Luminologies LLC

Information Security, Business Continuity and Disaster Recovery

We Consult with Integrity, Design for Simplicity and Integrate with Intelligence

Luminologies

CONSULTING FOR INFORMATION SECURITY & CONTINUTY OF SERVICE

Luminologies collaborative and agile Incident Response solutions provides organisations with dynamic incident response action plans based on industry standards, best practices, and global regulatory requirements

We provide organisations with workflows, intelligence, deep-data analytics, and simulation capabilities – making it easy to prepare for incidents, assess their impact, execute the response, and manage the process to closure

Our consulting teams take a process based approach to each assignment, with meticulous project planning and attention to detail. The approach has built in quality checks to ensure high quality delivery while adhering to project timelines.

The deliverables are structured to be clear and concise, and offer management not only a technological perspective, but a business perspective as well for each recommendation.

Luminologies Solutions

Security
Consultancy & End to End Solutions

Identity
Consultancy & End to End Solutions

BC/DR Services
Consultancy & Service Mgmt.
End to End Solutions

Secure Mobility
Consultancy & End to End Solutions

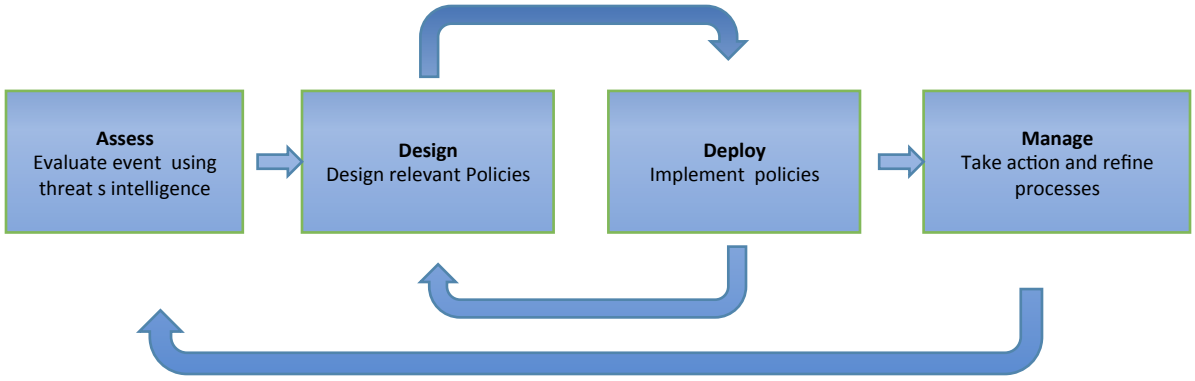
Training
Courses Tailored for all your needs

Benefits of working with Luminologies

- **Complete portfolio of Information Security Consulting services**
- **Consulting team with experience in executing complex projects**
- **Technology expertise across multiple domains and service stacks**
- **Partnerships with leading solution providers on Information security**
- **Comprehensive Training programs**

Luminologies

Response Methodology



Assess

Services Offered	Benefits to the organization
Enterprise Security Audit	To audit against international standards and frameworks and report on the compliance of processes, applications, technical security and user awareness.
Vulnerability Assessments	Assessment of Technical Controls and Prioritize the Implementation of Controls. Establish an effective Technical Vulnerabilities Reduction Metrics
Application Security Assessment	To check for the security of the applications as per the guidelines. Evaluate the portfolio of applications on web connected devises and each layer of application logic for potential vulnerabilities
Compliance Audit	Compliance to audit guidelines and other international security standards/ guidelines
Security Process Review	To check for the adequacy and compliance of the security policies, procedures and standards.
Recovery Process Review	Assess documented processes and procedures to restore service in a defined Disaster Recovery site.

Deploy

Services Offered	Benefits to the organization
Security Policy Deployment	To implement organization wide information security policies and procedures to ensure that corporate information and assets are protected from unauthorized access, disclosure and modification.
Change Management	Provide IT service constructs to support
Configuration Management	incorporation of DR services in organization IT Services model of support and life cycle
Release Management	management.

Design

Services Offered	Benefits to the organization
Certification Consulting	Top Driven and Consistent approach to address Compliance and Risk Management. Establishes Information System/Process Assurance . Our Consultants follows established methodologies to enable Organization get desired certifications
Security Policy Design	Designing and Developing Information Security Policies, procedures, standards and guidelines after a detailed study of the business process and security requirement.
Network Security Architecture	Study the existing network design, network and security device positioning and suggest/ recommend redesign of the network taking into consideration confidentiality, integrity and availability of information and ease of network and security administration
Business Continuity & Disaster Recovery Architecture / Policy / Process Development	Identify key services defined by a Business Impact Assessment (BIA) to design a recovery solution to meeting restoration and recovery business objectives.

