SHELT

MANAGED SECURITY SERVICES
Threat Monitoring, Detection & Response

LipaLater

We are pleased to enclose herein our proposal on **Managed Security Service for LipaLater in Kenya ("LipaLater")**

We trust this value proposal will allow the Company to overcome many of its Cyber Security challenges as we at SHELT are in the fore front of Cyber Security development having the appropriate experience, track record and history within the Financial industry in general and the Banking sector in specific.
We will be offering LIPALATER the following services based on their request

- Centralized Cyber Security and Resilience Management
- Integration of our Security Operation Center and Threat Detection and Response with leading End Point Protection and End Point Detection and Response mechanism to control and secure remote access of end users/employees to central systems
- Additional Security Services such as Honey Pot as a Service Decoy Mechanism
- Cyber Threat Intelligence on the Internet, Social Media and Dark Web
- Phishing Campaigns and Simulation
- Online Awareness Sessions including access to the most developed security awareness content videos, and ongoing scoring of internal employees security development

We are more than happy to respond to any further enquiry you may have about our proposal and we can be reached on the below contact details

We thank you again for your consideration and look forward to hearing from you soon.

Best Regards,

Bassam Touma
Business development
E btouma@shelt.com
M +961 3 55 98 59
W WWW.SHELT.COM

DISCLAIMER

This document is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this disclaimer is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this document is strictly prohibited. If you received this document in error, please notify us immediately by telephone and return the original document to us at the address below.

Document Control Page

Author(s)	SHELT	
Name	*Functional Section, Department*	*Signature/Date*
Bassam Touma	Business Development SHELT	

Reviewed by	LIPALATER	
Name	*Functional Section, Department*	*Signature/Date*
	LipaLater	

Approved by		
Name	*Functional Section, Department*	*Signature/Date*

Document Amendment Record

Change No.	Date	Prepared by	Brief Explanation
1.0	28/4/2019	Bassam Touma	Managed Security Proposal

Table of Contents

1 Introduction

LipaLater in Kenya, referred to herein this document as “LIPALATER” wishes to enhance furthermore the security of its information system by adopting a proactive approach and establishing a Controlled environment to secure its staff mobility and enhance its Cyber Resilience posture.

This proposal details the work that SHELT AFRICA Ltd., referred to in this document as Consultants will jointly undertake to implement the project related to the Implementation and Management of a centralized Cyber Protection project

It has been produced based on the information communicated to us by LIPALATER prior writing this proposal.

If any material change is made to the requirements, technical environment, scope of work or the operational approach as set out in this document Consultants reserve the right to revise this proposal accordingly.

1.1 Contact Details

Contact Details	SHELT
Address:	**SHELT AFRICA LTD.** **Dbayeh 66, Metn, 2501-0923, Lebanon**
Primary Contact:	**Bassam Touma**
Title:	**Business Development**
Telephone:	**+961 4 541880/1 ext. 61**
Fax:	
Mobile:	**++9613 559859**
e-mail:	**btouma@shelt.com**

Consultant is proposing to assist the customer by providing the building blocks of a Security Center (People, Process & Technology).

Consultant provides innovative, professional and reliable Security Services through its highly qualified experts. The approach of Consultant is established in order to be comprehensive, realistic and appropriate to the customer needs.

This document presents SHELT answer to LIPALATER Request for Proposal.

The document is the copyright of SHELT and is issued in confidence. It must not be used other than for the purposes of the contract to which it relates and is not to be reproduced in whole or in part without the prior written permission of SHELT.

1.2 SHELT SHAREHOLDERS/ PARTNERS

The purpose for which this Consortium between SHELT AFRICA LTD. and BCN is organized to engage in Kenya based on strategic partnership agreement signed, for its own account or to the account of third parties, in any or all activities related to Information and Communication Technology (ICT), including Information Security Services, Project Management, IT Security Consulting and other related activities by LipaLater agreement, through public or private awarding, through invitation to tender or in any other means.

Below brief on SHELT shareholders and partners

Telecel is an International Mobile Network Operator and large telecom service provider with strong foothold in Africa

Cyber Resilience is a Swiss based Cyber Battlefield that simulates networks, traffic and threats to practice real-world incident management scenarios

Telecel Global provides telecommunication services for Mobile Network Operators and has International presence in over 20+ countries and strong understanding of African business environment and technical challenges

Potech Consulting provides IT and Cybersecurity consulting services ranging from penetration tests to strategic planning

2 About SHELT

SHELT provides world class and professional IT Security services operating a recognized Security Operation Center with 24/7 facility

SHELT is a European Cybersecurity enterprise for the new digital world, with presence in Europe, Middle East and on the African Continent.

SHELT protects your business by providing a 24/7 Security Operations Center (SOC) with centralized dedicated security consultants.

SHELT teams are not only well recognized experts in the Cyber Security field but also capable to understand the business needs of our clients and provide adequate solutions and advisory services, aligning Business Strategy with Cyber Security strategy. Today's IT projects bring about more than just functional challenges. Issues such as security, scalability, redundancy, information architecture and speed of performance are just a few of the criteria that must be evaluated in the early stages of planning an information technology project. Our experienced team of consultants can handle projects large and small, from needs assessment through to implementation

Our mission is to provide services aiming to assess and help our customers operations to rapidly adapt and respond to internal or external dynamic changes, demands, disruptions or threats - and continue operations with limited impact to the business.

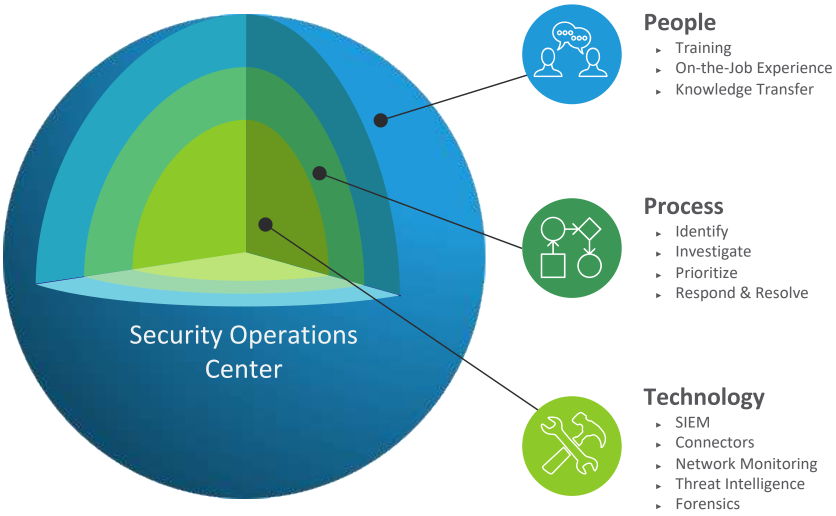
As a vendor independent firm, SHELT provides impartial security advice in line with the business requirements and solutions with measurable returns.

SHELT and SHELT Consulting undertakes projects in, Africa the Middle East and Europe and below a snapshot of similar references

Bank Audi
بنك بيروت Bank of Beirut Banking Beyond Borders
alfa
BANQUE LIBANO-FRANÇAISE A partner for your ambitions
ZADEA
BLOM BANK FRANCE
FRANSABANK
BC
SARADARBANK
LIBANK LEVANT INVESTMENT BANK SAL
الاعتماد اللبناني CREDIT LIBANAIS
بنك مصر لبنان BML
Federal Bank of Lebanon Redefining the art of banking
BLC bank FRANSABANK GROUP
HOLDAL
HSTCo
MTN
MIDCLEAR S.A.L.
EMIRATES LEBANON BANK بنك الإمارات ولبنان
MUCODEC
USJ Université Saint-Joseph de Beyrouth
الجامعة اللبنانية UNIVERSITE LIBANAISE
UNODC United Nations Office on Drugs and Crime
HDF
IDM the internet people

3 SOC as a service Summary of Work

3.1 SOC Building Blocks



People

- Training
- On-the-Job Experience
- Knowledge Transfer

Process

- Identify
- Investigate
- Prioritize
- Respond & Resolve

Technology

- SIEM
- Connectors
- Network Monitoring
- Threat Intelligence
- Forensics

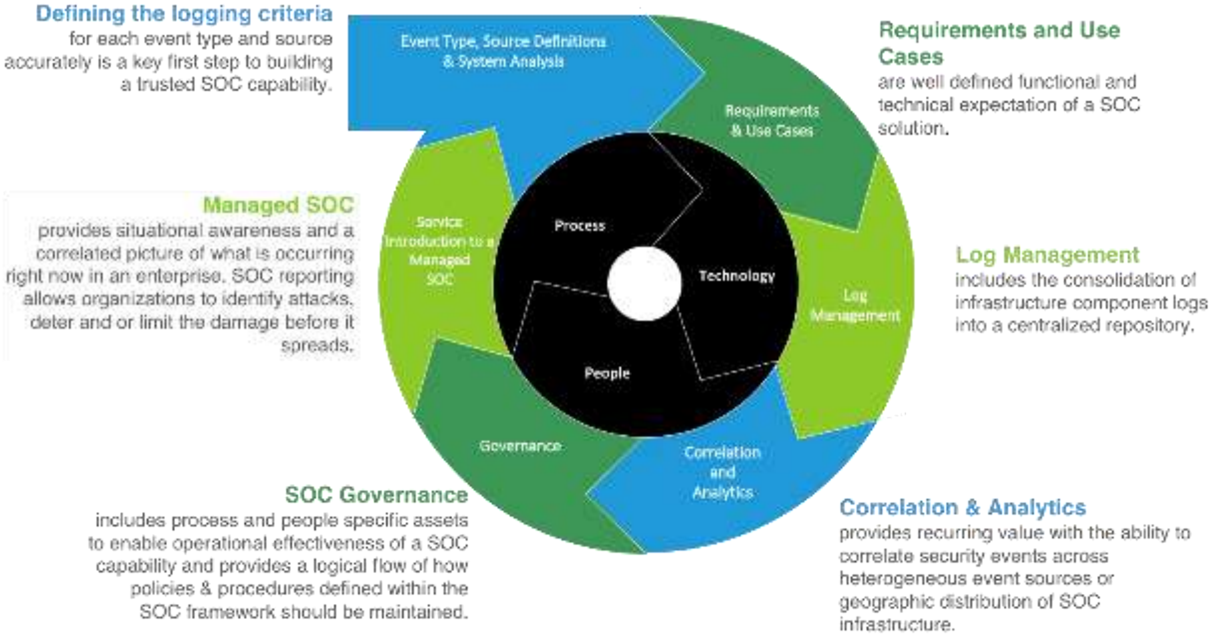
> “With the right **Security Operations Center** in place, you can see when an attack happens, and you’re given an opportunity to react to it”

3.2 Objective

Having a specialized team responsible of detecting and responding to information security incidents in order to:

- Detect and alert of possible attacks
- Mitigate and prevent major incidents and help protect its valuable assets
- Have a centralized and proactive handling of any response to security related incidents
- Have the expertise at hand to support and provide guidance to the customer through analysis and recommendations

3.3 SOC Lifecycle


Event Type, Source Definitions & System Analysis
Requirements & Use Cases
Log Management
Correlation and Analytics
Governance
Service Introduction to a Managed SOC
Process
Technology
People

Defining the logging criteria for each event type and source accurately is a key first step to building a trusted SOC capability.

Requirements and Use Cases are well defined functional and technical expectation of a SOC solution.

Managed SOC provides situational awareness and a correlated picture of what is occurring right now in an enterprise. SOC reporting allows organizations to identify attacks, deter and or limit the damage before it spreads.

Log Management includes the consolidation of infrastructure component logs into a centralized repository.

SOC Governance includes process and people specific assets to enable operational effectiveness of a SOC capability and provides a logical flow of how policies & procedures defined within the SOC framework should be maintained.

Correlation & Analytics provides recurring value with the ability to correlate security events across heterogeneous event sources or geographic distribution of SOC infrastructure.

3.4 Perimeter

- This service will cover devices up to specific Event Per Second for the customer’s Head Office and branches, including but not limited to the components below:
    - Active directory, DMZ servers, Windows and Linux servers
    - Core switch, Web Application Firewall, IPS, Firewall, Web Gateway, Proxy, Email Cloud Security
    - Endpoint Security, DAM, DLP, Network Tap, Vulnerability Management, Patch Management, Network Access Control, Multi-factor authentication
    - Etc.
- The appliances will be installed in the customers premises.

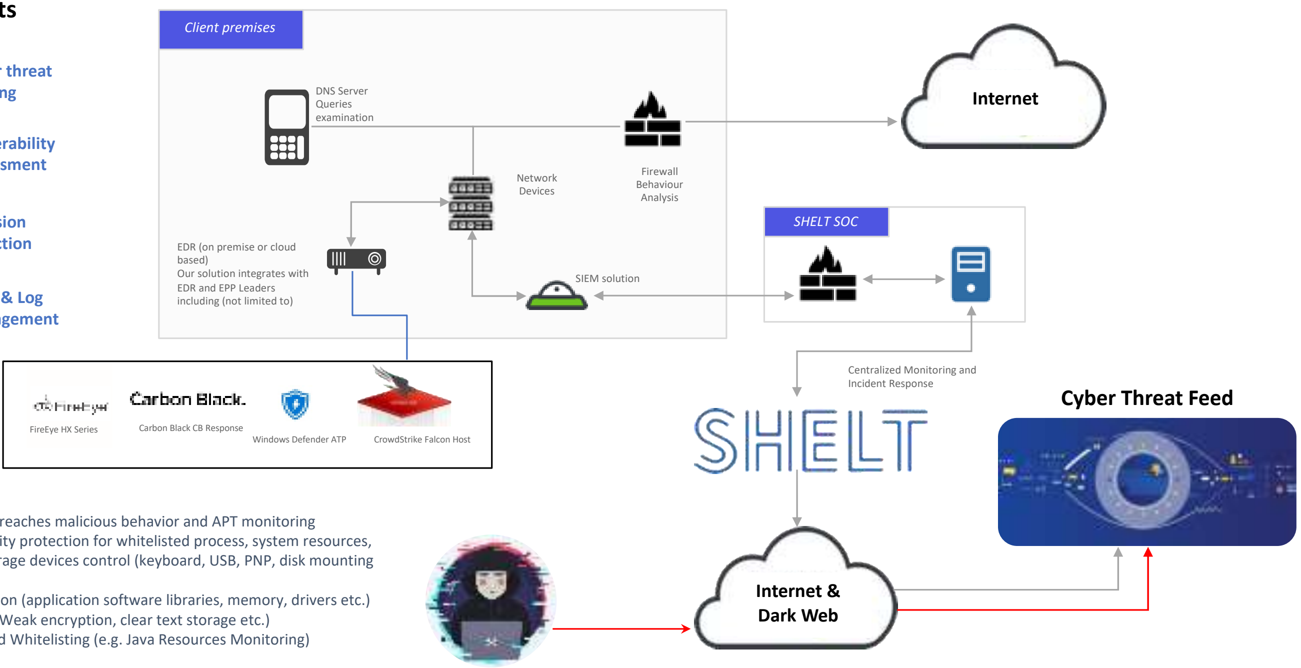
3.5 Solution capabilities

Our Methodology & Approach for Central Security Management

Breakdown of our Security Platform

Benefits

- Cyber threat hunting
- Vulnerability Assessment
- Intrusion Detection
- SIEM & Log Management

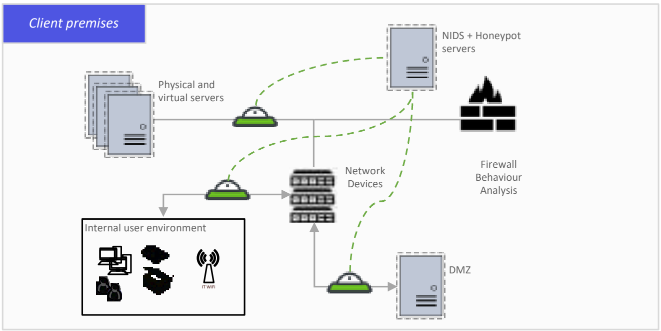

Client premises
DNS Server Queries examination
Network Devices
Firewall Behaviour Analysis
EDR (on premise or cloud based)
Our solution integrates with EDR and EPP Leaders including (not limited to)
SIEM solution
Internet
SHELT SOC
Centralized Monitoring and Incident Response
SHELT
Cyber Threat Feed
Internet & Dark Web
FireEye
FireEye HX Series
Carbon Black.
Carbon Black CB Response
Windows Defender ATP
CrowdStrike Falcon Host

EPP and EDR:

- Malware, attempted breaches malicious behavior and APT monitoring
- File and process Integrity protection for whitelisted process, system resources,
- External pluggable storage devices control (keyboard, USB, PNP, disk mounting etc.)
- Resources use protection (application software libraries, memory, drivers etc.)
- DLP (Data exfiltration, Weak encryption, clear text storage etc.)
- Application Control and Whitelisting (e.g. Java Resources Monitoring)

