InfoSec Fusion

Integrating Security Disciplines for Cyber Resilience

Author:
Subramanya Shankar, Senior Consultant, Application Security, Optiv
Cybersecurity today relies on disciplines working together.

Gone are the days of siloed departments working in isolation and not sharing information. Increasingly sophisticated attacks demand that all groups within the organization share information to stay ahead of threats and ensure compliance.

This was made painfully evident with the recent Apache Log4j/Log4shell vulnerability. The scope and scale of this extremely disruptive zero-day flaw and its impact on the industry was simply unprecedented. Organizations will be calculating the costs associated with their response and remediation efforts for many months.

This whitepaper seeks to promote awareness of the ways in which security practices such as governance, risk and compliance (GRC), application security, data protection, network and security operations and identity access management (IAM) can work together cohesively to safeguard the organization against known and emerging threats.
## Table of Contents

Risk Management Understanding and Prioritizing Risk ................................................................. 2  
Data and Asset Security – Classification of Assets and Data .......................................................... 3  
Network and Communication Security – Protect the Perimeter .................................................. 5  
Build Secure Applications and Test by Performing Periodic Application Security Testing – Application Security ................................................................. 6  
Protecting the New Perimeter – Identity .................................................................................... 8  
Security Operations – The Silent Defender .................................................................................. 9  
Conclusion ...................................................................................................................................... 10
**Risk Management**

**Understanding and Prioritizing Risk**

A core function for any cybersecurity team is to understand what risk a threat presents and how best to deal with it. A risk management plan is central to this task.

Risk identification, which includes identification, assessment management and monitoring of operational risks, can be achieved through a control governance framework.

---

**Steps for Risk Management**

1. Understand the organization, its products, activities and services – its interdependencies, risk appetite and tolerance, preferred method of risk assessment, etc.

2. Evaluation of risk and prioritization of controls

3. Effective communication strategy to all relevant stakeholders through the risk assessment process

4. Structure the assessment – includes monitoring variances in risk index, tracking KRI/KPIs/KCIs and effective communication of the changes across the organization

5. Establish process for measurement of risk index/risk appetite

6. Choose a risk management framework for cyber risk assessment (ex: NIST)

7. Use cyber insurance as a risk management tool; it transfers the risk to a third-party insurer, thereby protecting the organization against internal and external attacks

RSA Archer is a GRC tool widely used by organizations to manage risk and plan for audits. From an AppSec perspective, there are several relatively mature and effective application vulnerability management platforms in the market. Kenna (recently acquired by Cisco Systems), for instance, integrates well with QualysGuard and other vulnerability management systems to pull in scan reports. Another vulnerability management system of note that supports application level vulnerabilities is Brinqa.

---

**Governance Model**

- Risk Management Committee
- Information Systems Security Steering Committee
- BCM Team

**Proactive Measures**

- Product Management Committee
- Change Management Committee
- BCP

**Reactive Measures**

- Introduce New Controls After Analysis of Operational Losses
- External Events
- Incident Analysis

**Tools**

- Risk and Control Assessments
- Risk Indicators
- Loss of Data

---

*Figure 1: Governance Framework*

*Figure 2: Framework Breakdown*
Data and Asset Security – Classification of Assets and Data

This is the mantra: data is the new oil. Proper asset classification and segregation along with implementation of proper controls helps organizations prevent data theft and exposure, thus preventing fines and negative publicity.

Organizations need to first understand which assets are important and classify them based on internal guidelines. Clear asset classification will help security teams prevent data breaches.

Asset security can be divided into five steps:

1. **Data Policy**
   - Define a data policy that acts as a guide to help the organization collect necessary (and only necessary) information
   - A well-defined data policy provides appropriate guidance to higher management

2. **Data Governance**
   - The organization should have a data governance office to oversee data policy and outline stakeholder roles and responsibilities
   - The office will determine how the creation, transformation and use of data is managed by the organization, as well as data describing data governance

3. **Data Quality**
   - A data quality policy involves managing the integrity and reliability of data
   - This policy should be created with quality assurance and quality control teams

4. **Data Documentation**
   - Documenting all data creation will help organizations manage large data sets and use them for critical business decision making
   - Proper documentation of data supports effective data use

5. **Data Organization**
   - Data organization is applicable to both structured and unstructured data
   - This step involves arrangement and control of data

Data classification and management tools include:

1. **Tye**: Data cleaning. Data from multiple sources is cleaned after upload, duplicate records are removed and the data set is standardized

2. **Uniserv**: Data quality for large enterprises. Uniserv reduces project risk through structured and transparent project methodology

3. **Klassify**: Next-gen data classification suite. Helps enterprises classify unstructured data based on predefined categories

Data classification is also vitally important. Labelling data as secret, confidential, etc., helps prevent unauthorized access.

Figure 3: Asset Security Steps
Valuable asset and data classification tools include:

1. **Manage Engine Asset Explorer**: Web-based software for IT asset management. Lets you track and control enterprise-owned asset rights throughout the lifecycle, from planning to delivery, deployment and/or disposal.

