Next Level Labs Inc.

Jonathan Sabourin

Active Cyber Defense Architect

Architecture and Design Principles for Active Cyber Defense

What is Active Cyber Defense?

Active Cyber Defense is the ability to secure and defend an enterprise against threats in real-time.

Next Level Labs presents a holistic approach to IT Architecture and Design that will solve a variety of problems that many Organizations face today. This holistic architecture approach encompasses all aspects of an Organization's Operations. Organizations that use this methodology will be able to develop and maintain an inherently robust and future proof operating environment.

Organizations face a variety of challenges maintaining and enabling services across their organizations. Many have relatively new legislation requirements; many are trying to be proactive and are struggling to develop and operationalize processes that are efficient and effective. Many Organizations are reactive in their Security Planning and Architecture and attempt to bolt on technology such as SIEM's and Security Analytics into chaotic operating environments and expect to provide intelligence to Security Operations Teams. Security Operations Teams are struggling to develop effective incident response and problem management processes as a result.

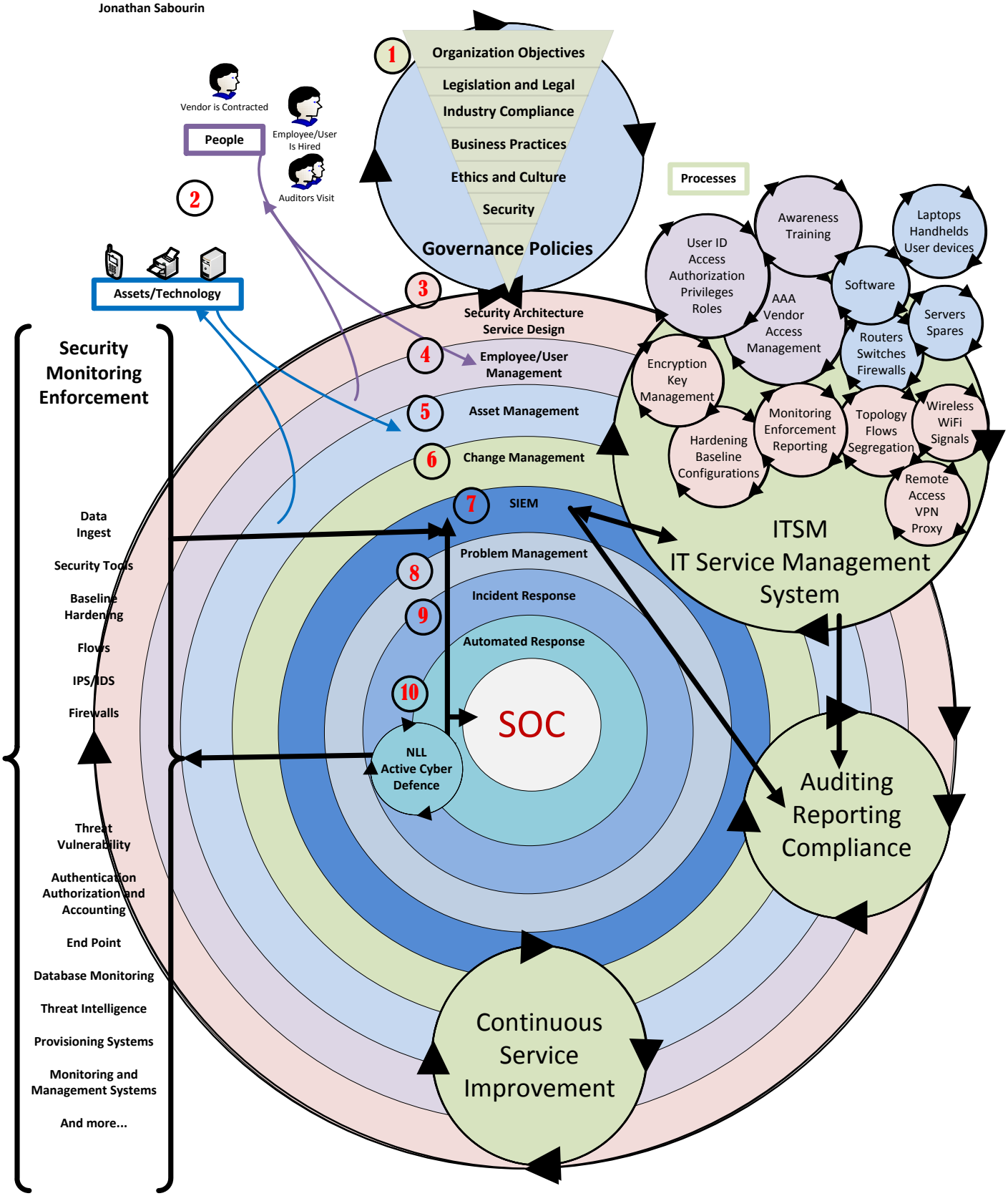
In this document I will attempt to describe to you an Architecture Methodology that will absolutely allow your Organization to become Cyber Resilient and Inherently Robust and enable an Organization to actively and in real time defend against even the most sophisticated Cyber Attacks.