Our Methodology & Approach for Central Security Management

SOC services – NIDS and Honeypot servers


Client premises
NIDS + Honeypot servers
Physical and virtual servers
Network Devices
Firewall Behaviour Analysis
Internal user environment
DMZ

Network Intrusion Detection System

- An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations
- The NIDS will be implemented in order to monitor different internal network segments such as:
  - ❖ Internal user traffic
  - ❖ Internal and external server farm traffic
  - ❖ DMZ monitoring
- The NIDS will be integrated with the installed SIEM in order to correlate and show internal and external abnormal traffic and threats

Honeypot service

- Honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems
- The honeypot service will help the client in the creation of an active internal honeypot environment that will be capable of detecting and misleading malicious attempts
- Several honeypots will be implemented in order to detect attacks both on the perimeter (DMZ) and the internal network. Multiple services will be covered such as:
  - ❖ HTTPS
  - ❖ SMB/Samba
  - ❖ SSH access
  - ❖ Etc.
- All logs will be sent to the installed SIEM and related alarms and reports will be generated

The SIEM solution includes the capabilities below:

- Built-in network intrusion detection system (NIDS), limited to 2000 Mbps, covering the customer Head Quarters
- Availability monitoring of all defined assets
- Vulnerability assessment tool
- Full access to alarms, logs, reports and OTX from the customer
- Ticketing system

3.6 Scope of work

The **Central Cyber Security Platinum Package** includes the below:

- 24h/7d monitoring and alerting
- Weekly compliance reports
- Alarm notification and escalation
- Incident response and assistance
- 10h per month regular assistance
- Continuous fine-tuning
- Monthly vulnerability assessments
- 2 days for social engineering per year
- **Cyber threat intelligence** on both the internet and dark web in order to detect, analyze and identify:
    - Possible email or accounts compromise
    - Social media fake profiles and websites related to the client
    - Key threat actors (internal and/or external)
    - Organizational assets (main data assets, information system inventory, third party applications, etc.)
    - Leaked financial data (Cardholder names, IBAN, etc.)
    - High-level members private data exposure (board members data such as private emails, social media, etc.)
- **Honeypot service** that will help the client in the creation of an active internal honeypot environment that will be capable of detecting and misleading malicious attempts.
- **End Point Detection and Response** which will include
    - Malware, attempted breaches malicious behavior and APT monitoring
    - File and process Integrity protection for whitelisted process, system resources,
    - External pluggable storage devices control (keyboard, USB, PNP, disk mounting etc.)
    - Resources use protection (application software libraries, memory, drivers etc.)
    - DLP (Data exfiltration, Weak encryption, clear text storage etc.)
    - Application Control and Whitelisting (e.g. Java Resources Monitoring)

3.7 Information provided by the customer

In order to deploy the solution, the customer will be asked to provide:

- The list of components to be added to the solution (Windows servers, production and test environment, switches, routers, security components, etc.) with their related Operating systems and versions
- Critical cyber threat information to be monitored, including but not limited to:
    - The customer's domain
    - Board members information (private and corporate emails)
    - Third-party platforms
    - Key threat actors provisioning (internal and/or external)
    - Organizational assets (main data assets, information system inventory, third party applications, etc.)
    - Financial related data (Credit Card numbers, BIN numbers, etc.)
    - High-level members private data (board members data such as private emails, social media, etc.)
    - Others

3.8 Technical requirements

Consultants will be installing the virtual machines requiring the below specifications:

3.8.1 USM Server:

- 24GB Ram
- 8 cores
- 1.2T storage (this may be subject to change depending on the number of logs collected)

3.8.2 USM Logger:

- 24GB Ram
- 4 cores
- 1.8/2.2T storage (this may be subject to change depending on the number of logs collected)

3.8.3 2x USM Sensor:

- 24GB Ram
- 4 cores
- 1.2T storage (this may be subject to change depending on the number of logs collected)

In order to monitor and fine tune the environment logs, the customer will be asked to provide HTTPS access to a specific IP address.

N.B.: SSH access might be required for a limited period of time in order to enhance, customize and fine tune the environment (e.g. troubleshooting logs problems, creating customized parsers, etc.).

3.9 Approach

Consultant will proceed as follows:

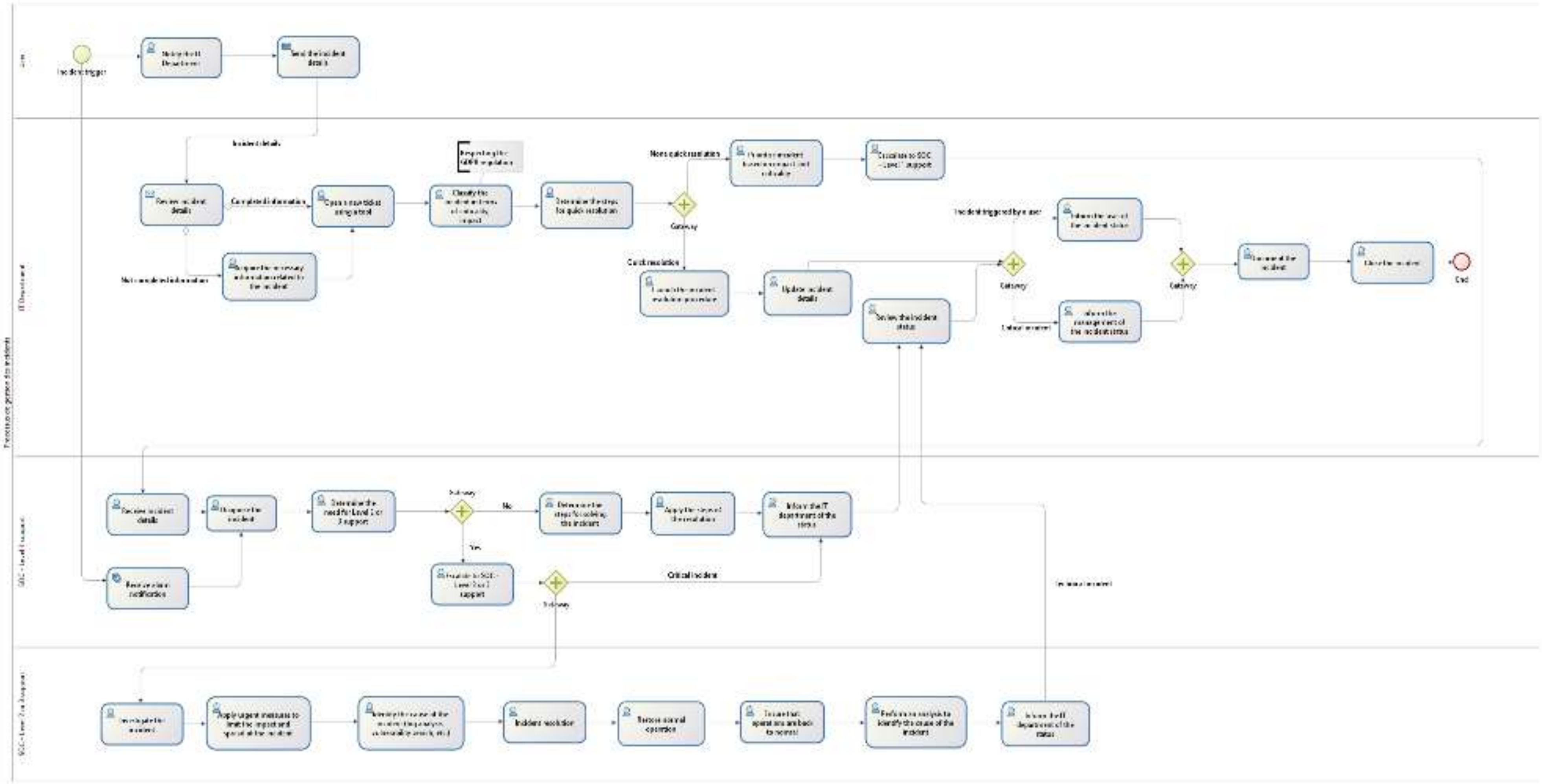
- **GAP assessment:** Determine, assess and perform GAP analysis of current capabilities
  - Identify the different components existing in the network with their related criticality and business needs.
  - Identify the critical data to be monitored on the internet
  - Identify the network security components with their current configuration and identify any fine-tuning opportunities within the Enterprise infrastructure.
- **Define and prioritize** infrastructure components (network, OS, legacy applications, databases, etc.)
  - Define the different enterprise components to be added to the logging solution based on the GAP assessment results.
  - Prioritize the different enterprise components by waves in order for them to be integrated first.
- **Deployment and collection**
  - Solution deployment and configuration on premises
  - Configuration of all connectors and log sources
- **Use cases development and log tuning** for critical business application and Windows environment
- **Definition of search parameters on the dark web**
- Implementation of **honeypot** service
- Ensure **daily and weekly reporting**
- Review and update **change and incident management procedures** in order to meet SOC practices
- Define and finalize the **escalation matrix**

3.10 Deliverables

The deliverable of this work package consists of:

- Email notification for a malware outbreak or a cyber security threat that the customer should be aware of
- Monthly cyber threat intelligence reports
- Daily monitoring and weekly compliance reports
- Incident reports

3.11Summary of an Incident Management Process


IT Department
Incident trigger
Notify the IT Department
Send the incident details
Incident details
Review incident details
Completed information
Open a new ticket using a tool
Not complete information
Request the necessary information related to the incident
Respecting the GDPR regulation
Classify the incident in terms of criticality impact
Determine the steps for quick resolution
Gateway
Non quick resolution
Quick resolution
Escalate to SOC - Level 1 support
Update incident details
Review the incident status
Incident triggered by a user
Critical incident
Gateway
Document the incident
Close the incident
End
Review incident details
Diagnose the incident
Determine the need for Level 2 or 3 support
Gateway
No
Yes
Determine the steps for solving the incident
Apply the steps of the resolution
Inform the IT department of the status
Receive alarm notification
Escalate to SOC - Level 2 or 3 support
Critical incident
Gateway
Investigate the incident
Apply urgent measures to limit the impact and spread of the incident
Incident resolution
Restore normal operation
Perform an analysis to identify the cause of the incident
Inform the IT department of the status

3.12 Team profile summary

The section below presents a brief overview of the different involved entities in this project (Tier 2 – Tier 3). Tier 1 engineers are not reflected herein

EZ – Manager, Head of cyber intelligence unit (Tier 3)

Over 8 years of experience in information system security consultancy and evaluation; strong technical expertise in penetration testing, source code review and digital forensics.

RF – Manager, Head of information security operations unit (Tier 3)

Over 8 years of experience in information system security consultancy and evaluation; strong technical expertise in penetration testing and systems hardening in addition to ISMS implementation.

JH – Manager, Head of business resiliency unit (Tier 3)

Over 7 years of experience in information system security consultancy and evaluation; strong technical expertise in business support, operational management and security consulting.

FS – Senior information security consultant (Tier 2)

Over 3 years of experience in information system security consultancy and evaluation; strong technical expertise in penetration testing and security assessments.

AK – Information security consultant (Tier 2)

Over 2 years of experience in information system security consultancy and evaluation; strong technical expertise in technical security assessments.

4 Managed SOC Detailed Approach and Methodology

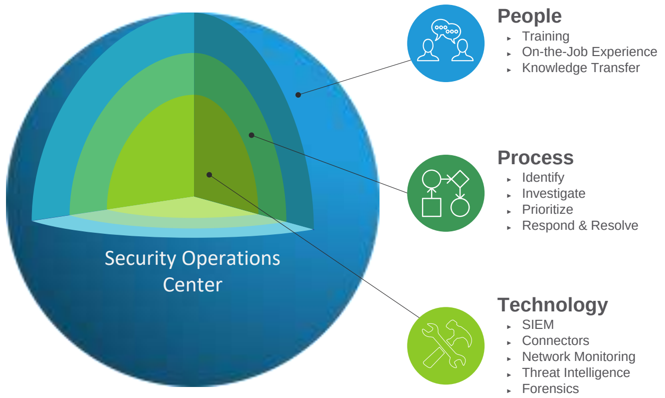
4.1 Introduction

Having a SOC is a key contributor to the organization's continuously improving its security posture. A SOC can provide significant value as long as proper planning occurs and complete processes have been created.

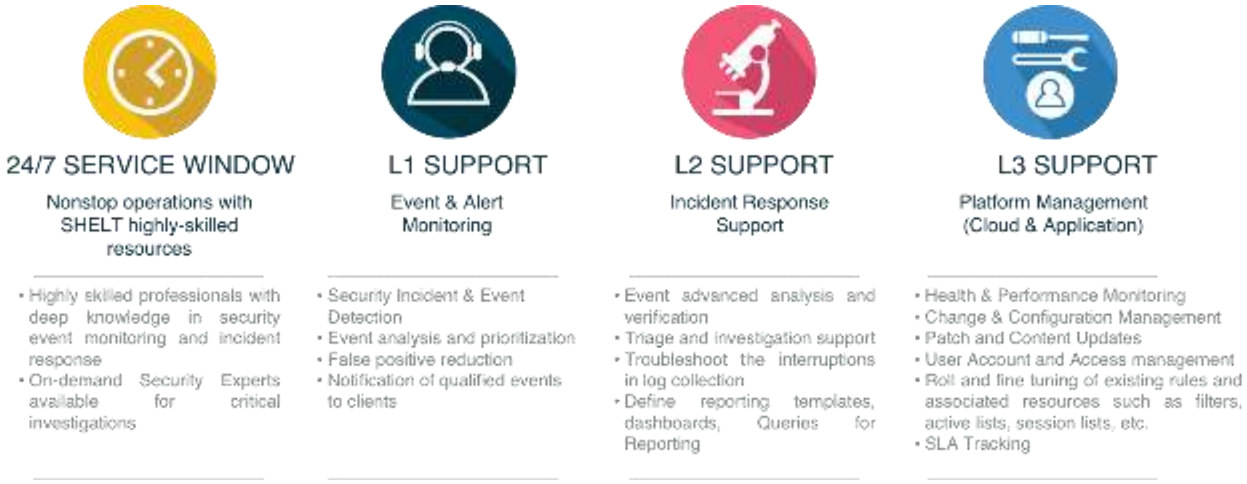
Goals of having a managed SOC is attempting to minimize and harden the attack surface and proactively detecting, prioritizing and investigating security incidents before and when they occur.

Therefore, protecting the Organization information system while adopting a proactive approach is one of the most important moves to undertake. The services provided by SHELT's team guarantee the scalability, high performance, security and accomplish better control.

Below guiding principal for the proper SOC functioning based on earlier defined



4.2 People


24/7 SERVICE WINDOW

Nonstop operations with SHELT highly-skilled resources

- Highly skilled professionals with deep knowledge in security event monitoring and incident response
- On-demand Security Experts available for critical investigations

L1 SUPPORT

Event & Alert Monitoring

- Security Incident & Event Detection
- Event analysis and prioritization
- False positive reduction
- Notification of qualified events to clients

L2 SUPPORT

Incident Response Support

- Event advanced analysis and verification
- Triage and investigation support
- Troubleshoot the interruptions in log collection
- Define reporting templates, dashboards, Queries for Reporting

L3 SUPPORT

Platform Management (Cloud & Application)

- Health & Performance Monitoring
- Change & Configuration Management
- Patch and Content Updates
- User Account and Access management
- Roll and fine tuning of existing rules and associated resources such as filters, active lists, session lists, etc.
- SLA Tracking

- SHELT supporting resources come from a pool of Security Operations Specialists who've been through numerous capability implementation, operation and transformation engagements

4.3 Process

Initial Assessment

- Determine, assess and perform GAP analysis of current capabilities
- Define and prioritize infrastructure components (network, OS, Legacy applications, databases, etc.)

Customized Tuning

- Fine tune the equipment logs
- Implement security use cases
- Fine tune reports, alerts and dashboards

Policies and Procedure Definition

- Create/Modify policies and procedures (incident management, Patch management, Change management, etc.)

