ENTERPRISE SECURITY MANAGEMENT

Better IT Security Management with a total threat detection, analysis and compliance management.

LOGRadar

```
    </div>
  </div>
  </body>
  <script type="text/javascript">
  <!--
  var currentImage = "bigImage1";
  var pages = Math.ceil(photos.length / 9);
  updatePages();
  updateAllImages();
  // document.getElementById('bigImage0').src = images
  // document.getElementById('bigImage0').style.display =
  changePhotoDescription( '1' );

  function updatePages() {
      var j = 0;

      var html = '<table style="width: 330px;" cellspacing="0" cell
      if ( page != 0 ) {
          html = html + '<a href="#" onclick="page=0; updatePages(); upd
      }
      html += '</td><td style="text-align: center;">';
```

THE NEXTGEN SIEM

LOG RADAR was developed to address the critical need for an effective SIEM administration and integration within its deployed environment. Security Management users will be able to tap into enriched data, powerful real-time correlation and mitigate advanced threats with clear resolution towards vulnerabilities.

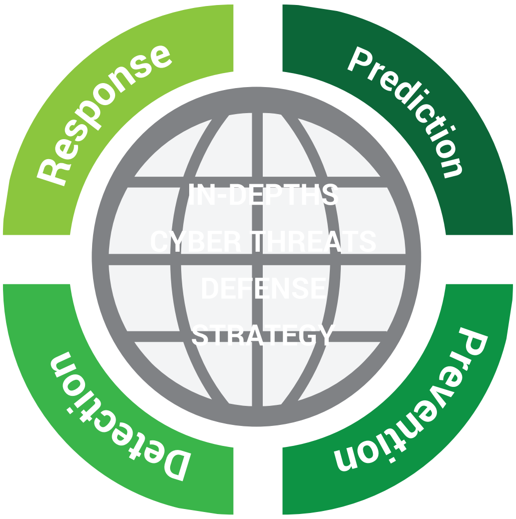
Our technology will enable you to have a better control over SIEM and an overall efficient usage and management.

www.tecforte.com   info@tecforte.com |

INTRODUCTION

Log Radar Enterprise Security Management is a powerful Security Information & Event Management (SIEM) solution that provides a holistic view of your existing security assets.

Unlike any other SIEM solution, Log Radar is built based on an In-depth Cybersecurity Defense Methodology via its 4 main components, specifically, **Prediction, Prevention, Detection & Response** towards the ever evolving cyber threats.



01 An In-depth Cybersecurity Defense Methodology

Tecforte has acquired much-needed experiences required over the years with many organisations and SIEM users to understand the intricate components and process to address the crucial needs and challenges in the successful implementation of SIEM.

Log Radar Enterprise Security Management combines all aspects of security operations and is suitable for organisations of all sizes or industry.

Log Radar can be used to ***monitor system health, implement smarter incident response, ensure an efficient running of an IT Security Operations centre or proactively manage IT risks before it affects business operations.***

