Stop Counting Chickens, Start Securing the Coop

Managing Cybersecurity Tools Before They Fly the Coop

whoami

Joe Tegg

- Collaborative. Pragmatic. Security Leader.
  - GRC, SecOps, Red Team, Pentesting
- Recovering Unix Admin
- Covert Technologist
- Certified Technical Cave Diver - yea, really...

Github - @avgjoesecurity/SecurityPresentations

Agenda

Problem Overview

- Example Cases
- How does it happen?

Solution

- Tool Management Standard
  - Functional Requirements
  - RACI
  - Key Metrics

Benefits

Problem Overview

Many organizations rush to deploy cybersecurity tools for compliance, only to end up with a tangled mess of misconfigurations, redundancies, and security gaps—kind of like building a chicken coop but forgetting to lock the door, leaving it wide open for trouble.

Example Case - Sellafield Nuclear Waste Management

Sellafield ordered to pay nearly

At that hearing, the court heard that a test had found that it was possible to download and execute malicious files on to Sellafield's IT networks via a phishing attack "without raising any alarms", according to Nigel Lawrence KC, representing the ONR.

An external IT company, Commissum, found that any "reasonably skilled hacker or malicious insider" could access sensitive data and insert malware that could then be used to steal information at Sellafield.

At the time, Sellafield said it did not have evidence of a successful cyber-attack. Greaney told the court that there was no evidence found for an "effective" cyber-attack on Sellafield. The court heard that Sellafield's operations centre was found to be "unable to adequately alarm and respond to tested attacks".

The regulator found that 75% of computer servers at Sellafield were vulnerable to cyber-attack.
Composite: Guardian Design/Alamy

Example Case - DISA Global Data Breach

Notice of Data Incident

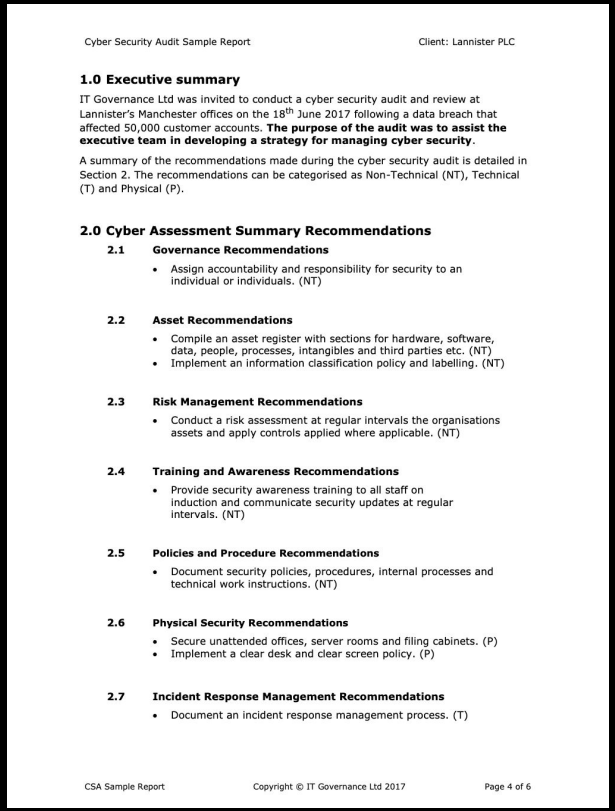
DISA Global Solutions, Inc. ("DISA") is a third-party administrator of employment screening services, including drug and alcohol testing and background checks. On April 22, 2024, DISA discovered that it was the victim of a cyber incident that impacted a limited portion of its network. Upon discovery, we immediately contained the incident and initiated an investigation with the assistance of third-party forensic experts. Our investigation determined that an unauthorized third party accessed a limited portion of our environment between February 9, 2024, and April 22, 2024, and procured some information. Although our forensics investigation could not definitively conclude the specific information procured, the affected files contained individuals' personal information, which came into our possession due to the employment screening services we provide employers and prospective employers. Presently, we are unaware of any attempted or actual misuse of any information involved in this incident.