If this methodology is adopted your organization will have a solid understanding of your business objectives and goals and develop solid processes and services management lifecycles to support them in Steps 1 through 6. Your Organization can efficiently and effectively deploy and operationalize SIEM technology and Security Analytics in Step 7. Your Organization will develop effective Incident Response and Problem Management processes in Steps 8 and 9. Finally an Organization will mature and naturally start developing and implementing Active Cyber Defense and Active Cyber Response capabilities in Step 10.

Many automated responses that Organizations can achieve today are automated firewall and IDP, IPS changes. Automated routing and topology changes, automated re-imaging of desktops and end point devices, automated sandboxing and there are a myriad of automated responses that can be developed once an Organization matures its Active Cyber Defense capabilities.

> *"If you know then enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself and not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle"*
> *–Sun Tzu, The art of War*

Active Cyber Defense Architecture Methodology



This drawing represents a Holistic view of a Sample Organizations' entire Business Operations, Objectives and Goals. This is a template that can be applied to any Organization. The template can be adjusted according to an Organizations Requirements, Objectives and Goals. The drawing is as generic and as minimalistic as possible and focuses on the Active Defense Architecture and Design Methodology. This methodology should be easily adopted by your Organization. This drawing is fundamentally based in ITIL Service Management Standards and any Compliance Standard can be applied. All Organizations should at least strive to achieve Steps 1 through Step 7 in this drawing. When an Organization realizes Step 7 they will naturally be able to apply Steps 8 through 10 very efficiently and effectively.

It must be noted that the ITSM "Information Technology Service Management" system will become your most valuable system in your Organization. This is where all of your business logic, processes, workflows, Change Management, Problem Management, Incident Management Processes will be orchestrated from. An ITIL or Pink Elephant Certified ITSM System needs to be utilized for this purpose. This is the most important part of the Active Defense Architecture Methodology. This is important as your ITSM will be able to provide efficiencies such as workflow automation. It's also most important because in Step 7 in the drawing you're going to integrate your ITSM directly into the SIEM and provide your SIEM with the knowledge of your entire Business Operations. Your SIEM will become intelligent enough to actually initiate an effective and efficient Active Cyber Response to threats in real-time.

1. Governance Policies:

An Organization needs to develop Governance Policies based on the Organizations Business Objectives and Goals. Governance Policies are of vital importance to an Organization as these will be used by an Architect and/or Service Designer to define the Organizations Operating Environment. Every Organization has different considerations that need to be taken into account and applied to their Governance Policy Development. These considerations need to be translated accurately into Governance Policies that reflect the Business Objectives.

It is important to note that Organizations should avoid or limit the use of ambiguous terms such as "SHOULD" "SHOULD NOT" and "MAY" "MAY NOT". These terms are highly subject to misinterpretation and are not easily enforceable.

Policies are required to be published and reviewed and updated yearly. Security Awareness Programs need to be created to ensure Employees are made aware of any change to the Governance Policies.