02 Intuitive Dashboard View with Flexible Tab Editor

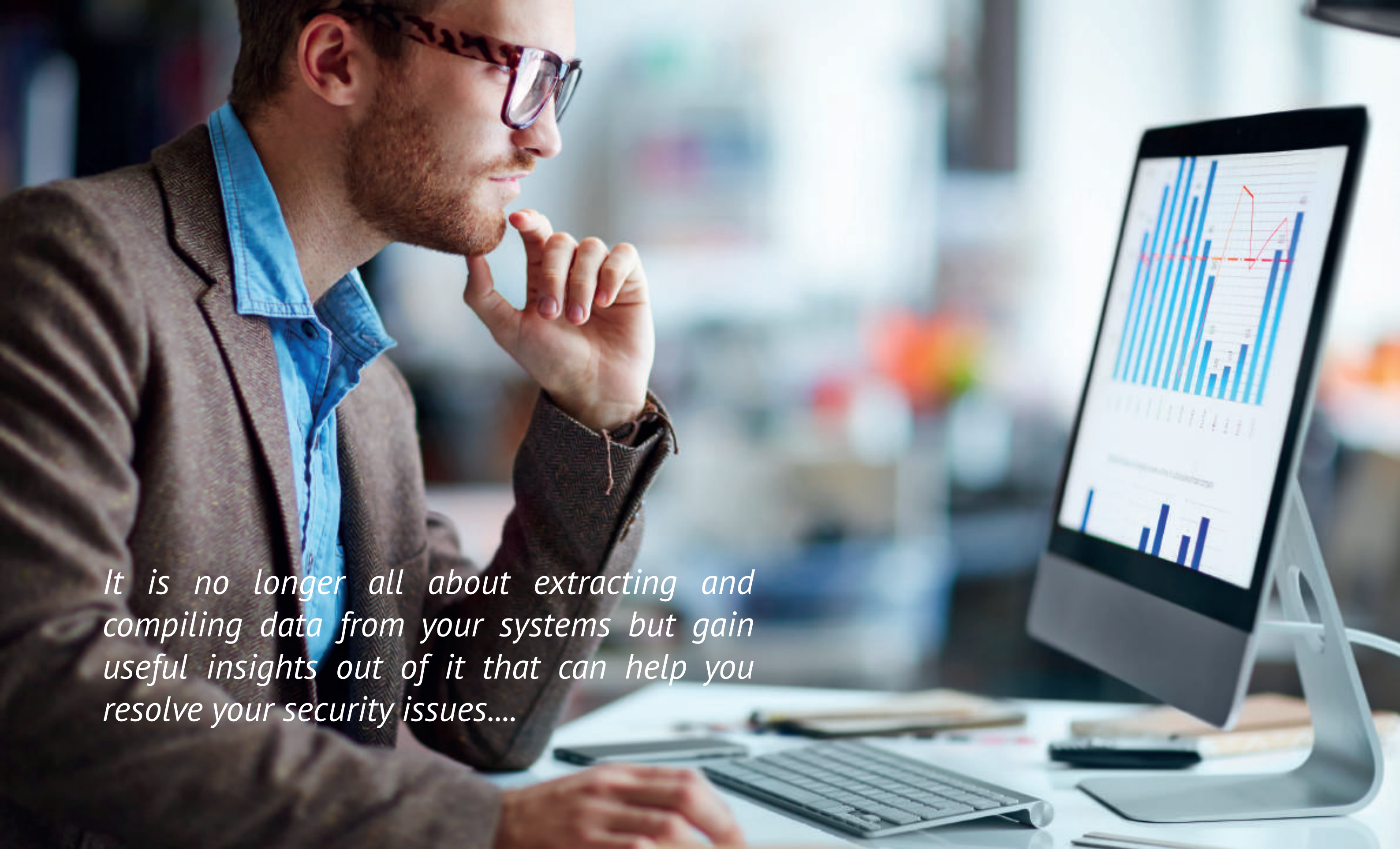
Implementing Log Radar Enterprise Security Management will provides organisations with the ability to:

Improve security operations with faster response times.

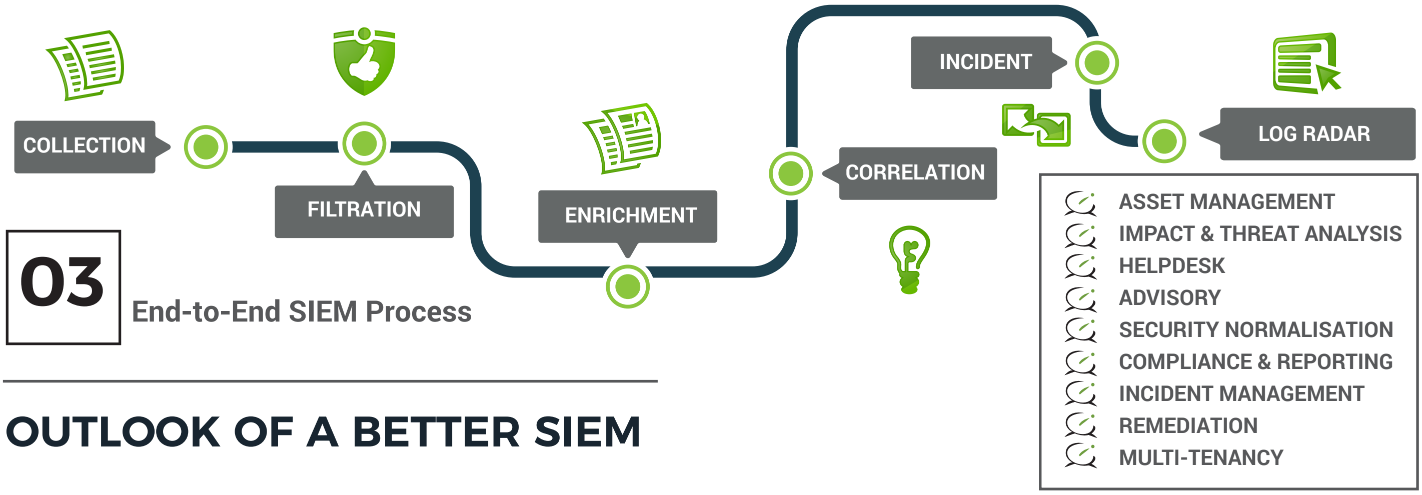
Gain visibility and deep insight over the entire network, security and system activity.

