Jonathan Sabourin
Information Security Architect

Architecture and Design Principles for Active Cyber Defense

What is Active Cyber Defense?

Active Cyber Defense is the ability to actively secure and defend an enterprise in near real time.

Next Level Labs utilizes a holistic approach to IT Architecture and Design that will solve a variety of IT Security and Compliance 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 increasing legislation and compliance requirements; many are trying to be proactive but are struggling to develop and operationalize processes that are efficient. 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 manage an onslaught of information and false positives and struggle to develop efficient and effective Incident Response and Problem Management processes as a result.

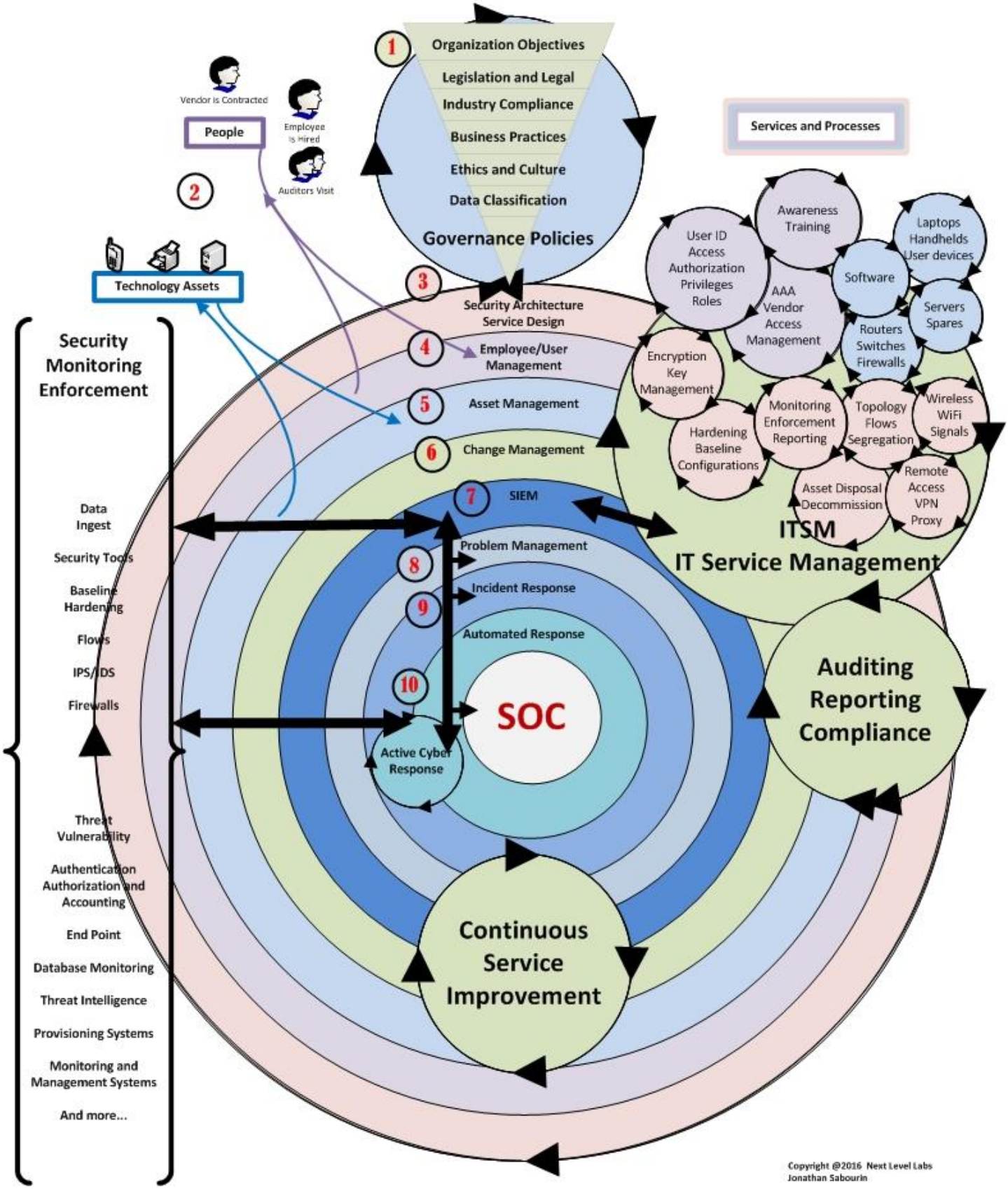
In this document I will describe to you an Architecture Methodology that will absolutely allow your Organization to become cyber resilient, inherently robust and future proof. Your Organization can begin to move forward and develop your Active Cyber Defenses.

