Security Operations & Analytics Services

Key Challenges

- **Average time to detect an attack (Dwell time) hovers around 175 to 210 days as reported by some leading research reports**
- **Existing monitoring capabilities are no match for the changing threat landscape**
- **Traditional SIEM technologies lack the sophisticated capabilities and visibility required to detect and protect against such advanced attacks**
- **Integrated monitoring of Operational and Security logs is not prevalent in many organizations**

Business Case for Security Analytics

Typically, organizations have tried to respond to evolving threats by implementing several point tools like Anti-Viruses (Anti-malwares), Firewall, IPS, URL filters, WAF, DLP solutions and SIEM solutions to prevent and detect security attacks.

Mechanisms like vulnerability assessments and penetration testing have also failed to mitigate the sophisticated attacks that bypassed the defense mechanism in place.

Here comes **Security Analytics** that uses behavior analysis for anomalies, which means detecting unusual behavioral patterns. To achieve best results from Analytics, we need to **baseline what is normal** and define thresholds.

Traditionally SIEM's have done a good job at collecting humungous logs from desperate systems and aid in correlation and compliance, but due to their limited analytical capabilities SIEM's have failed to provide real time threat detection and hence the delay in detection of breaches as reported in several research reports.

Our SaaS Solution

Our Security Analytics services provides a SaaS based model which is hosted on the cloud and can offer **Real Time Security Analytics**, depending on your need we can Implement the solution to use big data technologies and analyze logs it in real or near real time.

We can also configure threat indicators for identifying advanced threats by reverse engineering and using point tools like Firewall alerts, IPS rules, end point IPS, proxy servers, web application firewalls and other security tools. Alternatively use your existing SIEM to feed the logs and create a data lake to store the data from various other sources of data for our analytics engine to analyze these large data volumes using pre-configured rules.

Threat Intelligence

We can import threat intelligence feeds from your desired sources to use on our analytics platform and apply correlation to the collated data to predict the probability of a possible incident.

Log Collection Archival and Retention

Collecting log data from heterogeneous sources (Windows systems, Unix/Linux systems, applications, databases, routers, switches, firewalls, etc.) at a central place can be a daunting task for IT administrators.

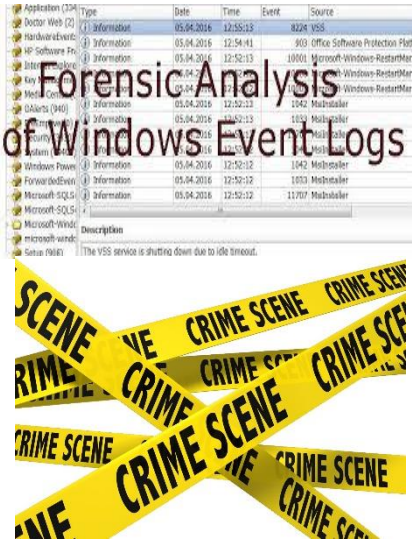
Log collection is done by using agents or through an agentless mechanism. IT administrators need a single, centrally located solution that allows them to decipher any log format from any source.

Archiving logs centrally is a mandate for many enterprises to meet compliance requirements. Log archiving depends of the policies laid down by the enterprise and the regulatory compliance it follows. The log archiving period varies according to the compliance needs. For example, PCI DSS requires 1 year, HIPAA requires 7 years, FISMA requires 3 years, etc. Another good reason for archiving logs in a central place is for log forensic investigation. Also, archived log data must be protected from changes to ensure authenticity.

PCI DSS, HIPAA, GDPR and other Regulatory Requirements

IT administrators need to furnish evidence to compliance auditors on complying with the regulatory requirements. Verbal assurance to compliance auditors is never sufficient. Compliance reports have to be ready, and the reports must be backed up with the appropriate log data and with the data management tools used. Meeting compliance requirements laid down by regulatory bodies such as FISMA, PCI DSS, SOX, HIPAA, ISO 27001, etc. is impossible without effective log management and effective Incident Management.

