CYBER DEFENCE EAST AFRICA 2013

NASHERA HOTEL, MOROGORO, TANZANIA

28TH-30TH AUGUST

INTENSIVE THREE-DAY TRAINING ON CRITICAL SECURITY CONTROLS OR PENETRATION TESTING FOR INFORMATION SECURITY PROFESSIONALS, INFORMATION SYSTEMS AUDITORS, IT RISK PROFESSIONALS AND IT ENTHUSIASTS. SHOWCASE OF STATE-OF-ART TECHNOLOGIES. NETWORKING. KEYNOTES.

INVITATION

NRD Norway Registers Development

ISACA Trust in, and value from, information systems Tanzania Chapter

Critical IT infrastructure baip

SimbaNET ...Keeping Africa Ahead — Member of the Wananchi Group

FireEye

BalaBit IT Security

LETTER FROM ORGANISERS

Dear Participant,

On behalf of ISACA Tanzania Chapter and Norway Registers Development AS, we would like to invite you to attend the **Cyber Defence East Africa 2013** conference which will be taking place on the **28th-30th August in Morogoro, Tanzania.**

The importance of cyber security in Tanzania is increasing due to country's rapid development. More and more businesses and government institutions are conducting their activities online and, therefore, relying heavily on information technology. Smooth business activity often depends on a smooth functioning of IT infrastructure: inoperative applications, such as financial systems, e-mail or any other kind of database failure may cause many problems, lead to financial loss or even disrupt the activities of an organization. Rise in mobile money transactions, increasing importance of data and IT infrastructure's availability also heighten security concerns.

Furthermore, the scope, dynamics, and harm to organisations inflicted by cyber attacks have been intensively growing during the last years. The nature of the threats has changed significantly: before random attacks were dominant, now - targeted to certain persons or their groups, organisations. Cyber-crime is getting more industrialised, data leakage is becoming especially frequent.

As a consequence, international community is uniting and seeking for cooperation in order to stop cyber-crimes. European experience is very important for East Africa because manifestations of similar cyber threats are already present (data leakage, DDoS, resilience issues) while readiness to withstand them is still very low.

In order to assist organisations in creating a secure digital environment in Tanzania and whole East African region as well as maintaining trust of both citizens and foreign investors, ISACA Tanzania Chapter together with Norway Registers Development AS is organising intensive three-day **training** on **critical security controls** or **penetration testing** for information security professionals, information systems auditors, IT risk professionals and IT enthusiasts.

This event will help to get organizations up to speed in information security and prepare them to react appropriately and minimize the damage in case of a security incident. Motivating educational programmes are designed with a reference to the best security practices, standards of business ethics, legal regulations and principles of business continuity. Introductory security courses educate on the current cyber threats, the attack cycle, defence techniques, risk management, forensic challenges and incident response planning among many other things. Furthermore, during the event the biggest, industry leading cyber security vendors will showcase their state-of-art technologies. In addition, participants will have networking opportunities with colleagues from Tanzania, Kenya, Uganda and Zambia during unofficial meetings and the Gala Dinner. **Participating in this event will also offer an opportunity to earn 24 CPE hours.**

We believe that your participation in this conference will bring many benefits both to you and to your respective organisations. **Therefore, we are really looking forward to seeing you there.**

Yours Sincerely,
CDEA'13 organising committee

P.S. In this package you will find full conference agenda, training descriptions, speaker profiles, registration details and all other relevant information.

AGENDA

DAY 1. 28TH AUGUST, 2013

Time	Day 1	
8:30- 09:30	Arrival, registration and coffee	
09:30 - 09:45	Welcome: *Mr. Boniface Kanemba* and *Dr. Vilius Benetis*	
09:45 - 10:00	Cyber Security in Tanzania — Government Perspective, *Hon. January Y Makamba*	
10:00 - 11:00	Overview of Cyber Security trends in the world, *BAIP*	
11:00 -11:30	Data backup and resilience in the network, *Mr. Stanley Ayittah, SimbaNET*	
11:30 - 12:00	Tea Break	
12:00 - 13:30	Track 1	Track 2
13:30 - 14:30	Lunch	
14:30 - 16:00	Track 1	Track 2
16:00 - 16:30	Tea Break	
16:30 - 18:00	Track 1	Track 2

DAY 2. 29TH AUGUST, 2013

Time	Day 2	
8:30 - 09:45	FireEye's appliances for defence against advanced Malware, Zero Day & Targeted APT attacks	How to defend your security perimeter ?
09:45 - 10:00	Break	
10:00 - 11:30	Efficient automation of your IT Governance, Risk, and Compliance from Lumension	Secure your desktops and servers – with Application and Device Control, Patch and re-mediation from Lumension
11:30 - 12:00	Tea Break	
12:00 - 13:30	Track 1	Track 2
13:30 - 14:30	Lunch	
14:30 - 16:00	Track 1	Track 2
16:00 - 16:30	Tea Break	
16:30 - 18:00	Track 1	Track 2
20:00 - 23:00	Gala Dinner	

DAY 3. 30TH AUGUST, 2013

Time	Day3	
8:30 - 09:30	Privileged User Monitoring with Balabit SCB	Vulnerability management with QualysGuard® in order to reduce the attack surface of your IT
09:30- 09:45	Break	
09:45 - 10:45	Security Intelligence and SIEM from IBM Q1Labs	Forensics ToolKit (FTK) for Incident response
10:45 - 11:00	Tea Break	
11:00 - 13:00	Track 1	Track 2
13:00 - 14:00	Lunch	
14:00 - 16:00	Track 1	Track 2

*Please note that organisers reserve the right to change the agenda and the speakers of the event. Content of the trainings is a non-changing part of the conference.

Keynote speakers

We are delighted to present you these prominent personalities that will open our conference. They will look into the topic of cyber defence with a reference to their own specific fields of expertise.

Hon. January Y Makamba,
Tanzania MP & DM — CST.

Hon. January Yusuph Makamba is the Deputy Minister - Communication, Science & Technology at The Government of The United Republic of Tanzania, a Ministry which is responsible for policy making for Information Communication Technology, including cyber security matters.