If this methodology is adopted your organization will have a solid understanding of your business objectives and goals and translate these objectives into workable and enforceable Governance Policies. Your architects can use these policies to develop services management lifecycles and your Organizations' ITSM to support them. Your Organization will efficiently and effectively deploy and operationalize SIEM technology and integrate it into various business and security enforcement infrastructures. Your Organization will begin to develop effective Incident Response and Problem Management processes. Finally an Organization will mature and naturally start developing and implementing Active Cyber Defense and Active Cyber Response capabilities.

Many Active Cyber Defense 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 as an Organization matures its Active Cyber Defense capabilities.

> ***"If you know the 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 Defence Architecture Methodology



This drawing represents a holistic view of Example Companys' entire Business Operations. This methodology can be incorporated into any Organizations' security architecture and planning. The methodology can be adjusted according to an Organizations goals and requirements. This drawing is as generic and minimalistic as possible to focus on the Active Defense Architecture and Design Methodology. This drawing is fundamentally based on ITIL Service Management Standards and any combination of Compliance Standards can be applied.

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 and Incident Management Processes will be orchestrated from. An ITIL or Pink Elephant Certified ITSM System needs to be utilized for this purpose. Your ITSM will be able to provide efficiencies such as workflow automation and reporting. The ITSM is also important because in Step 7 you're going to integrate your ITSM directly into your SIEM and provide your SIEM with the knowledge of your entire Business Operations. Your SIEM will become intelligent enough to dramatically reduce false positives and initiate an efficient and effective Active Cyber Response to threats in near real-time.

1. Governance Policies

Your Organization needs to develop Governance Policies based on your Organizations Business Objectives and Goals. Governance Policies are of vital importance to your Organization as these will be used by your Architect and/or Service Designer to define your 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 your Business Objectives.

It is important to note that Organizations should avoid or limit the use of ambiguous terms such as "SHOULD" and "MAY". These terms are highly subject to misinterpretation and are not enforceable. Use "SHOULD" and "MAY" whenever it is necessary to express non-mandatory provisions. "MUST" shall not be used to express mandatory provisions. Use the term "SHALL" to define mandatory provisions.

Policies are required to be published and reviewed and updated yearly.

Security Awareness Programs need to be developed to ensure employees are made aware of the policies and any changes and updates to them.

Once your Organization has developed your Governance Policies they can be given your 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

People are the most important aspect of Service and Process Design. Every Organization will need to utilize employees and technological assets to fulfill your Organizations' Objectives. These are the key components for your architect to consider if they are to be successful at designing an effective IT Services Roadmap and develop your Organizations Service Catalog. An architect needs to provide elegant, orchestrated and efficient services lifecycle design and supporting organizational processes. Workflows need to be fluid, realistic and usable if they are to be adopted by your users.

Your Organization can have as many service lifecycles as your Organization needs to achieve your business objectives. An Organization can have as many supporting workflows or processes as required to achieve their Operational Objectives.

3. Security Architecture and Service Design

Your architect can now begin to design your Organizations IT services' catalog, workflows and supporting processes. Your ITSM will become the tool of choice for implementing the services, workflows and processes that your Organization will need to operate efficiently. Your ITSM will allow your architect to be able to develop services and workflows that are highly efficient, orchestrated, integrated and provide for automation and orchestration. A good ITSM will allow your architect to create and modify provided templates for helpdesk, ticketing coordination, approval chains, user management, asset management, device provisioning, change management, problem management, incident management and provide SLA's and support auditing and compliance requirements.

Services and workflows should be developed to work together to orchestrate your Organizations Operations and provide opportunities for automation. Processes should be intertwined and woven together to complete a service lifecycle or workflow.

4. Employee and User Management

Architects should consider is that all Organizations require people, technology and processes to run them and achieve business objectives. By utilizing service 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 workflow can be initiated to allocate the required assets and resources for the employee to be able to perform their job functions efficiently and effectively. This workflow may entail creation of an ID Badge, issuing of communications devices, allocating a laptop and/or desktop, creating User ID's and provide access to your Organizations' data. 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 architecture and workflow design your organization can easy change workflows, add new workflows or create new workflows without having to rewrite entire Service Management Lifecycles.

Contracting a vendor will initiate a workflow similar to the Employee workflow but an Organizations' 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 but initiates the Remote Access and Vendor VPN workflow instead. This would be defined as a Vendor Management Lifecycle with inheritance from the User Management Service Lifecycle and other processes as required.

5. Technology Assets Service Management Lifecycle

Similar to the Employee Service Management Lifecycle your Organization will use Technological Assets to enable your employees and realize your business objectives.

Asset management is absolutely vital importance to an Organization. It is most likely that it will be a communications device or other asset that is manipulated and becomes the source of impact to your

Organizations' 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 disposed of. All aspects of the assets life will be recorded, monitored and reported on by the SIEM and the ITSM. The SIEM will utilize the ITSM asset database to synchronize monitoring and enforcement of business Objectives. The SIEM will use this information to monitor the Organizations' operating environment for a variety of anomalies including rouge asset discovery.