Enhance security discovery and inquiry capabilities using advanced analytics.

A complete security management platform from security monitoring, detection, forensic, incidence response and more.



It is no longer all about extracting and compiling data from your systems but gain useful insights out of it that can help you resolve your security issues....



- ASSET MANAGEMENT
- IMPACT & THREAT ANALYSIS
- HELPDESK
- ADVISORY
- SECURITY NORMALISATION
- COMPLIANCE & REPORTING
- INCIDENT MANAGEMENT
- REMEDIATION
- MULTI-TENANCY

03 End-to-End SIEM Process

OUTLOOK OF A BETTER SIEM

If advanced threat management with built-in incident management in a best-in-class technology features and network visibility are key factors to you, your organisation will benefit immensely with what Log Radar Enterprise Security Management has to offer:

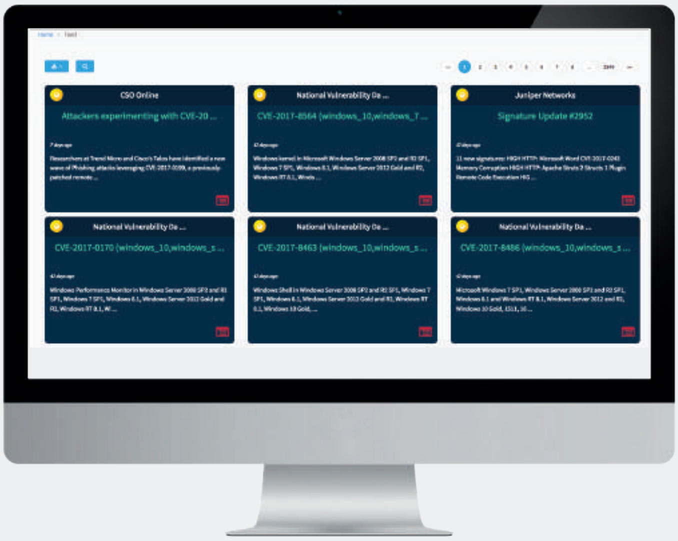
Asset Management

Log Radar Enterprise Security Management has a robust information security asset management and inventory tools that make it easy to keep track of all the devices being added or removed from the network. Besides providing decision makers with a holistic picture of their IT equipment, systems and processes, the module is integrated with incident management for faster response time.

Data Enrichment

Log Radar is capable of enriching the data with geolocation, user, asset and even custom information, giving user precise ability to do some pretty impressive geolocation plotting to make informed decisions during an investigation to help accelerate remediation process.

It also retains the event data origins within a stringent environment, providing a correct view of data segregation without causing any limitations to other processing features such as Filtration, Enrichment and Correlation. Attributes within original events are normalised and additional information is enriched into the normalised event while the raw log is maintained.


Home > Feed

1 2 3 4 5 6 7 8 ... 2499

CSO Online
Attackers experimenting with CVE-20 ...
7 days ago
Researchers at Trend Micro and Cisco's Talos have identified a new wave of Phishing attacks leveraging CVE-2017-0199, a previously patched remote ...