In addition to this notice, we are providing notice to individuals whose protected personal information was contained in the affected files. The personal information contained in these files may have included name, social security number, driver's license number, other government ID numbers, financial account information, and other data elements. Not every data element was present for every individual.

We take this incident seriously and sincerely regret any inconvenience this incident may cause affected individuals. Upon discovery, we secured our network, notified law enforcement authorities, safely restored our systems and operations, and implemented additional security measures. We also offer affected individuals access to credit monitoring and identity restoration services through Experian. Individuals also can review additional steps they can take to protect themselves if they feel it necessary to do so by clicking here.

How does this happen?

Audit Finding



1.0 Executive summary

IT Governance Ltd was invited to conduct a cyber security audit and review at Lannister's Manchester offices on the 18th June 2017 following a data breach that affected 50,000 customer accounts. **The purpose of the audit was to assist the executive team in developing a strategy for managing cyber security**.

A summary of the recommendations made during the cyber security audit is detailed in Section 2. The recommendations can be categorised as Non-Technical (NT), Technical (T) and Physical (P).

2.0 Cyber Assessment Summary Recommendations

2.1 Governance Recommendations

- Assign accountability and responsibility for security to an individual or individuals. (NT)

2.2 Asset Recommendations

- Compile an asset register with sections for hardware, software, data, people, processes, intangibles and third parties etc. (NT)
- Implement an information classification policy and labelling. (NT)

2.3 Risk Management Recommendations

- Conduct a risk assessment at regular intervals the organisations assets and apply controls applied where applicable. (NT)

2.4 Training and Awareness Recommendations

- Provide security awareness training to all staff on induction and communicate security updates at regular intervals. (NT)

2.5 Policies and Procedure Recommendations

- Document security policies, procedures, internal processes and technical work instructions. (NT)

2.6 Physical Security Recommendations

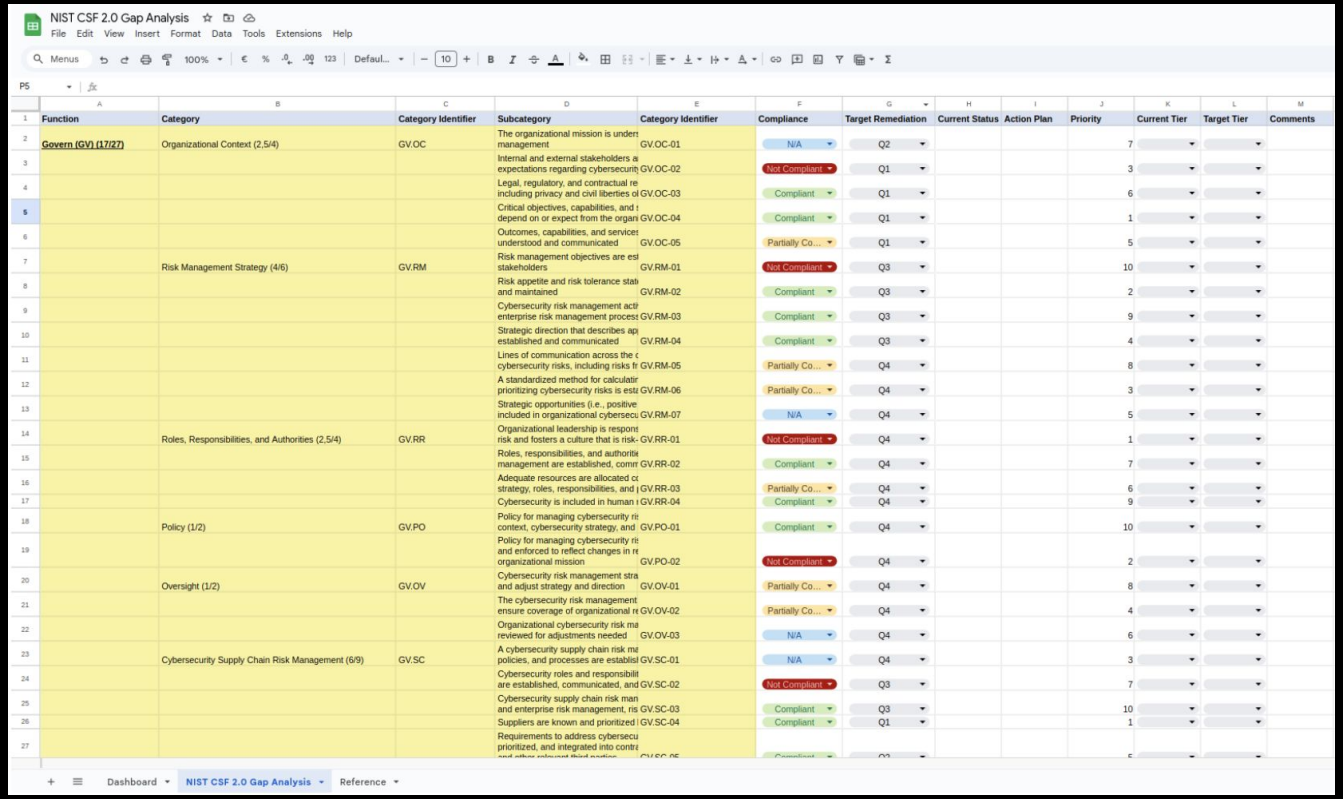
- Secure unattended offices, server rooms and filing cabinets. (P)
- Implement a clear desk and clear screen policy. (P)

