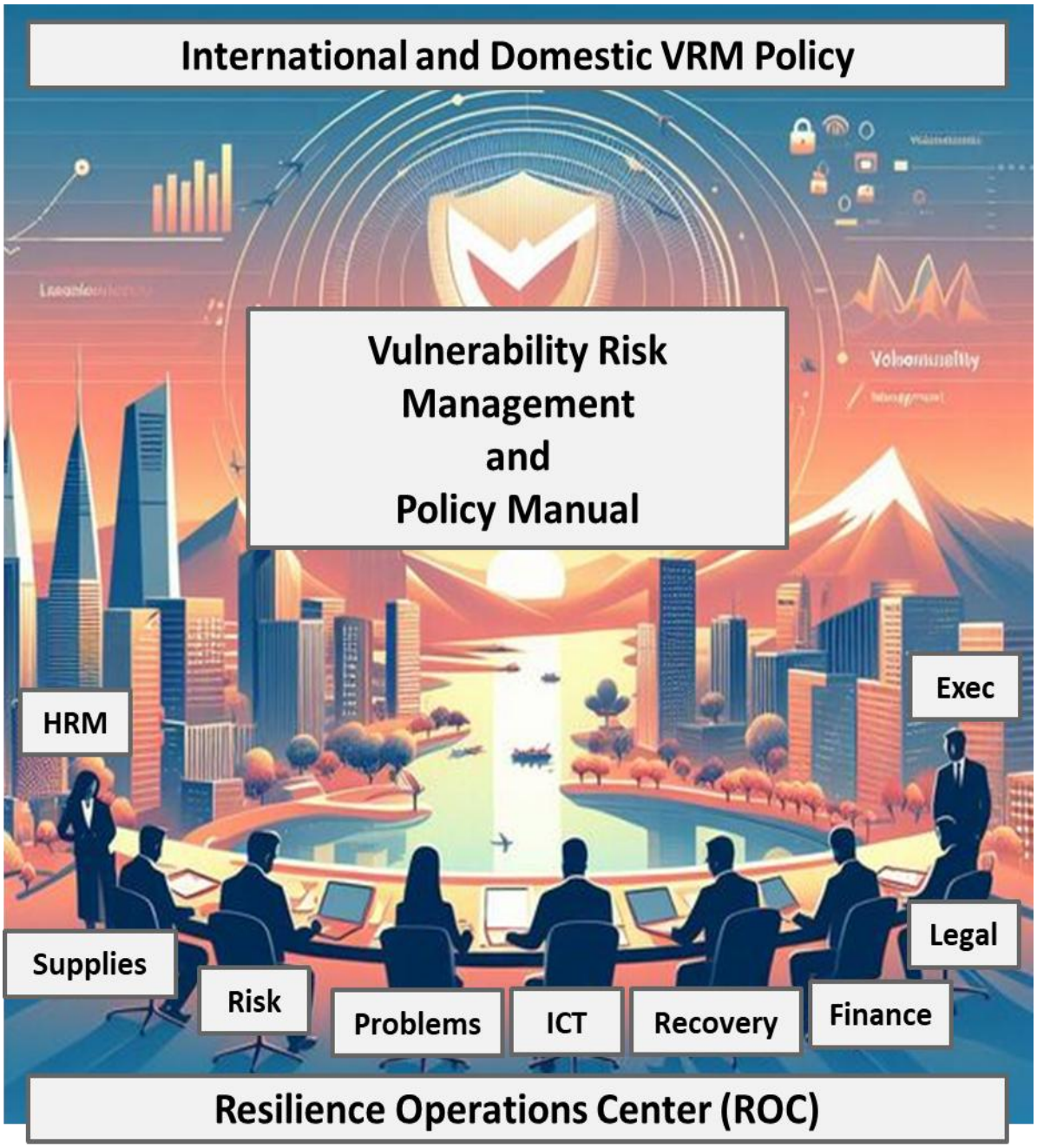


Thomas Bronack, CBCP

President, Data Center Assistance Group, LLC

Email: bronackt@gmail.com

Phone: (917) 673-6992

Contents

What is the Problem currently faced by Organizations?

Organizations are increasingly threatened by Nation-State actors and hackers seeking money through ransomware or stealing trade secrets via malware and lateral movement. Hackers also aim to disrupt business operations and services. Both government and businesses are impacted, prompting DHS/CISA to create the "***Secure by Design***" initiative, enhancing security standards for all components in consumer products and IT systems.

Hackers exploit vulnerabilities within hours or days, while organizations take months to respond with patches or new releases. Hackers can act on publicly available vulnerability information before organizations address the issues.