Manage

Services Offered	Benefits to the organization
Security Policy Deployment	To implement organization wide information security policies and procedures to ensure that corporate information and assets are protected from unauthorized access, disclosure and modification.

Services Offered	Benefits to the organization
Enterprise Security Management	To manage the security process and controls organization wide 24/7 and provide real time alerts and recommendations thereby ensuring proactive security measures and preventing disruption of service.
Security Product Management	To manage the networking & security devices (servers, routers, firewalls, IPS, UTM's etc) organization wide 24/7 and provide real time alerts and recommendations thereby ensuring proactive security measures and preventing disruption of service.
Education & Training	Customized sessions focusing on security concepts, policies & procedures for organizations

Luminologies

Cyber security: it's more than just technology

Creating resilience

Prevention

Prevention begins with governance and organization. It is about installing fundamental measures, including placing responsibility for dealing with cyber crime within the organization and developing awareness training for key staff.

Detection

Through monitoring of critical events and incidents, an organization can strengthen its technological detection measures. Monitoring and data mining together form an excellent instrument to detect strange patterns in data traffic, to find the location on which the attacks focus and to observe system performance.

Response

Response refers to activating a well-rehearsed plan as soon as evidence of a possible attack occurs. During an attack, the organization should be able to directly deactivate all technology affected. When developing a response and recovery plan, an organization should perceive cyber security as a continuous process and not as a one-off solution.

Turn Data into Actionable Insight

Data is helpful, but information drives insight **Luminologies** provides the ability to create customised dashboard widgets and pivot tables – enabling response teams to access and visualize the exact critical information they need when they need it, and apply those insights for process improvements. Users can track and map the data – including incident levels by severity and category.

Luminologies

Risk and Compliance/Auditing/Governance

These experts assess and report risks to the organization by measuring compliance with policies, procedures, and standards. They recommend improvements to make the organization more efficient and profitable through continuous monitoring of risk management.

The following courses are specially tailored mainly for **Auditors and Compliance Officers**

Implementing & Auditing Critical Security Controls

Auditing & Monitoring Networks , Perimeters and Systems

Up-to-date Documented Recovery and Continuity Plan

Penetration Testing/Vulnerability Assessment

Because offense must inform defense, these experts provide enormous value to an organization by applying attack techniques to find security vulnerabilities, analyze their business risk implications, write modern exploits, and recommend mitigations before those vulnerabilities are exploited by real-world attackers

•Below is a list of courses we offer in this profile suitable for **Penetration Testers , Ethical Hacker , vvulnerability Assessor and Cyberspace Engineer**

Hacker Tools techniques, Exploits & Incident Handling

Networks & Exploits	•Network Penetration Testing & Ethical Hacking •Advanced Penetration Testing , Exploits Writing , and Ethical Hacking •Advanced Exploits , Development for Penetration Testers
WEB	•Web App Penetration Testing & Ethical Hacking •Advanced Web Penetration Testing & Ethical Hacking
LAB - Centered	•Intense Hands – On Penetration Testing Skills Development • CyberCity Hands – On Kinetic Cyber Range Exercise
Mobile / Wireless	•Mobile Device Security & Ethical Hacking •Wireless Ethical Hacking , Penetration Testing & Defenses

Luminologies

Network Operations Centre, System Admin, Security Architecture

A Network Operations Centre (NOC) is where IT professionals supervise, monitor, and maintain the enterprise network. The NOC is the focal point for network troubleshooting, software distribution and updating, router and system management, performance monitoring, and coordination with affiliated networks. The NOC analysts work hand-in-hand with the Security Operations Centre, which safeguards the enterprise and continuously monitors threats against it.

- We offer the following courses suitable for **System / IT Administrators , Security Administrator and Security Architect/Engineer**

Securing Windows with the Critical Security Controls

Securing Linux / Unix

Implementing and Auditing the Critical Security Controls

Virtualization and Private Cloud Security

Security Operations Centre/Intrusion Detection

The Security Operations Centre (SOC) is the focal point for safeguarding against cyber-related incidents, monitoring security, and protecting assets of the enterprise network and endpoints. SOC analysts are responsible for enterprise situational awareness and continuous surveillance, including monitoring traffic, blocking unwanted traffic to and from the Internet, and detecting any type of attack. Point solution security technologies are the starting point for hardening the network against possible intrusion attempts.