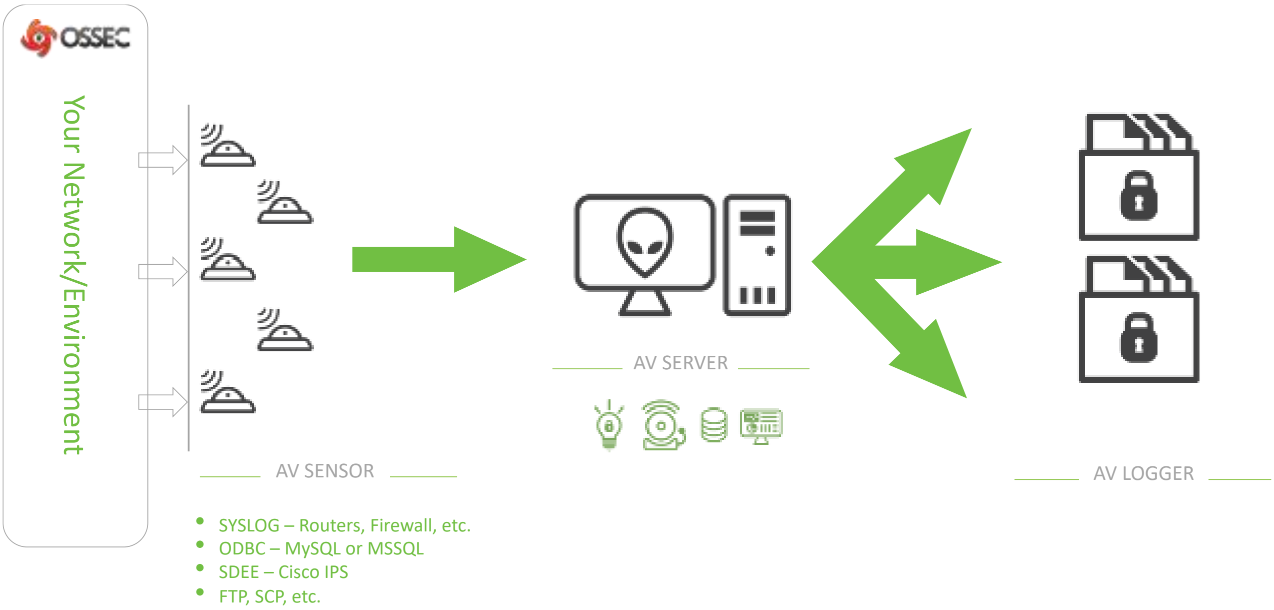
Escalation Matrix

- Define SOC roles and responsibilities
- Define SOC KPIs
- Define decision tree design

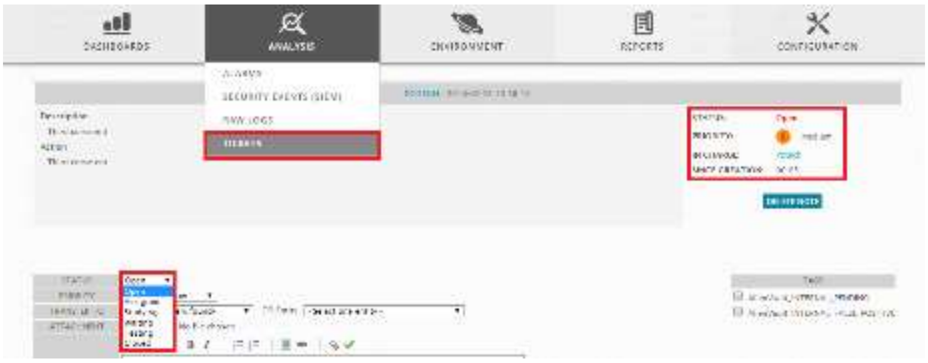
Continual Improvement

- Enhance SOC capabilities, effectiveness and efficiency of services and processes
- Introduce corrective measures where necessary

4.4 Security Events correlation: AlienVault



End-to-End Flow for Collection, Intelligence and Storage



With Ticketing solution in order to follow-up an review all incidents

Our AlienVault solution offers several benefits

Asset Discovery
Know who and what is connected to your environments at all times

Vulnerability Assessment
Know where the vulnerabilities are on your assets to avoid exploitation and compromise

Intrusion Detection
Know when suspicious activities happen in your environments

Behavioral Monitoring and OTX*
Identify suspicious behavior and potentially compromised systems using worldwide open threat exchange

SIEM & Log Management
Correlate and analyze security event data from across your environments and respond quickly

Organizations are failing at early breach detection, with more than 80% of breaches undetected by the breached organization. The situation can be improved with **threat intelligence**, **behavior profiling**, and **effective analytics**.

4.5 Advanced Cyber Threat Intelligence

We will offer in addition to our online OTX (threat exchange) and in-depth cyber threat intelligence, An Advanced Threat Intelligence platform that delivers powerful early warnings of hacking and fraud attacks via a sophisticated cyber intelligence platform. Scanning a wide range of sources (e.g., clear web, dark web, cyber-crime forums, IRC channels, social media, app stores, paste sites), it provides near-real-time alerts regarding cyber-threats. By converting security intelligence into actionable data, this platform enables our customers to detect unknown threats and minimize dangerous exposure.

Our platform provides a system for ingesting intelligence feeds and aggregating Indicators of Compromise, for our customers to monitor and investigate. In addition, all indicators are automatically integrated with security devices. Furthermore, the platform provides research and investigation tools to gain deeper insights regarding various threats.

4.5.1 Alert Discovery

The Threat Intelligence platform constantly scans a wide range of sources for threat intelligence, across the clear, deep, and dark web. It also uses existing search engines to gather additional valuable information (“piggybacking”). All this data is gathered by a proprietary browsing solution, which is able to overcome obstacles in the dark web i.e. anti-bot technologies. The data is then stored on ’s cloud database.

Subsequently, the platform analyses, categories, and priorities cyber threats in real time, using proprietary, patent-pending data mining algorithms and unique machine learning capabilities, to focus on the intelligence most relevant to each user. After ensuring relevancy and the existence of a cyber-threat, the information goes through a classification process, and then alerts the user on their dashboard.

Threat Intelligence platform delivers the following types of alerts:

Attack Indications

Hackers use websites, forums, and social media to plan and coordinate attacks. Our system detects and alerts users of these plans, which have been discovered in cyber-space, e.g., the company name on target lists, or a bid for attacking the company on hackers’ forums.

Data Leakage

Confidential data is often leaked from an organization. These leaks can occur due to hackers, who have penetrated the organization, or even frustrated or careless employees. Even the most advanced DLP can’t provide 100% certainty regarding data safety. Our system finds our customers’ leaked confidential data, and informs them, giving them the chance to protect themselves from it being used in future attacks, e.g., credentials that might be used for logging into their employees’ accounts, secret documents about company projects, information about the company’s internal network.

Brand Security

Social media has become an important arena for branding, marketing and communicating with customers. Many hackers create and manage fake accounts and applications to seduce innocent customers and steal their personal data, or even to hurt a company’s reputation. Our system detects and alerts users about imitation fake pages, profiles, applications, and even posts aimed at harming their reputation.

Phishing

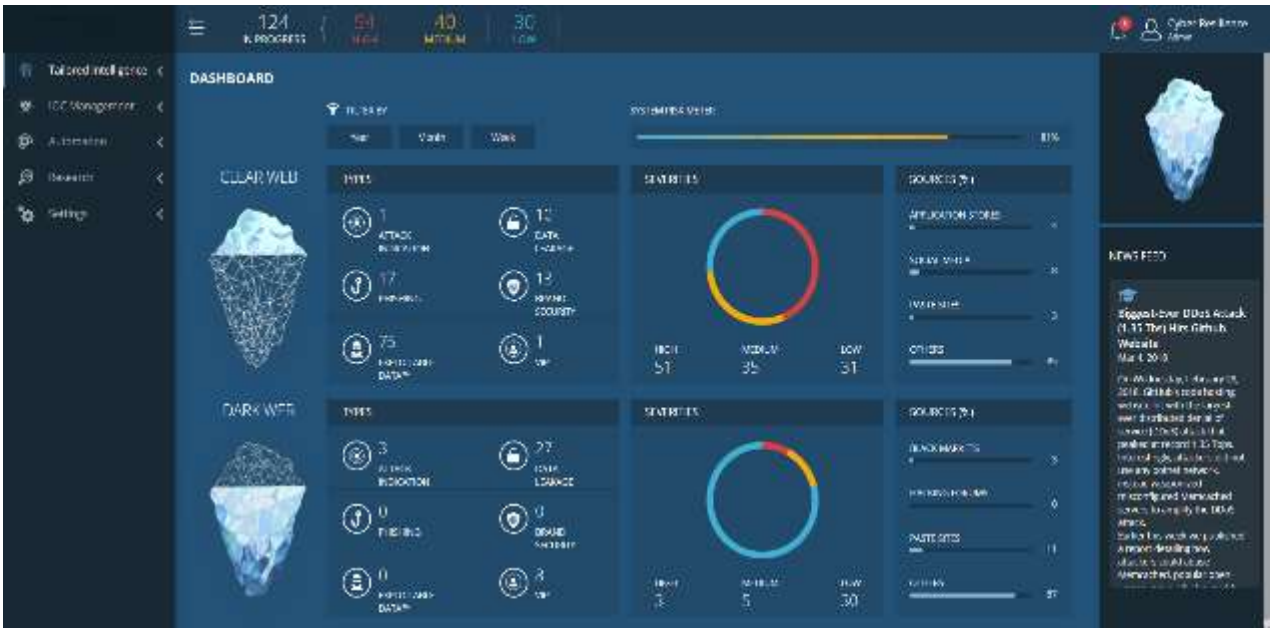
One of the most common social-engineering attacks is phishing, done by spear-phishing e-mails or phishing sites. In order to execute this kind of attack, the hacker must first open a fake domain to host the phishing site, or send the spear phishing e-mail. Our system provides early detection for potential phishing domains soon after registration, allowing users the time to prepare for, or prevent the attack.

Exploitable Data

Our unique methodology allows us to detect and report about information indexed by search engines that is exploitable by hackers. High-level hackers find this information and use it to piece together sophisticated cyber-attacks. Examples include published web vulnerabilities, information about your internal confidential network, databases, and software used — including exact version numbers.

VIP Protection

Company's VIPs are some of our customers' most important assets. Holding the most valuable experience and sensitive data about the company, their protection is a top priority. Our system detects and alerts users about potential attacks on their VIPs, secret data that has leaked from a VIP (e.g., secret documents, passwords), and fake VIP profiles on social media and other websites.



Threat Intelligence Dashboard – Different types of alerts

4.5.2 Remediation

Threat Intelligence platform provides "Remediation" services for most alerts. With a click of a button, we initiate an automated take-down process for removal of malicious content on the web. Remediation is offered for malicious web pages, social media profiles, fake applications and malicious domains.

4.5.3 Advanced Threat Intelligence Platform

The Advanced Threat Intelligence platform is aware of the need to ingest multiple intelligence sources, correlate them and act upon them, in order to mitigate the threats quickly and efficiently. Thus, it provides a Threat Intelligence Platform in order to meet these needs. It offers the following features:

Ingests and aggregates multiple intelligence sources - Threat Intelligence platform allows users to dynamically configure integration with multiple intelligence sources. It digests each intelligence feed, extracts indicators and aggregates the indicators from the sources. The system supports multiple formats, e.g., STIX, PRF reports, IOCs lists, etc.

Integration with security devices - For mitigation and monitoring purposes, our platform allows users to integrate intelligence data with security devices, e.g. firewall, SIEM, etc. The process can be dynamically pre-configured, and thus occur automatically. The automation cuts the time from detection to remediation drastically.

Intelligence sharing - The Threat Intelligence platform also performs as an intelligence sharing platform. It provides the infrastructure for sharing intelligence among different organizations, allowing the customers to be aware of threats targeting their sector or country, and to stay ahead of upcoming threats.

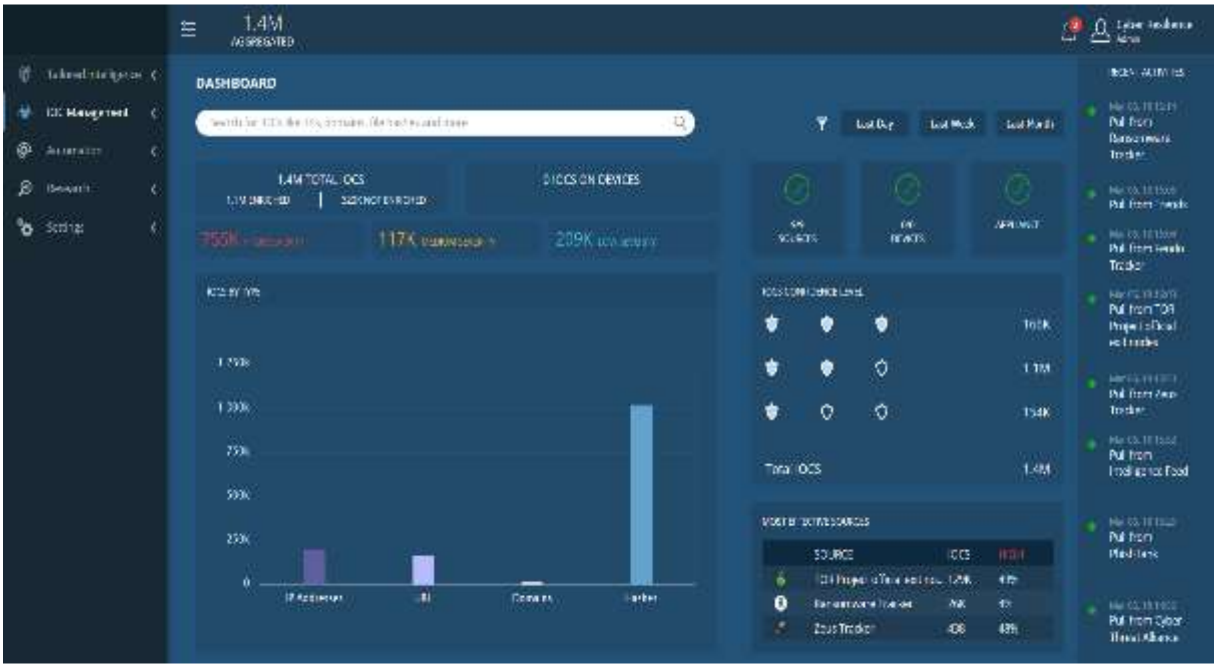


Figure 2. IOC

4.5.4 Research & Investigation

Threat Intelligence platform provides the tools to perform research and investigation, in order to gain deeper insights regarding threats. This incorporates drill down to emerging threats around the world, and investigation of indicators and incidents related to the specific organization. This includes the following features:

Trends

This section presents the latest trends in the cyber world, including the option to investigate each specific threat. This section is split into three sections: Threat actor, malware and campaigns, and is presented according to the level of interest created on social networks and forums.

Threat database

Threat Intelligence platform provides its users with the option to search for indicators and observables, to easily monitor and handle threats and data related to such threats, such as TTP and threat actors.

Search the Dark Web

Threat Intelligence platform scrapes hundreds of sources from the Deep & Dark Web, allowing its users to search for relevant data in order to gain a more comprehensive image regarding cyber threats.

Link Analysis

Threat Intelligence platform collects and aggregates data from various of sources. All the data is uploaded to its link analysis platform for investigation and research around customer-related indicators.

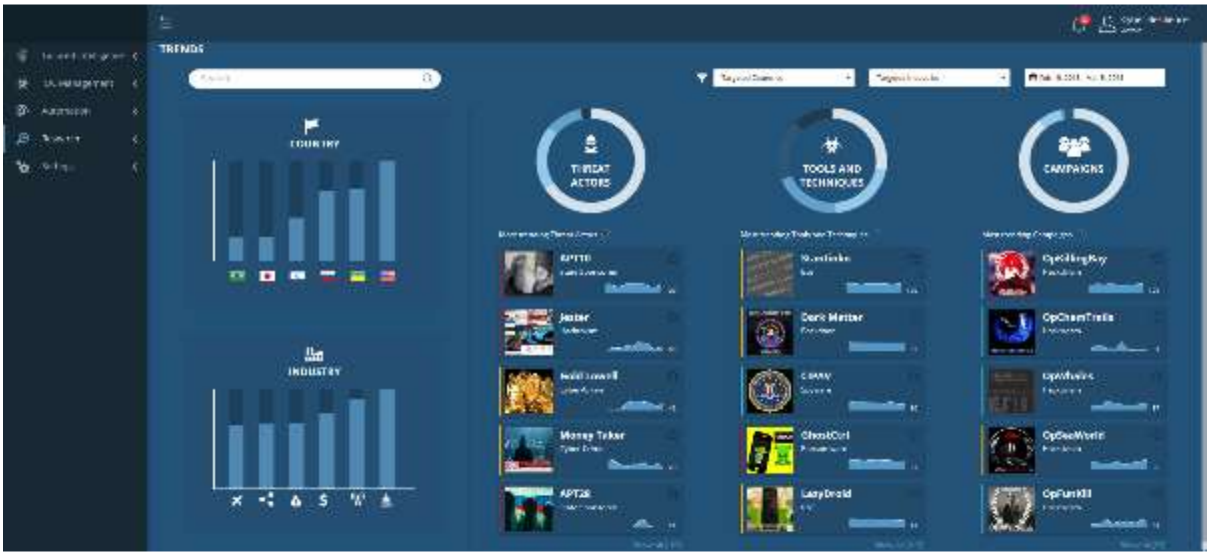
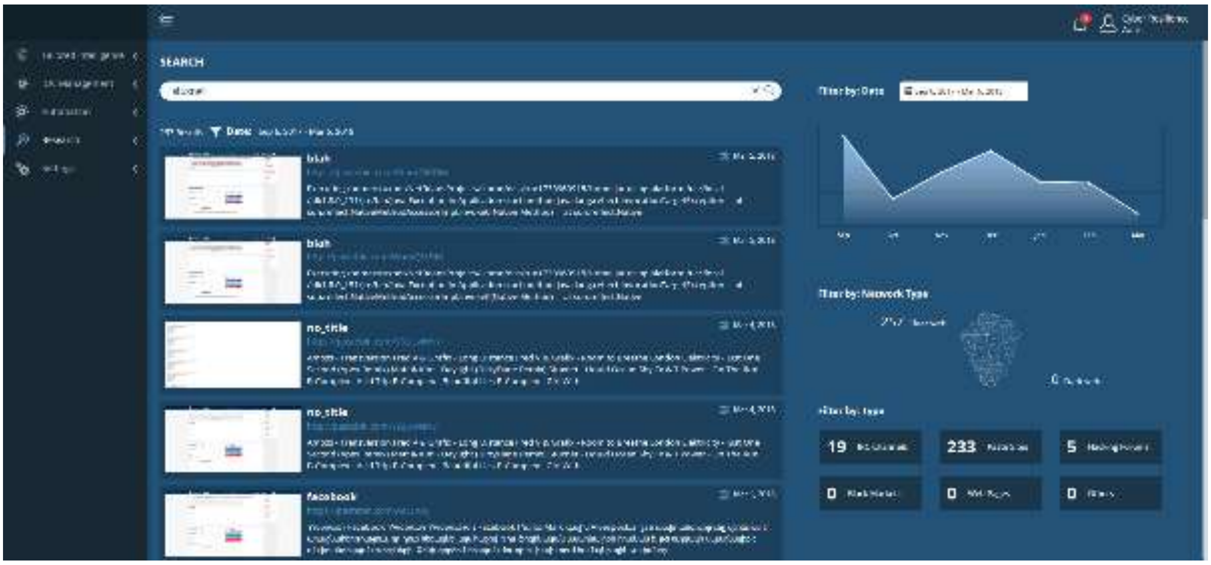


