Periodic Table of Cyber Metrics

🟥 Cyber Management
🟦 End Point Protection
⬜ Privacy Assurance
🟦 User Awareness
🟩 Vendor Risk Management
🟨 Infrastructure Resilience
🟨 Servers Protection
🟩 Cloud Risk Management

ROSI
Return On Security Investment
The ratio of the monetary benefits of a cybersecurity investment to its cost.

AGS
Assets Governance Score
A composite score reflecting the consistency, timeliness, completeness, and dependability of established accountability and fiduciary measures.

RAC
Risk Assessment Coverage
The percentage of business units or processes assessed for risk, ensuring comprehensive risk identification.

CE
Control Effectiveness
The percentage of critical controls tested and found effective, by asset type, policy or regulations..

Naiden Nedelchev © 2024

OIMS
Overall Infrastructure Maturity Score
Composite metric represents the cybersecurity maturity level calculated by aggregating scores from various dimensions.

NSE
Network Segmentation Effectiveness
A composite score of documented assets and flows, and effectiveness of operated methods and tools.

DET
Data Encrypted in Transmission
The percentage of data that is encrypted during transmission over internal networks and Internet.

DPIAS
Data Protection Impact Assessments Score
Completion rate of privacy impact assessments in a reporting period.

RMRRT
Risk Mitigation Rate and Response Times
The percentage of identified risks that have been adequately mitigated to an acceptable level.

AFCR
Audit Findings Closure Rate
The percentage of audit findings or recommendations that have been closed or addressed.

TPRE *
Third-Party Risk Exposure
The percentage of third-party vendors assessed for risk and their risk ratings.

TCE **
Training Completion and Effectiveness
The percentage of employees who have completed training and certification in security best practices and policies.

ESROI
Endpoint Security ROI
The ratio of the benefits and costs of all endpoint security investments.

MPC
Malware Protection Coverage
Percentage of endpoints covered by malware protection.

EDER
Endpoints Data Encrypted at Rest
Percentage of sensitive data is encrypted at rest on mobile computers and workstations.

EUM
Endpoints Under Monitoring
The percentage of organization endpoints covered by SIEM, SOAR, XDR or other solution.

SBFD
Servers Backup Frequency & Duration
The intervals and lengths of time between successfully completed backup jobs on organization's servers.

IRR
Incident Response Readiness
A composite score reflecting mean time metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

DLR
Data Leakage Rate
Quantification of the volume of data that leaves the organization against policies.

TIAS
Technology Impact Assessments Score
Completion rate of privacy implication assessments on newly adopted by the organization technologies.

CRI
Composite Risk Index
A cumulative risk value aggregating all reported, assessed and severity classified safety-related incidents to form an index.

PRACT
Policy Review and Approval Cycle Time
The average time to approve new or updated guiding documents to meet changing compliance requirements or best practices.

TPUM
Third-Parties Under Monitoring
The percentage of organization's supply chain integrated in security controls continuous monitoring.

DER
Data Encryption Rate
Percentage of data encrypted at rest

ADE
Anti-malware Detects/blocks at Endpoints
Number of detects/blocks of attacks targeting end users, per malware type.

CAMS
Current Anti-Malware Software
Percentage of systems with/without current endpoint protection engine/software.

RECV
Remediated Endpoint Critical Vulnerabilities
The percentage of critical vulnerabilities identified and remediated within the target timeframe.

TDRR
Threat Detection and Response Rate
Combined ratio of threats that are identified and reported, as well remediated and resolved by the endpoint security tools and teams.

SPC
Servers Patching Cadence
The average time it takes an organization to test and deploy a security update to servers groups and network appliances.

SVD
Servers Vulnerability Density
The ratio of the number of vulnerabilities to the servers groups or network appliances.

UDON
Unidentified Devices On the Network
The presence of unidentified devices connected to the corporate network.

PBN
Privacy Breach Notifications
Percentage of on-time regulator notification for privacy breaches.

SPDS
Security Policy Documentation Status
Percentage of security documents in the various lifecycle statuses.

TRCE
Total Regulatory Compliance Expense
All of the costs an organization incurs to maintain Cyber regulatory compliance.

AVSR
Average Vendor Security Rating
Average of the aggregated cybersecurity scores of all the third-party vendors associated with the organization.

EDB
Endpoint DLP Blocks/alerts
Number of DLP events for blocks and alerts on movement of sensitive data from endpoint devices.

IAUS
Inventory Authorized and Unauthorized Software
Ratio of compliant software installations from all detected software on corporate devices.

CTS
Current Threat Signatures
Percentage of systems with/without current endpoint protection signatures/updates

EPU
Endpoints Privileged Users
Number of privileged user accounts on endpoint systems – OS, apps, etc.

ELSP
Endpoints with Latest Security Patches
The percentage of endpoints that are currently running the latest security patches.

SSI
Server-side Security Incidents
The number and severity of security incidents that occur on organization's Servers.

DER
Data Encrypted at Rest
Percentage of sensitive data encrypted at rest in databases, file servers, other repositories.

DDNYC
Databases and Data-residents Not Yet Classified
The Ration of databases, devices, endpoints, file shares which are still not classified, marked and covered by a DLP system.

NPC
Number of Privacy Complaints
The number of justified complaints per period, by department, customer or regulator.

*

SVIV
Security Violations Involving Vendors
Number of security violations or incidents involving third-party systems or staff.

SLAC
Service Level Agreement Compliance
The rate at which a Cloud service is meeting contractual performance expectations/service levels.

CSI
Cloud Security Incidents
The number and severity of security incidents that occur in organization's Cloud environments by cloud provider, accounts, service types, etc.

CICC
Cloud Inventory Controls Converge
Percentage of Cloud inventory covered by security or compliance controls.

CSP
Cloud Security Posture
Overall level of Cloud infrastructure security and resilience, based on the implementation and effectiveness of various security controls.

CPV
Cloud Policy Violations
Number of Cloud policy violations and exceptions per vendor, account and service.

CSISD
Cloud Services Involving Sensitive Data
Number of Cloud services which store or process any data which is classified as sensitive by the organization.

HRCAD
High-Risk Cloud Apps Discovered
Number of high-risk Cloud apps detected based on risk classification parameters for apps, e.g. having AI, etc.

CCIB
Cloud Compliance with Industry Benchmarks
Compliance percentage with Cloud hardening benchmarks (number of enabled, passed and failed checks).

TASC
Trusted Advisor Security Checks
Number of independent Trusted Advisor security checks that Cloud vendor/app passed/failed.

**

CPP
Campaign Phish-prone Percentage
The average ratio of total failures divided by the total number of emails delivered all phishing campaigns.

UASR
User Authentication Success Rate
The percentage of successful user authentications compared to the total attempts.

TCI
Training Coverage and Inclusivity
Percentage of staff included in training and awareness encompassing all levels from entry-level employees to top management.

EPV
End-user Policy Violations
The number (or severity) of security policy violations by organization's workforces.

ADT
Attacker Dwell Time
The average time it takes to detect a successful cyber attacker targeting different groups or individuals of organization workforces.

NRO
Number of Repeat Offenses
Frequency of repeated policy violations by employees by policy, team, etc.

EFS
Employee Feedback and Surveys
Qualitative insights from employees about the cyber security policies, culture, and training effectiveness.

SSIB
Staff Security Incidents and Breaches
Frequency and type of reported staff security incidents and documented breaches.

CDR
Call Deflection Rate
The ratio of inquiries resolved through self-service channels versus those handled by direct cyber support staff.

SSSR
Self-Service Success Rate
The percentage of self-service interactions that resolve the end-user's cyber issue without escalation to live support.