2.7 Incident Response Management Recommendations

- Document an incident response management process. (T)

Add a New Tool!

Security Control Assessment



NIST CSF 2.0 Gap Analysis

File Edit View Insert Format Data Tools Extensions Help

	Function	Category	Category Identifier	Subcategory	Category Identifier	Compliance	Target Remediation	Current Status	Action Plan	Priority	Current Tier	Target Tier	Comments
2	Govern (GV) (17/27)	Organizational Context (2,5/4)	GV.OC	The organizational mission is under management	GV.OC-01	N/A	Q2			7			
3				Internal and external stakeholders a expectations regarding cybersecurit	GV.OC-02	Not Compliant	Q1			3			
4				Legal, regulatory, and contractual re including privacy and civil liberties o	GV.OC-03	Compliant	Q1			6			
5				Critical objectives, capabilities, and depend on or expect from the organ	GV.OC-04	Compliant	Q1			1			
6				Outcomes, capabilities, and services understood and communicated	GV.OC-05	Partially Co…	Q1			5			
7		Risk Management Strategy (4/6)	GV.RM	Risk management objectives are est stakeholders	GV.RM-01	Not Compliant	Q3			10			
8				Risk appetite and risk tolerance stat and maintained	GV.RM-02	Compliant	Q3			2			
9				Cybersecurity risk management acti enterprise risk management process	GV.RM-03	Compliant	Q3			9			
10				Strategic direction that describes ap established and communicated	GV.RM-04	Compliant	Q3			4			
11				Lines of communication across the cybersecurity risks, including risks fr	GV.RM-05	Partially Co…	Q4			8			
12				A standardized method for calculatir prioritizing cybersecurity risks is esta	GV.RM-06	Partially Co…	Q4			3			
13				Strategic opportunities (i.e., positive included in organizational cybersecu	GV.RM-07	N/A	Q4			5			
14		Roles, Responsibilities, and Authorities (2,5/4)	GV.RR	Organizational leadership is respons risk and fosters a culture that is risk-	GV.RR-01	Not Compliant	Q4			1			
15				Roles, responsibilities, and authoriti management are established, comm	GV.RR-02	Compliant	Q4			7			
16				Adequate resources are allocated cc strategy, roles, responsibilities, and	GV.RR-03	Partially Co…	Q4			6			
17				Cybersecurity is included in human r	GV.RR-04	Compliant	Q4			9			
18		Policy (1/2)	GV.PO	Policy for managing cybersecurity ris context, cybersecurity strategy, and	GV.PO-01	Compliant	Q4			10			
19				Policy for managing cybersecurity ris and enforced to reflect changes in re organizational mission	GV.PO-02	Not Compliant	Q4			2			
20		Oversight (1/2)	GV.OV	Cybersecurity risk management strat and adjust strategy and direction	GV.OV-01	Partially Co…	Q4			8			
21				The cybersecurity risk management ensure coverage of organizational re	GV.OV-02	Partially Co…	Q4			4			
22				Organizational cybersecurity risk ma reviewed for adjustments needed	GV.OV-03	N/A	Q4			6			
23		Cybersecurity Supply Chain Risk Management (6/9)	GV.SC	A cybersecurity supply chain risk ma policies, and processes are establis	GV.SC-01	N/A	Q4			3			
24				Cybersecurity roles and responsibilit are established, communicated, and	GV.SC-02	Not Compliant	Q3			7			
25				Cybersecurity supply chain risk man and enterprise risk management, ris	GV.SC-03	Compliant	Q3			10			
26				Suppliers are known and prioritized	GV.SC-04	Compliant	Q1			1			
27				Requirements to address cybersecu prioritized, and integrated into contr	GV.SC-05								