2. **Spiceworks**: Inventory management solution. Easily integrated with existing help desk, network monitoring or other ITSM systems. It automatically discovers, captures and categorizes any asset within your IT environment and provides detailed information associated with it.

3. **Service Now**: Unified asset management platform. Facilitates IT asset optimization and automation of intuitive IT workflows.

In addition to these DLP implementations, restricting USB access (among other granular protections) will help minimize data breaches, thus avoiding compliance-related fines.

Data classification affects the way risk is rated during an assessment. More sensitive data (ex: credit card, health information, HITRUST, financials, SOX and GLBA) will be rated as high compared to less critical data. Organizations will have to first perform a risk assessment and classify their data based on internal standards (confidential/sensitive/restricted/public). Security teams can then map data according to the rating and classification. Organizations adhering to GDPR have to be especially careful about how data is classified, as any sensitive data leakage may lead to financial repercussions.
Organizations need to have strong network security in place to prevent external attacks. Proper network segmentation, least privilege and domain separation, among other defenses, will help minimize attacks against the perimeter.

The payment card industry (PCI) mandates segregation and segmentation of cardholder data into a separate network (isolated from the main network). This ensures stored credit card data isn’t compromised in case of a breach. Organizations dealing with the PCI should ensure all industry mandates are followed.

Zero Trust networking is a powerful new tool for security teams. A Zero Trust approach should extend throughout the entire organization and should serve as an integrated security philosophy and end-to-end strategy. The Zero Trust networking philosophy must include the following:

1. Identities
2. Devices
3. Data
4. Infrastructure
5. Networks

Secure communication within and outside the organization is also fundamental to maintaining a competitive edge. Below are some of the ways implementing secure communication channels can help increase security:

1. Implement remote access security management
2. Deploy centralized remote authentication services such as RADIUS and TACACS
3. Implement software defined networking (SDN)
4. Trust no one: employ Zero Trust network access
5. Use CDNs for faster site loading, reduction in bandwidth requirements and improved security
6. Implement CASB to prevent data from being stolen
7. Invest in advanced threat protection (ATP)

Solutions from leading providers such as ZScaler, Netskope, Cisco and Proofpoint can help achieve the desired level of security. Security testers frequently use tools such as nmap, solarwinds and ossec for network security assessments.

Organizations are replacing physical hardware devices such as routers and switches with SDN, which offers significant benefits compared to traditional networking devices.
Securing the perimeter is not sufficient, as organizations usually have applications exposed on the internet, providing a gateway (once compromised) into the enterprise.

Implementing a secure software development life cycle (SDLC) process during development helps mitigate many security vulnerabilities at the design level. The secure SDLC process shown can ensure security is baked into the applications at the design level and at each phase of the development.

Secure SDLC is a necessity in today’s rapid software release environment, as vulnerabilities can be successfully addressed when security is a continuous management concern.

Secure SDLC also shows its worth in the following areas:

1. SSDLC fosters a security-focused culture.
2. It helps mitigate risks. Baking in security during the requirement gathering and design phases leads to more predictable deployments, fewer rollbacks and higher customer satisfaction.

Training developers in secure coding is fundamental to building secure software. These organizations offer learning platforms that can help developers produce secure code.

1. **Secure Flag**: The world’s first learning platform to offer hands-on secure coding practices. Secure Flag features:
   a. Labs
   b. Learning paths
   c. Metrics and reporting

2. **Secure CodeWarrior**: Helps developers enhance their security skills through training courses and labs. Secure CodeWarrior’s human approach uncovers the secure developer inside every coder, helping development teams ship quality code faster, thereby creating secure products.

3. **Veracode Security Labs**: Teaches developers how to shift left by giving them hands-on training in secure coding and helps them tackle real-life threats and patch code. This will also help them apply DevSecOps principles.

Development goes hand in hand with testing to ensure that code is indeed secure and no vulnerabilities have slipped through the cracks.

Application security testing can be broadly divided into five types:

1. **SAST**: Static application security testing analyzes source code for vulnerabilities. Developers can run their code through commercial and open-source scanners such as Veracode, Checkmarx and Fortify, which will identify vulnerabilities that may be present in the code.

2. **DAST**: Dynamic application security testing analyzes the application while it’s running. Security testers send requests to the application and, based on the responses, try to identify vulnerabilities during runtime. Many dynamic scanners, such as Burp Suite and Netsparker, allow for automating security testing as well as fine-tuning of manual test cases.
3. **SCA**: Software composition analysis analyzes source code dependency libraries, both from open-source and third-party sources. Often paired with SAST tools, this technology enables the generation and monitoring of software bills of material and can direct development teams to efficient remediation paths. Some of the leading tools in this space include Veracode, Sonatype and Snyk.

4. **IAST**: Interactive application security testing installs an agent on the web server and monitors the traffic for attacks (reports are generated automatically). Some of the best IAST related products are Contrast Security’s Contrast Assess and Hdiv Security’s Hdiv Detection.

