DTS SOLUTION
CYBER SECURITY REDEFINED

Next Generation
Cyber Security Operations Center 2.0

With the threat landscape ever changing within the cyber world, next generation of threats and attack vectors surfacing; information assets are more vulnerable than ever before.

In the past, large corporations have implemented traditional security operations centers as a means to maintain visibility regarding their information security posture. The most popular model has centered on building large command centers, where numerous analysts work side by side to assess real-time security data and manually respond to it. This is what is referred to as SOC 1.0. Although this model has proven effective, the days of SOC 1.0 are numbered.

DTS Solution Professional Services team can help your organization strategize, develop and build a Next Generation Security Operations Center SOC 2.0 to protect your information assets whilst counteracting the ever changing threat landscape.

SOC 2.0 - Enhanced Security O&M

Organizations are now having to accept that a shift in paradigm of Information Security Operations and Maintenance needs to be implemented to keep one step ahead of the intruders.

This has led to organizations to invest heavily in protecting their information assets perimeter wide - utilizing multiple security platforms such as next generation firewalls, intrusion prevention systems, data leakage prevention devices, endpoint security etc.

The huge level of investments made by CIO's has not necessarily translated into better protection or mitigation of information theft. Year 2011 has seen a vast number of major security breaches across major corporations and industries proving that as information security awareness continues to rise the shortfalls in proactive monitoring maintenance, management and threat mitigation of security still remains.

With the vast number of information security breaches and the increased number of high profile and well publicized security incidents have left many executives, security professionals wondering how effective the deployed controls have been.

It is difficult to imagine these large corporations (needless to mention them) did not have security mechanisms and controls in place. Indeed they did, but the matter of fact is, investing in security infrastructure to protect your assets does not by default entitle you with protection.

Information security needs to be built as a process that becomes the core of any organization. Developing and building a Security Operations Center 2.0 practice around this exact process empowers your organization to augment the different.

SOC 2.0 - Success Factors

Given today's economic challenges, building, developing and operating a SOC is a difficult financial proposition that is somewhat not easy to justify. In fact, SOC centers were originally designed to reduce the cost of security incidents by bringing numerous security engineers and analysts into a single space that can collaborate and react to the incidents that may involve multiple systems. But times have changed, threats have evolved, emerging technologies are now maturing, and there are now better ways to accomplish the SOC tasks by complimenting physical presence with virtual presence.

Several factors are driving the next generation SOC, including the transformation of the network operations center (NOC). The conventional NOC is designed to monitor network-level events and provide level-one triage and troubleshooting for corporate networks. But as companies begin to build more robust, agile and dynamic ITIL-based unified operations centers that will support and complement some security operations functions, it means tier-one and tier-two security operations can be collapsed and handled in the operations center. Typically tier-one and tier-two security operations does not necessarily require in-depth skill-set and as a result shared resources working as part of a virtual SOC team can be organized.

Furthermore SOC 2.0 focuses on the overall contextual correlation and situation awareness of IT assets as security risks and threats evolve within an organization. Dynamic risk profiling based on events received and incidents detected, correlation of multiple log events from different security systems, network forensics and analytics are all key components of SOC 2.0.

Traditional SOC centers have predominantly focused on decentralized event management systems that are unique for each technology vendor.

Traditional SOC would host silos of event management systems; each collecting and displaying logs from the different systems. SOC 2.0 emphasizes on the deployment of a centralized Security Information and Event Management (SIEM) solution where all the technology systems, devices and assets can send information, logs, and events; whilst providing enhanced correlation features and risk and offense categorization that is based on dynamic understanding of the context and asset in question. SIEM 2.0 is driving this evolution forward that really forms the core hub of SOC 2.0 concept.

It will be essential to consider the following three steps when building your SOC.

People	• Virtual SOC Teams • High Skill Set
Technology	• Emerging Technologies • Dynamic Risk Assignment • Network Forensics and Analytics
Process	• Business Process Oriented • Comprehensive Compliance and Incident Response

People

Identify the core people. As mentioned previously virtual team makeup will not be the traditional SOC 1.0 engineers, but rather highly trained and experienced security and risk professionals.

These VSOC (Virtual SOC) operators must be more experienced and better trained than NOC engineers. They must be security specialists with specific hands-on skills, such as firewalls, VPNs, and IDS/IPS, and security architects who are domain-specific designers working on the overall information security strategy.

Training and experience have increased priority. Also, this provides an incentive that benefits employee retention initiates, as VSOC engineers still get to be involved in InfoSec community.

Technology

Identify the core emerging technologies facilitating SOC 2.0. Security information and event management (SIEM 2.0) tools will be the core technical component of SOC 2.0, acting as the information repository necessary for delivering on the VSOC vision. It's important for these information management tools to be easy to use and intuitive; they must also have a Web interface that can be accessed from any browser in the world, as a VSOC engineer could be based anywhere in the world at the time of an incident.