Dashboard | NIST CSF 2.0 Gap Analysis | Reference

Add a New Tool!

Security Program Maturity Uplift

Approach

Fictitious example

Exemplary Cyber Security maturity actuals and planning

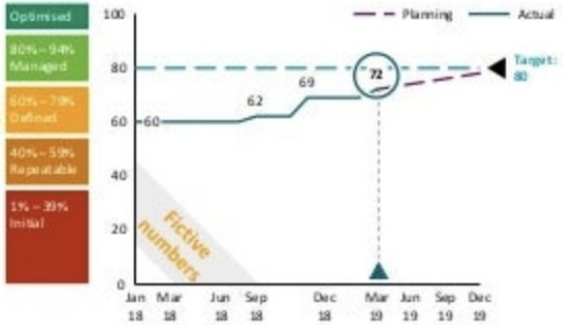
innogy

Current Cyber Security maturity [%]

		Company overview						
Control		Global	DE	UK	NL	PL	CZ	SK
CA.05	Information security policies	79	79	79	79	79	79	79
CA.06	Organisation of information security	80	80	79	80	80	81	80
CA.07	Human resources security	67	62	58	62	60	64	72
CA.08	Asset management	54	52	52	52	51	58	55
CA.09	Access control	65	62	59	64	60	79	68
CA.10	Cryptography	80	80	78	80	80	78	82
CA.11	Physical & environmental security	81	80	80	80	82	84	80
CA.12	Operations security	68	66	67	65	68	72	72
CA.13	Communications security	68	65	67	67	65	73	69
CA.14	System acquisition development & maintenance	49	43	54	43	48	62	43
CA.15	Supplier relationships	71	71	75	71	67	71	71
CA.16	Information security incident mgmt.	82	85	78	88	74	84	85
CA.17	Information security aspects of BCM	79	80	80	80	78	75	80
CA.18	Compliance	72	71	74	71	66	76	71
Total		72	70	70	70	68	75	72

