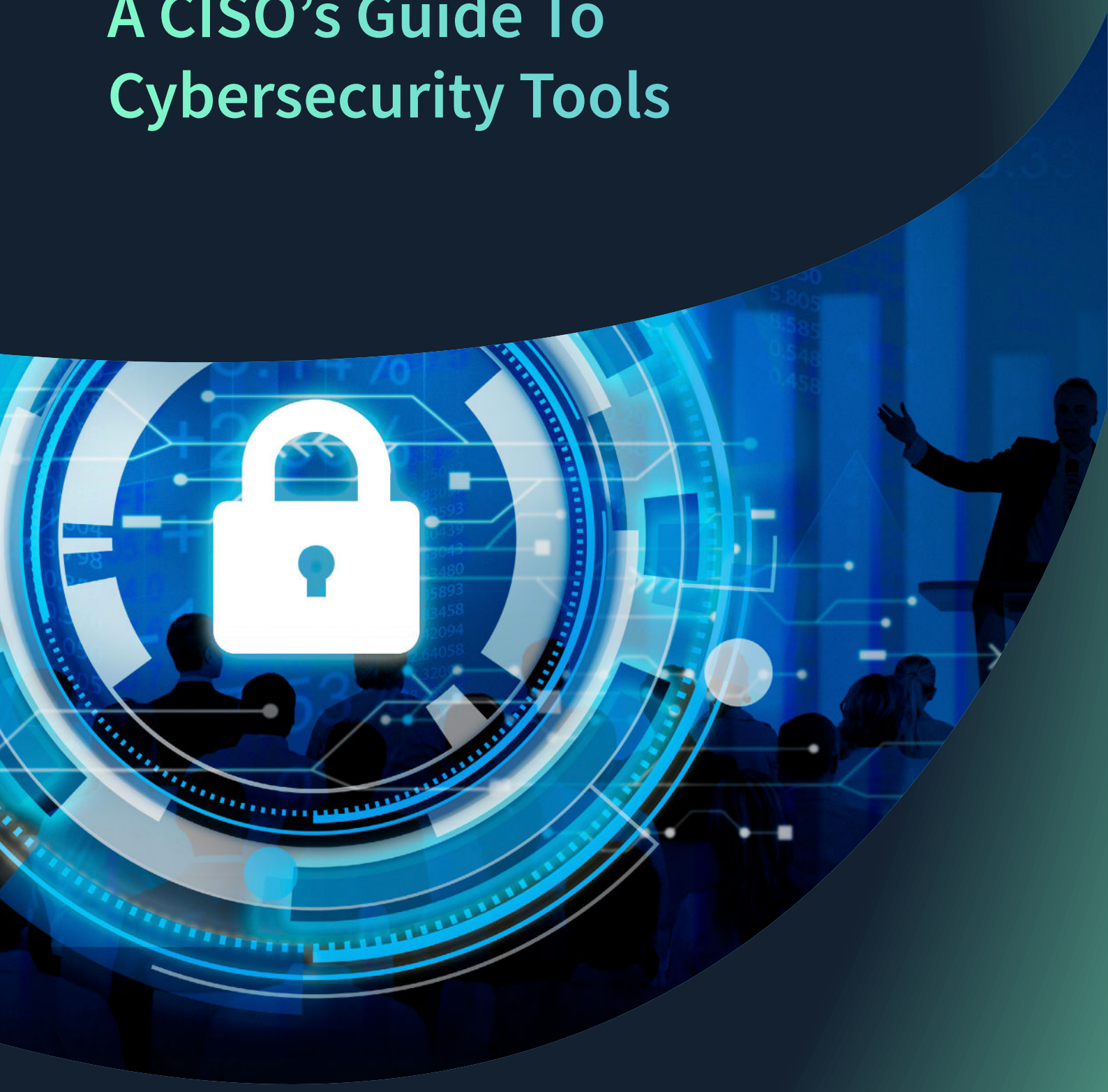
Scrut Automation

Demystifying The Jargons - A CISO's Guide To Cybersecurity Tools



Scrut Automation

Contents

Introduction

Acronym fatigue is real. CISOs at organizations of all sizes face constant pressure from other senior leaders to communicate risk throughout the organization, as well as hearing vendors throw around new terms to describe new technologies. Already a world of acronyms from the traditional tech world, like VPN, IT/OT, and others, these other security acronyms can be enough to overwhelm the average security professional.