National Vulnerability Da ...
CVE-2017-8564 (windows_10,windows_7 ...
42 days ago
Windows kernel in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windo ...

Juniper Networks
Signature Update #2952
42 days ago
11 new signatures: HIGH HTTP: Microsoft Word CVE-2017-0243 Memory Corruption HIGH HTTP: Apache Struts 2 Struts 1 Plugin Remote Code Execution HIG ...

National Vulnerability Da ...
CVE-2017-0170 (windows_10,windows_s ...
42 days ago
Windows Performance Monitor in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, W ...

National Vulnerability Da ...
CVE-2017-8463 (windows_10,windows_s ...
42 days ago
Windows Shell in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, ...

National Vulnerability Da ...
CVE-2017-8486 (windows_10,windows_s ...
42 days ago
Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 16 ...

04 Enhanced Feed Module

Smart Analysis

Log Radar with ‘Smart Analysis’, is equipped with the interface built specifically for security professionals. This interface allows the user to quickly verify a process or situation by making all the supporting information conveniently available. It also enables them to find patterns in the security data that a traditional SIEM tool could not find on its own. This tool allows the user to perform their investigations using:

- User-friendly and powerful complex search capabilities with Regular Expression.
- Ability to perform analysis with known detection indicator, quick basic search by keyword
- Advanced Search that support detection indicator with Rule Editor
- Analysis with preferred reputation lookup
- Construct ad-hoc analysis rule and scenario based on normalised, enriched and aggregated data
- Enhanced view analysis with custom column layout and by normalised/raw options

Innovative Incident Management

Incident Management is developed based on stringent CERT practised incident handling and response security standards. It also refers to Information Technology Infrastructure Library (ITIL) framework to ensure an integrated component optimises for the analyst workflow. It allows for conclusive end-to-end threat detection and response based on severity classifications as well as a framework with STIX and CybOX technical specifications.

2 -Tiers Event Filtration Option

A critical part of any SIEM is the process for responding to most valid incidents. Log Radar deploys -2Tiers event filtration option whereby the first filtration will enhance the processing speed needed for another module as it drops out-of-scope monitoring devices or data. The -2Tiers Event Filtration will produce data which is more extensive
in security data.