Figure 3. Search

Figure 4. Trends


SEARCH
Filter by: Date
blah
blah
no_title
no_title
facebook
Filter by: Network Type
Filter by: type
19
233
5
0
0
0

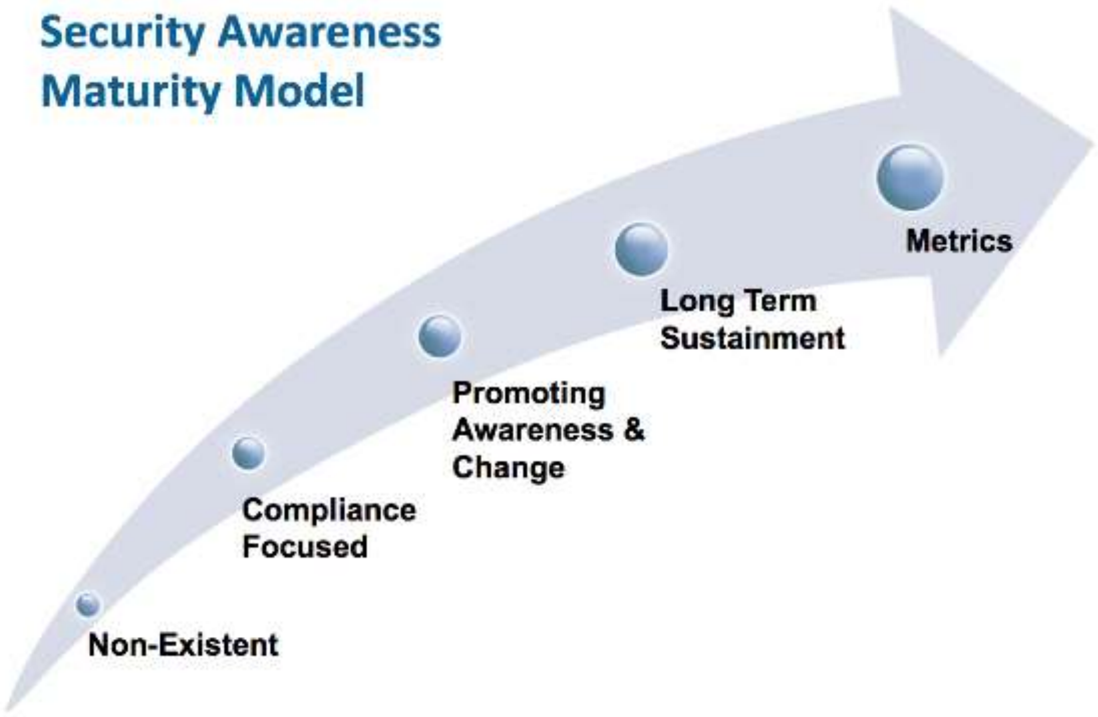
5 Information security awareness program development

5.1 Overview

One of the greatest threats to information security could actually come from within the organization. Inside attacks have been noted to be some of the most dangerous since these people are already quite familiar with the infrastructure. It is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee.

The focus will be on uninformed users who can do harm to the network by visiting websites infected with malware, responding to phishing e-mails, storing their login information in unsecured locations, or even giving out sensitive information over the phone when exposed to social engineering.

Thus, one of the best ways to make sure company employees will not make costly errors in regard to information security is to institute company-wide security-awareness training initiatives that include, but are not limited to training sessions, helpful hints via e-mail, or posters. These methods can help ensure employees have a solid understanding of the company's security policies, procedures and best practices.



5.2 Objective

To implement an active, engaging security awareness program that will empower personnel with the ability to recognize security threats and provide them the necessary knowledge to take appropriate actions to ensure that LIPALATER's confidential information remains protected.

5.3 Perimeter

The information security awareness program will cover all LIPALATER's staff.

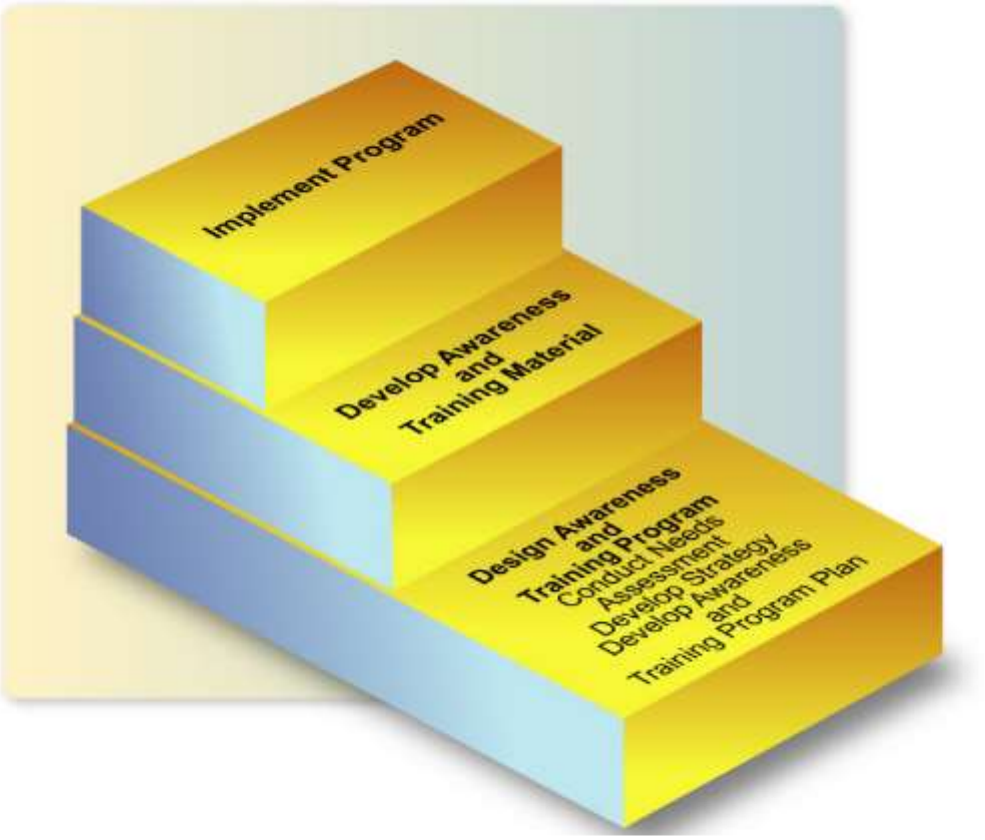
5.4 Frequency

The information security awareness program will be distributed as follows:

- One information security awareness session
- Monthly information security awareness emails
- Monthly information security awareness posters

5.5 Approach

In order to execute this task, SHELT Consulting will proceed with the following steps:


Implement Program
Develop Awareness and Training Material
Design Awareness and Training Program
Conduct Needs Assessment
Develop Strategy
Develop Awareness and Training Program Plan

5.5.1 Designing an awareness and training program

Awareness and training programs must be designed with the organization mission in mind. It is important that the awareness and training program supports the business needs of the organization and be relevant to the organization's culture.

Thus, SHELT Consulting will identify the following:

- What awareness, training, and/or education are needed (i.e., what is required)
- What is currently being done to meet these needs
- What is the current status regarding how these needs are being addressed (i.e., how well are current efforts working)
- Where are the gaps between the needs and what is being done (i.e., what more needs to be done)
- Which needs are most critical

This will help identify the required security awareness and/or training efforts that need to be made. Consequently, SHELT Consulting will develop an information security awareness plan.

5.5.2 Developing awareness and training material

One generic awareness session will be scheduled at first for all the staff in order to introduce the basic concepts of information security.

This session's program will cover the following:

- Aspects and goals of information security
- Top security breaches of 2017-2018
- Social engineering techniques
    - Information gathering
    - Human based attacks
    - Computer based attacks
- Counter measures
    - Social network security
    - Secure communication
    - Password security
    - Email security
    - Clear desk and clear screen
    - Mobile phones security
- Incident management

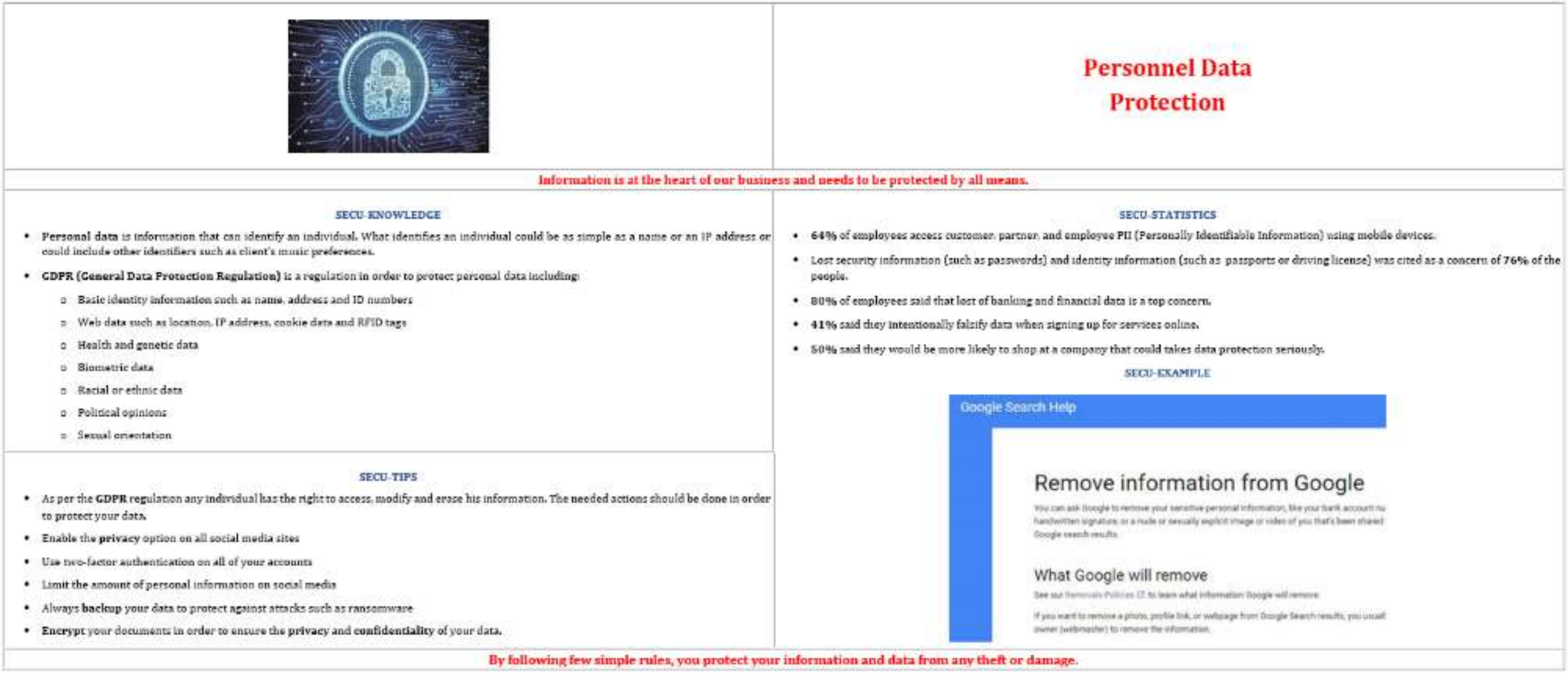
5.5.3 Implementing the awareness and training program

Many techniques exist to get an IT security awareness message, or a series of messages, disseminated throughout an organization. SHELT Consulting will implement the information security awareness program by:

- Executing generic awareness presentation for all staff
- Creating monthly information security awareness emails to the staff
- Creating monthly information security awareness posters
- Developing screensavers with information security related topics

5.5.4 Sample material

5.5.4.1 Awareness email



Personnel Data Protection

Information is at the heart of our business and needs to be protected by all means.

SECU-KNOWLEDGE

- **Personal data** is information that can identify an individual. What identifies an individual could be as simple as a name or an IP address or could include other identifiers such as client's music preferences.
- **GDPR (General Data Protection Regulation)** is a regulation in order to protect personal data including:
  - Basic identity information such as name, address and ID numbers
  - Web data such as location, IP address, cookie data and RFID tags
  - Health and genetic data
  - Biometric data
  - Racial or ethnic data
  - Political opinions
  - Sexual orientation

SECU-TIPS

- As per the **GDPR** regulation any individual has the right to access, modify and erase his information. The needed actions should be done in order to protect your data.
- Enable the **privacy** option on all social media sites
- Use two-factor authentication on all of your accounts
- Limit the amount of personal information on social media
- Always **backup** your data to protect against attacks such as ransomware
- **Encrypt** your documents in order to ensure the **privacy** and **confidentiality** of your data.

SECU-STATISTICS

- **64%** of employees access customer, partner, and employee PII (Personally Identifiable Information) using mobile devices.
- Lost security information (such as passwords) and identity information (such as passports or driving license) was cited as a concern of **76%** of the people.
- **80%** of employees said that lost of banking and financial data is a top concern.
- **41%** said they intentionally falsify data when signing up for services online.
- **50%** said they would be more likely to shop at a company that could takes data protection seriously.

SECU-EXAMPLE

Google Search Help

Remove information from Google

You can ask Google to remove your sensitive personal information, like your bank account nu handwritten signature, or a nude or sexually explicit image or video of you that's been shared Google search results.

What Google will remove

See our Removals Policies to learn what information Google will remove.

If you want to remove a photo, profile link, or webpage from Google Search results, you usuall owner (webmaster) to remove the information.

By following few simple rules, you protect your information and data from any theft or damage.

5.5.4.2 Awareness poster

IT IS ALL ABOUT YOUR DATA

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

- Never open attachments from unknown senders
- Make sure the email references the attachment

Contact the sender of an email message that contains an attachment/link

Use different complex passwords and don't save them

- Remember **HTTPS**
- Visit www.virustotal.com

Limit the amount of personal and confidential information you post

- Be wary of third-party applications (filters, emojis etc.)
- Pay attention to permission requests from applications & Update

6 Social Engineering Test

6.1 Objective

The biggest threat to information systems is sometimes the people who use them every day. Uncovering inadvertent disclosure of confidential information, such as operating system and applications' details, usernames and passwords, by employees can help avoid future system access by an external attacker.

The social engineering test, proposed by SHELT Consulting, identifies those lapses in human behavior that can jeopardize the customer's sensitive information.

6.2 Perimeter

The test will cover all the customer employees (Help Desk support, IT personnel, branches staff and other departments).

6.3 Frequency

This is a one-shot task.

6.4 Information provided by the customer

The customer will provide SHELT Consulting with the list of employees, their positions and the organizational chart.

6.5 Approach

To perform this task, SHELT Consulting is proposing to conduct the following scenarios:

- Online information gathering
- Phone calls to up to 10 individuals within the organization
- Carefully crafted phishing emails targeting the customer's employees that would attempt to coax information from the recipient

6.6 Deliverables

The deliverable of this work package consists of a report which documents all details of our activities, areas of vulnerability and recommendations for employees' awareness training and any technology solutions that might help.