Hon. Makamba is also a Member of Parliament (MP) for Bumbuli constituency in the Tanzanian National Assembly. He also serves as Politics & Foreign Relations Secretary at Chama Cha Mapinduzi (CCM). Prior to this post Honorable Makamba worked as Senior Aide to the President at The Presidency, United Republic of Tanzania.

Hon. Makamba holds Master of Science (M.Sc.), Conflict Analysis and Resolution and Bachelor's degree, Peace Studies and Conflict Resolution both from United States.

During the opening ceremony of the CDEA'13 Hon Makamba will deliver a speech on "Cyber Security in Tanzania – Government perspective".

Mr. Boniface Kanemba,

ISACA Tanzania
Chapter President.

Mr. Boniface Kanemba is a Senior Systems Auditor and the President of ISACA Tanzania Chapter, independent, non-profit, global association, actively involved in the development and implementation of consultative Tanzanian National Cyber security framework.

Mr. Kanemba derives his experience from implementation of ICT projects in the National Social Security Fund (NSSF), extensive trainings on Internet security and Cyber Laws (Singapore), IT Security Coordination and Computer Forensics (Germany) and multiple international conferences on the Information Security.

Mr. Kanemba holds Master of Science (M.Sc.) in Computer Security and Audit from Greenwich University (UK), Postgraduate Diploma in Information Security and Assurance and Postgraduate Diploma in Scientific Computing.

Mr. Kanemba will look at the cyber security from a perspective of a non-profit organisation. He will deliver a speech on "The role of ISACA in promoting Cyber Defence in Tanzania".

Mr. Stanley Ayittah,
General Manager,
SimbaNET (T) Ltd

Mr. Stanley Ayittah is the General Manager of SimbaNET (T) Ltd, a Leading data operator offering a range of services ranging from Internet and Data connectivity to Web, mail & Domain Hosting, Co-location of servers, and many other services.

He has been active on the Tanzania Internet industry for a over 10 years.

Prior to SimbaNET he was also the General Manager of Africa Online (T) Ltd, the Head of Business for iWayAfrica Tanzania and also SkyVision Global Networks for East and South Africa.

He has worked on various cutting edge solutions for various Corporate and Government establishment across Tanzania.

He is currently the vice- Chairman of Tanzania Internet Services Providers Association (TISPA).

Technology Specialists

Mr. Ala' Khalil,
Regional Channel Manager of FireEye Middle East, Turkey and Africa

Mr. Khalil holds Bachelor Degree in Electrical and Computer Engineering. Ala' has over 12 years of experience in Systems Engineering, Consulting and Business and Channel Development in the Information Security and Networking Space. In his position Ala' is responsible for FireEye Channel Strategy in the region including partner recruitment and enablement. Prior to FireEye, Ala' worked for several Leading Security Vendors, Value Added Distributors and System Integrators in the Middle East.

Mr. Khalil will be show a simulation of an APT attack with and without FireEye.

TRAINER PROFILES

MR. SEBASTIAN MARONDO,
CHIEF EXECUTIVE OFFICER NRD EA,
INFORMATION SECURITY EXPERT.

Mr. Marondo is an information security expert and auditor with more than 6 years experience and achievement across the whole spectrum of technical aspects of Information Technology, Information Security, Business Continuity, Networking, Systems Integration and physical security in Information and Communications Technology (ICT).

In the past 5 years he has been in various industries include Banks (NMB, Akiba Commercial Bank), private sector (software development and consultancy), and Government (IFM, TRA and National Audit office). Also Sebastian worked on various projects include information system audit for United Nation organizations, UNFPA, UNON, UNEP, ICTR and UN-Habitat. ERP implementation for Zanzibar Telecommunication (ZANTEL), Zambia Telecommunication (ZAMTEL), Fraud investigation and Risk Assessment to various clients.

Sebastian Marondo holds MBA in International Business, Certified Information System Auditor (CISA), Certified Information Security Manager (CISM) both from ISACA.

MR. AUGUSTAS GUTAUTAS,
EXPERIENCED IT SECURITY AND INFRASTRUCTURE PROFESSIONAL, NRD

Mr. Gutautas is an experienced IT security and infrastructure professional with more than 10 years of experience in international projects including but not limited to Lithuania, Latvia, Norway, Denmark, United Kingdom, Belarus, France, Thailand, Tanzania and Burundi. Augustas has educational background of Complexity Management in area of ICT. His work experience ranges from high availability solutions, architecture design, disaster recovery solutions as well as design and implementation of critical IT infrastructures and security controls, cyber security solutions and security assessments, penetrations testing in banks, financial institutions, telecoms and government institutions.

Mr. Augustas Gutautas has been leading international projects and has been actively involved in international activities of the company acting as a team leader, consultant and project manager through various stages of engagements starting from proposal preparation to project delivery and support.

Augustas Gutautas has BSc Computing and Systems Practice from UK, has been lecturing in Bujumbura ISGI University, Burundi.

Dr. Vilius Benetis,
CISA, CRISC
Senior Cyber Security Consultant, NRD

Dr. Vilius Benetis, CISA, CRISC is a senior consultant, focusing on cyber security, IT infrastructure audit and IT infrastructure architecture optimisation. He has been leading several projects on optimisation of IT infrastructure and data centres towards effectiveness, security (ISO 27001 based, as well as general security baselining) and Service management (ITIL).

Vilius Benetis specialises in Public Sector Information Security Consulting, IT Infrastructure Architecture, IT Audit Security Audits, Compliance Audits, Risk Assessment, IT security automatization (IAM, log and SIEM, encryption, security in depth, server security baselining, vulnerability management, patch and remediation, end point control, privileged user management, network segregation), Telecommunications Engineering and Compliance Management.

Dr. Benetis is one of the authors of the newly released ISACA publication “Transforming Cybersecurity: Using COBIT® 5“ and a subject matter expert reviewer of ISACA’s "Responding to targeted Cyber attacks".