Powerful Correlation

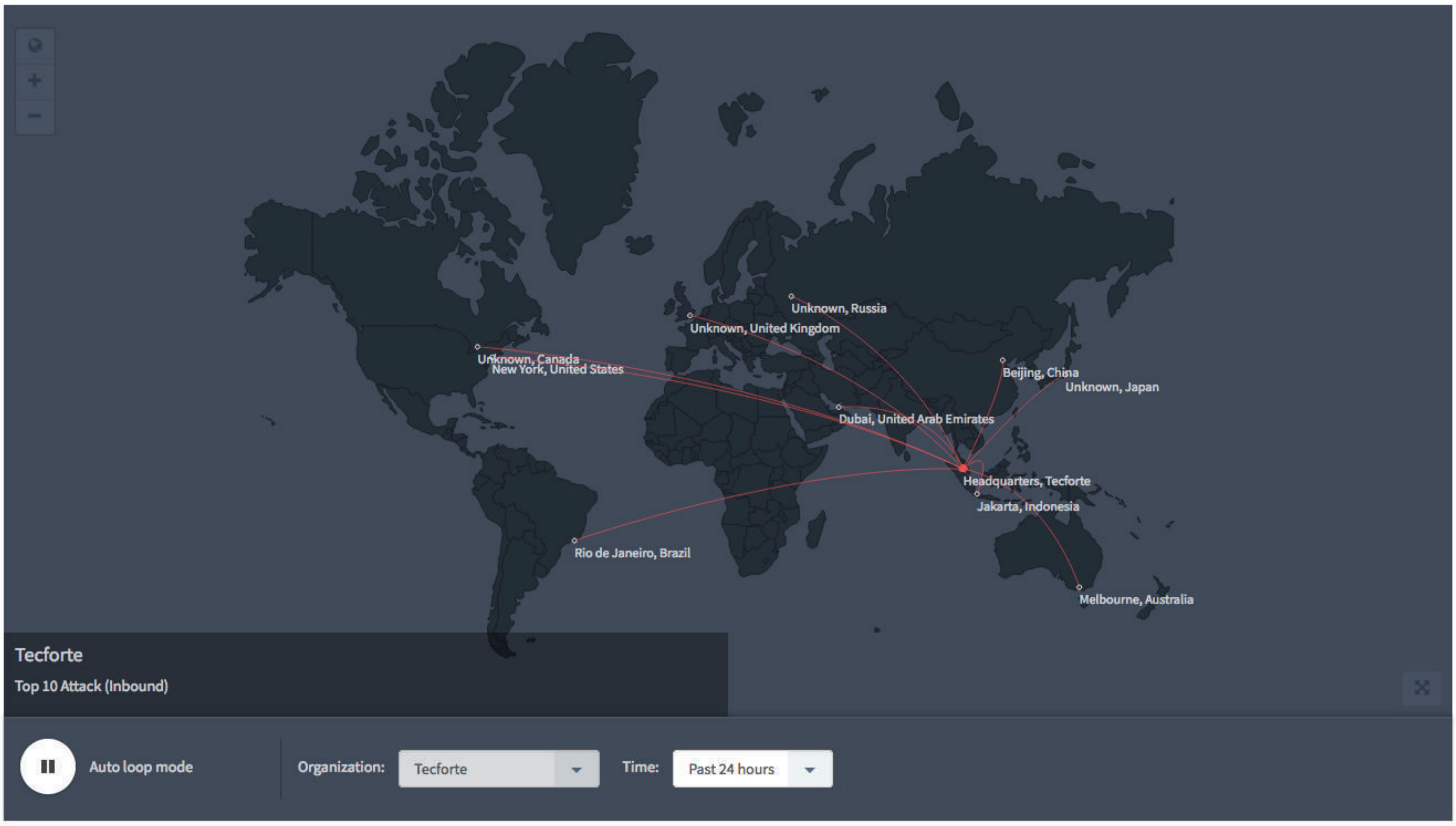
One of the biggest advantages of Log Radar is that it can help resolve the big puzzle by finding related pieces of a single event or related events in multiple logs and placing those parts together. Log Radar can automatically analyse all of these logs together with its correlation tool. Thus, they can produce a much richer understanding of what happened. It can help identify a complete series of related events, allowing a user to trace the incidents an attacker performed within the organisation.

Custom Reports

Key capabilities which include user and resource access reporting, vulnerabilities reporting as well as any ad-hoc reports requests based on user requirements. The reporting module will help to accommodate any urgent requests which will usually require additional resources to complete.

External Feeds

Log Radar use the information from RSS feeds which can significantly improve its real-time analytics by making attack detection quicker and more accurate indirectly giving the platform a stronger basis for prioritising its actions.



05 Real-Time Security Vulnerabilities as shown on detailed Cyber Map

Multi-Tenant Capability

The multi-tenant module within Log Radar lets the user create separate management environments within the system. It allows the user to configure different settings, policies or specifications based on their organisation's requirements. This feature is especially useful for enterprise that wants to protect confidential data among various divisions, branch or subsidiary offices within the same organisation.

Custom/Notification Template

Custom notification template for a faster escalation management, empowering the user to execute Incident Escalations, Alert Notifications, Update of Assets and other notification template as required.

Recommended Course-of-Actions

Eliminate errors through standardised course-of-actions while reducing time demands on the user. Utilizing on past processes documented and enhanced with Log Radar's knowledge base module, the company has the information on the next recommended course of actions for reference instead of relying on security professionals or external vendors.

Cyber Threats Map

The Cyber Threats Map provides a clear and concise graphical output of events happening in real-time. Visualise attack data based on origin, destination, risk level and numbers of occurrence plotted on a complete interactive map of the world. The Cyber Threats Map includes extensive details such as GeoLocation IP, Latitude and Longitude information which allows analysts to identify attack proximity for a complete overview of threats quickly. These displays help define patterns of attack that might otherwise go unnoticed.

To learn more about Log Radar Enterprise Security Management, please contact us at info@tecforte.com

Tecforte
SMARTER IT SECURITY MANAGEMENT