6.7 Security Awareness and Online Phishing campaign

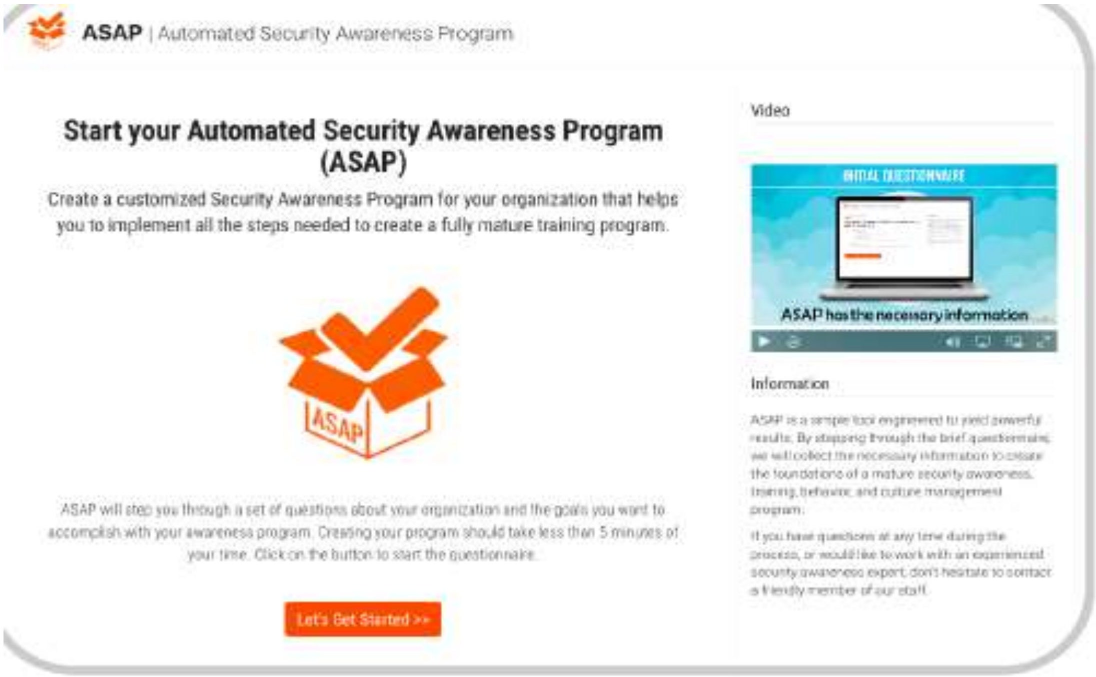
SHELT partners with KnowBe4 www.knowbe4.com , the world's largest integrated Security Awareness Training and Simulated Phishing platform with over millions of customers and more than 750 training content (the largest in the world!)

SHELT will craft a tailored security program using Knowbe4 Online platform to better manage IT security problems of social engineering, spear phishing and ransomware attacks.

Using the Online Platform SHELT Cybersecurity Experts will create crafted phishing campaigns to analyze the current standing of your phish-prone employees

6.7.1 ASAP (Automated Security Awareness Program)

ASAP is a tool which builds a customized Security Awareness Program for your organization that will show you the steps needed to create a fully mature training program.



ASAP | Automated Security Awareness Program

Start your Automated Security Awareness Program (ASAP)

Create a customized Security Awareness Program for your organization that helps you to implement all the steps needed to create a fully mature training program.

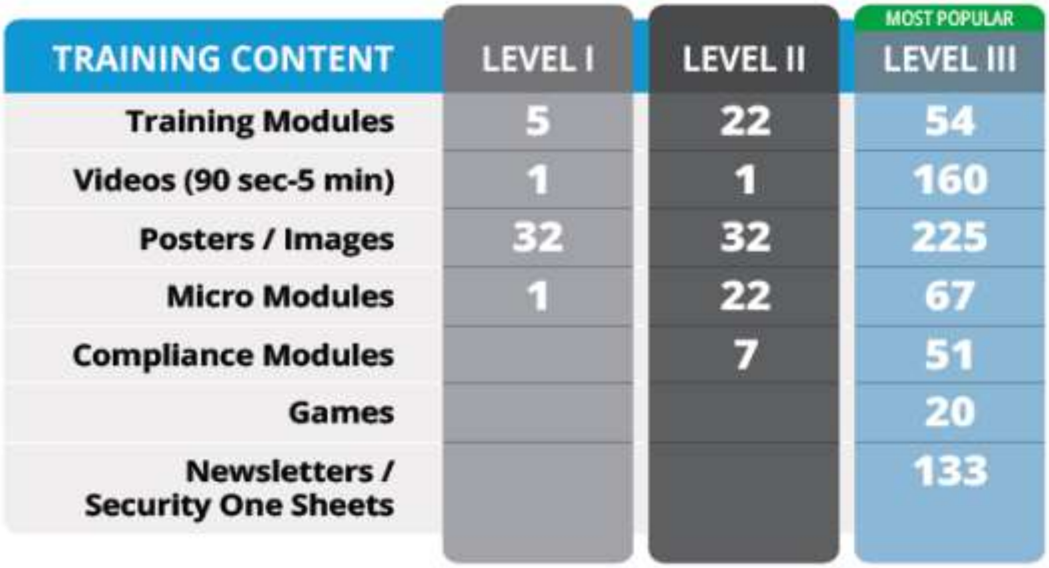
ASAP will step you through a set of questions about your organization and the goals you want to accomplish with your awareness program. Creating your program should take less than 5 minutes of your time. Click on the button to start the questionnaire.

Information

ASAP is a simple tool engineered to yield powerful results. By stepping through the brief questionnaire, we will collect the necessary information to create the foundations of a mature security awareness, training, behavior, and culture management program.

If you have questions at any time during the process, or would like to work with an experienced security awareness expert, don't hesitate to contact a friendly member of our staff.

The program is complete with actionable tasks, helpful tips, courseware suggestions and a management calendar. Your custom program can then be fully managed from within the KnowBe4 console.



TRAINING CONTENT	LEVEL I	LEVEL II	MOST POPULAR LEVEL III
Training Modules	5	22	54
Videos (90 sec-5 min)	1	1	160
Posters / Images	32	32	225
Micro Modules	1	22	67
Compliance Modules		7	51
Games			20
Newsletters / Security One Sheets			133

Three Training Levels: I, II, III depending on subscription level with a library being constantly updated

We will offer the above for all users of LIPALATER

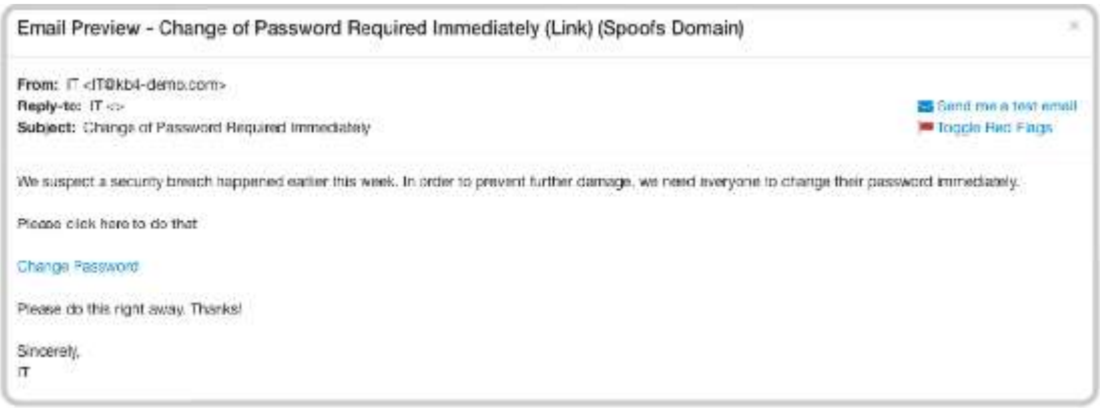
6.7.2 Phishing campaigns

SHELT will use Knowbe4 online Platform to prepare and schedule and send Simulated Phishing Security Tests (PSTs) to users during the subscription period.

Also, with our Professional Services we will create crafted spear phishing emails and customized landing pages

Knowbe4 uses a patented technology that turns every simulated phishing email into a tool to instantly train employees.

When a user clicks on any of the simulated phishing emails, they are routed to a landing page that includes a dynamic copy of that phishing email showing all the red flags.



Email Preview - Change of Password Required Immediately (Link) (Spoofs Domain)

From: IT <IT@kb4-demo.com>
Reply-to: IT <>
Subject: Change of Password Required Immediately

We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.

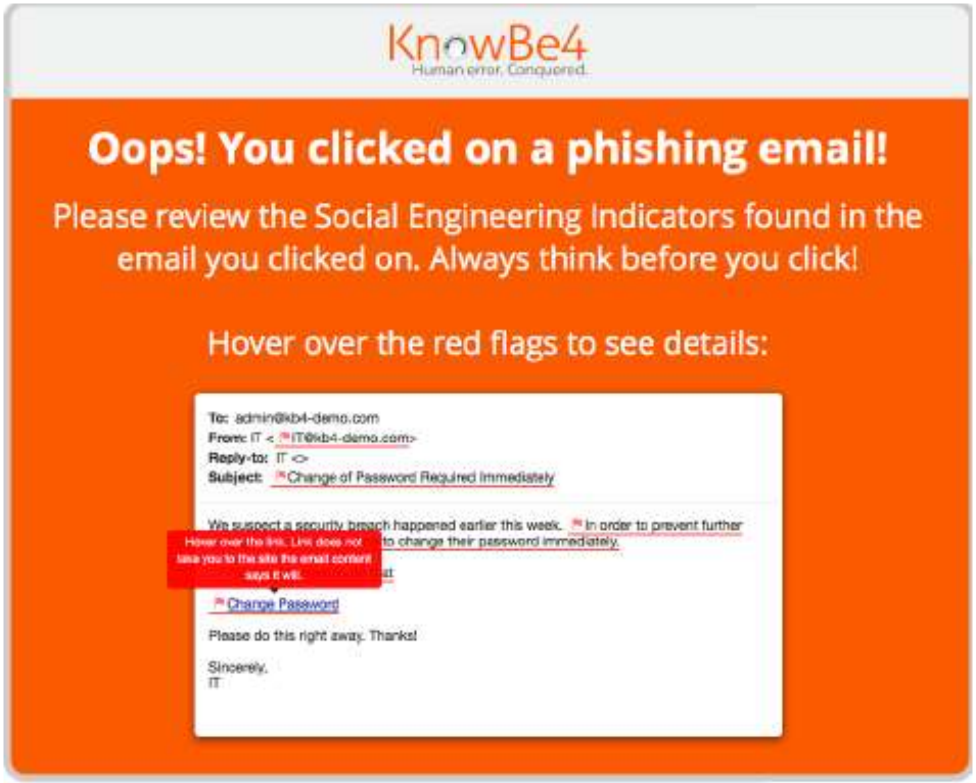
Please click here to do that

Change Password

Please do this right away. Thanks!

Sincerely,
IT

Users can then immediately see the potential pitfalls and learn to spot the indicators they missed in the future.



Oops! You clicked on a phishing email!

Please review the Social Engineering Indicators found in the email you clicked on. Always think before you click!

Hover over the red flags to see details:

To: admin@kb4-demo.com
From: IT < IT@kb4-demo.com>
Reply-to: IT <>
Subject: Change of Password Required Immediately

We suspect a security breach happened earlier this week. In order to prevent further [illegible] to change their password immediately.

Hover over the link. Link does not take you to the site the email content says it will.

st

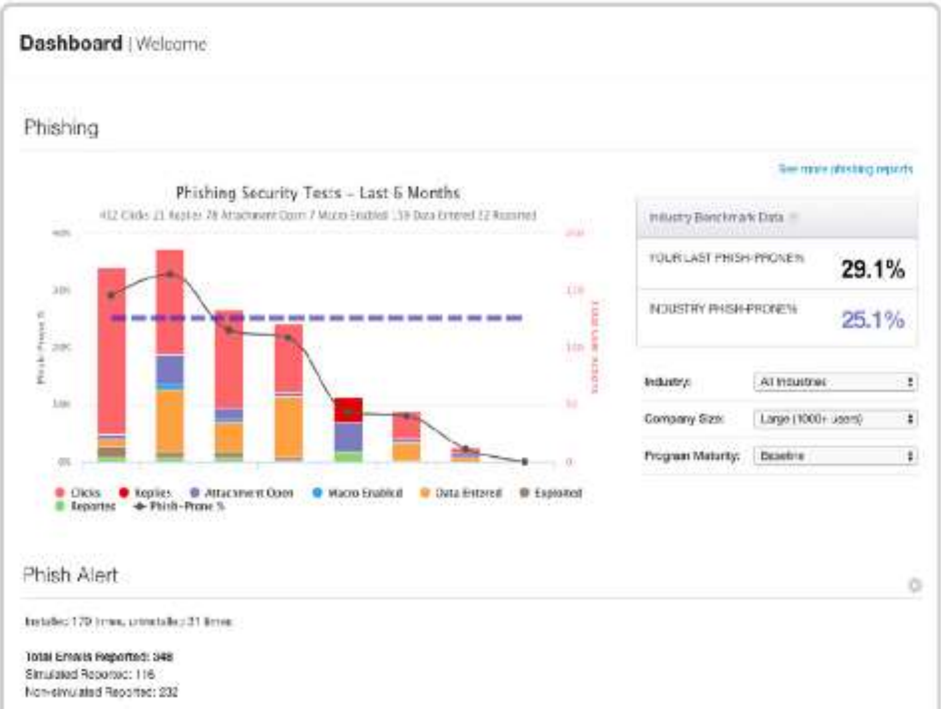
Change Password

Please do this right away. Thanks!

Sincerely,
IT

Phishing and Training Dashboard will allows to see how your end users are doing at-a-glance and in comparison to your peers across industries with Industry Benchmarking.

Sample Phishing and Training At-a-glance



Dashboard | Welcome

Phishing

See more phishing reports
Phishing Security Tests – Last 6 Months
412 Clicks 21 Replies 78 Attachment Open 7 Macro Enabled 139 Data Entered 12 Reported
40%
30%
20%
10%
0%
Phish-Prone %
200
150
100
50
0
Clicks
Replies
Attachment Open
Macro Enabled
Data Entered
Exploited
Reported
Phish-Prone %

Industry Benchmark Data

YOUR LAST PHISH-PRONE%	29.1%
INDUSTRY PHISH-PRONE%	25.1%

Industry: All Industries

Company Size: Large (1000+ users)

Program Maturity: Baseline

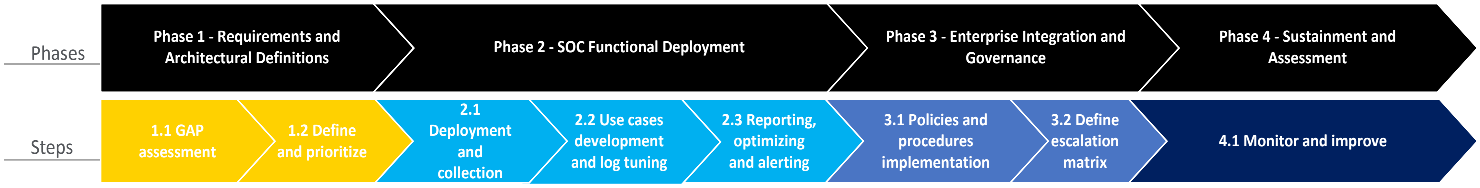
Phish Alert

Installed 179 times, uninstalled 31 times

Total Emails Reported: 348
Simulated Reported: 116
Non-simulated Reported: 232

7 High Level Methodology of Work

Our methodology is structured to enable and implement quick wins around enterprise logging, monitoring and business reporting.