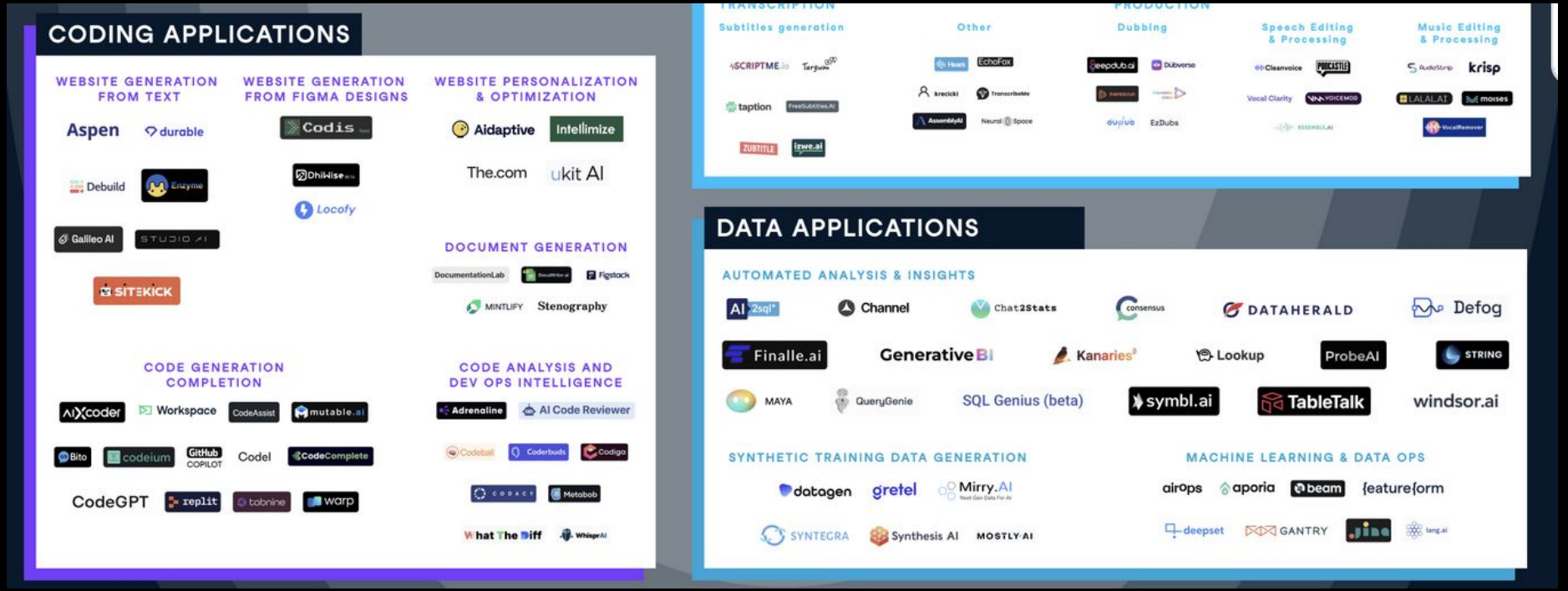
Cyber Security maturity planning [%]

CSMA methodology and tool awarded with the Security Innovation Award.



Add a New Tool!

New Technology



Add a New Tool!

Our coop has all the protections, right?


WHEN YOU TALK ABOUT THE 100 SECURITY TOOLS TO THE AUDITOR
YOU KNOW NO ONE MANAGES THEM AND THEY'RE DEFAULT INSTALLS
imgflip.com

Solution

Create and implement a Security Tool Management Standard

NIST 800-53

"Two fundamental concepts that affect the trustworthiness of systems are **functionality** and **assurance**. **Functionality** is defined in **terms of the security and privacy features, functions, mechanisms, services, procedures, and architectures implemented** within organizational systems and programs and the environments in which those systems and programs operate. **Assurance** is the **measure of confidence** that the system functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system—thus possessing the capability to accurately mediate and enforce established security and privacy policies." NIST 800-53 r5 Section 2.5

Security Tool Management Standard (minimum)

1. **Functional Requirements (Functionality)**
2. **RACI (Functionality / Assurance)**
3. **Key Metrics (Assurance)**
    a. Availability
    b. Coverage

Functional Requirements

What are Functional Requirements?	Why are they important?