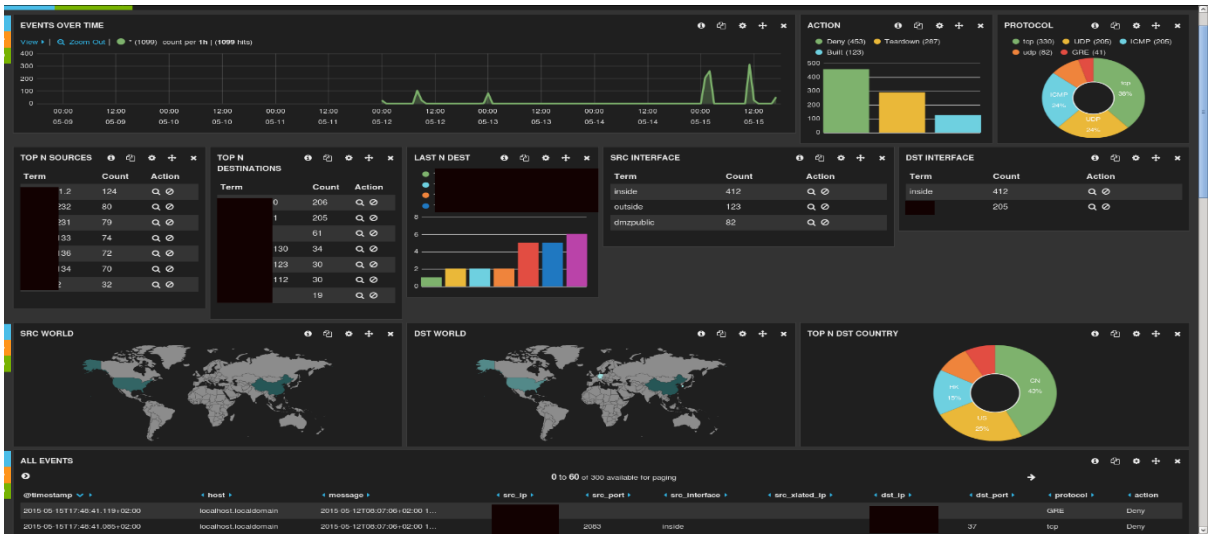
Forensics



Log forensic investigation enables conducting a root cause analysis to track down a network intruder or the event activity that caused the network problem. The log forensic process should be very intuitive and user-friendly, allowing IT administrators to search through the raw log data easily. Log search queries once entered by the IT administrator should quickly pinpoint the exact log entry that caused the security exception, find the exact time of occurrence, the person who initiated the activity, and the location from where the activity originated.

Dashboard and Reporting

We can customize your dashboard based on your specific needs. We understand that every organization has its unique needs and operate in a varied environment. Our Real Time Analytics Capabilities can provide you the much-needed information to take a decision on the fly.