Vilius has graduated from Kaunas Technical University, as well as from Danish Technical University in BSc in Computer Science, MSc and PhD in Teletraffic Engineering. Vilius has been on fellowship in Tsinghua University Hitachi Labs. He has as well extensive experience in corporate environment (Motorola, CA technologies, Dell), where he was supporting IT services and management project sales and implementations.

YOU ARE KINDLY INVITED TO CHOOSE ONE OF THE TRACKS WHEN REGISTERING:

TRACK 1: CRITICAL SECURITY CONTROLS TRAINING

The 20 critical security controls are set of controls recommended and complied by consortium of more than 100 contributors from government agencies, commercial forensic experts and penetration testers. These controls are minimum recommendations for organizations to implement in order to block or mitigate known attacks. They are the baseline of high-priority information security measures and controls that can be applied across an organization in order to improve its cyber defence. The controls are designed so that primarily automated means can be used to implement, enforce and monitor them.

The security controls give no-nonsense, actionable recommendations for cyber security, written in a language that is easily understood by IT personnel. The goal of 20 critical security controls is to leverage cyber offense to inform cyber defence, focusing on high payoff areas, ensure that security investments are focused to counter highest threats, maximize use of automation to enforce security controls, thereby negating human errors, and use consensus process to collect best ideas.

It focuses on various technical measures and activities, with the primary goal of helping organizations to prioritise their efforts to defend against the current most common and the most damaging computer and network attacks. The 20 controls and supporting advice are dynamic in order that they recognize changing technology and methods of attack.

The strength of the Critical Controls is that they reflect the combined knowledge of actual attacks and effective defences of experts in the many organizations that have exclusive and deep knowledge about the current threats. These experts come from multiple agencies of the U.S. Department of Defense, Nuclear Laboratories of the U.S. Department of Energy, the U.S. Computer Emergency Readiness Team of the U.S. Department of Homeland Security, the United Kingdom's Centre for the Protection of Critical Infrastructure, the FBI and other law enforcement agencies, the Australian Defense Signals Directorate and government and civilian penetration testers and incident handlers.

Top experts from all these organizations have pooled their extensive first-hand knowledge of actual cyber attacks and developed a consensus list of the best defensive techniques to stop them. This has ensured that the Critical Controls are the most effective and specific set of technical measures available to detect, prevent, and mitigate damage from the most common and damaging of those attacks.

OBJECTIVE OF THE TRAINING IS TO PROVIDE IN DEPTH UNDERSTANDING ON ALL 20 CRITICAL SECURITY CONTROLS.

→ Introduction to 20 critical security controls;
→ Main concepts:

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

→ Implementation and auditing of 20 critical controls.

Track 2: Penetration Testing training

As the world is advancing in use of cyber space with multi-tier network architectures, high speed connection, Web services, custom applications, and heterogeneous server platform environments, keeping data and information assets secure is more difficult than ever. This combination has formed complex systems that criminal organizations have organized their hacking efforts to break in; it is no longer just "script kiddies" trying to break into your network, but advanced technology is being used which includes supercomputing and distributed intelligent systems.

Although there are many ways to secure systems and applications, the only way to truly know how secure you are is to test yourself. By performing penetration tests against your environment, you can actually replicate the types of actions that a malicious attacker would take, giving you a more accurate representation of your security posture at any given time. Although most penetration testing methods have traditionally been somewhat ad-hoc, that has changed in the last several years. Robust, repeatable testing methodologies now exist, and high quality commercial tools can be implemented to ensure that both testing parameters and results are high-quality and trustworthy. Penetration testing provides an excellent view of the actual security state of an environment as well as organization's security state.

With penetration testing one can evaluate computer and network security by simulating an attack on a computer system or network from external and internal threats. This may include: attempt to gain access to resources without knowledge of usernames, passwords and other normal means of access. If the focus is on computer resources, then examples of a successful penetration would be obtaining or subverting confidential documents, pricelists, databases and other protected information. This process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, and operational weaknesses in the process or technical countermeasures. The main thing that separates a penetration tester from an attacker is permission. The penetration tester will have permission from the owner of the computing resources that are being tested and will be responsible to provide a report.

The ultimate goal of penetration testing is to seek improvement of the system and resources which are being tested.

Objective of the training is to provide in depth understanding on the following concepts:

→ Penetration Testing;
→ Security Assessments;
→ Automated Testing;
→ Manual Testing;
→ Enumerating Devices;
→ Denial of Service Emulation;
→ Web Application testing;
→ Tools for conducting tests.

To achieve these objectives, the following topics are to be covered:

→ Penetration Testing Concepts;
→ Types of Pen testing;
→ Pen testing techniques;
→ Pen testing phases;
→ Penetration Testing Tools.

TECHNOLOGY DEMONSTRATIONS

When your organisation is designing a new information security infrastructure or when there is a need to update the old infrastructure with specific functions, renew or purchase software or hardware, you face a difficult challenge of having to choose the technology that best suits your needs.

In order to make this choice a more informed one, during the CDEA'13 we are going to introduce you to a set of proven, effective, state-of-art technologies and tools. After the demonstrations you will understand the purpose, benefits and operational features of these industry-standard and leading technology solutions.

FIREEYE'S APPLIANCES FOR DEFENCE AGAINST ADVANCED MALWARE, ZERO DAY & TARGETED APT ATTACKS

The challenge in defending against advanced persistent threats comes from their complex and sophisticated nature (low-volume, professional, highly customized, well-funded, combining multiple methodologies) and their ability to threaten even the most protected information systems, especially if they rely on traditional, signature-based security techniques such as content-scanning, sender verification, reputation and creation of safe/unsafe lists.

FireEye(R) has invented a purpose-built, virtual machine-based security platform that provides real time threat protection against the next generation of cyber attacks. The FireEye platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including Web, email, and files. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time.

FireEye appliances provide integrated Web & Email Protection via full automated virtual execution engines, which run code and observe behavior in order to notice malicious activity, and stop its movement via email attachments (documents), or download. Additionally, they block botnet command and control communication.