Once your Organization has developed their Governance Policies they can now be given to the Architect and/or Service Designer who will translate them into services, processes and workflows and begin to design or redesign and your Operations Environment.

2. People, Processes and Technology:

This is the most important aspect of Service and Process Design. Every Organization will need to utilize Employees and Technological Assets to fulfill their Organization Objectives. These are the key components for an Architect to consider if they are to be successful at designing an effective IT Services Roadmap, Plan and Services Catalog. An Architect needs to provide elegant, orchestrated and efficient services lifecycle design and supporting organizational processes. I've added two services lifecycles that every organization should have People and Technological Assets. An Organization can have many service lifecycles as their Organization needs to achieve their objectives. An Organization can have as many supporting workflows or

processes as required to achieve their Operational Objectives. For instance another popular Service Lifecycle is Customer Management and a Customer Lifecycle may require many supporting workflows and processes.

3. Security Architecture and Service Design:

The Architect now utilizes the People, Processes, Technology and the Organizations Governance Policies to Design the Organizations IT Service's Portfolio and Operating Environment. The ITSM will become the tool of choice for implementing the services, workflows and processes that an Organization will need to operate efficiently. The ITSM will allow an Architect to be able to develop services and workflows that are highly efficient, orchestrated, integrated and provide for automation. A good ITSM will allow an Architect to create or modify provided templates for helpdesk, ticketing coordination and approval chains, user management, asset management, device provisioning, change management, problem management, incident management and all the services an Organization requires to provide an efficient operating environment. Services and workflows should be developed to work together to orchestrate the Organizations Operations and provide opportunities for automation. Processes need to be developed that are elegant, fluid and efficient. Processes should be intertwined or woven together to complete a service lifecycle.

4. Employee and User Management:

An Architect should consider is that all Organizations require people and technology to run them and drive them forward. By utilizing lifecycle management methodologies an employee management lifecycle can be designed that will enable the employee to perform optimally throughout their employment at the Organization.

For instance when an employee is hired the Employee or User Service Management process can be initiated in order to allocate the required assets and resources to the employee to be able to perform their job functions efficiently. The User Service Management lifecycle may encompass many other workflows in order to achieve the desired results. For instance when a new employee is hired many workflows are initiated in such as creation of an ID Badge, issuing of a communications devices, allocating a laptop desktop and create User ID's and be provided Access and Authorization to an Organization resources. All of these workflows should be able to work independently of each other, they should be modular and allow for workflows to be nested or coupled together to create larger workflows. By utilizing modular service and workflow design an organization can easy change workflows add new workflows without having to rewrite entire Service Management Lifecycles.

For instance hiring a vendor will initiate a workflow similar to an Employee but an Organization Governance Policies may not allow a vendor a communications device but instead provide a vendor a VPN Token for remote access. In this case a workflow can be created based on the Employee Service Management Lifecycle that is designed specifically for vendors that doesn't use the Device Provisioning workflow and initiates the Remote Access and Vendor VPN workflow. This would be encapsulated into the Vendor Management Lifecycle workflow with inheritance from the User Management Service Lifecycle.

5. Technology Assets Service Management Lifecycle:

Similar to the Employee Service Management Lifecycle an Organization will use Technological Assets to enable their Business operations. Asset Management has been traditionally difficult to manage and maintain. This does not need to be difficult anymore.

Asset management is absolutely vital importance to an Organization. It is most likely that it will be a Technological Asset that is manipulated, gets a virus and becomes the source of impact to your Organization Operations.
A good Asset Management Service Lifecycle will manage, monitor and maintain all aspects of the technological Asset from the time it is purchased and provisioned to the moment it is removed from service. All aspects of the Assets life will be recorded and monitored and reported on proactively by the SIEM. The SIEM will utilize the ITSM Asset database to maintain monitoring and enforcement of business Objectives. The SIEM will use this information to monitor the operating Environment for a variety of anomalies including rouge Asset discovery. For instance the SIEM sees new traffic from an unknown device or Asset. The SIEM knows it's an unknown Asset because the SIEM has queried the ITSM Asset Database and could not find a record for the newly discovered Asset. The SIEM automatically raises an alert "Policy Violation" creates associated Problem and/or Incident Management Tickets and using Automated Cyber Response the SIEM safely in real time quarantines the unidentified Asset thereby removing it from the Operating Environment as directed in the Organizational Governance Policies.