Functional requirements define the specific behaviors and functionalities a security tool must have to meet its intended purpose.
 	
Key Components of a Functional Requirements document:
 	
• **Functional Requirements:** A detailed list of the required functions and capabilities of the implemented security tool.
• **Non-Functional Requirements:** Specific outcomes and metrics that must be met or achieved with the implementation and operation of this tool.
• **Assumptions & Constraints:** Specific business, operational, technology constraints that may impact the required settings or use cases for the tool when implemented.
	• **Alignment & Clarity**
	  ○ Ensures that there is clearly defined requirements and outcomes related to the implementation and continued use of the tool.
	  ○ Helps avoid duplication of functional use cases across the security tool ecosystem.
	• **Improved Communication & Collaboration**
	  ○ Does this tool meet our needs? A common question that comes up and this document solidifies the functional outcomes for the tool and drives alignment to the needs.
	• **Compliance & Risk Management**
	  ○ Helps in meeting regulatory requirements by ensuring the security controls impacted by the use of this tool are clearly documented.
	• **Operational Efficiency**
	  ○ Reduces security tool sprawl and duplication of functions due to the increased awareness for deployed security tools.

Functional Requirements - examples

- **Authentication & Access Control**
  - Support for multi-factor authentication (MFA)
  - Role-based access control (RBAC)
  - Integration with identity providers (LDAP, SAML, OAuth)
- **Threat Detection & Prevention**
  - Real-time monitoring of network and system activity
  - Signature-based and behavior-based detection
  - Alerting mechanisms for suspicious activity
- **Logging & Reporting**
  - Comprehensive logging of security events
  - Customizable reporting dashboard
  - Ability to export logs to SIEM solutions
- **Incident Response & Remediation**
  - Automated incident classification
  - Playbook execution for common security incidents
  - Integration with ticketing systems
- **Integration & Interoperability**
  - APIs for third-party integrations
  - Compatibility with security frameworks (MITRE ATT&CK, NIST)
  - Support for multiple operating systems
- **Performance & Scalability**
  - Ability to handle high volumes of data
  - Low-latency processing of security events
  - Horizontal scaling support

POLL TIME

What functions should a chicken coop perform?

1. Predator protection
2. Adverse weather cover
3. Squeeze them in like sardines so profits go up
4. Provide a safe place to lay eggs

RACI

What is a RACI?	Why is it important?

A **RACI matrix** (Responsible, Accountable, Consulted, Informed) is a framework used to define roles and responsibilities for different stakeholders involved in the implementation, operation, and maintenance of a security tool. It ensures clarity in ownership, reduces confusion, and enhances efficiency in security operations.
 	
Key Components of a RACI Matrix
 	
• **Responsible (R):** The person or team who performs the work to complete a task.
• **Accountable (A):** The person ultimately answerable for the task's success and decision-making.
• **Consulted (C):** Subject matter experts or stakeholders who provide input before decisions or actions are taken.
• **Informed (I):** Individuals or groups who need to be kept up to date on progress and outcomes.
	• **Role Clarity & Accountability**
	  ○ Ensures that every security-related task has clear ownership, reducing ambiguity.
	  ○ Helps avoid duplication of work and missed responsibilities.
	• **Efficient Decision-Making**
	  ○ Clearly defines who is accountable for approvals, making security operations more streamlined.
	• **Improved Communication & Collaboration**
	  ○ Defines who needs to be consulted for expertise and who should be kept informed, ensuring transparency.
	• **Compliance & Risk Management**
	  ○ Helps in meeting regulatory requirements by ensuring responsibilities for logging, auditing, and policy enforcement are well-defined.
	• **Operational Efficiency**
	  ○ Prevents delays in security operations by assigning the right people to the right tasks.