During the Cyber Defence East Africa 2013 FireEye representative will provide live demonstration of three APT protection appliances:

• Web Security - The Web Malware Protection System stops Web-based attacks that traditional and next-generation firewalls, IPS, AV, and Web gateways miss. It protects against zero-day Web exploits and multi-protocol callbacks to keep sensitive data and systems safe.

• Email Security - The FireEye Email Malware Protection System secures against spear phishing email attacks that bypass anti-spam and reputation-based technologies. The integrated Email MPS and Web MPS offers the only solution to address blended, advanced targeted attacks using spear phishing, zero-day exploits and malicious URLs.

• Central Management System - The Central Management System consolidates the management, reporting, and data sharing of Web MPS, Email MPS, File MPS, and Malware Analysis Systems in an easy-to-deploy, network-based appliance.

Efficient automation of your IT Governance, Risk, and Compliance from Lumension

Organisations often lack the ability to identify, measure, manage, monitor, review and report on IT risks and compliance gaps. However, failure to monitor organisation's security state, track IT security metrics and map this information with business risk might cause business disruption, loss of important data and non-compliance with both internal policies and external regulations. This session will demo how you can fast-track in easy and cheap way compliance and risk management process for your organisation. From asset identification to threat remediation plans with something even simpler than with Excel.

Lumension® Risk Manager enables you to automate the compliance and IT risk management workflow, providing clear visibility of IT risk across your entire network. Risk Manager simplifies and facilitates the enterprise risk and compliance management process in the field of IT GRC (governance, risk, and compliance). Administrative overhead is reduced by using automation, work flow, and a central repository for relevant key information. Risk Manager enables security engineers to manage day-to-day tasks effectively and run security assessments. Risk Manager also allows upper-level management to view reports and check metrics through the Home tab dashboard.

Lumension Risk Manager combines risk management and compliance management into a single process. This streamlines risk assessment and remediation.

Risk management and compliance management are often treated as separate enterprise IT security processes. While each organization has a unique business process around these areas, they include similar elements. Overlap is specifically related to defining control requirements for IT resources and assessing implementation of the required risk management controls for the resources. Lumension Risk Manager correlates IT resources, business interests, compliance regulations, and controls with a scoring framework.

Lumension Risk Manager gives you a comprehensive risk compliance view spanning hundreds of global regulations, mandates and internal policies. This comprehensive view improves the efficiency of controls and reduces risk. Risk Manager provides the flexibility to easily accommodate evolving requirements and enable real-time visibility of the level of compliance achieved. Risk Manager enables visibility for compliance and risk through four key capabilities:

- Risk profiling
- Risk and compliance reporting
- Controls framework
- Controls assessment

Secure your desktops and servers – with Application and Device Control, Patch and remediation from Lumension

Outdated endpoint software patch management creates an easy path for cyber criminals. By eliminating vulnerabilities in third party applications and heterogeneous operating systems, IT risk can be effectively reduced, while endpoint operations can be improved. However, it is time consuming, costly and difficult to manually keep up and apply security or software changes across the entire organization. During this demonstration you will be introduced to Lumension® Endpoint Management and Security Suite—an agile solution suite that reduces complexity for both security and IT operations teams, optimizes TCO, improves visibility and delivers control back to IT.

Lumension® Endpoint Management and Security Suite:

- More effective endpoint security
- Holistic visibility and policy management between IT ops & security
- Centralized agent management and reportin
- Modularly licensed products
- Scalable and agile architecture

The Lumension® Endpoint Management and Security Suite:

- Reduces complexity and TCO via an agile, single console, single agent, single server architecture that can manage thousands of endpoints regardless of their location.
- Delivers best-of-breed, modularly licensed, product capabilities that meet growing IT requirements.
- Unifies IT operational and security workflows to enable greater control, visibility, and more effective policy management while still allowing for customized, role-based user interfaces to be assigned.
- Simplifies management of systems, agents and policies in real time - from a single console.
- Optimizes resources by extending policy or remediation efforts to a single endpoint or group.
- Centralizes reporting and logging to increase accuracy, reduce the compliance burden, and enhance visibility.

Lumension® Endpoint Management and Security Suite for Endpoint Operations

- Lumension® Patch and Remediation - Reduces organizational risk and optimizes IT operations through the timely, proactive elimination of operating system and application vulnerabilities across all endpoints and servers. Heterogeneous platform and 3rd party vulnerability content support includes Microsoft® Windows®, UNIX®, Linux® Mac®, Adobe® and more.
- Lumension® Security Configuration Management - Ensures that endpoints are securely configured and in compliance with industry best practices and regulatory mandates while reducing configuration drift.
- Lumension® Power Management - Reduces endpoint power consumption costs of both online and offline endpoints, with enhanced Wake-on-LAN capability to ensure endpoints are available for management and to maintain security posture.
- Lumension® Content Wizard - Delivers customized extensibility through wizard-driven and custom scripting tools to take any action on endpoints including deploying and removing software, remediating configurations, performing systems management tasks and delivering custom patches.
- Lumension® Reporting Services - Provides integrated, pre-configured and centralized business intelligence which can be customized to meet organizational needs.

Lumension® Endpoint Management and Security Suite for Endpoint Security

- Lumension® Application Control - Defines and enforces trusted application usage through whitelist policies to ensure that only applications explicitly authorized or trusted are allowed to execute. Includes Advanced Memory Protection to defend against sophisticated memory injection attacks.
- Lumension® AntiVirus - Provides blacklist protection and removal for all malware including viruses, worms, spyware, Trojans and adware.
- Lumension® Device Control - Enforces usage policies for device and ports while providing data encryption for removable media to prevent data loss / theft.
- Lumension® Disk Encryption - Reduces risks and costs of data breach when workstation is lost or stolen via with transparent and easy-to-use full disk encryption.
- Lumension® Intelligent Whitelisting™ - Integrates Lumension® AntiVirus, Lumension® Application Control and Lumension® Patch and Remediation into a seamless solution workflow that dramatically improves your overall security posture, reduces your operational headaches and reclaims control of your endpoints.