There are many Active Cyber Defense Responses that can be developed easily by maintaining an accurate Asset Inventory Database.

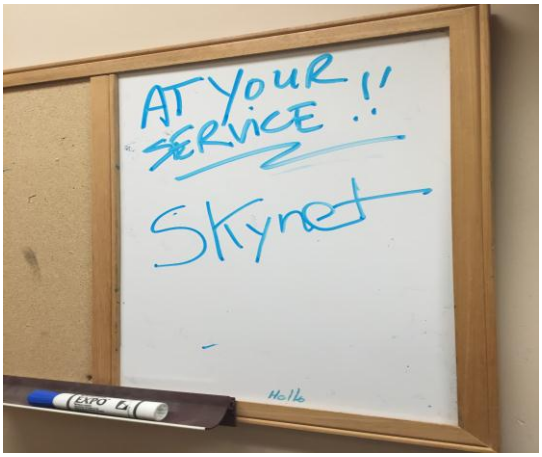
6. Change Management:

Change Management Service is important to an Organization as it is used to manage changes to the Organizations Operating Environment. In the context of Active Cyber Defense; Change Management is used to populate the SIEM Step 7 with vital information to allow the SIEM to make intelligent decisions and enforce an Organizations Governance Policies and Actively Defend the Organization.

For instance a marketing department has requested to deploy 6 servers overnight. The changes are approved; implementation plans are submitted and recorded into the ITSM. The ITSM is going to tell the SIEM that there are a group of servers being deployed with information such as IP addresses, Mac Addresses, Criticality and details about services it has running on it. The SIEM will automatically apply a monitoring and alerting template to the servers that allows for proactive monitoring, reporting and enforcement of the Organization Governance Policies. When the servers are deployed and the SIEM starts seeing traffic from the servers the SIEM can send notifications to the ITSM that the servers are operating as expected from the change management details or the SIEM can send an Alert to the ITSM that the servers have been deployed and they are behaving outside of the parameters of the change request which may indicate a configuration error or other problem that should be addressed by the Implementation and Engineering teams. The SIEM can automatically quarantine the server from the network or many other proactive and automated responses if they are desired in the Governance Policies.

7. SIEM:

This is where the results of the Organizations efforts to work toward Active Cyber Defense become reality.



Step 7 is deploying your SIEM and integrating it into your ITSM System. Your Organization can start developing your Security Analysts and SOC capabilities. Steps 8 through 10 are all SOC capabilities that can now be achieved much more efficiently and with greatly reduced costs.

In the drawing you will see that the SIEM receives Intelligence Information from the Organizations Operations Environment in real-time. This can be sent to the SIEM in Syslog messages from any device. It comes from Passive TAP's or Data Aggregators that capture all data on the network to be forwarded to the SIEM for analysis, collation and archiving. The SIEM receives Threat and Intelligence Information from 3rd Party sources in near real-time. The SIEM utilizes integrated vulnerability scanning and vulnerability management, it provides network baseline monitoring and real-time topology map generation. It provides advanced forensics and evidence gathering capabilities; it provides integrated risk management and assessment capabilities. A good SIEM will have Advanced Analytics Engines, Network Anomaly Detection capabilities, Behavioral Anomaly Detection capabilities and various other preprogrammed Algorithms built in to Identify and Alert on Anomalies in real-time. SIEM technology in the near future will start utilizing Machine Learning; Artificial Intelligence and other yet to be developed technologies to aid in Anomaly Detection and Isolation.

