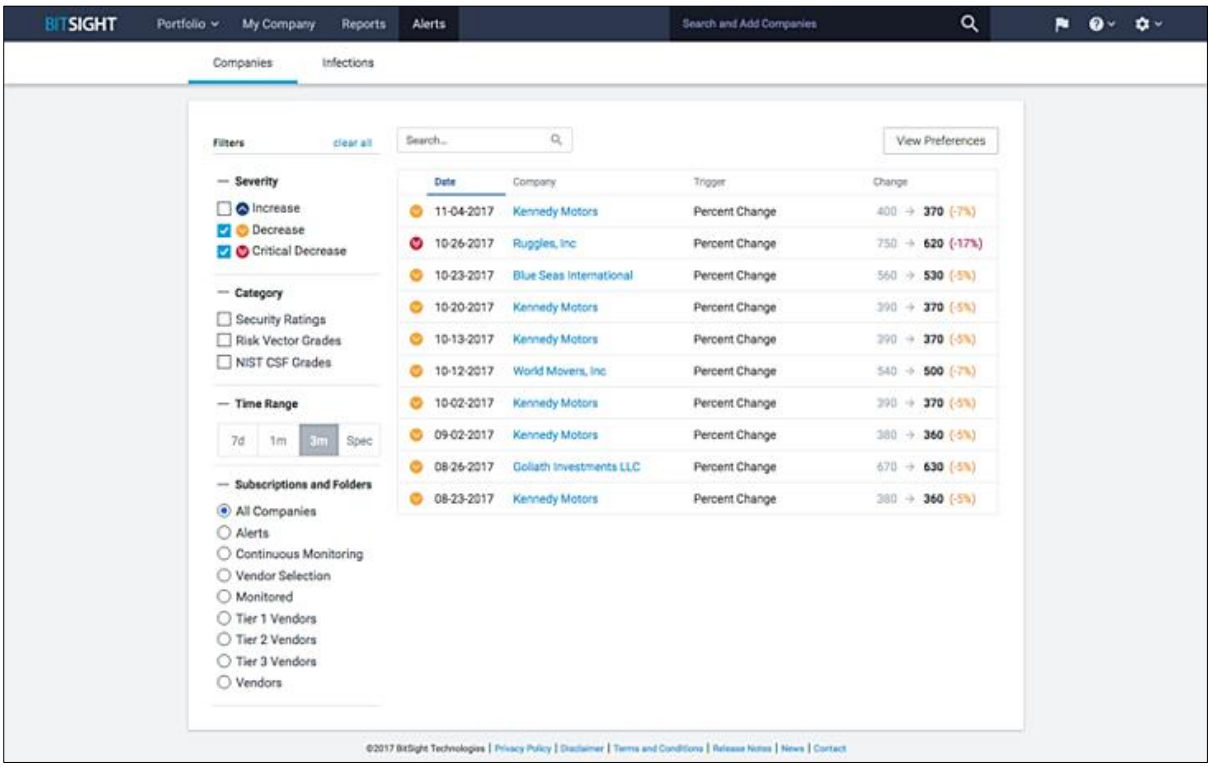
- Rule creation and tuning:
    - Not specified in the web.

3.4 Dashboard Preview:

- BitSight dashboard main page:



- BitSight Company thread event display page



4. Exabeam Threat Data Lake Dashboard

4.1 Dashboard version: i33

4.2 Vendor Company: Exabeam, Inc.

4.3 Dashboard Key Features:

Dashboard User Interface Key Features:

- Customized dashboard visualization with the chart builder.
- Result display type:
    - User and entity behaviour analytics (UEBA)
    - Patented smart timeline: automated building of users' timeline, host-to-IP mapping, lateral movement detection.

Dashboard Function/Control Key Features:

- Data Lake unlimited logging, open architecture and scalability of data.
- Events Indexing and filtering, threat event sorting.
- Customized searching.
    - The user can query specific log events, search for specific conditions within a rolling time window and identify patterns in data set. The exabeam dashboard also supports field level searches and search logical statements config.
- Report generation.
    - User can create a dashboard's current data/compliance reports periodically.
- Access restrictions for saved objects.
    - Access permissions are granted or denied based on user roles.
- Alert handling control.
    - User can define different alert rules and forward alerts using correlation rules.

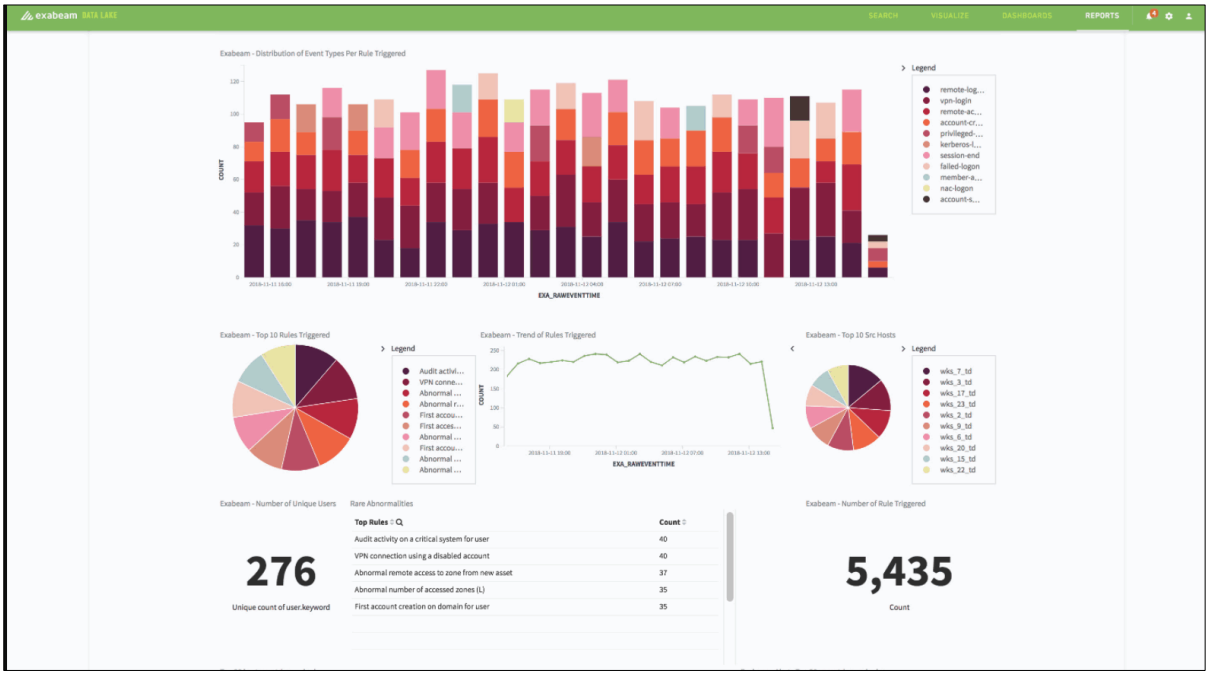
Threat Detection and Analytics Key Feature:

- Type of scoring: Risk scoring
- Threat detection
    - External threats: Malware, Phishing, Ransomware, Brute force attack, Crypto mining.
    - Compromised insiders: Compromised credentials, Lateral movement, Privilege escalation, Privileged activity, Account manipulation, Data Exfiltration, evasion.
    - Malicious insiders: Data leak, Privilege abuse, Data access abuse, Audit tampering, Destruction of data, Physical security, Workforce protection, Abnormal access and authentication.
- Threat analytics
    - Behavioural baselining, machine learning for host classification, statistical analysis for anomaly detection, dynamic peer grouping.
- Rule creation type
    - Blacklist: Checks a certain field against a blacklist, and match if it is in the blacklist.
    - Frequency: Matches when there are at least a certain number of events in a given time frame. This may be counted on a per-query key basis.
    - Any: Matches everything. Every hit that the query returns will generate an alert.
    - Cardinality: Matches when the total number of unique values for a certain field within a time frame is higher or lower than a threshold.

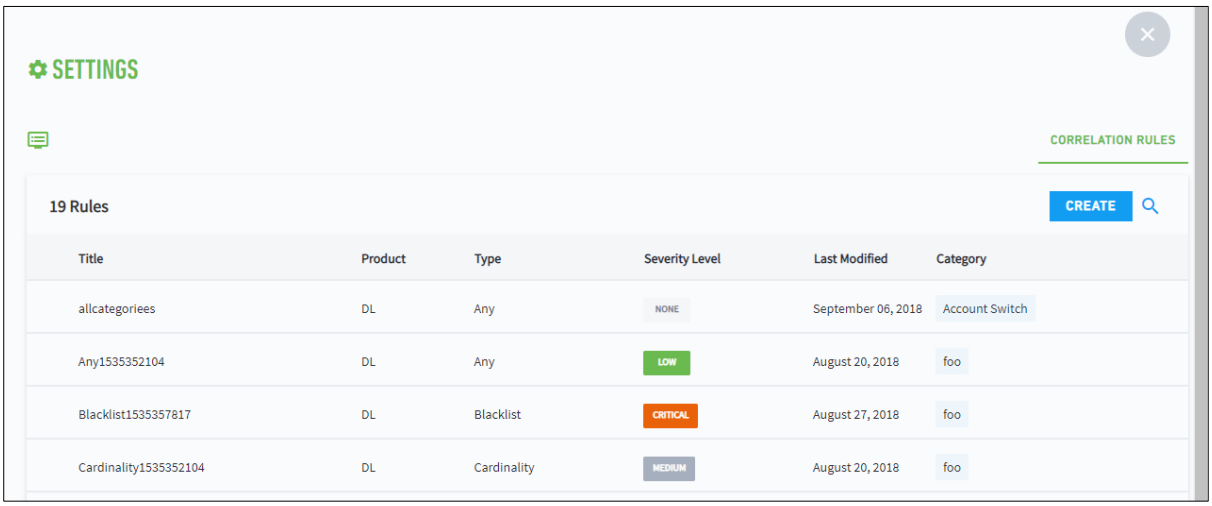
- Change: Monitors a certain field and matches if that field changes. The field must change with respect to the last event with the same query key.
- Flatline: Matches when the total number of events is under a given threshold for a time period.
- Metric Aggregation: Matches when the value of a metric within the calculation window is higher or lower than a threshold.
- Whitelist: Will compare a certain field to a whitelist and match if the list does not contain the term.

4.4 Dashboard Preview:

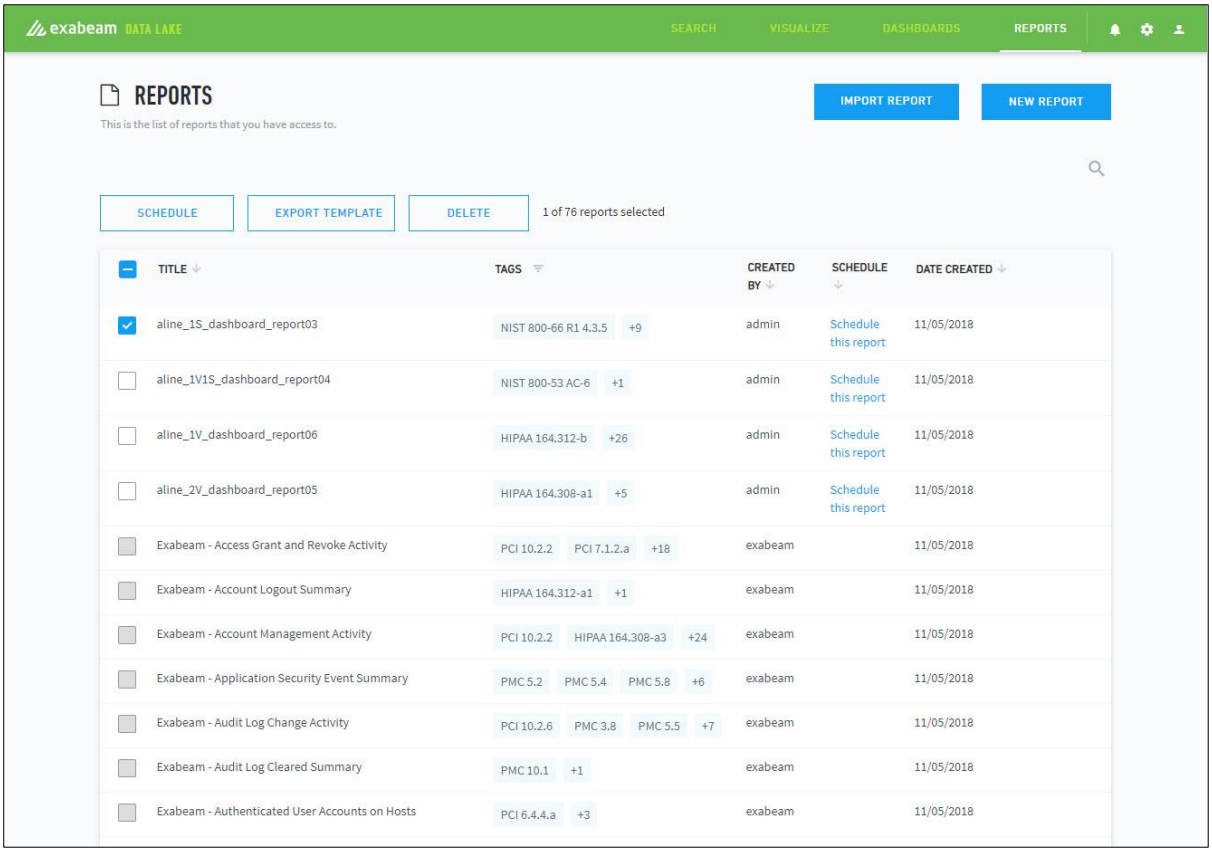
- Exabeam dashboard main page view:



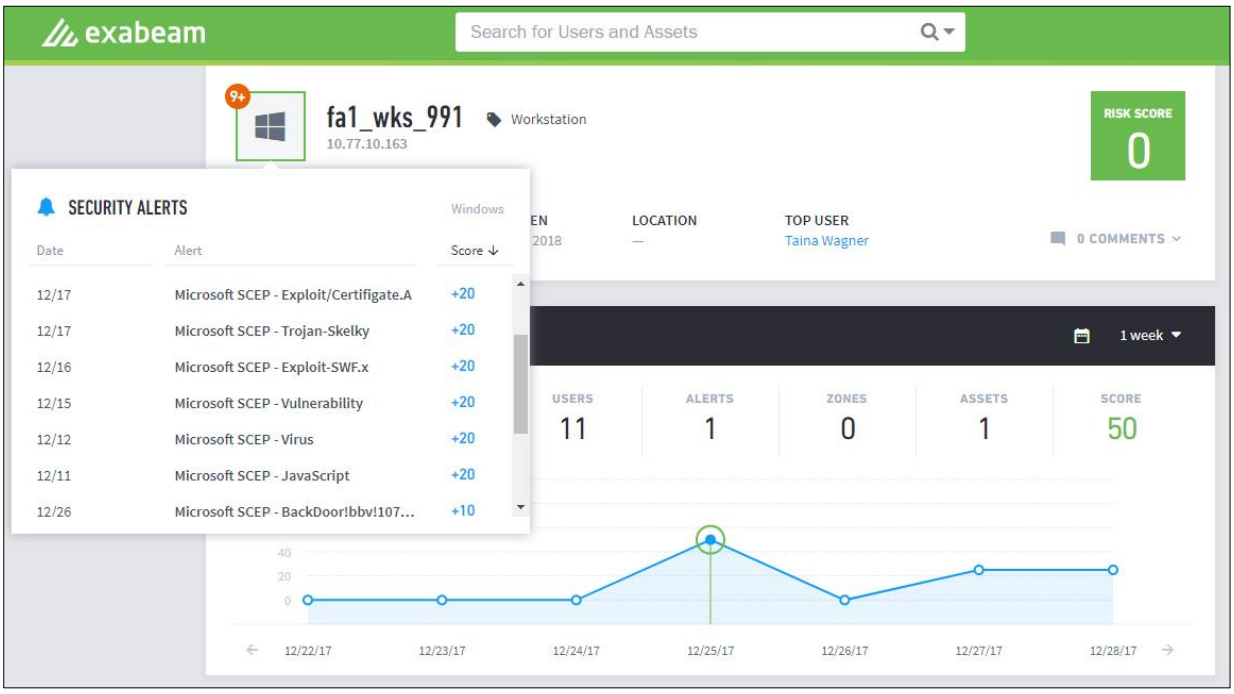
- Exabeam rule setup and configuration page:



- Exabeam report view page:



- Exabeam risk scoring view page:



5. Extrahop Potential Security Monitoring Dashboard

5.1 Dashboard version: 8.5

5.2 Vendor Company: ExtraHop Networks

5.3 Dashboard Key Features:

Dashboard User Interface Key Features:

- Customizable Dashboard:
    - Provide different security overview subpages templates in the Extrahop system dashboard.
    - Customized dashboard visualization (Drag and drop for editing)
- Result display type:
    - Security information and event management (SIEM): The ExtraHop Detection SIEM Connector supports ExtraHop integrations with security information and event management systems (SIEMs) by formatting and transmitting detection data over syslog.

Dashboard Function/Control Key Features:

- Threat detection technology control.
    - Provide config and control function for high-risk detections, trending security metrics, rotating activity maps and machine learning detection.
- Intelligence searching function.
- Custom threat collection.
    - Support user uploading a custom threat collection/sample to their ExtraHop-managed sensors.
- Dashboard sharing:
    - Support dashboard one time link access for sharing or costumer free trail.

Threat Detection and Analytics Key Feature:

- Type of scoring: Risk scoring
    - Measures the likelihood, complexity, and business impact of a security detection. This score provides an estimate based on factors about the frequency and availability of certain attack vectors against the necessary skill levels of a potential hacker and the consequences of a successful attack. The icon is colour coded by severity as red (80-99), orange (31-79), or yellow (1-30).

- Threat detection
    - Built-in rule-based threat detection: Rule-based detections identify security hygiene issues by comparing observed behaviours on the network against security best practices. This uncovers risks such as the use of the vulnerable SMBv1 protocol or password information sent cleartext, and more.
    - Custom rule-based threat detection: Organizations can also create custom rule-based detections that identify policy violations, such as cleartext data movement between network segments housing PII or health data, that may be unique per environment. Extrahop Reveal(x) includes a scripting capability for real-time parsing of enterprise protocols.