We offer the following courses suitable for **Intrusion Detection Analyst , Security Operations Analyst / Engineer Cyber Threat Analysts**

Hacker Tools Techniques, Exploits & Incident Handling

Endpoint Monitoring

- **Advanced Security Essentials – Enterprise Defender**
- **Advanced Digital Forensics and Incident Response**

Network Monitoring

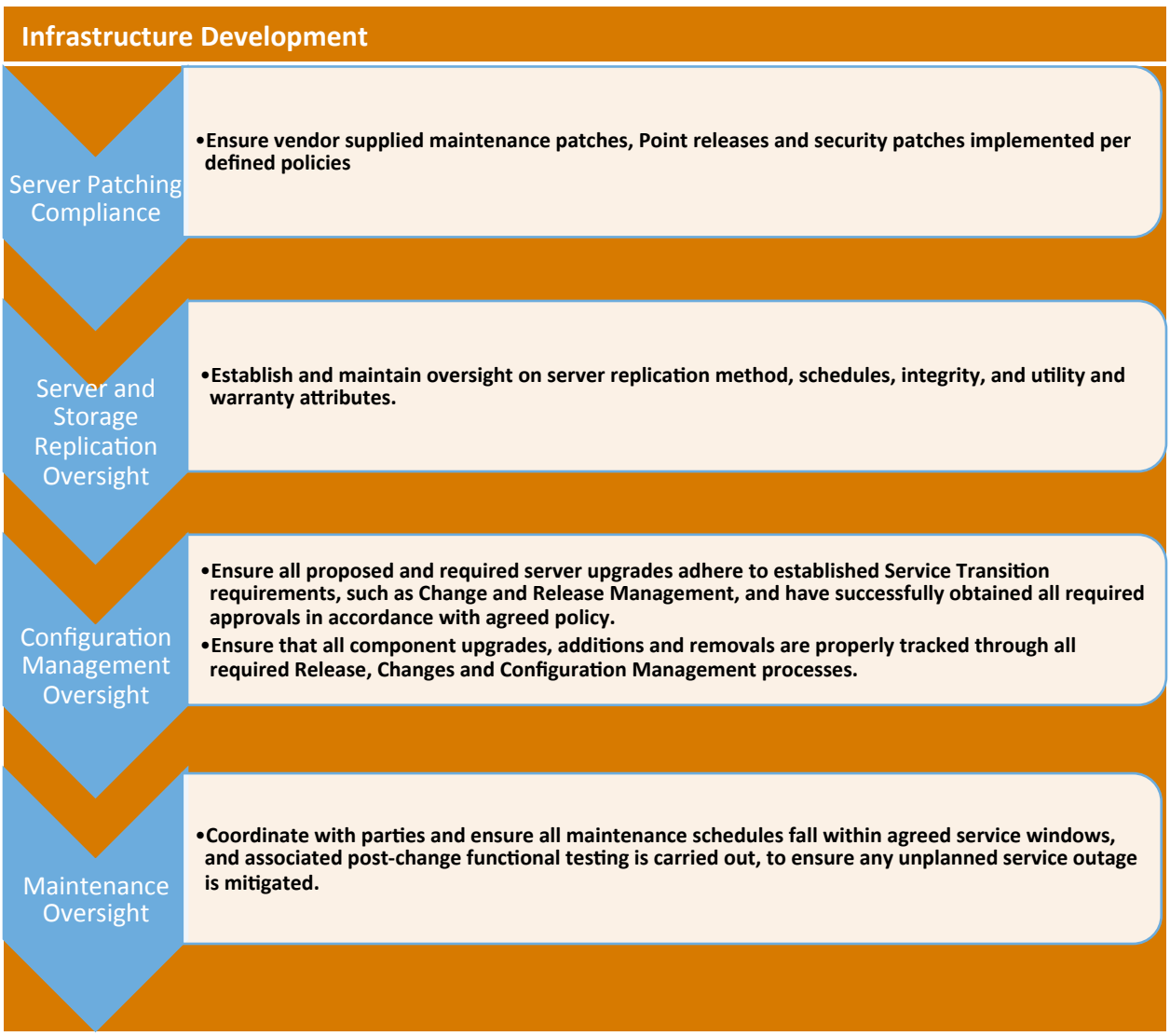
- **Perimeter Protection**
- **Intrusion Detection**
- **Advanced Network Forensics & Analysis**
- **Continuous Monitoring and Security Operations**

Luminologies

Business Continuity and Disaster Recovery Services

Based on defined event types ranging from security incidents (Ransomware, data corruption), major planned or unplanned maintenance events, or mandated by policy a robust mechanism to failover or redundant services are available to with high confidence of recovery.

•Below is a list of defined services to provide a robust BC/DR managed program



Luminologies

Business Continuity and Disaster Recovery Services

Business Continuity Process Development

Failover and Failback Runbooks Management

- Create and maintain all Runbooks related to the operation of the Secondary System.
- Develop process and control mechanisms to ensure that Runbooks are:
  - Updated, as required, and maintained in a current state; and
  - Are managed through to the Secondary System;

Major Event Notification and Response Management

- Review, and agree, a standard Priority Assessment and Classification schema and structured process – to ensure consistency.
- Create a process that coordinates back to a distinct Major Event trigger, and that coordinates escalations across multiple stakeholders, technical teams, and other parties, as required, and ensure that effective controls are enabled to enforce agreed Notification and associated Response protocols are followed, consistently..