Privileged User Monitoring with Balabit SCB

The human factor is a common cause of security breaches. Privileged users' accounts are especially vulnerable because these users are able to directly access and manipulate sensitive information. Therefore, mismanagement of privileged identities puts your company at tremendous risk. However, at the same time, privileged accounts are especially difficult to manage and trace. During this demonstration, practical demos, user experience and practical case scenarios where instruments must be deployed to ensure security will be presented.

Balabit Shell Control Box is an activity monitoring appliance that controls privileged access to remote servers and networking devices and records activities in movie-like audit trails that can be searched and replayed. All data is stored in encrypted, timestamped and signed files, preventing any modification or manipulation. In case of any problems (server misconfiguration, database manipulation, unexpected shutdown) the circumstances of the event are readily available in the audit trails, thus the cause of the incident can be easily identified.

SCB is a proxy gateway: the transferred connections and traffic are inspected on the application level, giv-

Benefits for the IT

- Turnkey appliance for privileged user monitoring
- Fast deployment, low OPEX
- Centralized authentication & access control
- Faster and higher quality security audits
- Lower troubleshooting and forensics costs
- Easy scalability and HA option
- Direct 7/24 vendor support (option)

Benefits for the Business

- Improved regulatory and industry compliance
- Better employee & partner control
- Improved accountability of staff
- Strong evidence in legal proceedings
- Enhanced security against human risks

Modes of operation

Different operation modes: transparent bridge, router, and bastion mode. To simplify integration with firewalled environments, SCB supports both source and destination address translation (SNAT and DNAT). Can be configured in HA mode for DRP scenarios.

Integration with other security systems and directories

SCB can also remove the encryption from the traffic and forward the unencrypted traffic to an Intrusion Detection System (IDS), making it possible to analyze the contents of the encrypted traffic. That way traffic that was so far inaccessible for IDS analyzes can be inspected real-time. Other protocols tunneled in SSH can be inspected as well. Similarly, the list of files transferred and accessed in the encrypted protocols can be sent to a Data Leakage Prevention (DLP) system.

SCB can connect to a remote LDAP database (for example, a Microsoft Active Directory server) to resolve the group memberships of the users who access the protected servers. Rules and policies can be defined based on group memberships. When using public-key authentication in SSH, SCB can authenticate the user against the key or X.509 certificate stored in the LDAP database.

Administrators and auditors accessing the web interface of SCB can also be authenticated to an LDAP database. RADIUS authentication (for example, using SecurID) is also supported both for accessing the web interface, and also to authenticate the audited SSH sessions.

Application areas

Remote sessions auditing (recording) is a solution for your organization if you:

- need to implement policy compliance (PCI DSS, SOX, HIPAA, Basel II Accord etc.),
- have outsourced or out-tasked IT,
- allow remote IT management,
- use thin clients,
- need to monitor file transfers or access in real time,
- need to control SSH,
- use jump hosts.

Vulnerability management with QualysGuard in order to reduce the attack surface of your IT

Most of the cyber attacks exploit known security flaws for which remediation are available because organisations fail to manage and patch these vulnerabilities effectively. Vulnerability Management software helps to maintain control over your network security by automatically identifying security vulnerabilities with external and internal scans, prioritising them according to the severity levels and impact on business, providing extensive, centralised reports (for both executive level and technical personnel) and verified remedies.

QualysGuard® Vulnerability Management (VM) automates the lifecycle of network auditing and vulnerability management across the enterprise, including network discovery and mapping, asset prioritization, vulnerability assessment reporting and remediation tracking according to business risk. Driven by the most comprehensive vulnerability KnowledgeBase in the industry, QualysGuard delivers continuous protection against the latest worms and security threats without the substantial cost, resource and deployment issues associated with traditional software. As an on demand Software-as-a-Service (SaaS) solution, there is no infrastructure to deploy or manage, besides dropped virtual or physical scanner probe, fully instructed from SaaS.

QualysGuard VM enables small to large organizations to effectively manage their vulnerabilities and maintain control over their network security with centralized reports, verified remedies, and full remediation workflow capabilities with trouble tickets. QualysGuard provides comprehensive reports on vulnerabilities including severity levels, time to fix estimates and impact on business, plus trend analysis on security issues.

By continuously and proactively monitoring all network access points, QualysGuard VM dramatically reduces security managers' time researching, scanning and fixing network exposures and enables companies to eliminate network vulnerabilities before they can be exploited.

QualysGuard® Features

Manage Your Network Assets

QualysGuard VM helps you prioritize and fix vulnerabilities intelligently — tailored to your needs. Rapidly identify, visualize and organize your network assets into Business Units and Asset Groups. Define your "mission critical" assets by their importance to your business operations using a 5 tier rating system from Low to Critical.

Identify Network Security Vulnerabilities

Driven by the largest and most up-to-date KnowledgeBase of vulnerability checks in the industry, QualysGuard's external and internal scanners safely and accurately detect security vulnerabilities across your entire network. As an on demand service, new signatures are delivered weekly, giving users the ability to scan for the latest threats. QualysGuard's extremely accurate scans eliminate the time drain of chasing false positives, false negatives and host crashes.

Analyze Threats with Powerful Reporting

Intuitive and easy-to-read reports provide both executive-level summaries and detailed technical analysis. QualysGuard VM provides a detailed description for each vulnerability that includes: the security threat, consequences if the vulnerability is exploited, and the recommended solution to fix the vulnerability, including links to the appropriate patches. QualysGuard provides powerful reporting options. You can build your own customized reports, or use the report templates provided by Qualys.

Exploitability Information

QualysGuard Vulnerability Management (VM) includes correlated exploitability information from real-time feeds to provide customers with up-to-date references to exploits and related security resources. With this feature customers running vulnerability scans can easily view the latest correlated exploits from third party vendors including Core Security, Immunity, Exploit Kits, The Exploit DB, and Metasploit. This helps customers to prioritize remediation activities according to risk assessment performed by the correlated running exploits.