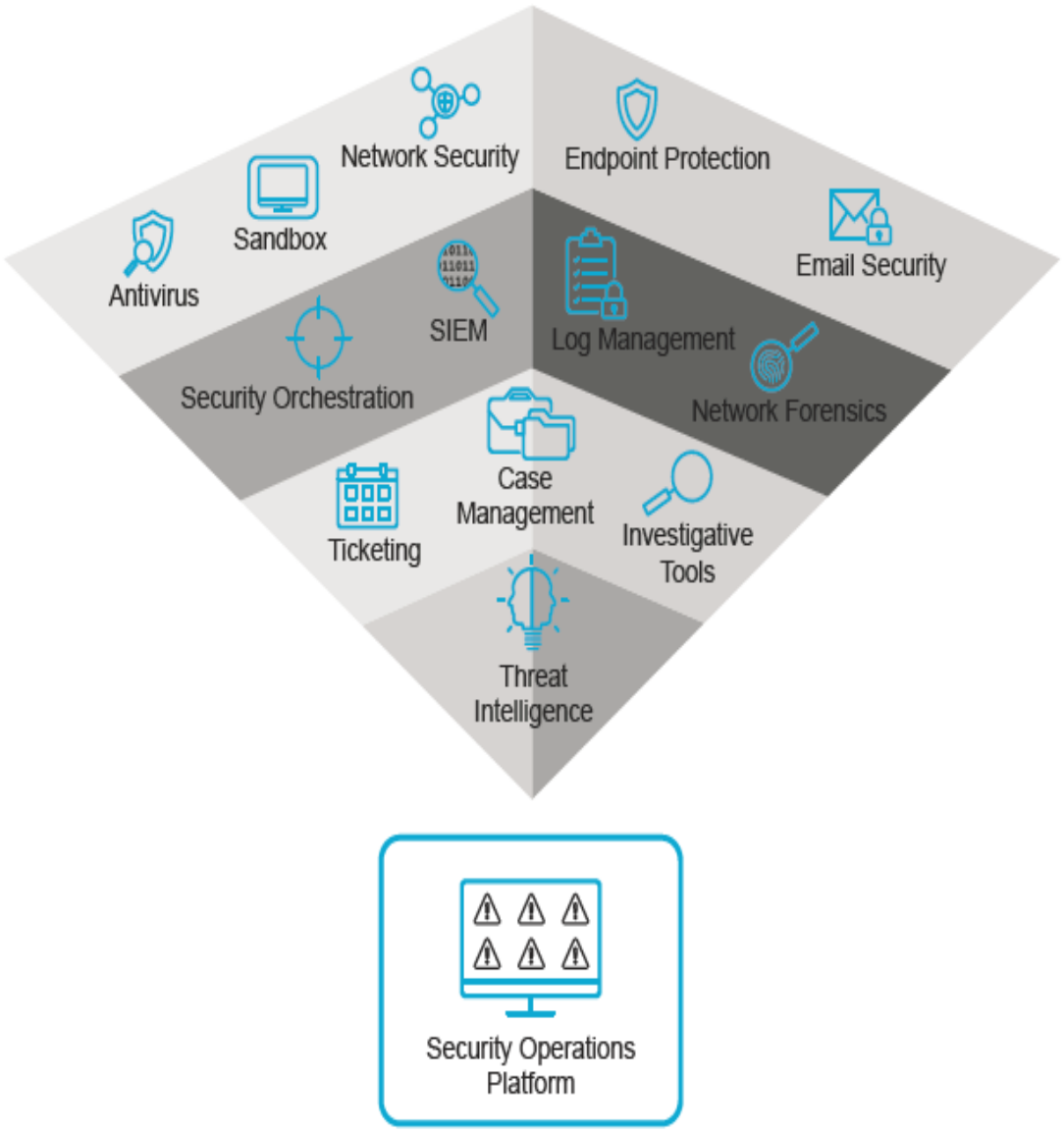


NIST Incident Response Framework

Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing

a successful incident response capability requires substantial planning and resources. The NIST Framework helps organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. The Framework provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. Our services align with the NIST guidelines

SOC (Security Operations Center) Building Blocks



Key Security aspects of our SaaS solution

Secure SSL Tunnel

All connections to our SaaS service are enabled with SSL/ Https via Transport Layer Security

IDM

There is an option to integrate the access thru the common Identity Management Solution

Encrypted Log Data at Rest

Log Data at rest is stored in an encrypted format using AES 256 bit encryption

Back up and Availability

All logs are automatically backed up and stored for 30 days max unless otherwise agreed

Remote Log Storage

Logs are stored in the cloud. As required by many compliance requirements that logs should not be stored with IT Administrators Our solution fulfills this requirement

Data Sovereignty

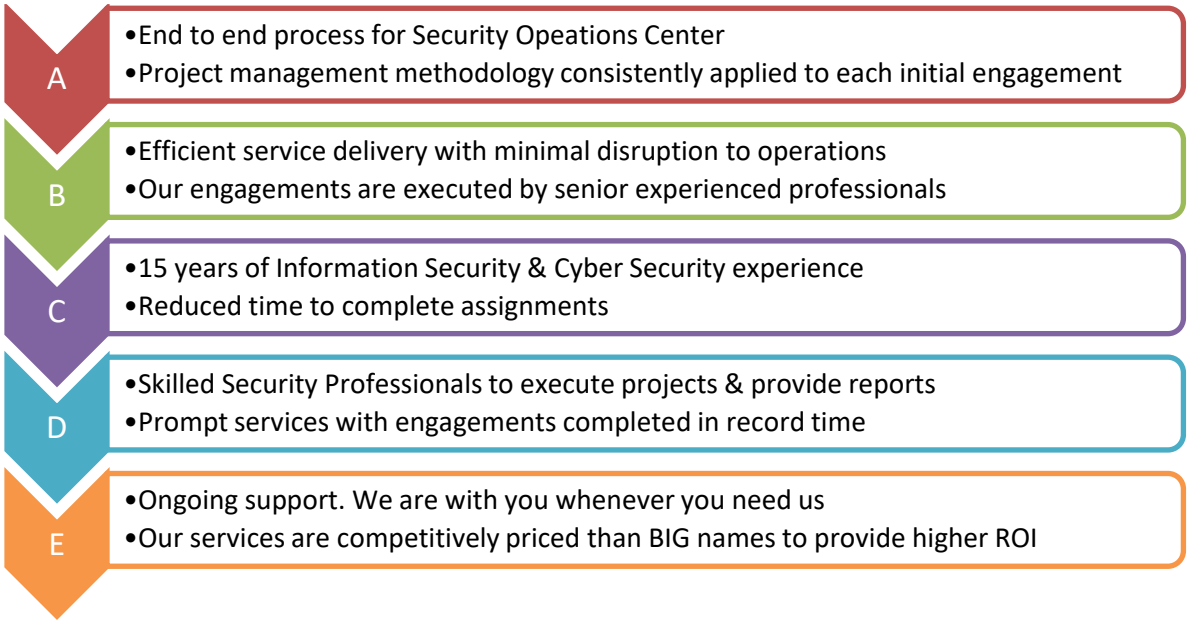
We can create a separate instance and store logs in a specific location if you have data sovereignty challenges

Value delivery

Knowing how much extra value our services can deliver, many clients find that it is easier to interact with our team who are skilled in helping organizations be more thorough and thoughtful in how they approach their issues. Using a Security Analytics service is a matter of clear thinking and smart planning. Working with cyber security specialized consulting specialists such as ours, helps you dig into areas such as cloud security, data security, incident response, change management processes and much more.

We provide end to end process for your Security Operational needs. With the rapid Cloud adaption and increased use of IoT, Big Data and Analytics, Cloud Security and Privacy concerns are on the rise. We can consolidate operational and security logs and implement best practices to evaluate your environment and to reduce the duplicate efforts to save costs for you

Some of the advantages of working with us are:



To discuss your specific need please email info@ecominfotech.biz