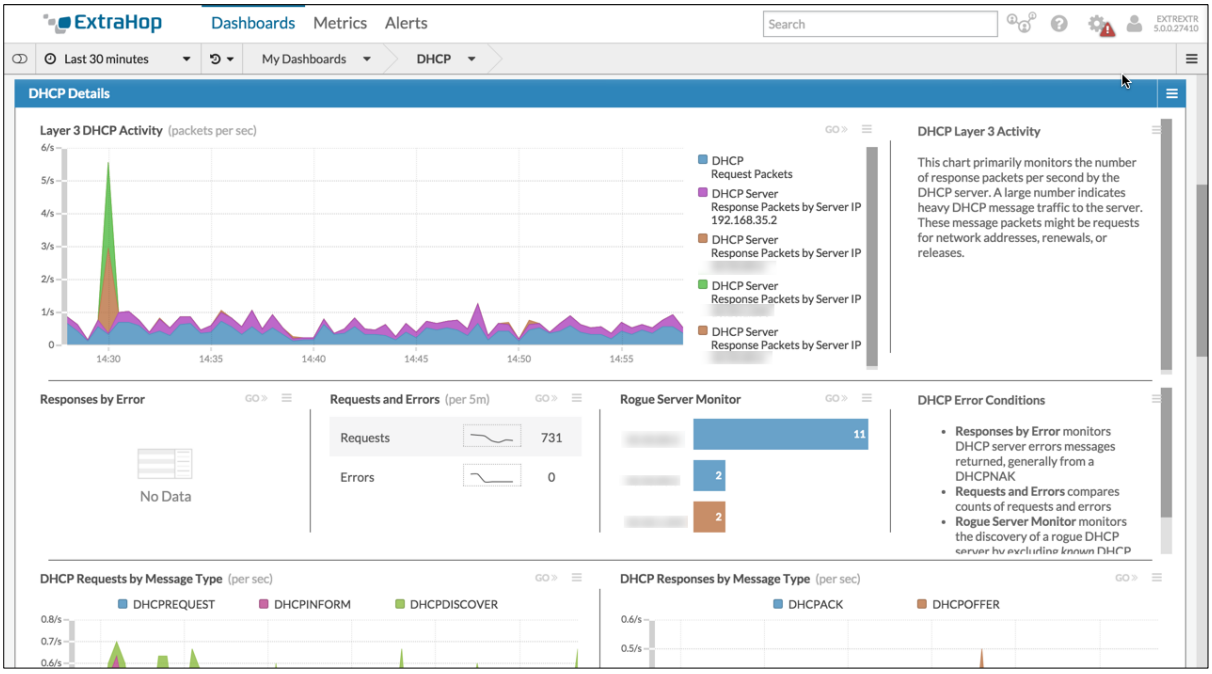
- Machine Learning: Extrahop Reveal(x) uses machine learning to model behaviours of entities on the network and contextually identify behaviours that resemble known/unknow attack techniques.

- Threat analytics
  - Time-series Analysis, Behaviour Graph Analytics, Autonomous Root Cause Analysis, Detector-specific Root Cause Analysis, ML-powered behavioural analysis.

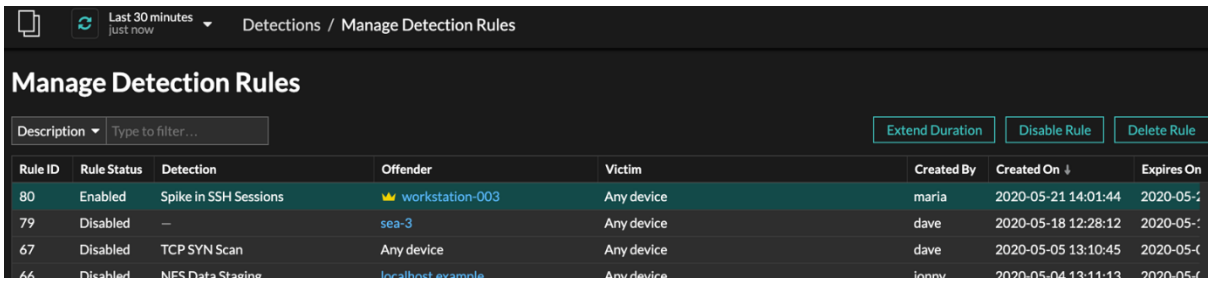
- Rule creation and tuning
  - Rule customized: user can configure the rule criteria: Type, Category, Technique, Offender, Victim, Device Role, Source, Site to create their own rule.

5.4 Dashboard Preview:

- Extrahop dashboard main page view :



- Detection rules management page



6. LogRhythm NextGen SIEM Platform

6.1 Dashboard version: 7.7x

6.2 Vendor Company: LogRhythm, Inc

6.3 Dashboard Key Features:

Dashboard User Interface Key Features:

- Customizable dashboard and report page.
    - The dashboard page and reports page provide user with a customizable, widget-based web interface for dashboard editing and direct accessing to the authorized report packages.
- Hot key config page.
    - User can define and use hot key to control the dashboard or switch pages.
- Result display type:
    - User and entity behaviour analytics (UEBA)
    - NextGen SIEM
    - Log management
    - File integrity monitoring
    - Network detection and response
    - Security analytics
    - Compliance automation
    - Threat hunting
    - Security orchestration, automation, and response (SOAR)

Dashboard Function/Control Key Features:

- Alarm configuration and control.
    - The alarms page can show as many LogRhythm alarms as user deployment. The Alarm detail is configured to cache in the LogRhythm configuration manager.
- Customized data searching.
    - The searching feature includes a wide range of filter and group selections along with Boolean logic for targeting specific data sets. The searching page provides access to user's search history on the web console and user's saved investigations on the client console.
- Task planning and event filtering.
- Cloud AI threats detection management.