Other tools that will be important to SOC 2.0 are network monitoring tools, which provide insight into the state of the network and computer forensic and analytic tools to provide deep investigation into incidents that have moved beyond the service center. This toolset is sometimes referred to as NAV or Network Analysis and Visibility.

Understanding attack modeling in a complex environment requires determining which systems, people and processes have access to valuable information also known as situational awareness is an important component of SOC 2.0. Once the threat surface is modeled, organizations can then determine potential attack vectors and examine defense steps to isolate compromised access points efficiently and quickly.

Self- learning and predictive analysis also form an important component of enabling SOC 2.0. To remain relevant in tomorrow's IT environment, a SOC will need to truly integrate compliance monitoring and risk management. The system should continually monitor the environment to identify typical states which can then be applied to identify problematic patterns early. Statistic-based predictive modeling will be able to help correlate various alerts. Developing such a system will require real-time behavior analysis innovations, although some of these elements are available today.

Automated, risk-based decision systems provide contextual based dynamic risk mitigation. A key differentiator of a more intelligent SOC will be its ability to assess risks instantly and vary responses accordingly. Similar to risk-based authentication, the SOC will employ predictive analytics to find high-risk events and then automatically initiate remediation activities.

The prospect of dynamic typography is one of the most exciting areas of this type of systems automation for the cloud. To implement an APT, an attacker must understand network mapping and be able to model it. In response to this, organizations can remap their entire network infrastructure to disrupt an attacker's reconnaissance efforts. This is akin to physically rearranging a city at frequent intervals - and the entire process can be automated so that links between systems stay intact and dependencies are handled without human intervention.

Process

Identify the core responsibilities and processes. The success of SOC 2.0 and the transition from the traditional SOC to the VSOC depends on the ability to transfer day-to-day security tasks to the operations center. The command center within the operations center must be able to mitigate tier-one and tier-two security incidents and recognize when to escalate tier-three incidents to the VSOC. It's therefore imperative to identify the core responsibilities of theVSOC vs. the operations center, and to come to an agreement on how responsibilities are to be divided between IT security management and IT operations.

SOC 2.0 must be aligned and integrated into the business process of an organization that is centered around information security principles that drive protection of valuable assets.

The developed SOC 2.0 operations framework must integrated into the Risk Management, Business Continuity, Compliance and Governance processes; whilst ensuring Incident Response and Escalation procedures are well defined, Change Management, Alert and Notification policies are clearly communicated to business units.

SOC 2.0 - Emerging Technologies

SIEM - Security Intelligence	Big Data Security Analytics	Vulnerability Management	Incident Response
LogRhythm The Security Intelligence Company	elastic	tenable Qualys	CYBERSPONSE ADAPTIVE SECURITY

SOC 2.0 - Functional Components

OSS/SIEM 2.0

PROACTIVE MONITORING	ALERT & NOTIFICATION	EVENT CORRELATION
Automated Monitoring – SNMP Categorization of Monitored Objects Automated Monitored Object Reporting Integrated to Business Process Automated assignment of Risk Level	Automated Alert and Notification – SNMP Trap / IF-MAP event Alerts categorized based on Risk Level Notifications to Business Process Owner	Contextual correlation of events Situational awareness Mapped to Business Process

AUTOMATION

COMPLIANCE & AUDIT	CHANGE MANAGEMENT	CONFIGURATION MANAGEMENT
Compliance templates created Compliance enforcement Compliance reporting Compliance violation reporting Auto-Archival Auto-Remediate Auto-Validate	Device change management process Automated approval process Linked to compliance template Change Control Validation Change Management History Log	Configuration Archival Configuration change mapped to change control Configuration Management Database Complete history of archived configuration Configuration Rollback

RISK MANAGEMENT 2.0

RISK RANKING	VULNERABILITY MANAGEMENT	REMEDIAL ACTION ASSIGNMENT
Alerts/Events and Compliance Results are ranked based on risk level Automated Risk Based Detection Systems Risk based authentication Mapped to Risk Management Framework	Automated Vulnerability Assessment and Audit Vulnerability ID mapped to Risk Level Reference	Automated Owner Assignment Process based on business process / system owner Validate of remedial action completion

INCIDENT HANDLING

INCIDENT RESPONSE	BEHAVIOURAL ANALYSIS	REPORTING
Network Forensics Investigation and Analysis Evidence Gathering Escalation Management	Network Behavioural Analysis Detection Anomaly Detection Predictive Analysis Business Process Profiling	Reporting based on incident Feedback and Review Process Prosecution / Disciplinary / Litigation

DTS SOLUTION
CYBER SECURITY REDEFINED

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

☎ 800 HACKED

ABU DHABI: Office 253, Al Bateen C6 Tower - Bainunah, King Abdullah Bin Abdulaziz Al Saud Street | **T:** 971 2 2076777
LONDON: 160 Kemp House, City Road, London, EC1V 2NX, United Kingdom | **T:** +44 2081230 387 (DTS)
www.dts-solution.com