RACI - example

Example RACI Matrix for a Security Tool

Task / Activity	Security Team	IT Admins	Compliance Team	CISO	End Users	Vendor / MSSP
Tool Selection & Procurement	R	C	C	A	I	C
Installation & Configuration	R	R	C	A	I	C
Access Control & User Management	R	R	C	A	I	C
Threat Monitoring & Incident Response	R	I	C	A	I	R
Log Management & Retention	R	R	A	C	I	C
Policy Compliance & Audit Reports	R	C	A	C	I	C
Security Updates & Patch Management	R	R	C	A	I	R
Training & Awareness	C	C	A	C	R	I

POLL TIME

Who should manage the coop for chicken access?

1. The Chicken Hawk
2. The Fox
3. The Farmer’s son
4. The Farmer

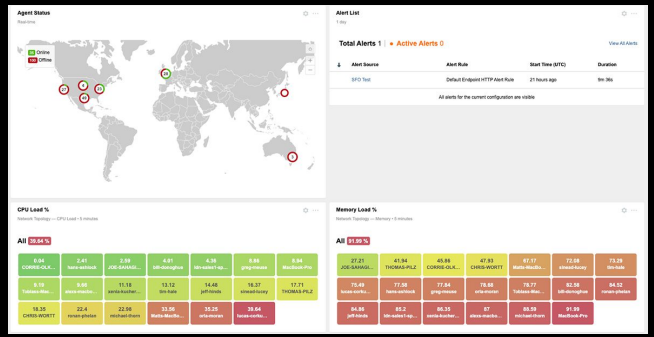
Key Metrics

A security tool that is unavailable, misconfigured, or underperforming **cannot protect the organization.**

Availability	Coverage
The availability of a security tool is **critical** to maintaining a strong cybersecurity posture. If a security tool is down, misconfigured, or underperforming, it creates gaps in security coverage that can be exploited by attackers. Monitoring the availability of security tools is **just as important as monitoring for cyber threats**.	Security tool coverage refers to the extent to which a security solution is actively protecting an organization's assets, including endpoints, network traffic, logs, and users. Monitoring the coverage is **essential** because gaps in protection can lead to undetected threats, compliance violations, and increased security risks.

Key Metrics - examples

Availability	Coverage
• Tool UI uptime over 3 months • Tool API uptime over 3 months • Tool configured automation success rate over 3 months	• Tool deployment/scanned percentage over 3 months • Tool functional efficacy over 3 months • Tool critical assets monitored percentage over 3 months



Metrics - a note of thought

The **SYMBIOSIS** method is a structured approach for developing meaningful cybersecurity metrics that align with an organization's security goals. It ensures that metrics are relevant, actionable, and support decision-making.

Key Aspects of the SYMBIOSIS Method:

- Strategic Alignment
- Yield Meaningful Insights
- Measurability
- Balance Between Technical & Business Perspectives
- Integration with Security Operations
- Objective Data-Driven Approach
- Scalability & Adaptability