Threat Detection and Analytics Key Feature:

- Type of scoring
    - Risk scoring, Cloud AI event scoring and User anomaly Scoring
- Threat detection
    - Known attacks: IP Address, URLs and user agents.
    - Botnets: IP address, URLs
    - Associated with fraud: IP address URLs.
    - Associated with Malware: IP Address, URLs User Agent, processes, File path, file names.
    - Used for Phishing: IP Address, URLs, Email Addresses, Email subjects.
    - Suspicious: IP address, URLs

- Threat analytics (Threat Analytics Module)
    - Malicious Software analysis: Malware Outbreak analytics, Abnormal Process Activity analytics, New Auto Run Process analytics, Novel Software Installation analytics, Local Security Override analytics.
    - Host Access Attempts analysis: Pass the Hash, PowerShell Execution, Local Account Created and Used, Multiple Object Access Failures
    - Windows Firewall Events analysis: Multiple Firewall Changes, Process Added to Firewall, Firewall Rule Added/Modified, Security Event Then Firewall Change

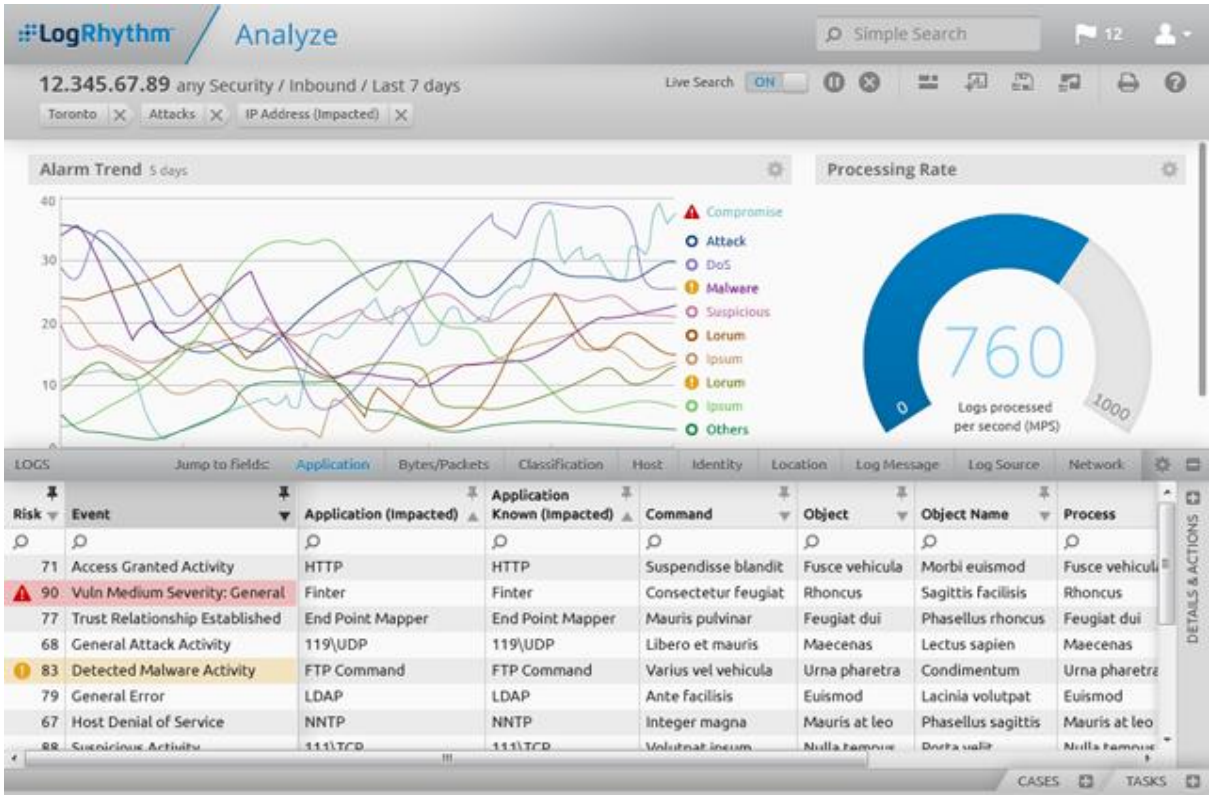
- Diagnostic Alarm Rules (rule ID and Name)
    - 105 - AI Engine: Critical Condition
    - 106 - AI Engine: Excessive Warnings
    - 107 - AI Engine: Successive Errors
    - 194 - AI Engine: Rule Suspended Due to Memory Triage

6.4 Dashboard Preview:

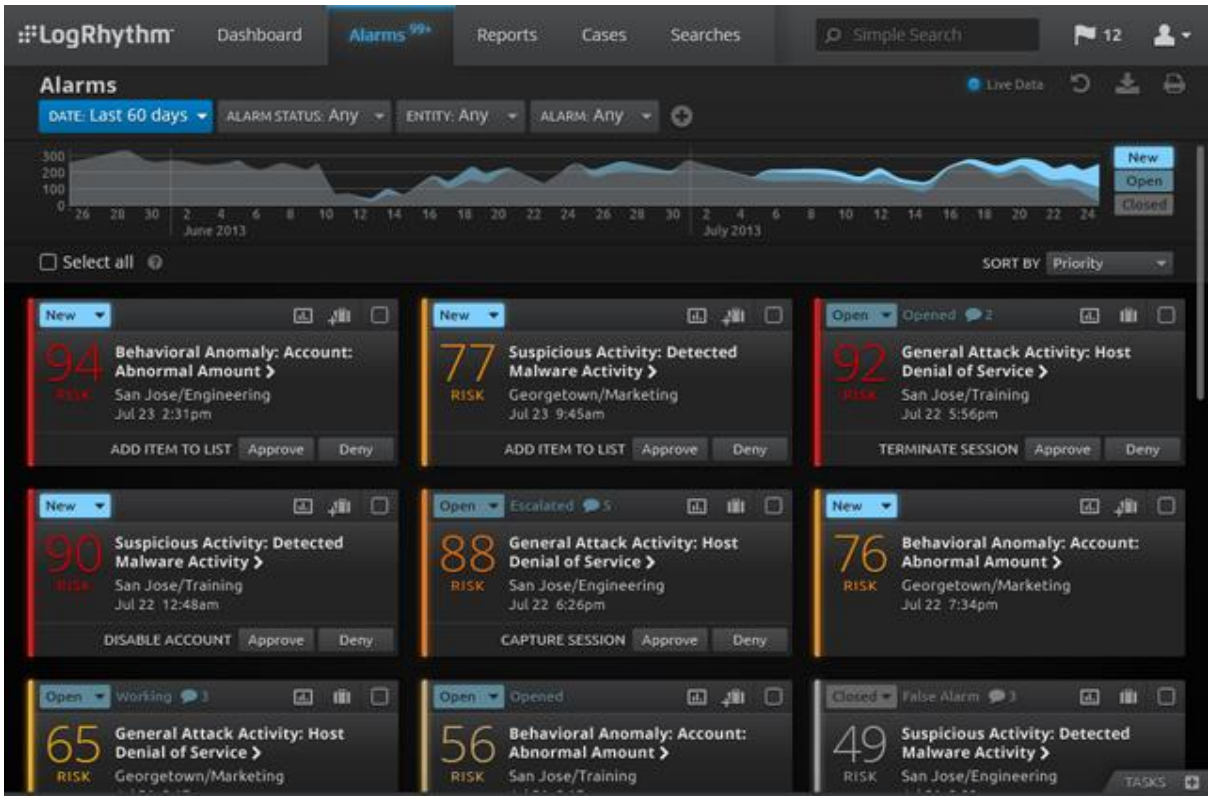
- LogRhythm dashboard main page view:

- LogRhythm Next-Gen SIEM dashboard:

- LogRhythm Dashboard Analytics page:



- LogRhythm Dashboard Alarm page:



7. Splunk Enterprise Threat Monitoring Dashboard

7.1 Dashboard version: 8.1.4

7.2 Vendor Company: Splunk Technology

7.3 Dashboard Key Features:

Dashboard User Interface Key Features:

- Customizable dashboard.
    - Customized the UI layout and Interactions. Support 3rd party visualizations widgets.
- Result display type:
    - Analytics-driven Cloud SIEM
    - 120+ use cases in UEBA products.
    - Splunk SOAR

Dashboard Function/Control Key Features:

- Splunk Knowledge management function.
    - Maintenance of knowledge objects for a splunk enterprise implementation.
    - Knowledge sharing control to ensure that knowledge objects are being shared and used by the right groups of people in the organization.
    - Normalize event data.
    - Build data models for pivot users.
- Report acceleration, data model acceleration, summary indexing, batch mode search.
- Event config and control.
    - The user can design their own events from a data set based on certain criteria.
- Dashboard sharing and exporting.
- Data model control
    - The indexed data can be modelled into one or more data sets that is based on specialized domain knowledge.

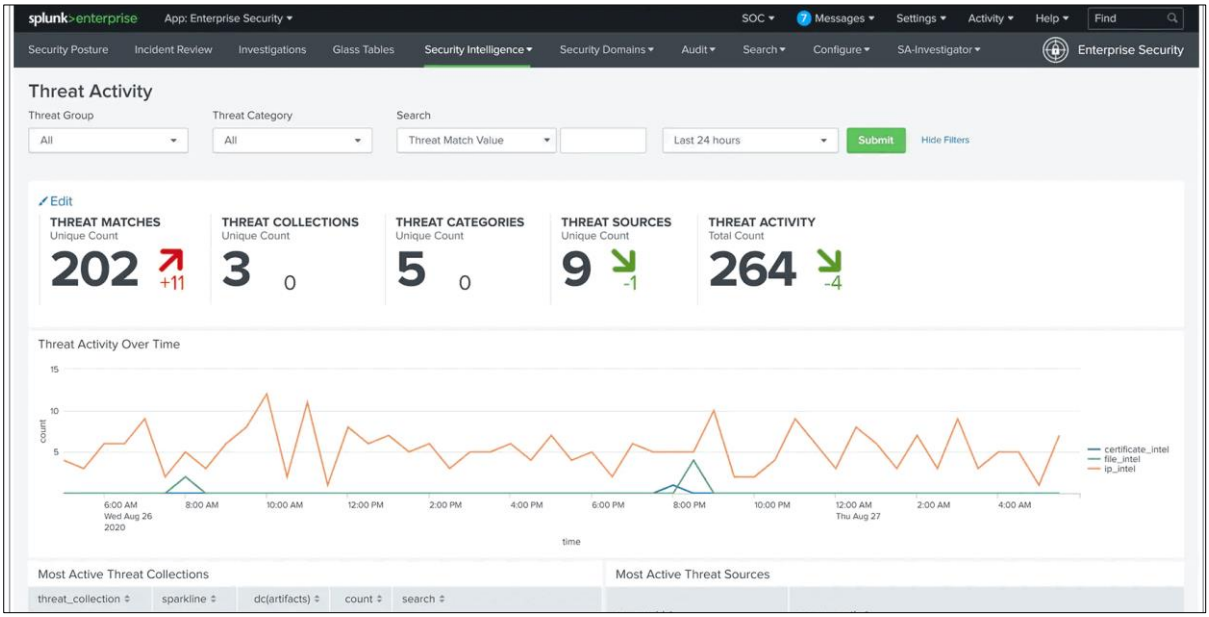
Threat Detection and Analytics Key Features:

- Type of scoring:
    - Customizable anomaly scoring (Fraud Risk Scoring)
- Threat detection
    - 20+ Threat types under 7 use cases: Account misuse, Compromised user account, Compromised /infected machine, Data exfiltration, External attack, lateral movement, Suspicious behaviour/unknown threat.
    - Privileged Account Abuse: Detect inappropriate usage of access permissions.
    - Privilege Escalation: Detect transformation of identity and access credentials.
    - Data Exfiltration: Detect the act of stealing private, confidential and sensitive data within an organization by malware or an attacker.
    - Unusual activity: Detect accessing external domains, remotely accessing high privileged assets, and unusual login duration, time or location.
    - Credential Compromise: Detect stealthy takeover of accounts for malicious purposes.
- Threat analytics
    - Enhance visibility and advanced thread detection.
    - Accelerate investigation.
    - Integrated with Splunk Enterprise security, a proven, market-leading SIEM.

