Data Sheet

DTS SOLUTION
CYBER SECURITY REDEFINED

Cyber Security
Metrics

DTS can help your organization build cyber security metrics using the PRAGMATIC metametrics approach. **PRAGMATIC** is an acronym for the basis of the method in using metrics that are predictive, relevant, actionable, genuine, meaningful, timely, independent and cost.

The PRAGMATIC method has application both in designing security metrics from scratch, and in systematically improving your current metrics. If you are using security metrics that 'ought to work' in theory but for some reason don't seem to work out so well in practice, the PRAGMATIC method helps you understand why they don't work and identify what would need to change to make them more valuable. Simply altering the way, the security metrics are analyzed and presented may be sufficient, otherwise it may be worth exploring whether changing the phrasing or definition of metrics will turn things around.

At the end of the day, some security metrics are so poor they are simply irredeemable: the PRAGMATIC method gives you a way to put lame metrics out of their misery, saving money and encouraging management to focus their attention on the remaining fit-for-purpose metrics. Lacking this crucial step, metrics systems tend to grow, and we end up measuring what we can, not what we should.

DTS can help your organization to design, build and manage the cyber security metrics and performance measurement system using the **PRAGMATIC metametrics approach**.

Metrics are tools to facilitate decision making and improve performance and accountability. Measures are quantifiable, observable, and objective data supporting metrics. Operators can use metrics to apply corrective actions and improve performance. Regulatory, financial, and organizational factors drive the requirement to measure IT security performance.

Potential security metrics cover a broad range of measurable features, from security audit logs of individual systems to the number of systems within an organization that were tested over the course of a year. Effective security metrics should be used to identify weaknesses, determine trends to better utilize security resources, and judge the success or failure of implemented security solutions.

In information security, it is no different. Effective management of varying performance indices can mean the difference between a practical and efficient project and a complete waste of money. Although IT managers have been following KPIs for quite some time now, in information security, this is an uncommon and still developing practice to track cyber security metrics.

Cyber security metrics should be identified and created for various different audiences ranging from management level to C-level and executives.

OUR APPROACH

- Keep the cyber security metrics meaningful
- Tie the metrics to your cyber program processes
- Keep the metrics reproducible
- Develop rigorous and objective definitions
- Build useful desk procedures/checklists
- Keep the metrics manageable
- Leverage existing automated sources of data
- Make practical decisions to narrow scope as needed
- Provide an increased level of transparency

STEPS TO CREATE THE METRICS

- Define the metrics program goals and objectives
- Decide which metrics to generate
- Develop strategies for generating the metrics
- Establish benchmarks and targets
- Determine how the metrics will be reported
- Create an action plan and act on it
- Establish a formal program review/refinement cycle

RIGHT METRICS FOR THE RIGHT AUDIENCE

- Current State of Security
- Risk Year-on-Year Statistics
- Hygiene/Health
- Effectiveness Index
- Current Risk Posture and Changes Over
- Time Trends
- Employee Awareness Index
- Security Initiative Performance
- Investments
- Incident Index
- Regulatory Compliance Reports
- Updates Benchmark Reports
- Budget Performance

MANAGEMENT

- Trend Analysis Data
- Security Posture Trends
- Vulnerability Management / Patch Reporting
- Emerging Network Threats
- Incident Response Times
- Audit Compliance and Findings
- % of Risk Accepted Threats

SERVICE OWNERS & SUPPORT TEAMS

- # of Incidents Investigated
- Type and Severity of Security Incidents
- Vulnerability External / Internal (Highs/Mediums/Lows)
- % Servers, Apps, Patched to Current Patch Level
- Detail info on Threats
- Top/Emerging Exploits

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