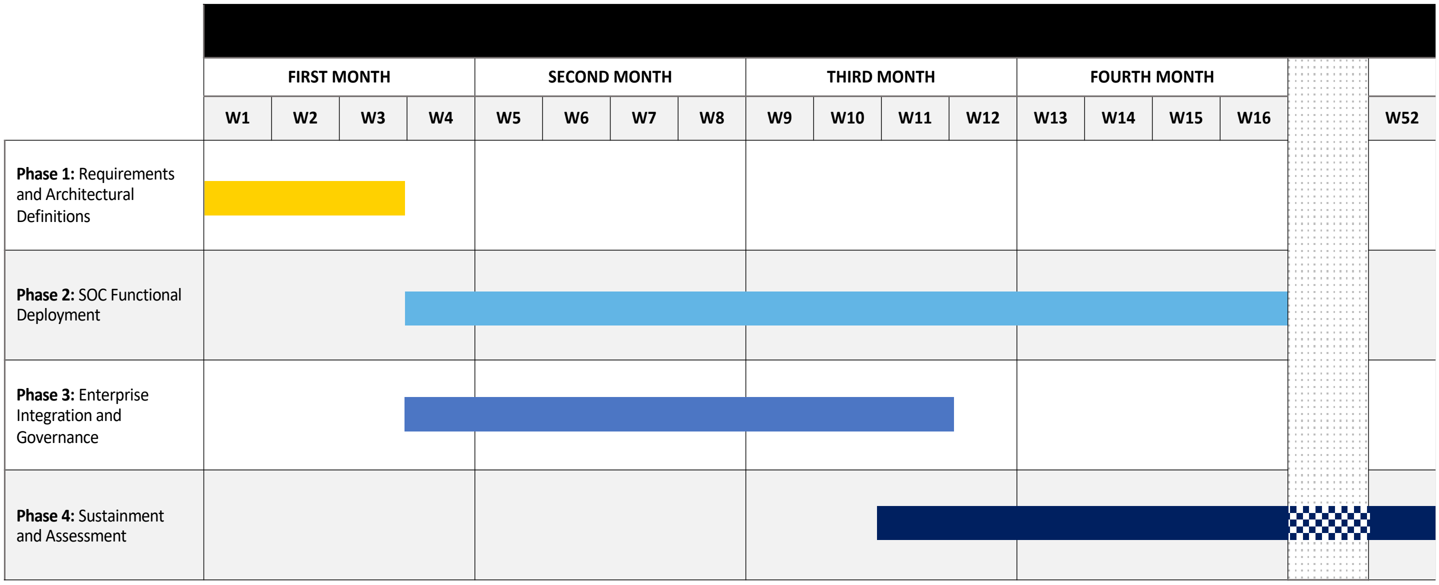

Phases
Steps
Phase 1 - Requirements and Architectural Definitions
Phase 2 - SOC Functional Deployment
Phase 3 - Enterprise Integration and Governance
Phase 4 - Sustainment and Assessment
1.1 GAP assessment
1.2 Define and prioritize
2.1 Deployment and collection
2.2 Use cases development and log tuning
2.3 Reporting, optimizing and alerting
3.1 Policies and procedures implementation
3.2 Define escalation matrix
4.1 Monitor and improve

7.1.1 Phasing & Detailed Approach

Please check our Appendix A LIPALATER SOC Detailed Approach Presentation

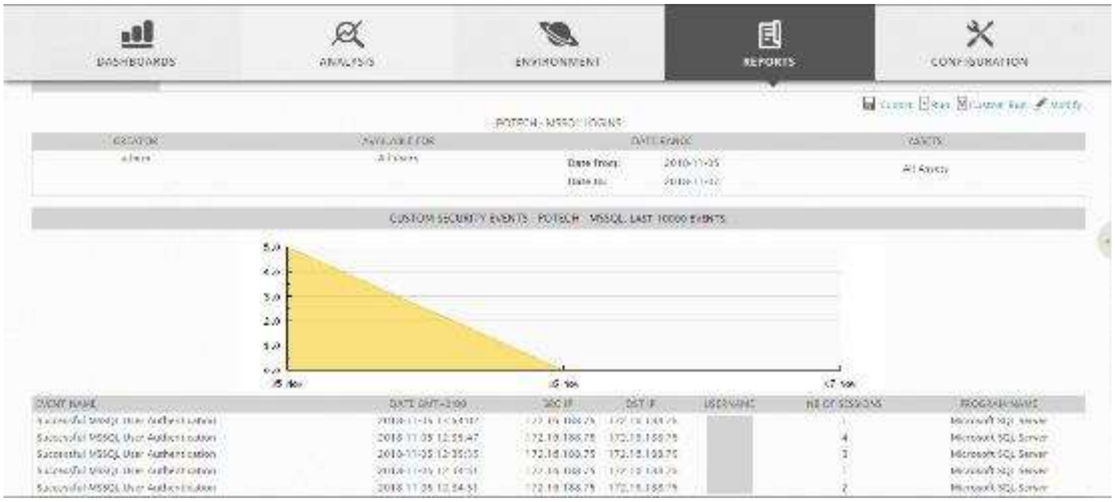
7.2 Project Timeline

Preliminary project planning foresees four months' time frame to complete all the implementation activities



7.3 SOC Reporting Samples

Reporting examples 1 – MSSQL logins



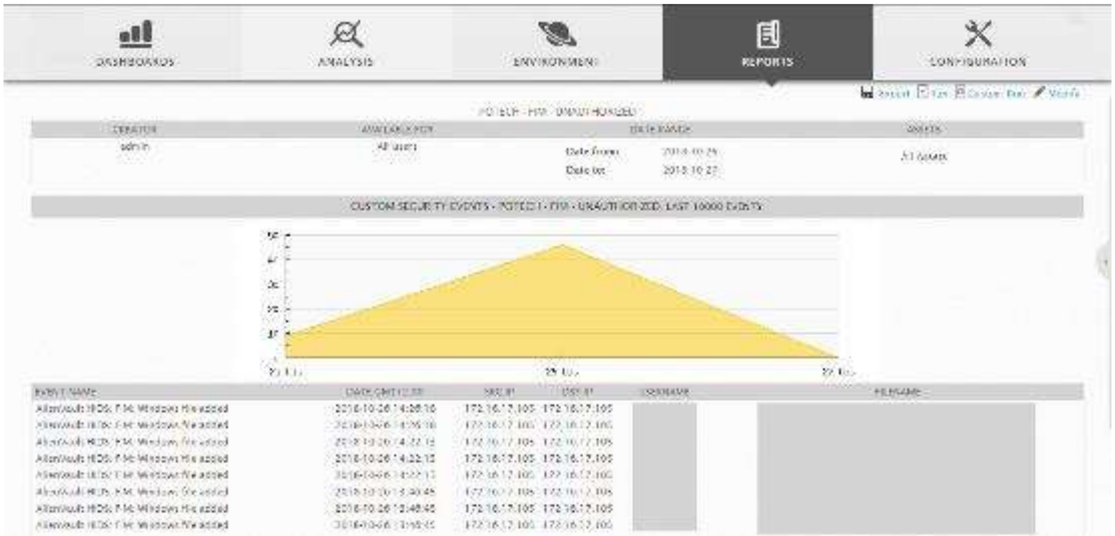
POTECH - MSSQL LOGINS

CREATOR	AVAILABLE FOR	DATE RANGE		ASSETS
admin	All users	Date from:	2018-11-05	All Assets
		Date to:	2018-11-07	

CUSTOM SECURITY EVENTS - POTECH - MSSQL: LAST 10000 EVENTS

EVENT NAME	DATE GMT+3:00	SRC IP	DST IP	USERNAME	NB OF SESSIONS	PROGRAM NAME
Successful MSSQL User Authentication	2018-11-05 12:54:17	172.18.188.75	172.18.188.75	[redacted]	1	Microsoft SQL Server
Successful MSSQL User Authentication	2018-11-05 12:55:47	172.18.188.75	172.18.188.75	[redacted]	4	Microsoft SQL Server
Successful MSSQL User Authentication	2018-11-05 12:35:35	172.18.188.75	172.18.188.75	[redacted]	3	Microsoft SQL Server
Successful MSSQL User Authentication	2018-11-05 12:19:51	172.18.188.75	172.18.188.75	[redacted]	1	Microsoft SQL Server
Successful MSSQL User Authentication	2018-11-05 12:54:51	172.18.188.75	172.18.188.75	[redacted]	2	Microsoft SQL Server

Reporting examples 2 – File integrity monitoring



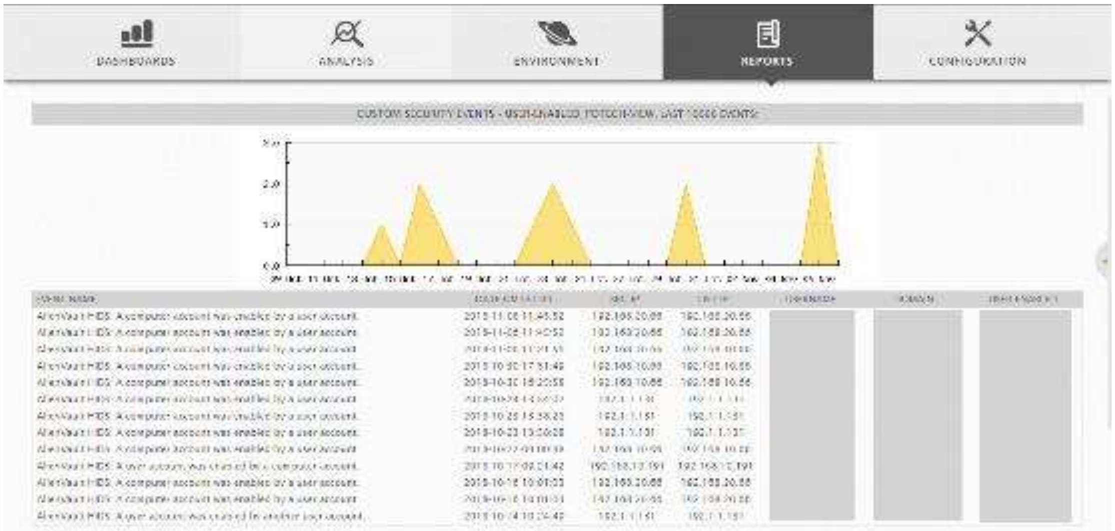
POTECH - FIM - UNAUTHORIZED

CREATOR	AVAILABLE FOR	DATE RANGE		ASSETS
admin	All users	Date from:	2018-10-25	All Assets
		Date to:	2018-10-27	

CUSTOM SECURITY EVENTS - POTECH - FIM - UNAUTHORIZED: LAST 10000 EVENTS

EVENT NAME	DATE GMT+3:00	SRC IP	DST IP	USERNAME	FILENAME
AlienVault HIDS: FIM: Windows File added	2018-10-26 14:26:10	172.16.17.105	172.16.17.105	[redacted]	[redacted]
AlienVault HIDS: FIM: Windows File added	2018-10-26 14:26:10	172.16.17.105	172.16.17.105	[redacted]	[redacted]
AlienVault HIDS: FIM: Windows File added	2018-10-26 14:22:15	172.16.17.105	172.16.17.105	[redacted]	[redacted]
AlienVault HIDS: FIM: Windows File added	2018-10-26 14:22:15	172.16.17.105	172.16.17.105	[redacted]	[redacted]
AlienVault HIDS: FIM: Windows File added	2018-10-26 14:22:15	172.16.17.105	172.16.17.105	[redacted]	[redacted]
AlienVault HIDS: FIM: Windows File added	2018-10-26 13:40:45	172.16.17.105	172.16.17.105	[redacted]	[redacted]
AlienVault HIDS: FIM: Windows File added	2018-10-26 13:40:45	172.16.17.105	172.16.17.105	[redacted]	[redacted]
AlienVault HIDS: FIM: Windows File added	2018-10-26 13:40:45	172.16.17.105	172.16.17.105	[redacted]	[redacted]

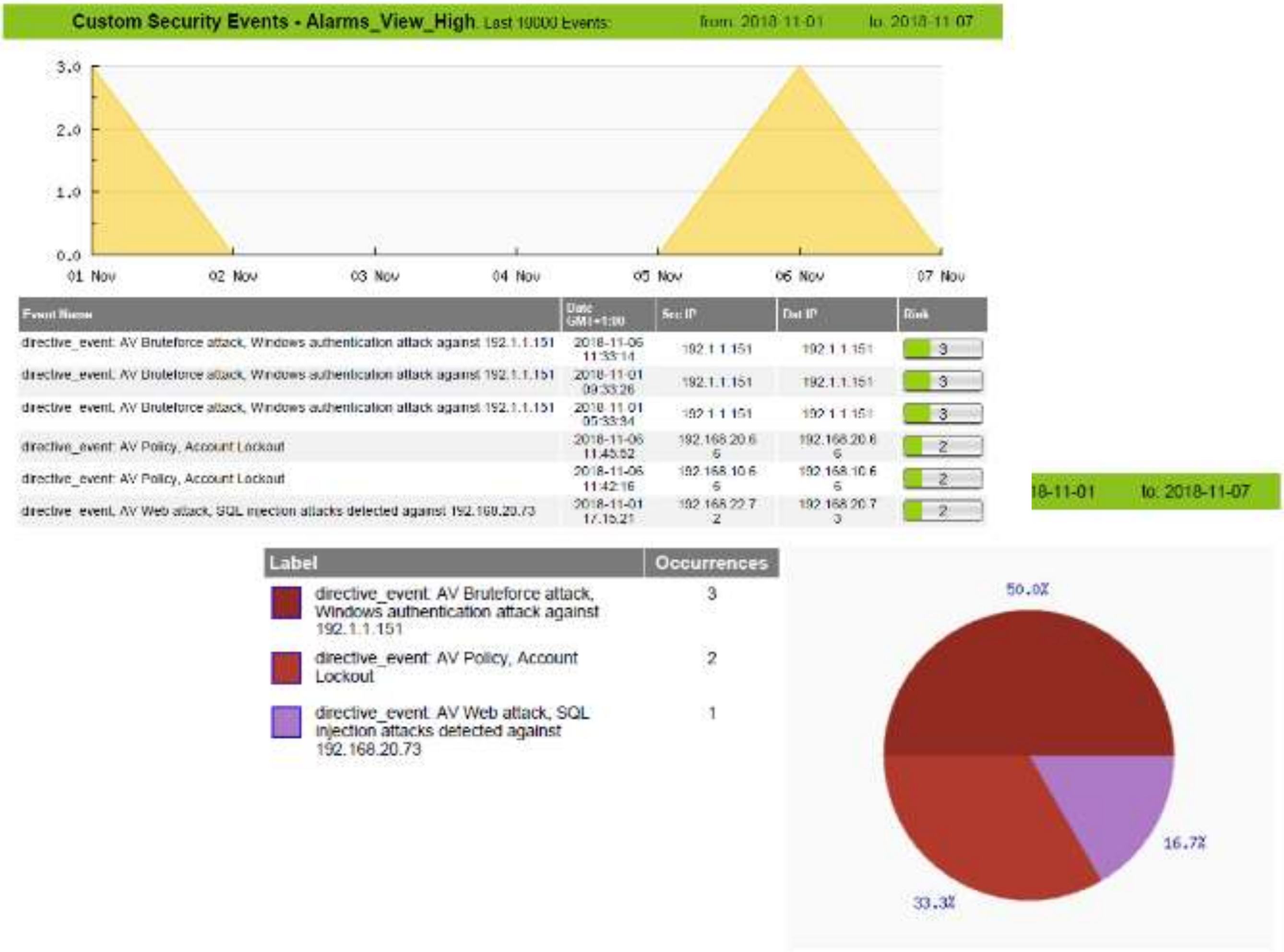
Reporting examples 3 – Enabled accounts



CUSTOM SECURITY EVENTS - USER-ENABLED_TOTOCH-VIEW. LAST 10000 EVENTS:

EVENT NAME	DATE GMT+1:00	SRC IP	DST IP	[illegible]	[illegible]	[illegible]
AlienVault HIDS: A computer account was enabled by a user account.	2018-11-06 11:45:52	192.168.20.66	192.168.20.66			
AlienVault HIDS: A computer account was enabled by a user account.	2018-11-06 11:40:52	192.168.20.66	192.168.20.66			
AlienVault HIDS: A computer account was enabled by a user account.	[illegible]	[illegible]	[illegible]			
AlienVault HIDS: A computer account was enabled by a user account.	2018-10-30 17:51:49	192.168.10.66	192.168.10.66			
AlienVault HIDS: A computer account was enabled by a user account.	2018-10-30 16:20:56	192.168.10.66	192.168.10.66			
AlienVault HIDS: A computer account was enabled by a user account.	[illegible]	192.1.1.151	[illegible]			
AlienVault HIDS: A computer account was enabled by a user account.	2018-10-26 15:38:23	192.1.1.151	192.1.1.151			
AlienVault HIDS: A computer account was enabled by a user account.	2018-10-23 13:06:08	192.1.1.151	192.1.1.151			
AlienVault HIDS: A computer account was enabled by a user account.	[illegible]	[illegible]	[illegible]			
AlienVault HIDS: A user account was changed by a computer account.	2018-10-17 09:21:42	192.168.12.191	192.168.12.191			
AlienVault HIDS: A computer account was enabled by a user account.	2018-10-16 10:01:03	192.168.20.66	192.168.20.66			
AlienVault HIDS: A computer account was enabled by a user account.	[illegible]	[illegible]	[illegible]			
AlienVault HIDS: A user account was created by another user account.	2018-10-14 10:24:42	192.1.1.151	192.1.1.151			

Reporting examples 4 – Alarms high



Custom Security Events - Alarms_View_High. Last 10000 Events: from: 2018-11-01 to: 2018-11-07