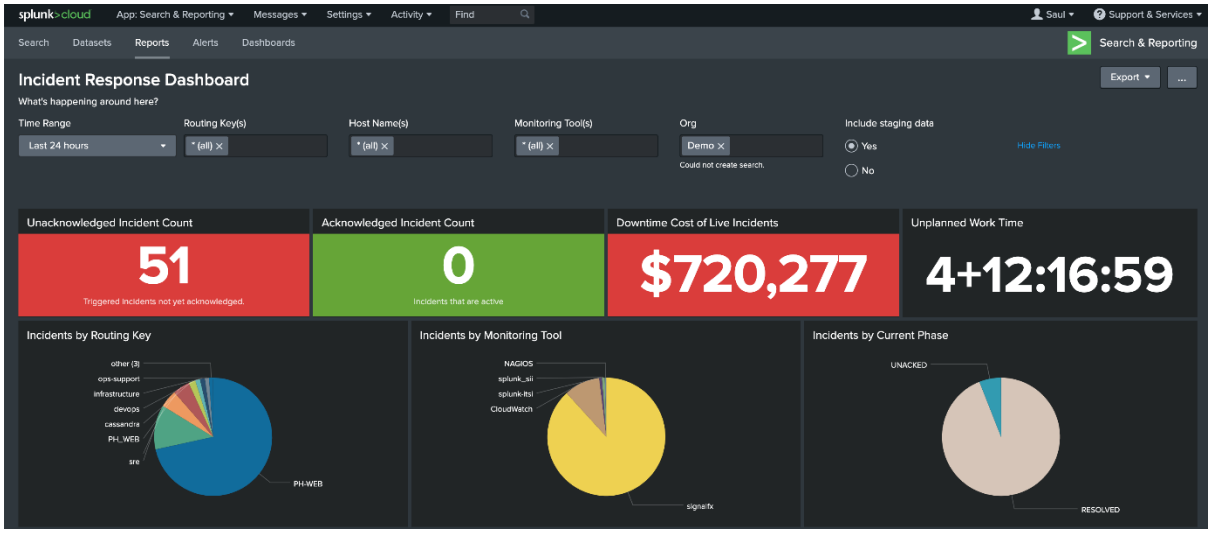
- Rule type supported:
    - App: Name of the app
    - Role: Name of the role
    - index: Name of the index
    - user: Name of any valid user
    - search_type: adhoc, scheduled, datamodel_acceleration, report_acceleration, and summary_index
    - search_mode: real time and historical
    - search_time_range: An absolute time range during which the rule is valid. Currently supports alltime only.
    - adhoc_search_percentage: The percentage of the total search concurrency limit that you want to allocate to ad hoc searches.

7.4 Dashboard Preview:

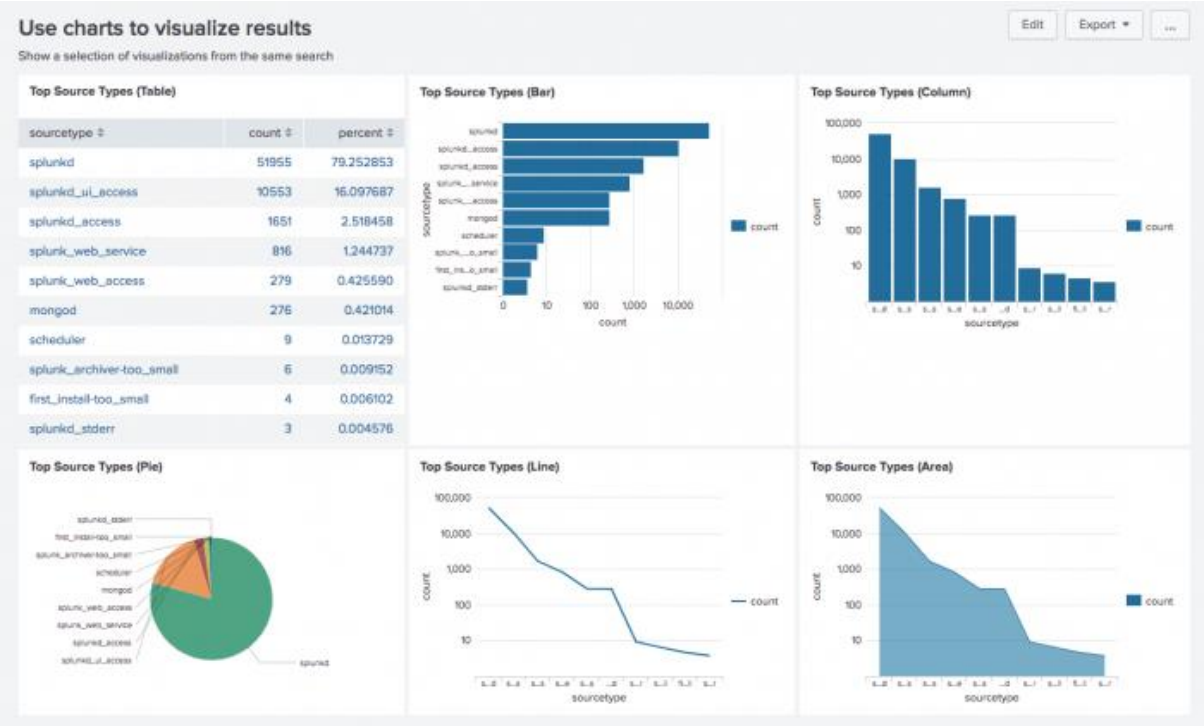
- Splunk dashboard threat activity page view:



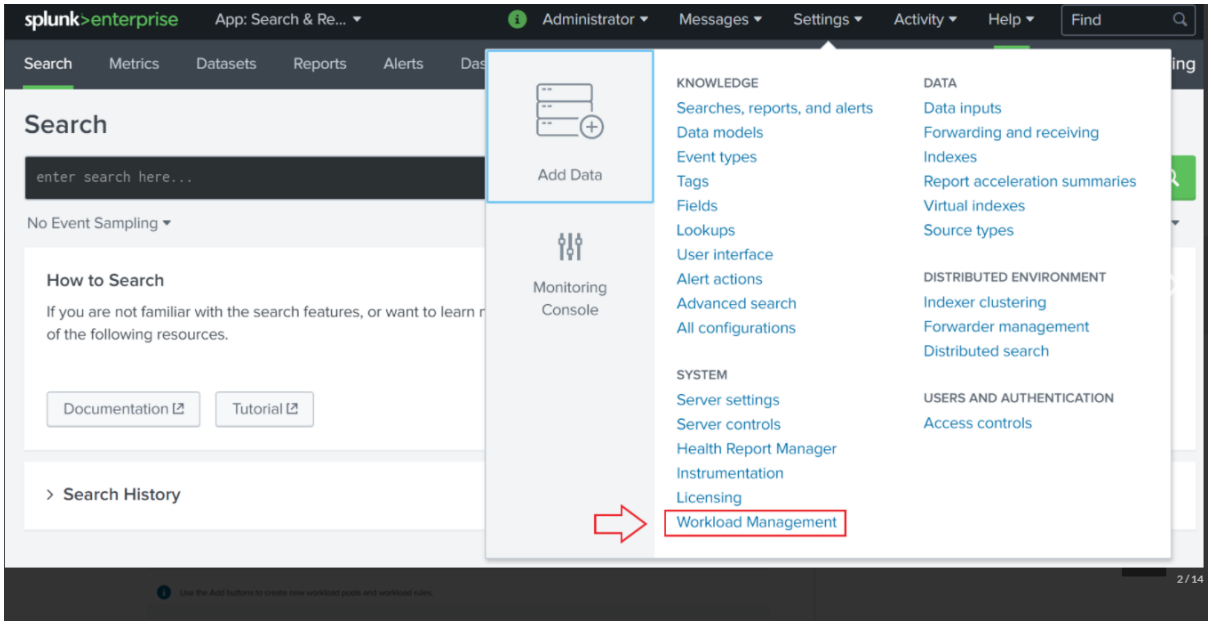
- Splunk cloud dashboard page:



- Result display selection page:



- Search config page:



Section II. Dashboards Feature Comparison Table

1. Dashboard User Interface Key Features Comparison Table

Dashboard User Interface Feature Comparison Table							
Features\Dashboard	**Fusion Portal**	**Anomali**	**BitSight**	**Exabeam**	**Extrahop**	**LogRhythm**	**Splunk**
SIEM	√	√	×	×	√	×	√
UEBA	×	×	×	√	×	√	√
SOAR	√	√	×	×	×	√	√
Customizable widgets and layout	√	√	√	√	√	√	√
3rd party widgets support	×	×	√	×	×	×	√
Multiplatform UI optimization	√	×	×	×	×	×	√
Hot key UI control configuration	×	×	×	×	×	√	×
Report page	√	√	√	√	×	√	√
Event/activity page	√	√	√	√	×	√	√
Alert/Alarm page	√	×	√	√	√	√	√
Support page	√	×	×	×	×	×	×
Research community page	×	√	×	×	×	×	×
Organization security rating page	×	×	√	×	×	×	×

√ - Supported × - Not Supported.

2. Dashboard Function/Control Key Features Comparison Table

Dashboard Function/Control Key Features Comparison Table							
Features\Dashboard	**Fusion Portal**	**Anomali**	**BitSight**	**Exabeam**	**Extrahop**	**LogRhythm**	**Splunk**
Data searching and data set finding	√	√	√	√	√	√	√
Assets management	√	×	×	×	×	×	×
Threat events Indexing, filtering and sorting	√	√	√	√	√	√	√
Customized event	×	×	×	×	×	×	√
Combined Findings	√	√	×	×	×	×	√
Security testing function	√	×	√	×	×	×	×

Access permission control	√	√	√	√	√	√	√
Knowledge/data sharing control	√	×	√	×	√	×	√
Task planning	√	×	×	×	√	√	×
Threat sandbox detonation	×	√	×	×	×	×	×
Threat analysis tools selection	×	√	×	×	√	×	×
3rd party threat analysis tools/app support	×	√	×	×	×	×	×
Machine learning and AI detection control	√	×	×	×	√	√	√
Periodic report generation config	√	√	√	√	×	√	√
Security awareness training	×	×	√	×	×	×	×
Security level rating config	×	×	√	×	×	×	×
Custom threat collection/upload	×	×	×	×	√	×	×

√ - Supported × - Not Supported.

3. Dashboard Threat Analytics Key Feature Comparison Table

Dashboard Threat Analytics Key Feature Comparison Table							
Features\Dashboard	**Fusion Portal**	**Anomali**	**BitSight**	**Exabeam**	**Extrahop**	**LogRhythm**	**Splunk**
SIEM analytics	√	√	×	×	√	√	√
UEBA analytics	×	×	√	√	×	√	√
SOAR analytics	√	√	×	×	×	√	√
Rule-based analytics	√	√	×	√	√	√	√
Statistical analytics	√	√	√	√	√	√	√
Time-series analysis	√	√	√	√	√	√	√
Machine leaning analytics	√	×	×	√	√	√	√
Behavioural graph/baselining analytics	×	×	√	√	√	√	√
Anomaly detection	√	√	√	√	√	√	√
Risk analytics	√	√	√	√	√	√	√
Dynamic peer Grouping (UEBA)	×	×	√	√	×	√	√
Centrality graph analytics	√	√	×	×	√	√	√

Community graph detection	√	√	√	√	√	×	×
Connectivity graph analytics	√	√	√	√	√	×	×
Path(P2P) graph analysis	√	√	√	×	√	×	√
Root cause analysis	√	√	×	√	√	√	√

√ - Supported × - Not Supported.

3. Feature Gaps Between Trustwave Fusion Portal and Other Vendors Dashboard Program

3.1 Dashboard UI Feature Gaps

- Some vendors' dashboards provide drag and drop editing, page template selection and support third party widgets for dashboard building.

- Fusion Portal is the only dashboard integrated support and live chart page to help user do trouble shooting.

- Some vendors combined the research community website, security awareness training website and show the security rating system in their dashboards.

- Fusion Portal is the only dashboard did UI fully optimization for most of the platform/devices and provide the assets management page.

3.2 Dashboard Function/Control Feature Gaps

- Some vendors dashboards provide customizable detection tool selection function, AI detection control and support adding the third-party detection tools in the system.

- Some vendors dashboards give user flexibility for defining their own event, uploading their threat collection, and providing sandbox technology for testing.

3.3 Threat Detection and Analytics Key Features Gaps

- Some other vendors' analytics covered all the three main information security systems analytics frameworks (SIEM, UEBA, and SOAR) which are widely used in the market.

- Some other vendors' analytics function support the dynamic update and 3rd party analytics function/App plugin for their analysis process.

- Some other vendors' analytics function will focus more on collecting/monitoring the individual user/company/organization's behaviours data (even non risk behaviours data) to build their nodes map for analysis process.