Manage and Eliminate Your Network Vulnerabilities

QualysGuard's integrated remediation and trouble-ticketing workflow system is highly automated. The system generates tickets based on your policy rules and tracks each vulnerability until it is verifiably fixed. Each remediation ticket is assigned a unique number and includes: general information, vulnerability details, remediation history and actions. During the next scan, QualysGuard automatically verifies that vulnerabilities are fixed and automatically closes the tickets. QualysGuard VM also provides an array of remediation reports providing security managers with a current snapshot on remediation status and progress.

Executive Dashboard

The executive dashboard provides a summary of your overall security posture. The dashboard displays the number of New, Active and Reopened vulnerabilities, and a graph with vulnerabilities by severity level. From the dashboard, you can start and schedule new vulnerability scans, view a list of the most vulnerable hosts in your account, download reports and more.

Asset Tagging

Asset tags allow you to tag assets with custom information for enhanced classification levels and tracking. QualysGuard asset tags can be customized for each scan, and provide a powerful way to tag, track and manage every networked device. And QualysGuard provides additional asset qualification levels, allowing customers to group assets into specific business units in any way desired. This provides businesses a powerful way to track and manage networked devices.

Security Intelligence and SIEM from IBM Q1Labs

Failure to effectively manage the massive amount of data generated in the event logs that network, security and other devices collect, perform the necessary analysis and respond to detected anomalous user behaviours and suspicious events can have a serious impact on the information security of the organisation. Toughest correlation and visibility engine for Security information and event management from IBM will be explained and demoed. Value will be dissected and shown what to evaluate in SIEM functionality and why – everything in clear language, understood by everyone.

Q1Labs QRadar SIEM is an appliance, which is the market leader for Security Information and Event Management, for centralized operational security information in organization - i.e. core engine for Security Operations Center.

QRadar SIEM provides an integrated network security solution that converges typically siloed network and security information into a single, cohesive system. QRadar SIEM's unique approach enables organizations to deliver an unparalleled set of network security intelligence services, including:

- Log management
- Threat/Fraud management
- Compliance management
- Security Event and Information Management
- User Activity Monitoring
- Application Monitoring

Unique and mandatory features for successful SIEM are cross-correlation of monitored Logs, flow-metadata and vulnerability data, together with global intelligence feeds about bad and malicious internet resources (IP addresses, etc.)

Network Activity Collectors:

QRadar's Network Activity Collectors offer a cost-effective solution for gathering the most sophisticated and actionable network intelligence (flow data) available from your network. Network Actvity "QFlow" Collectors provide Layer 7 analysis as well as aggregation of other flow sources including JFlow, NetFlow, SFlow, and Packeteer's Flow Data Records, delivering an unmatched level of IT security intelligence for the most complete collection of activity possible.

Virtual Activity Collectors:

Like QRadar's Network Activity Collectors, QRadar's Virtual Activity Collectors offer a cost-effective solution for gathering the most sophisticated and actionable network activity data available from your network including Layer 7 analysis and aggregation of external flow sources but also, by providing unique visibility into the activity within your virtual environment.

QRadar SIEM provides full visibility and actionable insight to protect networks and IT assets from a wide range of advanced threats, while meeting critical compliance mandates.

Key Capabilities

• Sophisticated correlation of events, flows, assets, topologies, vulnerabilities and external data to identify & prioritize threats
• Network flow capture and analysis for deep application insight
• Workflow management to fully track threats and ensure resolution
• Scalable architecture to support the largest deployments

Benefits

• Reduce the risk and severity of security breaches
• Remediate security incidents faster and more thoroughly
• Ensure regulatory and internal policy compliance
• Reduce manual effort of security intelligence operations

Advantages

• Real-time activity correlation based on advanced in-memory technology and widest set of contextual data
• Flow capture and analysis that delivers Layer 7 content visibility and supports deep forensic examination
• Intelligent incident analysis that reduces false positives and manual effort
• Unique combination of fast free-text search and analysis of normalized data
• Scalability for world's largest deployments, using an embedded database and unified data architecture

Forensics ToolKit (FTK) for Incident response

Even if your organisation is effectively protecting all of the weakest parts and all of the main resources, it is still vulnerable because there is no way to know the time, tools, direction and goals of a possible cyber-attack. Therefore, it is important that in case of fraud, intellectual property theft, industrial espionage, network compromises, employee misuse or malware you have the right knowledge and tools to properly handle a forensics investigation. During this session you will be introduced to the use cases and will see a demo session with AccessData FTK and ADLab. Who, when, what and why needs forensics tools? What benefits they bring? How these tools are compare to alternatives? Why you should care becoming a Certified Examiner?

AccessData Forensics Toolkit (FTK) is market leading tool for IT forensics examiners for many years.

Integrated Computer Forensics Solution

- Create images, process a wide range of data types from forensic images to email archives, analyze the registry, conduct an investigation, decrypt files, crack passwords, and build a report all with a single solution.
- Recover passwords from 100+ applications.
- KFF hash library with 45 million hashes.
- Advanced, automated analysis without the scripting.

Unlike other products on the market, FTK **is database driven so you will not experience the crashing associated with memory-based tools.** In addition FTK components are compartmentalized, so for example, if the GUI crashes, the processing workers continue to process data.

Unmatched processing

FTK is different from other computer forensics solutions in that it processes data up front, so you're not wasting time waiting for searches to execute during the analysis phase. However, the product is designed to provide the fastest, most accurate and consistent forensic processing possible with distributed processing and true multi-threaded / multi-core support. Every copy of FTK includes a total of 4 processing workers – 1 on the examiner machine and 3 distributed. If you are interested in having multiple examiners share a common processing farm and centralized database for collaborative analysis, please contact your sales representative to inquire about AccessData Lab.

- Wizard-driven processing ensures no data is missed.
    - Cancel/Pause/Resume functionality
    - Real-time processing status
    - CPU resource throttling
    - Email notification upon processing completion
- Pre- and post-processing refinement
- Advanced data carving engine allows you to specify criteria, such as file size, data type and pixel size to reduce the amount of irrelevant data carved while increasing overall thoroughness.

Single-node enterprise

Install a persistent or "dissolving" agent on a single computer to enable the remote analysis and incident response capabilities of AD Enterprise. Preview, acquire and analyze hard drive data, peripheral device data, and volatile/memory data on Apple® , UNIX® and Linux® operating systems. Uninstall the agent at any time, and push it out to a different computer for multi-machine analysis.