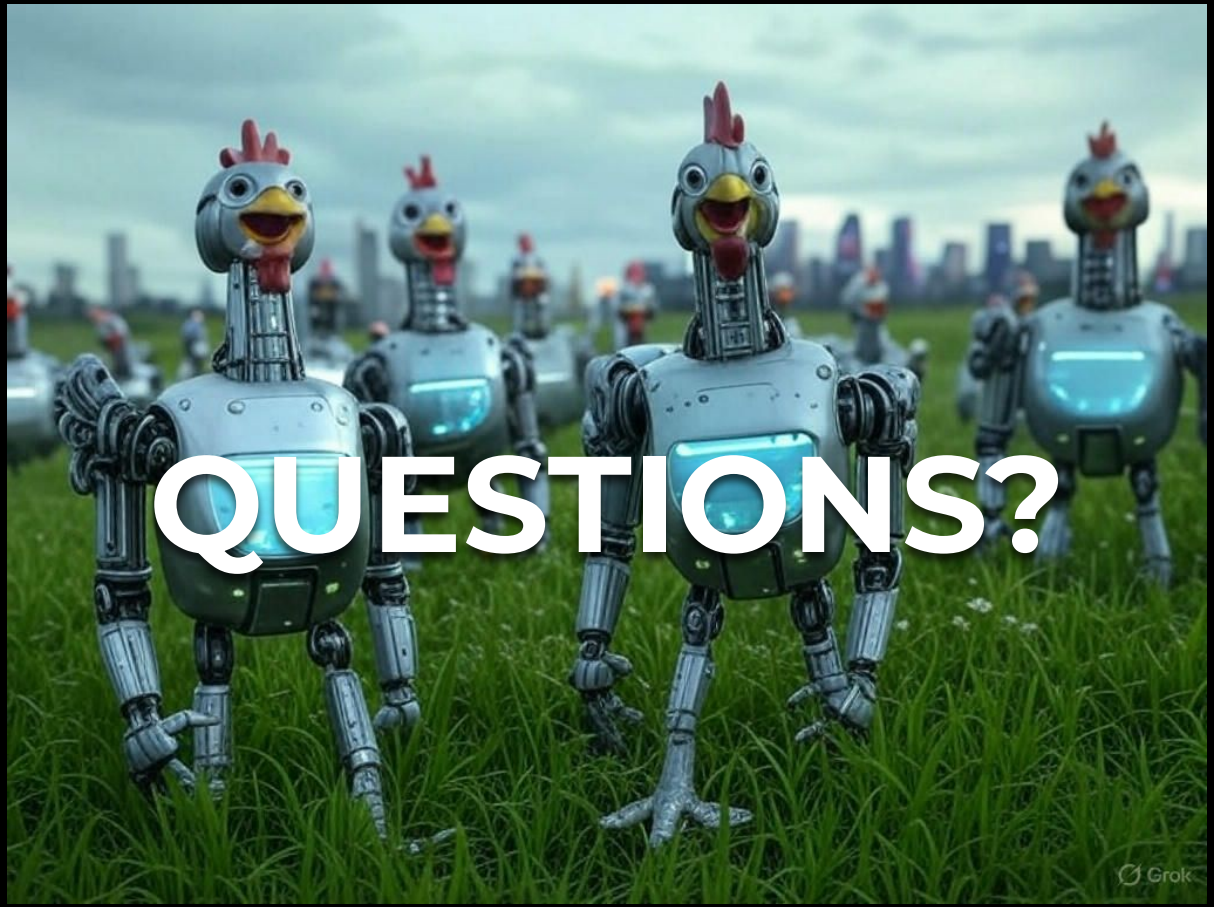
POLL TIME

What metric would be best to measure the availability of the egg boxes?

1. Wind speed outside the coop
2. Number of rooster crows at 5am
3. Number of eggs being harvested
4. Number of hens drinking water

Benefits

Business Benefits	Security Team Benefits
1. Reduces Business Risk & Prevents Financial Losses • Security tools protect against cyber attacks, data breaches, and financial fraud. **2. Ensures Compliance & Regulatory Adherence** • Compliance frameworks like PCI DSS, GDPR, HIPAA, and NIST require effective security controls. **3. Maximizes ROI on Security Investments** • Organizations invest heavily in security tools—mismanaged tools lead to wasted resources. **4. Improves Business Continuity & Operational Efficiency** • Security tool failures can disrupt operations, leading to downtime or breaches.	**1. Strengthens Threat Detection & Response** • Well-managed security tools provide accurate, real-time alerts without overwhelming analysts. **2. Reduces Analyst Fatigue & Alert Overload** • Poorly managed tools generate excessive noise, false positives, and duplicate alerts. **3. Enhances Visibility & Coverage** • Security gaps arise when tools are misconfigured, outdated, or missing coverage. **4. Enables Faster Incident Response & Recovery** • Mature security tools are integrated, automated, and optimized for rapid containment and remediation.


QUESTIONS?
Grok