The staff is currently managing a high workload and using tools to identify problems, analyze their impact, address issues and flaws, report incidents to the product owner, and assist in mitigating the problems. Sometimes, the issue may necessitate a system recovery, and it is important for a manager to be responsible for announcing the need for such a recovery.

There is need for

1. automation to assist in identifying and mitigating encountered technical problems and security violations, and
2. better tool selection, integration, policies, documentation, and personnel training

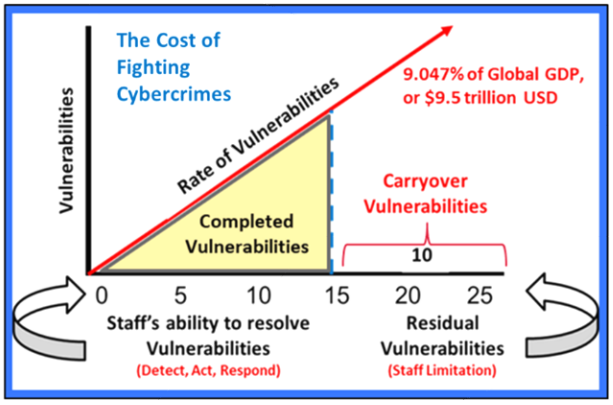
There is a move from SOAR type of products to integrating security and protection with an AI Agent RAG systems design. This movement is supported by the "Secure by Design" philosophy and should be adopted within organizations of all shapes and sizes.

So What?

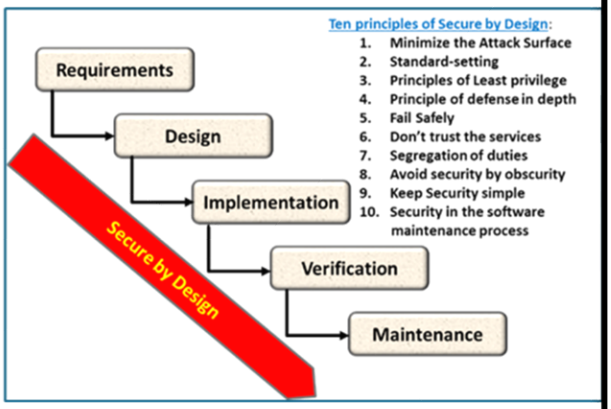
Failing to address the rise in cybercrimes and technology threats can cause your organization to lag competitors, damage its brand reputation, and trigger regulatory fines. Moreover, it could lead to customer loss and publicized attacks. There is no insurance for poor leadership; thus, your organization must reassess its strategies to protect against technical issues, cybercrimes, human errors, and natural disasters.

A new direction will be used by modern technologies to create a shorter path to problem detection and mitigation, resulting in a reduced workload for your staff and a decrease in turnover due to burnout. Your customers will receive better services and products will tend to be error-free and more dependable. The resulting increase in reputation and reliability will increase your bottom line and make for a happier and healthier workplace.

Fighting Vulnerabilities and Secure by Design



The **cost of fighting cybercrimes** and technology threats is estimated at $9.5 Trillion and 9.04 % of Global GDP. Improving the vulnerability fix rate will greatly reduce costs and improve business service continuity and resilience.



The government has developed a "**Whole of Nation**" approach to combat these costs through the "**Secure by Design**" methodology developed by DHS/CISA to safeguard Government, Business, Infrastructure, and Utilities from cybercrimes and technology threats.

What now?

We recommend using vulnerability management tools to identify weaknesses in programming products and vendors within your testing cycle and prior to entry into the production environment. These tools will include the ability to locate software component levels within an application (like assemblies and components that make assemblies in cars). Once located, programs will be examined against vulnerability databases to determine if there are any known problems associated with them that can be corrected through patches or new releases. The corrections will be performed prior to the production