Major Event Management

- Establish a framework that defines and coordinates the end-to-end response to Major Events that impact, or are likely to impact Business Services within the Avatar ecosystem.

Declarations to Invoke BC/DR Plans

- Develop a framework around making BC and/or DR declarations a managed and structured, collaborative exercise with clear protocols agreed by all parties in advance.
- The output of this exercise will be clear protocols used that ensure any DR Declaration is a result of a coordinated approach and collaborative engagement

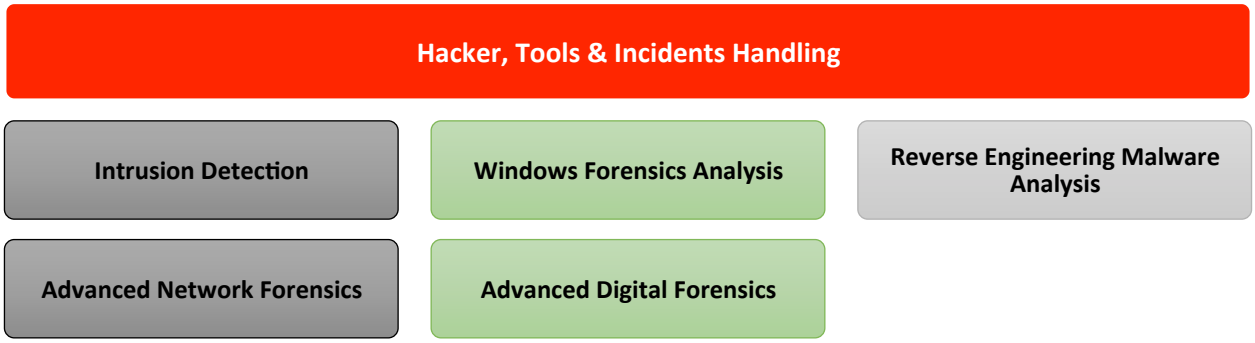
Coordination of Failover and Failback Processes

- As a subcomponent of an overall Service Continuance Strategy, ensure that clear protocols have been agreed and that DR Plans are validated (according to agreed schedules), and concise Implementation Plans (IPs) are maintained in a ready state that list ordered component and system startup sequences

Luminologies

Incident Response

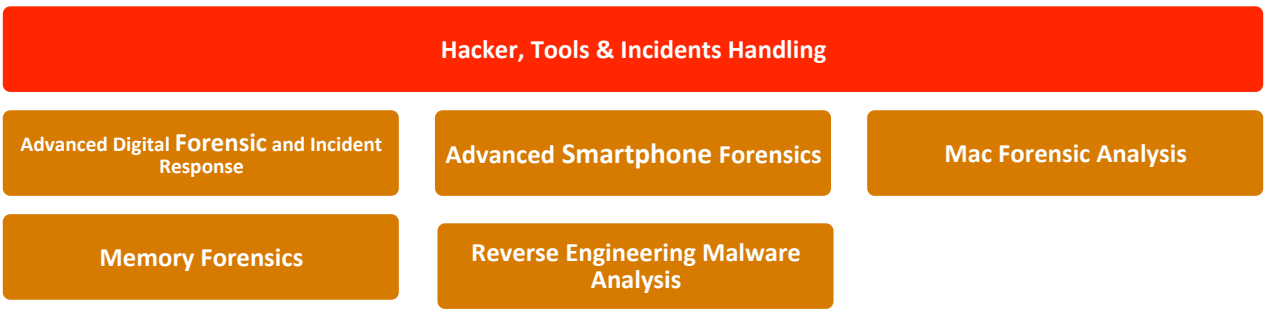
When the security of a system or network has been compromised, the incident responder is the first-line defense during the breach. The responders not only have to be technically astute, they must be able to handle stress under fire while navigating people, processes, and technology to help respond to and mitigate a security incident . Below courses are suitable for **Security Analyst/Engineer Cyber Threat Analyst Malware Analyst**



Digital Forensic Investigations and Media Exploitation

With today's ever-changing technologies and environments, it is inevitable that every organization will deal with cybercrime, including fraud, insider threats, industrial espionage, and phishing. Government organizations also need skilled personnel to perform media exploitation and recover key intelligence available on adversary systems. To help solve these challenges, organizations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together a comprehensive account of what happened

The courses below are suitable for people in following careers ;
Computer Crime , Investigators , Law Enforcement , Digital Investigations Analyst Media Exploitation Analyst IT litigation Support / Consultant Insider Threat Analyst



THANK YOU

luminologies.com