- Easy, wizard-driven agent deployment.
- Secure remote device mounting using the Pico agent

- Advanced Volatile/Memory analysis
- Exceptional Apple® OS Analysis
- Faster, more comprehensive index and binary searching
- Broad file system. File type and email support
- Broad encryption support
    - **FTK is the only computer forensics solution that can identify encrypted PDFs.**
- Explicit image detection (EID) add-on
    - This image detection technology not only recognizes flesh tones, but has been trained on a library of more than 30,000 images to enable auto-identification of potentially pornographic images.

Rich reporting

- Generate detailed reports in native format, HTML, PDF, XML, RTF, and more – with links back to the original evidence.
- Define Registry Supplemental Reports (RSR) during pre-processing or additional analysis.
- See which files could not be processed or indexed with the Processing Exception/Case Info report.
- Create a CSV of processed files that can be imported into Excel or a database application.
- Export MSGs for all supported email types.

VENUE AND ACCOMODATION

The event will take place at the **Nashera Hotel**, a four-star hotel, located just over 3km from the centre of Morogoro and defined by the panoramic views of the Uluguru Moutain.

Room reservations for the conference participants are offered at corporate rates.

	B&B	Half Board
Deluxe	$115	$135
Twin	$145	$165
Executive suit	$250	$270

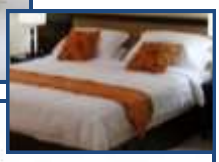
AFTER THE TRAININGS YOU WILL HAVE AN OPPORTUNITY TO CONTINUE DISCUSSIONS WITH OTHER PARTICIPANTS IN A MORE RELAXED AND INFORMAL ENVIRONMENT OR ENJOY ONE OF MANY OTHER ATTRACTIONS THAT THE NASHERA HOTEL AND MOROGORO HAVE TO OFFER.

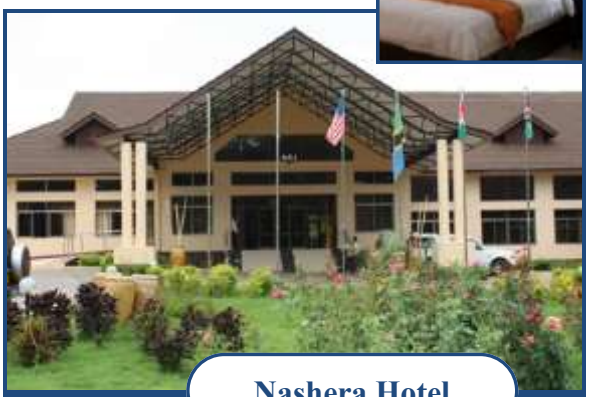
On site attractions:

→ Volleyball court
→ Pool
→ Zumba - lessons available (5,000 tsh/pp)
→ Souvenir shop
→ Outdoor BBQ area
→ Morning/evening walks up road at foot of mountain
→ Hike/Trek from hotel through beautiful Uluguru Mountains (4hrs to peak)
→ Travel Counter for Safari Arrangements
→ Massage Service

GALA DINNER

The conference programme also includes a Gala Dinner on the 29th August. This event will provide an opportunity for networking with your trainers and around 100 other information systems auditors, IT risk professionals and IT enthusiasts from the most successful, innovative and influential companies with East African presence.





Nashera Hotel

Boma Road, LITI Area, P.O. Box 237
Morogoro, Tanzania

Phone: +255 716 678233

Email: info@nasherahotels.com

Off site attractions:

→ Morogoro Golf Club - a 9 Hole Golf Course facility within 5 minutes of Nashera (no driving range, vintage sand greens, approx. $10 for 9 holes, private rental sets may be available upon request)
→ Masai Market visit (Friday's 9am-4pm)
→ Local shops
→ Nearby Mikumi
→ Sustainable Tourism Opportunities through Chilunga Cultural Tourism Program (http://www.chilunga.or.tz/)
  → Where one can visit old German settlements
  → Visit Traditional Healers
  → Can see what the local nature offers such as waterfalls and bird watching.
  → A number of restaurants serving a range of local and international cuisine can also be found within 5 min. drive of the property.

REGISTRATION AND TICKETS

You are kindly invited to register for the conference by sending an email to registration@nrd.no. Please write your name, organisation, title and which training track (Track 1/Track2) you are choosing.

DEADLINE FOR BOOKING: 25th August 2013.
ON-SITE REGISTRATION WILL NOT BE AVAILABLE. PLEASE BOOK IN ADVANCE.

INCLUDED IN YOUR TICKET:

⇒ Three-days conference pass;
⇒ Training materials;
⇒ Tea and lunch on all days;
⇒ Gala Dinner;
⇒ Attendee bag.

REGISTRATION FEES CAN BE PAID BY BANK TRANSFER TO THE FOLLOWING ACCOUNT:

Account Name: Norway Registers Development East Africa limited
Account number: 10100686207
Swift code: AKCOTZTZ
Akiba commercial Bank. Bank code: 12
Branch code: 0001
Do not forget to mention your **full name, organization and CDEA 2013** on the bank transfer slip. All bank fees must be paid by the participant.

PRICES ARE INDICATED IN THE TABLE BELOW:

Registration fee	
ISACA members	**US$400/Tsh 650,000**
Other	**US$500/Tsh 830,000**

CONFIRMATION OF REGISTRATION

The registration will be confirmed by email after we receive the payment. Those who do not receive a confirmation notice before the conference are strongly recommended to contact us at registration@nrd.no.

CANCELATION AND REFUND POLICY

⇒ Before 27th July, 2013: 50 % will be refunded from the payment.
⇒ After 27th July, 2013: No payment will be refunded.

Refunds will be issued after the conference. Bank charges will be deducted from the refund. For refunds please state your full bank account.