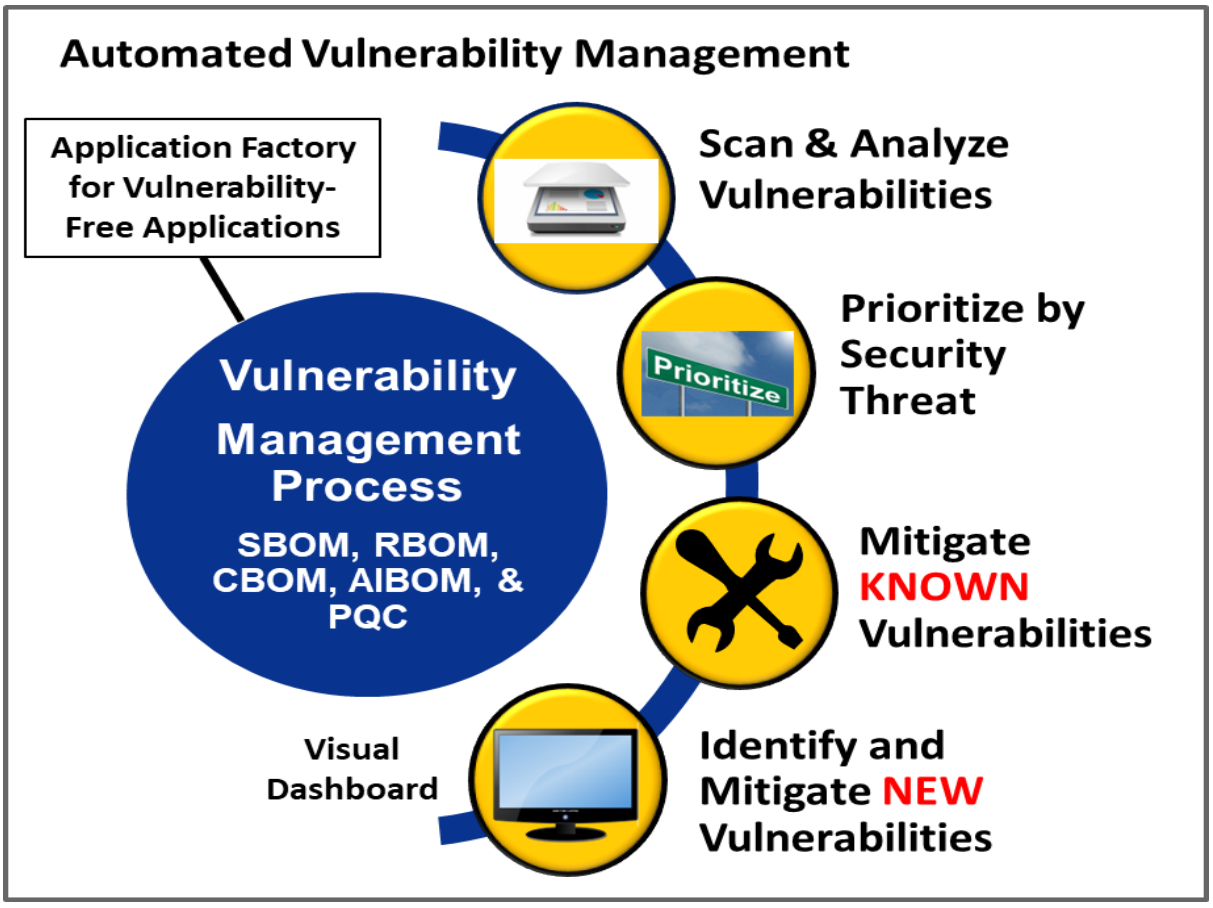
acceptance process. A Security Score will be developed for all your applications, with acceptance levels that function as gateways to a product's lifecycle. If your security score is too low, then you will not be allowed to pass the gate.

A vulnerability management study should be conducted within your organization to uncover weaknesses that can be corrected through automation, new policies, and standardized procedures – a Vulnerability Management Policy based on tools and actions associated with those tools.

What is Vulnerability Management and why does your company need it?

Vulnerability management helps businesses identify and fix potential security issues before they become serious cybersecurity concerns. By preventing data breaches and other security incidents, vulnerability management can prevent damage to a company's reputation and bottom line.

How vulnerability management works



Threat and vulnerability management uses a variety of tools and solutions to prevent and address cyberthreats. An effective vulnerability management program typically includes the following components:

Asset discovery and inventory

IT is responsible for tracking and maintaining records of all devices, software, servers, and more across the company's digital environment, but this can be extremely complex since organizations have thousands of assets across multiple locations. That is why IT professionals turn to asset inventory management systems, which help provide visibility into what assets a company has, where they are located, and how they are being used.

Vulnerability scanners

Vulnerability scanners usually work by conducting a series of tests against systems and networks, looking for common weaknesses or flaws. These tests can include attempting to exploit known vulnerabilities, guessing default passwords or user accounts, or simply trying to gain access to restricted areas.

Patch management

Patch management software is a tool that helps organizations keep their computer systems up to date with the latest security patches. Most patch management solutions will automatically check for updates and prompt the user when new ones are available. Patch management systems also allow for deployment of patches across multiple computers in an organization, making it easier to keep large fleets of machines secure.