For example the SIEM sees new traffic from an unknown device or asset. The SIEM knows it's an unknown asset because the SIEM has synchronized the ITSM asset database and could not find a record for the newly discovered asset. The SIEM automatically raises an alert "Policy Violation" and creates associated Problem and/or Incident Management tickets and using Automated Cyber Response your SIEM safely in real time quarantines the unidentified asset thereby removing it from the Operating Environment as directed by your Organizations' Governance Policies.

6. Change Management

Change Management Service is important to an Organization as it is used to record and manage changes to your Organizations Operating Environment. In the context of Active Cyber Defense; Change Management is used to populate the ITSM with change information. The SIEM will synchronize this information to reduce false positives and provide intelligent and effective Automated Cyber Response to enforce your Organizations Governance Policies and Actively Defend your Organization.

An example might be 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 monitoring and alerting templates to the servers that allow for proactive monitoring, reporting and enforcement of your Organization Governance Policies. When the servers are deployed and the SIEM starts seeing traffic from the servers the SIEM can automatically perform a variety of tests against the servers to ensure that they are compliant and operating within the change management parameters. 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 are behaving outside of the parameters of the change request which may indicate a configuration error or other problem that should be addressed by your implementation and engineering teams. The SIEM can automatically quarantine the server from the network or many other proactive and automated responses if they are defined in your Organizations Governance Policies.

7. SIEM

At this stage the results of your Organizations efforts to work toward Active Cyber Defense start maturing and becoming a reality.

Organizations' that have an existing SIEM, SOC and Security Team would have many of the integrations with the ITSM and other infrastructures already in place as the Organization shifted towards Active Cyber Defense Architecture Methodologies. These Organizations' will have already realized a reduction in false positives and realize much more accurate Intelligence Information.
Other Organizations' will need to deploy SIEM technology and start maturing their Security Team and SOC capabilities.

In the drawing you will see that the SIEM receives Intelligence Information from your Organizations operations environment in real-time. This data is sent to the SIEM via a variety of methods including passive TAP's and data aggregators that send full network packet data 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 provides network baseline monitoring and real-time network topology mapping. The SIEM provides advanced forensics and evidence gathering capabilities for legal and legislative requirements including Lawful Intercept. A good SIEM will have advanced analytics engines, network anomaly detection capabilities, behavioral anomaly detection capabilities and various other pre-programmed customized algorithms to identify and alert on anomalies in near real-time. SIEM technology in the near future will utilize Machine Learning; Cognitive Analytics and other yet to be developed technologies to aid in anomaly detection and provide Active Cyber Response.

By Integrating the SIEM with the ITSM the SIEM will become Intelligent about your Organizations Business and Operations Objectives. The SIEM will use this Intelligence to reduce false positives and enable Automated Response and Active Cyber Defense capabilities. The SIEM will greatly enhance the Security Analysts and SOC teams' ability to accurately and effectively enforce the Organizations Governance Policies.

8. Problem Management

A Problem Management Service is a service that is designed to identify problems before they become incidents and before they impact your Organization operations. A Problem Management Service is absolutely essential for your Organization to develop to become proactive at identifying and mitigating potentially impacting events.

Your SIEM will provide Intelligence to the ITSM Problem Management Service. The SIEM will provide your Security Analysts and SOC with the situational intelligence they require to identify anomalies and potential problems in near real-time and utilize Active Cyber Responses before they impact your Organizations operations.

9. Incident Response

Your 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 must be 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 Active Cyber Response capabilities. Your ITSM will be able to store the results of previous incidents and accumulate intelligence information for your SOC teams to use as reference during future events and for developing Active Cyber Responses. Your ITSM will allow your Organization to modify and/or create nested Incident Response Plans for different anomalies or pre-conceived situations. An Incident Response Plan developed in the ITSM can have advanced programmatic and cognitive logic to enable Active Cyber Responses to various anomalies.

10. Automated Response

Active Cyber Response is the final Step to achieving Active Cyber Defense. In this step you will achieve Active Cyber Defense. In fact if your Organization has been practicing these Architecture Methodologies your SOC and Security Analysts have already noticed a dramatic decrease in false positives that are analyzed each day. Your Security Operations Teams are naturally becoming more proactive and effective at identifying problems before they become incidents. The amount of alerts generated daily will continue to reduce as your Organization realizes Active Cyber Defense.

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 pre-cognitive situations.
2. Whitelisting and Blacklisting Bad IP addresses or Bad Domains
3. Automated Quarantining, Scanning and Vulnerability assessments
4. Dynamically Re-Imaging of 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 pre-cognitive situations such as network quarantining of problem devices.
7. Automated patch management

The Active Cyber Responses that can be designed and implemented are limited only by your Security Analysts and 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.

The next time your Organization is attacked where do you want to be? Would it be nice to have complete situational awareness and intelligence to confidently and effectively make intelligent and effective Operations decisions that allow for Active Cyber Responses that enable your Organization to be inherently cyber-resilient?