You can find more information on registration at www.cybersecurity.co.tz.
You can also follow our updates on Facebook: Norway Registers Development East Africa Ltd
Linkedin: Norway Registers Development AS
And Twitter: NRDEALtd

About Norway Registers Development in East Africa

NRD has been actively engaged in cyber security initiatives in the East African region for a while now: multiple seminars on cyber security, MoU with ISACA Tanzania Chapter on cooperation in the development and implementation of consultative Tanzanian National Cyber security framework, as well as recently signed two-year Cooperation and Services Agreement with local agent – SimbaNET. The main objective of these initiatives is to create a secure digital environment for East African states, governments, corporations and citizens.

In March 2013, in order to be closer to its clients, NRD AS has decided to invest in one of its partners. Newly acquired Norway Registers Development East Africa Ltd. (NRD EA) provides on-site delivery of the NRD services and is responsible for cyber-defence strategy design and implementation services for Government and corporate institutions. NRD EA supports Tanzanian companies in the delivery of information security technologies as a value added distributor. At the same time the new entity is actively involved in the improvement of the Business Climate in the East African Community.

Furthermore, with this acquisition, NRD is now fully equipped to assist other organisations investing in East Africa in the creation, development, maintenance and security of their information technology infrastructure.

Norway Registers Development AS has during the last 18 years been specializing in helping governments and institutions in all continents to build vital economy facilitating infrastructure together implementing necessary legal and organizational changes, particularly in the area of business registers.

The NRD services and experiences cover consultancy, legal research and drafting, institutional capabilities building and training, system designing and implementation as well as operation services as integrated solutions for effective operation of the required services. The NRD AS fields of experience cover the complete range of activities from the raising of awareness and political commitment to project designing and preparations, implementation support and execution, operation and maintenance.

Having been particularly specialized in complex registration reforms, NRD has accumulated a wide experience in designing, implementation and management of register projects. This experience gave NRD perfect ground to expand services to other fields where complex data management requirements come together with a necessity for legal and organizational reforms.

About ISACA Tanzania Chapter

ISACA is an independent, non-profit, global association, engaging in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide.

About JSC BAIP

BAIP, a company having more than 20 years of experience in critical ICT infrastructure and cyber security areas, is a part of BAIP group. BAIP group is a group of companies that specializes in the field of design, development, resilience and cyber security of critical information systems for governments and corporations.

BAIP, referring to the approach by SANS institute and „Critical Security Controls" methodology believes that the critical factor that can eliminate up to 80% of cyber security threats is on-time, financially rational cyber hygiene and appropriate technologies. Therefore, it pays a lot of attention not only to cyber security but also to information system resilience by following methodologies (Cobit, Critical Security Controls), standards (ISO 27000), and practices (NIST, CPNI, NATO CCDCOE, ISACA, SANS institute), as well as cooperating with specialised technological and consultation partners.

BAIP is involved in various cyber security projects and cooperates with government, national regulatory institutions and educational institutions in the EU, CEE, East and West Africa: Liberia, Rwanda, Mauritius, Malawi, Ghana, Tanzania, Uganda and Burundi. For implementation of these projects, BAIP is in partnerships with major global ICT infrastructure and cyber security vendors which allows matching high quality technology to the specific project's requirements and delivering it at reasonable prices. In addition, BAIP provides 24/7 support and maintenance services.

BAIP's specialists are authors and subject matter expert reviewers of international academic publications, such as "Transforming Cybersecurity: Using COBIT® 5" (ISACA), "Responding to targeted Cyber attacks" (ISACA), COBIT adaptation in Lithuania. BAIP is an active member in developing Lithuanian national cyber security strategy. Company makes recommendations to the Ministry of the Interior, Information Society Development Committee, Ministry of National Defence, Government and Seimas of the Republic of Lithuania, the Communications Regulatory Authority of the Republic of Lithuania. BAIP also collaborates with Kaunas University of Technology (KTU) - launched an initiative to make KTU a centre of digital forensics studies. BAIP cyber security team worked with KTU to design the curriculum, and KTU received a license to use industry-standard Forensic Toolkit® technology.

BAIP provides critical IT infrastructure services and cyber security services, assisting clients in consolidation, virtualization, security and management of their IT environment by means of BAIP proprietary methodology CIMF (Critical Infrastructure Maintenance Framework). The main specialization areas are IT infrastructure design, virtual environments, IT services management, storage, backup and recovery, security and cloud computing.

Company delivers cloud and supercomputing services, it also specialises in large scale system design, implementation and maintenance. BAIP expertise includes design and implementation of highly scalable distributed systems, high performance interconnected networks and large scale parallel and distributed storage systems. Company assists its customers in design and development of cloud and HPC based business services platforms which can be integrated into cloud infrastructure.

ABOUT SimbaNET

SimbaNET Limited is a Licensed Public Data Operator in providing Voice, Video, data and Internet connectivity in Kenya, Tanzania and Uganda.

The network is connected via three different redundant Submarine Optic Fibre cables to all international destinations. The last mile connectivity is delivered either by using Fibre (Fibre to the Business), Wi-MAX Wireless media under a licensed band, Satellite (remote and marine connectivity) or 3G (mobile).

SimbaNET also specializes in IT services and implementing UTM solutions for its clients across the East African Region.

ABOUT CTWO Products

CTWO Products is a leading manufacturer of manageable secure flash solutions. SafeXs, CTWO's flagship product is a feature rich hardware encrypted secure USB flash drive that is developed and produced in Sweden and deployed to organisations globally.

SafeXs® provides mandatory password protection and automatic hardware encryption of all stored data. SafeXs drives are manageable world-wide on an enterprise scale with the SafeConsole® management software, offering full control, remote life-cycle management and device enhancement such as remote password recovery, customised password policy, audit for compliance as well as a whole raft of security and productivity features.

ABOUT FireEye

FireEye(R) has invented a purpose-built, virtual machine-based security platform that provides real time threat protection against the next generation of cyber attacks. The FireEye platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including Web, email, and files. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time.

FireEye appliances provide integrated Web & Email Protection via full automated virtual execution engines, which run code and observe behavior in order to notice malicious activity, and stop its movement via email attachments (documents), or download. Additionally, they block botnet command and control communication.