DefenseStorm

A SECURITY DATA PLATFORM

DefenseStorm aggregates all your network and security events into a single view, simplifying IT Security activity so your team can spend more time investigating and remediating threats.

GOVERNANCE INSIGHT

C-level reporting across every IT system that demonstrates your policies are being met, so you can manage risk effectively.

- **Incident Workflow:** Built-in processes for better incident management and faster resolution
- **Incident Resolution Type:** Track whether your Service Level Agreement (SLA) was met and which policies were violated
- **SLA Alerts:** Automatic alerts remind you when incidents are not resolved within, so that nothing falls through the cracks
- **Dashboard Metrics:** At a glance visuals show how your team is performing
  - » **Pipeline Dashboard:** The most important data points for measuring events, alerts and incidents - quantity, type, severity and associated policy
  - » **Incident Velocity Dashboard:** Metrics that tell you time in triage, time to resolution and false positive rate
- **Reporting:** Cybersecurity insight that makes creating boardroom-ready reports simple
  - » **Platform Summary:** An overview of events, alerts, incidents and resolutions
  - » **Event History:** The total number of events per day
  - » **Incidents by Source:** How many incidents were identified from each source
  - » **Incident Breakdown by Severity:** Severity of incidents based on priority status (Low, Medium, High)
  - » **Average Time to Resolution:** The average number of days to resolve incidents
  - » **Incident Breakdown by Resolution:** Incident counts by resolution type
  - » **Alerts Breakdown by Type:** How many alerts were dismissed, escalated, or deemed false positives
  - » **Ground Asset Breakdown:** Grouping of network assets by asset type
  - » **User Activity Level:** Displays user activity levels by user types
  - » **Windows Objects Activity:** Details what objects are most active
  - » **User System Logins:** Number of user logins by user

DefenseStorm

ANALYTICS-DRIVEN SECURITY

Real-time threat detection and remediation using Big Data analysis. All your data is in one place, viewable from easy-to-use dashboards.

- **PatternScout:** Anomaly detection through machine learning algorithms, so you can detect when something strange happens in your network using behavior-based pattern recognition
- **ThreatMatch:** Automatically aggregates threat intelligence feeds to find known bad actors (IP, domain name, file hash) that are affecting your network now or in the past
- **Search Capabilities:** Up to 120x faster queries for more agile threat investigation
- **Big Data Capabilities:** Ability to handle all of your disparate, unstructured data sets, so that you can detect more threats and have the structured data you need to resolve them quickly
- **Event Dashboard:** Configurable dashboard to visualize your events so you have a view across your entire network
- **Alert Investigation Tools:** View events and drill into data flow, determine if there is an incident that needs to be resolved
  - » **Pivot Search:** Drill into activity for a specific IP address
  - » **Natural Language Query:** Investigate without needing complex search language
  - » **Reputation Search:** Point and click reputation lookup for external IP addresses, domain names and file hashes
- **Incident Management Tools:** Manage end-to-end issue detection and resolution
  - » **Incident History:** Every note, file, search and incident update is captured, so that you have a complete record to reference
  - » **Incident Watcher:** Stakeholders can monitor progress on key incident tickets
- **Event Classifier:** Spend less time dealing with non-essential security alerts, allowing you to dedicate more time to critical security

OPERATIONAL INTELLIGENCE

24/7 Support from security experts with deep understanding of the challenges confronting FIs in today's digital world.

- **Built-in Best Practices:**
  - » **Policies:** Built-in policies for cybersecurity, firewall, Windows, network and physical
  - » **Alerts:** Built-in alerts that are linked to policies for Windows/Mac/ *nix environment, network infrastructure, client PCs, core system, BYOD, wireless networks and perimeter security
- **Expedited Onboarding:** White glove on-boarding process to ensure a speedy and hassle-free launch
  - » **Security Assessment:** Full review of IT, policies, controls and procedures
- **Guardian:**

DefenseStorm

INTEGRATIONS: OPTIMIZED SUPPORT FOR THE FOLLOWING

- » Security experts to monitor your network for anomalies and threats
- » Assistance in investigating threats
- » Advice on how to better secure your network

- **Connect:**
  - » An online community of peers
  - » Security best practices from DefenseStorm
  - » Actionable recommendations for the most important security bulletins via Connect
  - » Share and learn with your peers via Connect
  - » Carefully curated industry content to help filter out the noise

- **Security Tools:**
  - » Carbon Black
  - » IBM QRadar
  - » OSSEC
  - » Security Onion/Bro/Snort
  - » Virus scanners (McAfee, Norton, Symantec, etc.)
- **Network Tools:**
  - » Barracuda (spam firewall, webfilter)
  - » Cisco (ISE, ASA, PIX, switches, firewalls)
  - » Cisco Meraki
  - » FortiGate
  - » Palo Alto: (NextGen firewall, threat detection, web filtering)
  - » Pony Express
  - » SonicWall
  - » WebSense
- **Operating Systems:**
  - » Linux (auditd, auth, syslog)
  - » Mac OS X
  - » Windows (IIS, Snare, SQL Server, Exchange, SharePoint)
  - » Unix environments
- **Other:**
  - » Common Applications (Apache, nginx, postfix, etc.)
  - » Common Event Format (CEF)
  - » Custom Application Logs
  - » Java

STRUCTURED VS UNSTRUCTURED DATA

It's difficult to structure data properly. DefenseStorm does it in a way that optimized for security analysis, so that it is faster to query, understand and get results. So what about new data sources? DefenseStorm handles both structured (optimized) and unstructured data, so you have the best of both worlds.