Despite this, organizations large and small need to understand the technologies they need to secure enterprise. Cloud-native organizations especially have an acute need for distinct technologies to secure themselves against attack. With the added challenge of not necessarily having the ability to understand everything that's needed.

This eBook will seek to demystify some of the jargon of cloud-native security tools and others so that CISOs can make decisions with confidence. We'll categorize tools across multiple different areas and focus on the ones that cloud-native organizations need to know to enhance their security.

The technology areas covered in this guide include:

- **Cloud Security**
- **Endpoint Security**
- **Network Security**
- **External Security Posture**
- **Orchestration**
- **Operational Technology**
- **Identity And Access Management**
- **Application Security**

After reading this guide, you will be empowered to better understand the full landscape of security tools available to you.

Cloud Security

First up is the core need for cloud-native organizations. Cloud security is the primary need here, not just at cloud-native companies but also at other companies that have adopted the cloud. This solution class is going to be hugely important over the course of the next few years. Cloud is especially critical as organizations shift their operations to a distributed model, and

DID YOU KNOW?

cloud security is crucial as 27% of organizations have experienced a security incident in their public cloud infrastructure within the last 12 months [according to Check Point.]

Here are the technologies in cloud security that you need to understand:

CASB

Cloud Access Security Broker

CASBs are security policy enforcement solutions. They act as an intermediary between cloud service users and cloud service providers to unify and add enterprise security policies as users access cloud-based resources.

CIEM

Cloud Infrastructure Entitlement Management

CIEM solutions manage identities and privileges in cloud environments. These tools are used to enforce the principle of least-privileged access when end-users access cloud environments.

CSPM

Cloud Security Posture Management

Cloud security posture management, or CSPM, solutions help manage the risks of cloud security. This is most commonly done through connecting to and analyzing the settings and configuration of the cloud service provider or CSP. CSPMs take a continuous view of your CSP and look for any known security issues while also tracking changes over time.

CWPP

Cloud Workload Protection Platforms

Cloud Workload Protection Platforms (CWPP) secure cloud applications or workloads in runtime, up through memory, code, container layer, and often behavioral process monitoring.

CMDB

Cloud-Native Configuration Management Database

A configuration management database (CMDB) is used to track all of the hardware and software used throughout the enterprise. It provides an organized view into your environment to allow you to view, visualize, and slice and dice data any way you need it. Cloud-native CMDBs are an evolution of the traditional tool.

CNAPP

Cloud Native Application Protection Platform

Cloud-native application protection platforms (CNAPP) unify configuration and runtime protection. Security in cloud-native applications during runtime and at rest is increasingly critical.

Scrut Automation

Endpoint & Network Security

Endpoint security and network protection tools are the classic tools in cybersecurity.

Endpoint protection includes traditional signature-based antivirus as well as next-gen antivirus that integrates machine learning.

Network security ranges from the classic firewall to other tools designed to protect corporate networks. These are the basics of securing the enterprise and should be the first step in any security strategy.

Here are a few acronyms to be aware of:

XDR

Extended Detection & Response

Extended detection and response tools are a merging of telemetries gathered from the cloud, the network, and the endpoint into a single dashboard for cross-organization response to threats.

SASE

Secure Access Service Edge

SASE is meant to unify wide area networking, or WAN, with CASB, Firewall as a Service, and Zero Trust, into a single, cloud-delivered service model.

ZTNA

Zero Trust Network Access

A methodology where all network traffic is verified before users are allowed to access it.