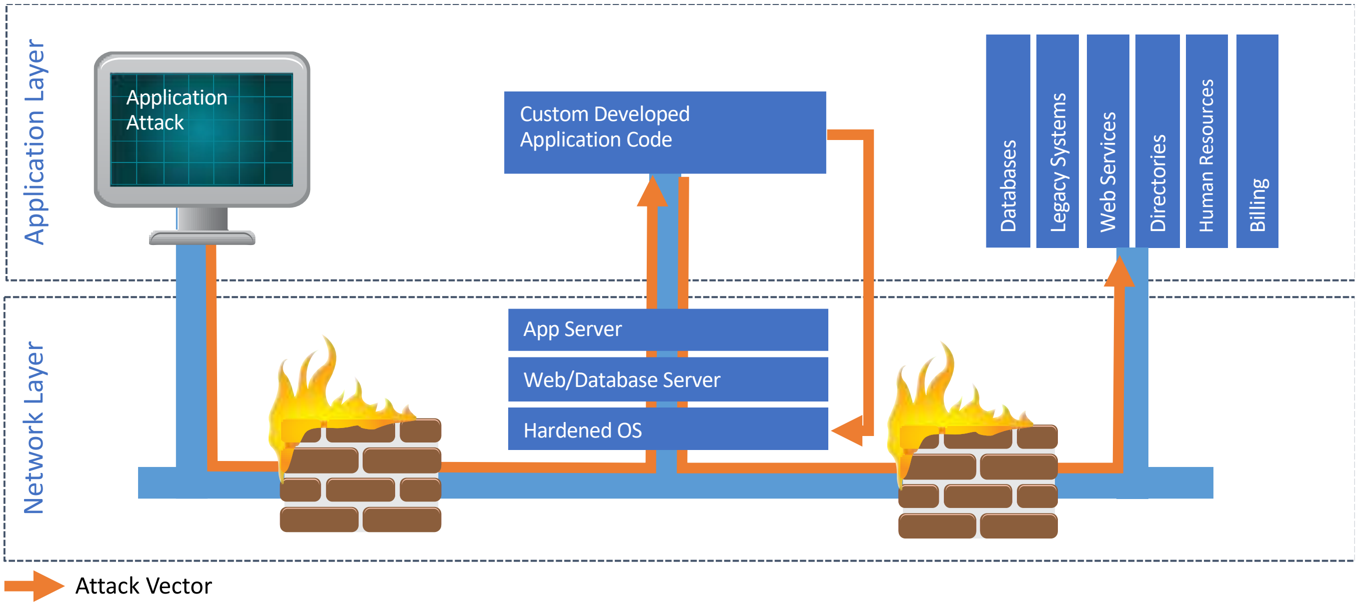
Event Name	Date GMT+1:00	Src IP	Dst IP	Risk
directive_event: AV Bruteforce attack, Windows authentication attack against 192.1.1.151	2018-11-06 11:33:14	192.1.1.151	192.1.1.151	3
directive_event: AV Bruteforce attack, Windows authentication attack against 192.1.1.151	2018-11-01 09:33:26	192.1.1.151	192.1.1.151	3
directive_event: AV Bruteforce attack, Windows authentication attack against 192.1.1.151	2018-11-01 05:33:34	192.1.1.151	192.1.1.151	3
directive_event: AV Policy, Account Lockout	2018-11-06 11:45:52	192.168.20.66	192.168.20.66	2
directive_event: AV Policy, Account Lockout	2018-11-06 11:42:16	192.168.10.66	192.168.10.66	2
directive_event: AV Web attack, SQL injection attacks detected against 192.168.20.73	2018-11-01 17:15:21	192.168.22.72	192.168.20.73	2

Label		Occurrences
🟥	directive_event: AV Bruteforce attack, Windows authentication attack against 192.1.1.151	3
🟥	directive_event: AV Policy, Account Lockout	2
🟪	directive_event: AV Web attack, SQL injection attacks detected against 192.168.20.73	1

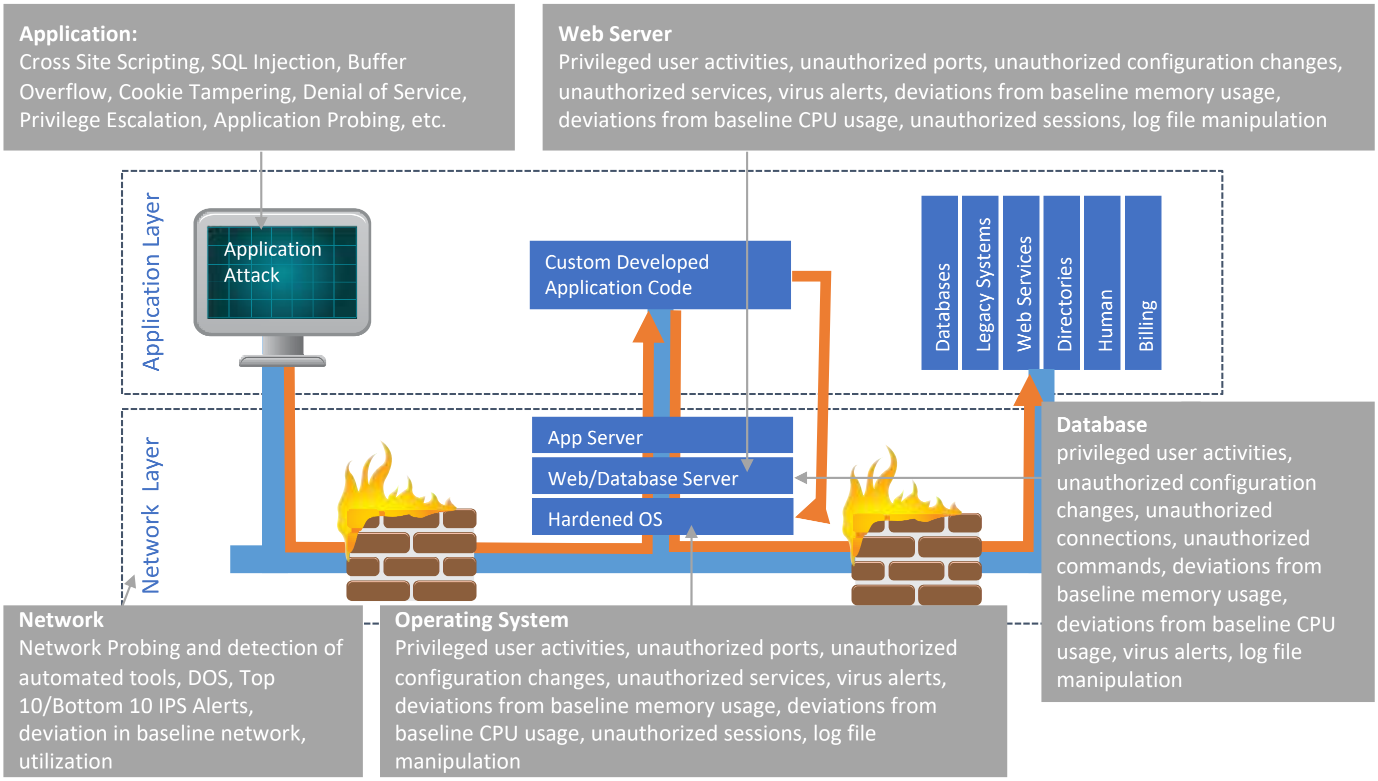
8 USE CASES

Category	Use Case
Asset Management	• Identify and isolate unauthorized devices • Identify and isolate unauthorized software
Configuration Management	• Alert on unexpected server configuration changes • Alert on unplanned system or service startup or shutdown
Network Boundary Defense	• Identify and isolate outbound requests to high risk external domain • Report all login attempts to network devices
Application Security	• Identify web application attacks (XSS, SQL Injection, etc.)
User Audit	• Monitor for activity on disabled (e.g. guest) accounts • Identify user activity during non-business hours • Identification of shared user accounts
Administrative Privileges	• Identification of unauthorized activity by privileged users • Alert on addition of new administrative users
Malware Defense	• Top 10 most attacked ports • Outbound traffic to
Data Protection	• Identify and isolate unapproved network traffic between trust zones • Alert on unexpected database changes

92% of reported vulnerabilities are in applications, not networks!!
In the Open System Interconnection (OSI) reference model, every message travels through seven network protocol layers. The application layer includes HTTP and other protocols that transport messages with content, including HTML, XML, Simple Object Access Protocol (SOAP) and Web services.



Use Cases drives the value of SIEM investments and removes the notion of "garbage-in-garbage-out". Here are a variety of Use Cases to be considered:



Application:
Cross Site Scripting, SQL Injection, Buffer Overflow, Cookie Tampering, Denial of Service, Privilege Escalation, Application Probing, etc.

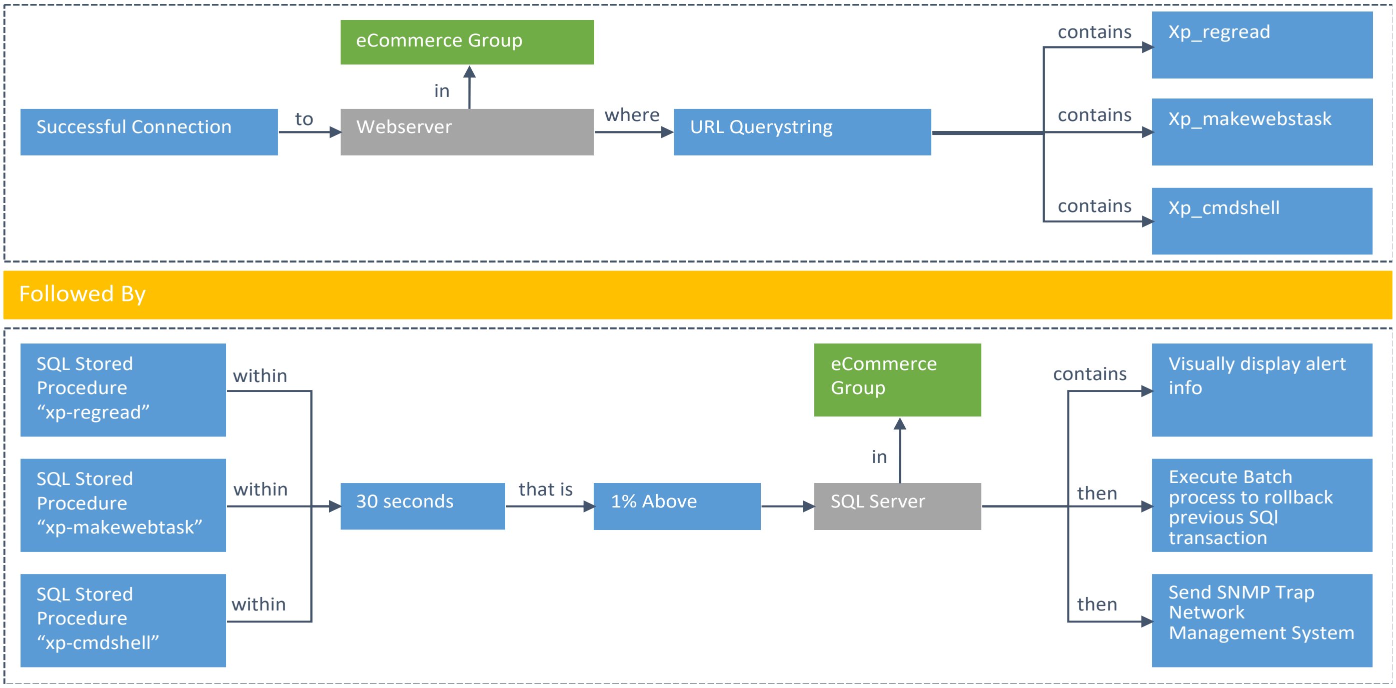
Web Server
Privileged user activities, unauthorized ports, unauthorized configuration changes, unauthorized services, virus alerts, deviations from baseline memory usage, deviations from baseline CPU usage, unauthorized sessions, log file manipulation

Database
privileged user activities, unauthorized configuration changes, unauthorized connections, unauthorized commands, deviations from baseline memory usage, deviations from baseline CPU usage, virus alerts, log file manipulation

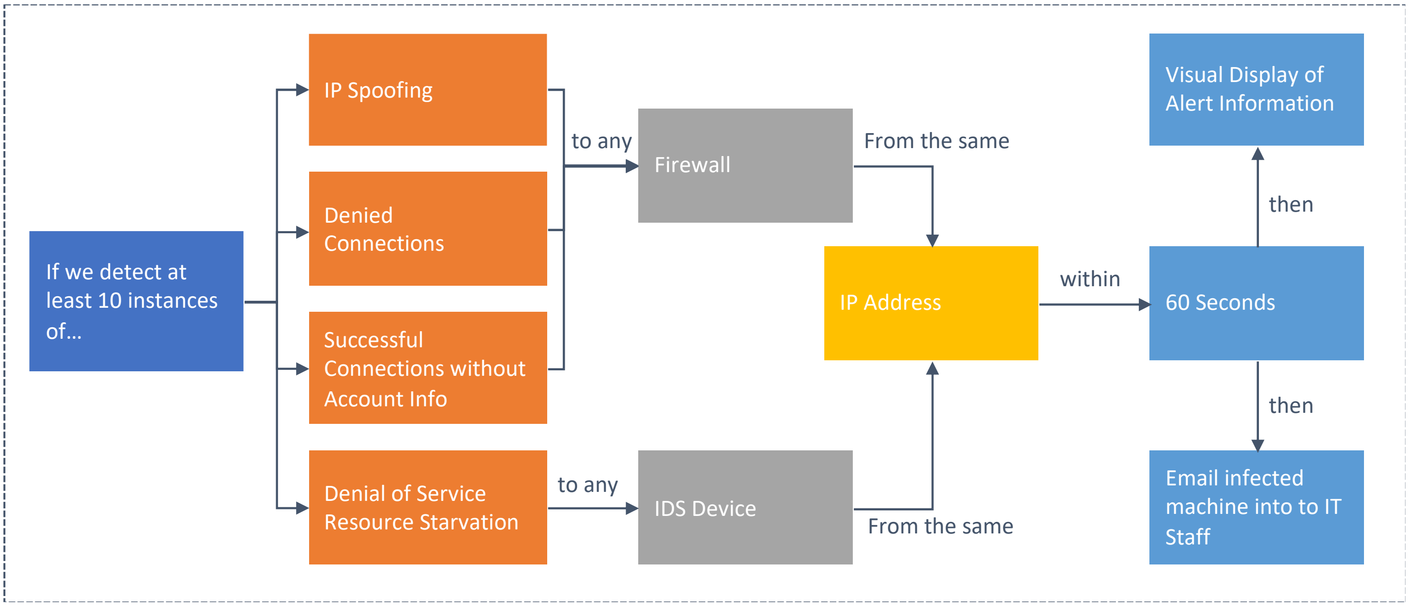
Network
Network Probing and detection of automated tools, DOS, Top 10/Bottom 10 IPS Alerts, deviation in baseline network, utilization

Operating System
Privileged user activities, unauthorized ports, unauthorized configuration changes, unauthorized services, virus alerts, deviations from baseline memory usage, deviations from baseline CPU usage, unauthorized sessions, log file manipulation

Website Attack (via SQL Injection) The goal of this use case or "correlation pseudo-code" is to detect information theft from E-Commerce websites through the exploitation of the trusted connection between the web server and the database.


Successful Connection
to
Webserver
in
eCommerce Group
where
URL Querystring
contains
Xp_regread
contains
Xp_makewebstask
contains
Xp_cmdshell
Followed By
SQL Stored Procedure “xp-regread”
within
SQL Stored Procedure “xp-makewebtask”
within
SQL Stored Procedure “xp-cmdshell”
within
30 seconds
that is
1% Above
SQL Server
in
eCommerce Group
contains
Visually display alert info
then
Execute Batch process to rollback previous SQl transaction
then
Send SNMP Trap Network Management System

Worm Detection The goal of this rule is to detect Blaster worm variants as well as other malicious code by analyzing network traffic patterns.


If we detect at least 10 instances of…
IP Spoofing
Denied Connections
Successful Connections without Account Info
Denial of Service Resource Starvation
to any
Firewall
to any
IDS Device
From the same
From the same
IP Address
within
60 Seconds
then
Visual Display of Alert Information
then
Email infected machine into to IT Staff

9 Appendix A: SHELT Defense-In-Action^{TM} SLA

1 Defense-In-Action^{TM} Active Monitoring, Detection & Response Service Level Agreement

This Service Description and Service Level Agreement ("SLA") describes the Service defined below being provided by SHELT to XXXX ("Customer") by the entity identified in the below

Customer XXXX	
Whose office is at	
Contact Details	XXXX

AND

SHELT	
Registered office Address	
Primary Contacts Details	
Secondary Contacts Details	

The Defense-In-Action Service Level Agreement ("SLA") provides proactive security monitoring and administration of customer IT assets listed in below Schedule A of this document , 24 hours a day, 7 days a week, and 365 days a year as per the Service Scope in section 2

Shelt Threat Intelligence Platform and its highly expert team of security analysts will deliver to the Customer a complete and customized Managed Security monitoring and detection service , to boost its security standing, postulate a full analysis on the current security issues, enable device availability as well as to provide different reporting features.

Shelt will provide Customer with customized dashboards, and different self-service security tools including periodic vulnerability scanning capabilities and other proprietary event correlation mechanisms and notification systems throughout Shelt Threat Intelligence online platform.