By Integrating the SIEM with the ITSM the SIEM will become Intelligent about the real-time state of your Operating Environment. The SIEM will use the additional information in the ITSM to reduce false positives and enable Automated Response and Active Cyber Defense capabilities. The SIEM can collate the information from the network and test it against the information in the ITSM to reduce false positives and enhance the Security Analysts and SOC teams' ability to accurately and effectively enforce the Organizations Governance Policies.

8. Problem Management:

Problem Management Service is a service that is designed to identify problems before they become Incidents.

The difference between a Problem and Incident are that an Incident is an event that is impacting an Organizations ability to conduct it Operations. A problem is an event that is not impacting the Organizations Operations but if the Problem is not addressed efficiently it will or may become an Incident

and Impact the Organizations ability to Operate.

A Problem Management Service is absolutely essential for an Organization to become proactive in its Organizations Operations. It is essential for an Organization to Identify and isolate problems before they impact your Organizations Operations.

Your SIEM will be utilized for providing Intelligence for the Problem Management Service. The SIEM will provide your Security Operations Analysts and SOC with the capabilities to identify anomalies and potential problems in real-time and alert on these anomalies before they become impacting to your Organizations Operations.

9. Incident Response:

The Incident Response Service is an important Service that should be developed by your SOC and Security Analysts and should include all pertinent stakeholders and coordinators when developing the Incident Response Plan.
An ITIL Incident Response Plan can be highly directed and orchestrated and workflows can be easily created to be as efficient as possible. A workflow can be created in your ITSM that includes other workflows, automated data and evidence gathering capabilities, automated notifications and centralized coordination and communications for Incident Response Teams. An entire Incident Response plan can be created in your ITSM that is integrated with your SIEM to provide fast and efficient Incident Response Capabilities. Your ITSM will be able to store the results of previous incidents and accumulate intelligence Information for future Incidents. Your ITSM will allow your Organization to modify and/or create nested Incident Response Plans for different anomalies or preconceived situations. An Incident Plan developed in the ITSM can have advanced programmatic logic to query the SIEM to facilitate faster Incidence response resolution times and enhanced situational awareness during an incident.

10. Automated Response:

Automated Response is the final Step to achieving Active Cyber Defense. In this step you will achieve Active Cyber Defense. In fact if you have been practicing these Architecture Methodologies your Security Operations Teams have already noticed that the SIEM Intelligence Capabilities are accurate and enforceable. Your Security Operations Teams are starting to naturally become proactive and effective at identifying problems before they become incidents. Your Security analysts will have noticed that the amount of alerts and offences generated daily has steadily been dropping as the SIEM collates the ITSM information against real-time network and third party intelligence. Your Security Analysts have noticed that the quality of the reports and information provided by the SIEM is highly accurate and false positives are becoming nearly nonexistent. This is all a result of the ITSM Integrations with the SIEM in Step 7.

Now it's time for your Organization to start using the SIEM and ITSM to start automating your Active Cyber Response and achieve Active Cyber Defense. Active Cyber Responses that can be easily implemented are:

1. Dynamic firewall, IPS and IDS changes for a variety of precognitive situations.
2. Whitelisting and Blacklisting Bad IP addresses or Bad Domains
3. Automated Quarantining, Scanning and Vulnerability assessments
4. Dynamically Re-imaging End point devices , desktops or laptops in a variety of precognitive situations
5. Automated server and system baseline, hardening and configuration monitoring and enforcement.

6. Dynamic Routing and Topology changes for a variety of precognitive situations such as Network Quarantining of problem devices.
7. Automated patch management

The amounts of Active responses that can be designed and implemented are only limited by the Security Analysts and/or Architects Imagination. By utilizing Active Cyber Defense an Organization can proactively thwart known and unknown attacks in real-time with absolute certainty of the outcome. Many creative and precognitive Active Responses can be created as required by an Organization.

The next time your Organization is attacked where do you want to be? Wouldn't it be nice to have complete situation awareness and intelligence to confidently and effectively make intelligent and effective Operations Decisions and Achieve Active Cyber Defense?

Thank You