IDS

Intrusion Detection System

An intrusion detection system (IDS) monitors a network for malicious activity or policy violations. It is typically installed alongside an IPS or intrusion prevention system.

IPS

Intrusion Prevention System

An intrusion prevention system (IPS) constantly monitors a network for malicious activity and tries to prevent it. Typically it is installed alongside an intrusion detection system.

DLP

Data Loss Prevention

A DLP solution is designed to protect against intentional and unintentional data loss from your endpoints or network.

SD-WAN

Software Defined Wide Area Network

An SD-WAN is a virtual wide area network architecture that allows you to leverage any transport services to securely connect users to applications.

SDP

Software Defined Permiter

An SDP is a boundary based around software instead of hardware and is often part of a zero-trust strategy. This is in contrast to a traditional perimeter, which is defined by specific hardware installations.

Identity and Access Management

Identity and access management solutions provide the ability for organizations to verify that users are who they say they are and control access to critical systems.

Most organizations would do well to enforce the principle of least privilege in their security policies, ensuring that users have access to the least critical data necessary to do their jobs.

Here are the acronyms that you need to know in the Identity And Access Management realm:

SSO

Single Sign On

A technology that allows users to log in to multiple systems with the same credentials. It is often used to reduce the number of accounts that users need to create passwords for.

2FA/MA

2FA/MFA

Two-factor authentication (2FA) or multi-factor authentication (MFA) are methods used to verify a user in addition to using a password. This is a key security technology to prevent account takeovers.

PAM

Privileged Account Management

Two-factor authentication (2FA) or multi-factor authentication (MFA) are methods used to verify a user in addition to using a password. This is a key security technology to prevent account takeovers.

External Security Posture

External security posture solutions as a class of tools allow enterprises to assess their controls and overall organizational hygiene.

This area of security incorporates asset discovery solutions as well as security testing and risk ratings, which are especially important components of understanding organizational risk exposure as well as the overall cyber hygiene of suppliers.

Some key acronyms to know within the **External Security Posture** space are:

EASM

External Attack Surface Management (EASM)

tools are designed to discover internet-facing assets that could be accessible and vulnerable to threat actors. These are typically used to surface shadow IT and discover any risky assets outside of what the IT security team already knows about.

SRS

Security Ratings Services (SRS)

are software tools that provide a numerical or letter grade to security posture. This is typically used as part of validating the security of suppliers.

3PRM/ TPRM

3PRM/TPRM

refers to third-party risk management. These tools allow organizations to manage the security risks of their suppliers. Often, 3PRM tools also include security attestation forms where vendors self-report their controls.

CART

Continuous Automated Red Teaming

refers to Continuous Automated Red Teaming, which is a class of solutions designed to automate a red team engagement to validate your security controls. This is an up-leveled version of a penetration test that can be performed on an ad hoc interval instead of needing to hire a specific firm every time.

Scrut Automation

Application Security

Application security refers to the class of solutions designed to ensure that applications in development are secure

This class of solutions is especially important when it comes to ensuring open-source code is secure. Deploying application security effectively means that your software products are created with secure coding practices already baked in.

Here are some of the most important acronyms for you to understand in Application Security:

DAST

Dynamic Application Security Testing

involves analyzing an application through the front end to find vulnerabilities through simulated attacks. DAST evaluates the application from the "outside-in" by attacking it like a malicious user would.

SAST

Static Application Security Testing

involves analyzing the application's code for potential vulnerabilities. This has more in common with a code review but is targeted toward ensuring overall secure code.

IAST

Interactive Application Security Testing

is an application security tool built for both web and mobile applications to detect and report issues regardless of whether the application is running or not.

SCA

Software Composition Analysis

solutions identify the open-source software in a codebase. SCA is done to evaluate security, license compliance, and code quality.

RASP

Runtime Application Self-Protection

tools are integrated into an application to analyze inward and outward traffic and end-user behavioral patterns to prevent attacks on application memory.