5. **RASP**: Rapid application security protection is deployed in post-production (on production web servers) and blocks attacks in real time. Vendors release signatures periodically and these must be applied to the RASP product to ensure the latest attacks are caught. Fortify Defender, Contrast Security’s Contrast Protect and Hdiv security’s Hdiv Protection are commonly used by top enterprises.

6. In addition to these methodologies, testers heavily rely on **manual testing**, which helps in creating proofs of concept and identifying obscure or complex business logic vulnerabilities that automated scanners often miss.

Internal audits corresponding to compliance codes like ISO and GDPR and producing SSAE 16 compliant reports (SOC 1, 2 and 3) will help ensure that robust and secure software is delivered to clients.

Compliance-as-code is a new concept that organizations need to embrace. This helps integrate various compliance-related elements into the code, saving time on manual audits.

Contino is one provider of compliance-as-code services.

Organizations need to create a security testing strategy depending on the risk associated with each application. It’s imperative that an application risk analysis is conducted before strategy is developed. Some higher-risk applications, such as financial apps dealing with PCI, may warrant regular code reviews after each release and a monthly security test to ensure they’re safe from high-/medium-risk issues. Shifting left and employing DevSecOps with integration of automated scanners with CI/CD will help mitigate many vulnerabilities. Manual testing can provide verification.
Protecting the New Perimeter – Identity

Identity is the new perimeter. Identity access management (IAM) provides the right people with the right access at the right time, and it’s now possible to securely sign in via social login or single sign-on (SSO) in a corporate setting.

Here’s how IAM works.

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Authorization</th>
<th>User Management</th>
<th>Central User Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO</td>
<td>Role- and Rule-Based</td>
<td>Delegated Administration</td>
<td>AD/Kerberos Directory</td>
</tr>
<tr>
<td>Session Management</td>
<td>Remote Authorization</td>
<td>User and Role Management</td>
<td>Virtual Directory</td>
</tr>
<tr>
<td>Strong Authentication</td>
<td></td>
<td>Self-Service Password Management</td>
<td></td>
</tr>
</tbody>
</table>

Tools such as Okta allow for embedding of credentials into the CI/CD pipeline. Several offerings (such as Okta Advanced Server Access) allow for access credentials to be embedded in the DevOps pipeline. This ensures the secure transmission of credentials without compromising the surface area. As security is embedded into the pipeline, it cultivates a culture of security among developers, resulting in a more secure product. Other tools, such as (CyberArk), allow for secrets to be embedded within applications using their solutions.

For organizations with employees working remotely, a centralized IAM solution can help IT gain visibility and maintain control on laptops and devices.

For C-Suite execs, privileged identity management (PAM) solutions protect against identity thefts and abuse of privilege. PAM is based on the principle of least privilege, wherein users only receive the minimum levels of access required to perform their job functions.

Popular PAM providers include:

- BeyondTrust
- Thycotic
- Cyberark

For small businesses, cloud-based identity as-a-Service (IDaaS) solutions can be beneficial. IDaaS combines the benefits and functions of an enterprise-class IAM with the operational advantages of cloud. IDaaS providers include Azure and Okta.

In addition to implementing these solutions, organizations should focus on basics such as proper access control. For instance:

1. Do you have a proper authentication mechanism?
2. Are access controls implemented properly?
3. Are public and private clouds properly segregated to prevent inadvertent or deliberate access?
4. Is there a secure channel between the corporate data center and public-facing entities with proper authentication and authorization in place?

Other steps to manage identities and ease administration include:

1. Implementing unified endpoint management
2. Using MDM and enterprise mobility management (EMM)
3. Using multi-factor authentication
The security operations center (SOC) is key to keeping an organization secure, as it monitors devices present within the organization and logs events that can be used for forensic analysis or other type of investigations if required. SOC is the heart of a large security organization.

Event logging will help in:

1. Identifying security incidents
2. Monitoring policy violations
3. Business process monitoring (e.g., sales process abandonment, transactions, connections, etc.)

The security industry uses SIEM for log aggregation, processing and analysis. Some of the popular SIEM vendors in the market are Arcsight, QRadar and Splunk.

SIEM functionality can be broken down as follows:

- Centralize and Index
- Instrument and Collect
- Search and Analyze
- Monitor and Alert
- Report and Dashboard

Implementing SOAR along with SIEM provides better visibility into security events. SOAR can be used in conjunction with SIEM for security threats and data alerts.

Using AI-driven techniques, SOAR tools analyze large quantities of data and the output can be used to fine tune policies, examine anomalies and guide incident response.

Organizations can adopt in-house SOC or go all in with cloud tools like Slack and O365, which offer better insights when combined with tools such as Splunk and LogRhythm to generate dashboards based on metrics.
Conclusion

By combining risk metrics with application security, integrating IAM solutions with cloud and perimeter, and keeping an eye on all these using the full capabilities of the SOC, organizations can bolster cyber resilience and be prepared to tackle present and future threats.

Proper classification and risk analysis of data helps prevent breaches to a large extent. Using PIM and SSO tools to embed secrets and credentials into code/applications enhances security from start to finish.
Want to learn more?

Visit optiv.com