Shelt managed support is limited to components and assets for which Customer has a valid license and vendor support contract. The following service components are included with the managed service:

- Security event monitoring and alerting

- Device availability monitoring and alerting
- Vulnerability Assessment
- Threat Intelligence content

1.1 Customer Obligations

Customer agrees to perform the following duties and acknowledges and agrees that the ability of SHELT to perform its obligations hereunder, including the SLAs below, are dependent on

Customer's compliance with the requirements in this section. Noncompliance with SHELT requirements may result in suspension of managed services and/or SLAs. In addition to the Customer obligations listed in this Section 1.1, further Customer responsibilities are detailed throughout Section 2

1.1.1 Hardware and Software Procurement

Customer is responsible for purchasing, upgrading, replacing the hardware and software under this SLA coverage (referred to in Schedule A) for SHELT to be able to deliver the Service. Customer is responsible for ensuring that its hardware and software stays within the supported models and versions of the main related vendor prior of Service activation. SHELT SLA will not apply to platforms or versions that are End-of-Life ("EOL"), end of support, or are otherwise not receiving updates by the vendor

1.1.2 Support Contracts and Licensing

Customer is responsible for maintaining current vendor licensing, vendor support and vendor maintenance contracts for the equipment covered by this SLA. Customer is also responsible for facilitating direct contact between Shelt team and existing vendor support and maintenance contacts whether in country or remote, and enforce clear and transparent communication in between the vendor and Shelt team. Customer also needs to provide all support document to Shelt for review prior activation of Shelt service. In case support agreement with vendor is not in place for a certain IT asset covered by this SLA, then this equipment will be removed from the Schedule A list of approved covered equipment until a support agreement to cover the item in question is enabled in between Customer and vendor .

1.1.3 Scripting and other customized code

Any script or code creation for use with, usage of, maintenance of, troubleshooting of or any integration with other third-party or custom tools are not included in this Service, and are the responsibility of the customer.

1.1.4 Connectivity

Customer will provide and maintain remote network connectivity to the device(s) necessary for Shelt to manage the equipment under this SLA. Customer should communicate any network or system changes that could impact service delivery to Shelt Security Operations Center ("SOC") by raising a ticket through SHELT Support. SLAs will not apply to devices that are experiencing connectivity issues that are beyond the control of Shelt.

1.1.5 Communications

Customer will communicate with Shelt via phone call or different means specified in later stages. In all cases a support ticket will be opened for each communication initiated by the Customer and the support process will follow the flow mentioned in the previous incident support flow chart

1.1.6 Maintenance

Customer will provide Shelt with at least 24 hours' notice for planned customer-side network maintenance so that Shelt may avoid unnecessary health event escalations to Customer.

2 Service Details

2.1 Security Event Monitoring and Alerting

A key component of our Service purpose is the ability to leverage our expert research and visibility and convey it to customers as an intelligent corrective measure to improve their security capabilities and adapt to continuous change in their security requirements. SHELT team analyzes millions of event logs each day, analyzing and comparing information within individual networks, across each enterprise and across our customer base. The effort between our SOC and leading research lab and many of our high-profile security consultants will result in a rapid deployment of custom defenses, so that when an attack occurs on one network, we will be able to notify you with all the details and apply specific controls before the attack reaches your environment

2.2 Security Incident Identification Methods

The SHELT security monitoring service incorporates numerous methods of threat identification through well-defined standardized processes and the use of technology.

These methods for detection and selection of false positives, signature-based detections, and human interaction with customized in house developed tools for advanced analytics. Our main objective is to rapidly identify malicious attacks or threats

The following describes handling of security incidents.

Real-Time Security Incidents	SHELT process all Security Events using well defined technologies from different vendors in order to identify patterns that may indicate malicious activity. This process includes analyzing events correlated from different monitored assets in the environment to help with contextual identifications of activities and reduce the number of false-positive Incidents.

2.2.1 Security Event and Incident Priorities

When a Security Event is detected, initial correlation, de-duplication and false positive reduction is performed by the SOC team. All notable security events will be marked either high, medium or low severity.

For Events classified as a medium or high severity, a ticket is either automatically generated by our Intelligent Platform or generated manually by a security analyst.

The below describe security events categorize based on their severity levels

PRIORITY	DESCRIPTION	NOTIFICATION
HIGH SEVERITY	Security Events that may require immediate attention and or represent significant threat to the customer environment (e.g., host infection(s), successful exploitations, and unauthorized internal scanning from unknown sources)	Telephone Email Automatic Ticket will be opened on portal
MEDIUM SEVERITY	Security Events that do not require immediate attention or represent a significant threat to a customer asset (e.g., login failures and reconnaissance activities)	Email Automatic Ticket will be opened on portal
LOW SEVERITY	Security Events that have no impact to a Customer asset or have been determined to be a false positive (e.g., instant messaging usage, adware, remote access software such as TeamViewer)	No Escalation Resolved and provided in the monthly report

2.2.2 Security Incident Information

Upon determination of a Security Incident classified either medium or high severity by the SOC, SHELT provides Customer with the following Incident information via Email.

To note that some incidents will have different kind of information available and therefore content may vary between Incidents based on detection methods.

- A description of the security event(s) and the activity that has been identified.
- A copy of the security event(s) including packet captures when provided by the identifying device.
- Technical details on the threat or activity that have been identified, including references.
- Source and destination information including hostnames when available.
- Recommendations on next steps based on the identified activity.
- Additional content and context may be added, but can vary based on the types of devices SHELT is monitoring and the activity that is taking place

In-depth analysis, incident response, forensics, and other security measures implementation beyond policy changes to the Devices or other SHELT managed devices are not included in this Service.

Customer may purchase these areas of advanced support under a separate, signed Service Order

2.2.3 Security Event Reporting

SHELT access Portal provides a secure mechanism to create, customize, and access executive reports, high level dashboards for online real time gauging of events as well as detailed technical level reports with historical events along a specific period of time.

This online portal enables Customer to create both standard and customized reports

2.3 Device Availability Monitoring and Alerting

To provide this service, SHELT must be able to connect to the Device(s) using Internet Control Message Protocol ("ICMP") or Secure Shell ("SSH") depending on which is more relevant to the device.

SHELT regularly performs a device availability check called Host Status on the Monitored Device. If a failed or negative response is received from a Host Status check, an automatic alert is sent to SHELT, which then generates a ticket.

Upon receipt of this Host Status ticket, SHELT will perform additional troubleshooting in an attempt to resolve an availability issue. If troubleshooting is unsuccessful within the time specified in the SLA, SHELT will notify the Customer via telephone call and email, and will work with the Customer to perform further troubleshooting steps until the issue is resolved or is able to identify the root cause of it

In addition, SHELT will perform with the support of its automated tools ongoing health checks to detect devices that are not sending logs to the on premises platform. If the threshold for a loss of event flow of a device is reached, an automatic alert is sent to SHELT, which then would generate a ticket. Upon receipt of this ticket, SHELT will perform additional troubleshooting before notifying the customer by ticketing workflow within the Portal, and determine if:

- The root cause of the incident is due to a device covered by the SLA, SHELT will attempt to restore connectivity or event flow. SHELT will work with Customer's designated points of contact to address any device-related issues.
- If the root cause of the incident is not related to a device covered in the SLA, such as a network change, outage, SHELT is not responsible for troubleshooting issues

2.4 Business Hours

SHELT provides 24-hour access to its SOC for questions and support. While SHELT endeavors to answer Customer's questions immediately, some inquiries may result in a ticket being handled by other support teams during business hours

2.5 Tuning and Customization Period

During a period of time Shelt will tune and customize relevant policies on the customer environment for a period that is approximately 12 weeks or less, beginning on the Service Start Date. During this tuning period, Shelt facilitates weekly policy tuning recommendation Customer. This is an important period of time for the most effective run of the SOC service, as it will be crucial for the SOC to receive relevant frequent security events from the environment without overwhelming analysts and hindering effective monitoring

This initial policy tuning period may vary depending on the complexity of the deployment, number of applications, and other factors, and is not subject to the SLA terms.

2.6 Vulnerability Scanning

Shelt will undertake vulnerability scanning services on a once per month schedule and will integrate continuous basic vulnerability scan results into the monthly reports sent to customers. Scans identify known vulnerabilities and exposures. This information will be used by the Shelt team to detect and prevent threats that may compromise exposures.

2.7 Attacker Database

The SHELT Attacker Database will be provided as a part the Service offered by SHELT. The SHELT Attacker Database contains a list of domain names and IP addresses used to conduct malicious activity.

The threat intelligence data feed provided by the Attacker Database, this information will enable SHELT and Customer to prevent cyberattacks and SHELT team will proactively inform the client about malicious domain names and IP addresses in order for them to block them on the required security components

2.8 Customer and SHELT Responsibilities

The following responsibility assignment matrix describes the level of engagement required by both Customer and SHELT in order to expedite and effective and successful service delivery.

SHELT uses the standard RACI model to clarify roles and responsibilities for managing ongoing project and service delivery. These roles are defined as such:

- R – Responsible: Means Role(s) assigned to do the work. For any task, there could be multiple roles responsible for it.
- A – Accountable: Means Role(s) that take the final decision and has ultimate ownership on the task.
- C – Consulted: Means Role(s) consulted as a subject matter expert (SME)
- I – Informed: Means Role(s) updated with status of the task and end result

Managed Security Operation Center Service			
Activity	**Description**	**Customer**	**SHELT**
Service Preparation	Create and modify escalation procedures for tickets	A,C,I	R
	Ensure Device meets hardware and software specifications prior to service launch	R,A	C,I
	Prepare an installation environment as required to implement Service, which may include virtual environment, computer resources, network connectivity, internet access, etc.	R,A	I
	Provide all authorized contacts for service initiation	R,A	I
Service Implementation	Provide Managed Device details	R,A	I
	Provide implementation guidelines for service implementation	I	R,A
	Configure implementation rules	I,C	R,A
	Configure and ship SHELT Service Enabler Devices and tools	I	R,A
	Stage SHELT Service Enabler Devices	R,A	I
	Install SHELT Service Enabler Devices (remotely or on site)	I	R,A
	Provide access to Monitored Devices	R,A	I
	Configure Managed Devices for security event logging	I	R,A
	Complete post-install quality check	R,A	I
Security Monitoring	Monitor logs or the purpose of creating security events	C,I	R,A
	Perform real-time analysis of security events and escalation of Security Incidents (using agreed-to escalation procedures)	C,I	R,A
	Create and maintain custom IP watch lists and related alerting procedures	R,I	A,C
	Perform log correlation where possible to identify internal sources and destinations of traffic related to escalated incidents	I	R,A
	Request for resource for incident response for security event tuning call and provide sample of events or incidents prior to the tuning call	R,A	I
Change Management	Submit approved and validated change for scheduled implementation	R,A	I
	Provide explicit approval for emergency IP blocks	R,A	C,I
	Perform change completion validation	R,A	C

	Validation with stakeholders to identify unexpected business impact from changes	R,A	I
	Create ticket or engage SOC for any ad-hoc changes/troubleshooting	R,A	I
Support	Customize and maintain event workflow tuning and incident creation mechanism	C,I	R,A
	Perform software upgrade modifications and maintenance (must be SHELT supported)	R,A	C,I
	Provide maintenance window to implement any software upgrades.	R,A	I
	Provide local onsite support for device software upgrades, hardware changes, device reboots/power cycling	R,A	C,I
	Critical device vulnerability notification and requests to customer for authorization to apply a patch or patches (if applicable to device)	C,I	R,A
	Investigation on health events on covered devices	C,I	R,A
	Support Health validation for upgrades and updates made on covered Devices	I	R.A
	Maintain and create health checks on all supported managed platforms	I	R,A
	Phone notification of connectivity loss from covered Devices via Host Status ticket	I	R,A
	Notification of a health incident via the Portal ticket with E-mail	I	R,A
General	Maintaining up-to-date authorized contact information	R,A	I
	Submission of all requests for in scope work via the Portal or via phone call to the SHELT SOC	R,A	I
	Provide initial and subsequent escalation procedures for tickets of each ticket type	R,A	I
	Update and modify escalation procedure based on Customer input for tickets of each ticket type	A,C,I	R
	Providing advanced notice of details regarding Customer-authorized scans or customer network maintenance periods to avoid unwanted SHELT escalations during these activities	R,A	I
	Network design	R,A	I
	security policy audits	R,A	I
	Ensure timely communication of network changes to SHELT SOC	R,A	I

2.9 Out-of-Scope

The Services outlined above comprise SHELT' standard service offering. Any other services are out-of-scope. Upon request, SHELT may provide out-of-scope technical support on a time and materials basis pursuant to a separate Service Order or Statement of Work ("SOW"), including:

- On-site installation and provisioning of device
- Configuration and or integration of IT products
- Custom analysis or reports
- Forensics
- Any change requests not specified in this document
- Vendor API Integration
- Rule set design and validation
- Policy auditing
- Security best practices consulting
- Security Architecture Review
- Thorough red teaming exercise and penetration testing
- Code security review

3 Service Initiation

3.1 Provisioning Activities

Service Initiation refers to the Service provisioning activities. The standard provisioning period begins at receipt of the signed Service Order by SHELT team, and ends with the activation of the Service.

Device provisioning and installation activities performed by SHELT include:

- Scheduling a kick-off call/meeting
- Configuring a Customer implementation ticket in the Portal. Configuring Device such as servers, loggers and sensors (s) in accordance with the latest hardware and/or software versions supported
- Scheduling a service activation call with Customer (NOTE: Customer must acknowledge equipment is properly racked and cabled).
- SHELT does not provide SLAs for completing Service setup within a specified period of time; the duration of the provisioning period is dependent on a number of factors, such as the number of Physical/Virtual Appliances required (where applicable), the number of physical sites where contracted devices will be activated for service, the complexity of the Customer environment, and the ability of Customer to provide SHELT with requested information within a mutually agreed-upon timeframe.

3.2 Provisioning Methodology

The SHELT provisioning methodology is comprised of the following phases.

Phase 1: Information Gathering

When SHELT receives the Services Order, SHELT will provide a Service Initiation Form to be completed by the Customer. When the Customer returns the completed SIF, SHELT will schedule a technical review call to review the SIF and other relevant information with the Customer.

Phase 2: Environment Check

SHELT will work jointly with the Customer to validate the accuracy of the information used to create the original Service Order against the actual Customer environment where Services will be performed

As a result, changes in the types (i.e. hardware make and/or model and software package or version) of equipment, the number of locations, or the quantities of devices to be provisioned may be identified

Customer acknowledges that in order for SHELT to provide Service coverage across such changes, an amended or additional Service Order may be required, which may include changes to scope and fees, and without such an amended or additional Service Order, SHELT may only be able to provide Services as scoped, defined, and charged per the original Service Order.

Phase 3: Enable Devices Deployment

The Servers, Sensors and Loggers (and other Enabler Device) deployment phase begins upon the completion of the Information Gathering phase described above

Customer is responsible for ensuring that the implementation site complies with SHELT' Systems requirements, which shall be provided to Customer prior to commencement of their deployment.

Customer must provide access and appropriate privileges within the environment to enable SHELT to deploy and configure the systems and relevant servers, loggers and sensors.

Service interruptions or failure to achieve the SLAs (as defined herein) will not be subject to penalty in the event of Customer's non-compliance with the above deployment guidelines.

Phase 4: Service Provisioning and Installation

The Service Provisioning and Installation phase begins upon the completion of the Information Gathering and Deployment phases described above.

Service Provisioning and Installation is performed in the following manner:

- SHELT provides telephone support to the Customer contact at the implementation site during installation of all Customer premises devices.
- Once Customer premise contracted devices are in place, SHELT accesses the device(s) (whether physical or virtual) remotely and performs the remaining configuration and Service activation tasks which may require a mutually agreed upon

SHELT schedules Service provisioning and installation in accordance with change management procedures communicated by Customer during the Information gathering phase. Standard installations are performed during local business hours. Installation may be performed at other times when scheduled in advance with the SHELT implementation team.

3.3 Additional Items

- Customer is responsible for ensuring that its hardware and software are at versions that are supported by SHELT enabling devices prior to provisioning of the service(s)
- In the case of provisioning in a virtual environment, Customer is responsible for providing information about the environment and may be required to make configuration changes. Customer must provide access and appropriate privileges within the virtual environment to enable SHELT to deploy and configure the Services.
- Any effort that is required to upgrade software or replace hardware in support of service implementation requirements can be performed by SHELT via a separate SOW

4 Service Level Agreement

SLA	Service	Penalty Fee
Security Monitoring	Customer shall receive electronic notification of a security incident (in accordance with Customer's defined escalation procedures) within fifteen (15) minutes of the determination by SHELT that the given activity constitutes a security incident. This is measured by the difference between the time stamp on the incident ticket created by SHELT SOC personnel or technology /tools used and the time stamp of the correspondence documenting the initial escalation Event(s) deemed low severity will not be escalated, but will be available for reporting.	1/30th of monthly fee for Service for the affected device

SHELT

MANAGED SECURITY SERVICES