NGWAF

Next-Gen Web Application Firewall

A NGWAF is the next evolution of WAF in that it brings intelligent application context to the WAF model. This can improve the overall security of your web applications.

WAF

Web Application Firewall

tools are plugged into application servers and apply a set of rules to an HTTP request. The idea here is to prevent XSS or SQL injection attacks.

Orchestration

Security orchestration tools are a major component of your security strategy.

Orchestration tools include technologies that empower teams with insight across the entire security architecture.

A few of the acronyms to understand in this area are:

SOAR

Security Orchestration and Response

tools use AI to assist security operations teams with prioritizing alerts and organizing response to security events. These tools often ingest data from other security tools.

SIEM

Security Information Event Management

collects and organizes pertinent log and event data from around the enterprise. This data includes security, network, server, application and database sources.

DFIR

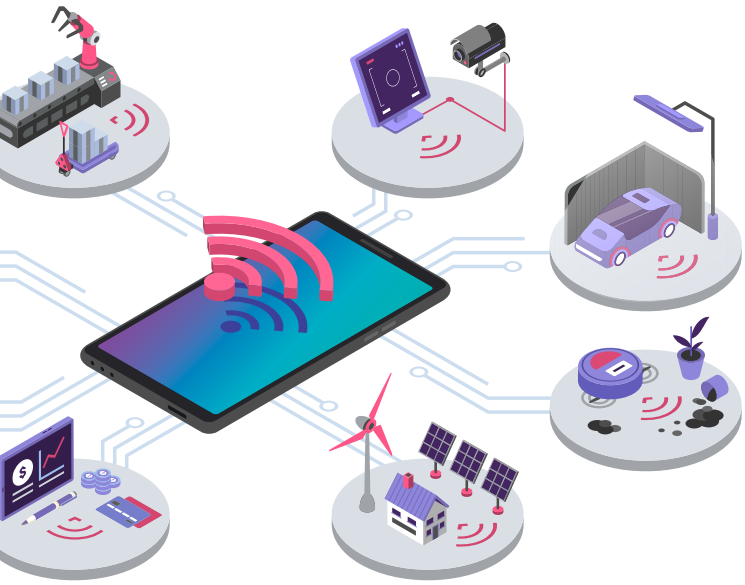
Digital Forensics & Incident Response

After a breach occurs, digital forensics and incident response services and solutions are critical to understanding two things. Digital forensics allows you to understand the attack chain and incident response allows you to remediate the problem.

Scrut Automation

Operational Technology Security

For the most part, this ebook has focused on technology that emphasizes IT security. The other side of cybersecurity that is often less discussed is operational technology. These are typically heavy machinery and industrial systems in manufacturing, medical machinery, food production, and other similar industries.



A few of the acronyms to be aware of here are:

ICS

Industrial Control Systems

are electronic control systems used to manage industrial processes. An ICS can be anything from a few panels to a huge computer system. They are often found in heavy industries like oil and gas, food production, utilities, and manufacturing. These systems receive data from a large volume of remote sensors.

IACS

Industrial Automation and Control Systems

is an umbrella term that refers to a collection of networks, control systems, SCADA systems, and others deemed to be vulnerable to attack. These systems together comprise the IACS landscape.

OT

Operational Technology

refers to the system of fixed-function machinery common in industrial applications, such as an oil pipeline control mechanism or water monitoring in utilities.

IOT

Internet of Things

refers to connected devices like doorbell monitors or medical devices that send information over the internet.

Conclusion

The acronyms included in this guide are only a few of the most prominent solutions that CISOs are likely to encounter. The issue with modern cybersecurity solutions is that there are always new technologies being developed and new acronyms being used.

It is a major challenge for even the savviest CISO to stay on top of all the jargon being used within the vendor community. Hopefully, this guide helped disambiguate some of the most common acronyms and provide a richer context for the modern CISO.

If you're looking for a risk-managament platform that will guide you through imminent procedures and processes required to keep your organization's security posture in the best condition, then book a free demo with Scrut today.