Configuration Management

Security Configuration Management (SCM) software helps to ensure that devices are configured in a secure manner, that changes to device security settings are tracked and approved, and that systems are compliant with security policies. SCM tools include features that allow organizations to scan devices and networks for vulnerabilities, track remediation actions, and generate reports on security policy compliance.

Security incident and event management(SIEM)

SIEM software consolidates an organization's security information and events in real time. SIEM solutions are designed to give organizations visibility into everything that is happening across their entire digital estate, including IT infrastructure. This includes monitoring network traffic, identifying devices that are trying to connect to internal systems, keeping track of user activity, and more.

Penetration testing

Penetration testing software is designed to help IT professionals find and exploit vulnerabilities in computer systems. Typically, penetration testing software provides a graphical user interface (GUI) that makes it easy to launch attacks and see the results.

Products also offer automation features to help speed up the testing process. By simulating attacks, testers can identify weak spots in systems that could be exploited by real-world attackers.

Threat intelligence

Threat protection software provides organizations with the ability to track, monitor, analyze, and prioritize potential threats to better protect themselves. By collecting data from a variety of sources—such as exploit databases and security advisories—these solutions help companies identify trends and patterns that could indicate a future security breach or attack.

Remediation vulnerabilities

Remediation involves prioritizing vulnerabilities, identifying appropriate next steps, and generating remediation tickets so that IT teams can execute on them. Finally, remediation tracking is a valuable tool for ensuring that vulnerability or misconfiguration is properly addressed.

Problem Statement

- **Weekly Cost** of performing Vulnerability Management in **2019 was $1.5 million.**
- **Vulnerability volume surpasses staff ability to keep up**, increasing potential losses to companies and shareholders (**cybercrime costs** are predicted to reach a staggering **$9.5 trillion in 2024)**.
- **Hackers track vulnerabilities and take advantage of the exposures** listed to create harm before companies respond to posted vulnerability repairs (Patches, New Releases, Reconfigurations, etc.).
- **Cost of Vulnerability Management by Staff was $1.5 million in 2019** and has grown every year since.
- **Newly introduced laws and regulations** impact Board of Directors (**SEC Rule 2023-139**) and require a vulnerability-free production environment (**EO 14028**) with the use of a Software Bill of Material (**SBOM**) providing a list of all application software components (Open-Source, Vendor, External/Internal) that identifies existing vulnerabilities to be corrected prior to production.
- **DHS/CISA introduced "Secure by Design"** concept to support vulnerability reduction through improved development and deployment techniques, like: DevSecOps, MLOps, Improved Testing and Acceptance, Code Verification (Statis, Dynamic, Interaction, and Runtime), SBOMs, Continuous Threat Exploitation Management (CTEM), and more.
- **Global firms must adhere to international and domestic laws and regulations by deploying a Vulnerability Management** Policy with supportive staff to maintain documents and procedures going forward.

Future Costs associated with Cybersecurity Management

1. **Global cybercrime costs** are predicted to reach a staggering **$9.5 trillion in 2024**, a 15% increase from 2023. (Source: Cybersecurity Ventures).
2. **Eighty-five percent of cybersecurity professionals** believe the use of generative **AI by attackers** will lead to more sophisticated and undetectable phishing attacks. (Source: Cobalt.io).
3. **Sixty-two percent of phishing attacks in 2023 used spear phishing** attachments, highlighting the growing threat of supply chain attacks. (Source: IBM Security X-Force).
4. **Ninety-four percent of malware is delivered via email,** making businesses prime targets for cyberattacks. (Source: Panda Security).
5. **Ninety-five percent of security breaches are caused by human error**, emphasizing the importance of cybersecurity awareness training. (Source: Specops Software).
6. The **global cybersecurity market is expected to reach $266 billion by 2025**, reflecting the increasing demand for security solutions. (Source: Exploding Topics).
7. **Eighty percent of organizations plan to adopt AI-powered security solutions by 2024**, recognizing AI's potential in threat detection and prevention. (Source: Crowdstrike).
8. **The shift to remote work has expanded the attack surface**, with 70% of office workers using work devices for personal tasks, potentially introducing security vulnerabilities. (Source: NinjaOne).
9. **The global cybersecurity workforce is facing a significant skills gap**, with an estimated 3.5 million unfilled positions by 2025. (Source: Cybersecurity Ventures).
10. **Cybersecurity insurance is becoming increasingly popular**, with 60% of organizations** expected to have cyber insurance by 2025. (Source: Varonis).
11. **Chalubo Malware** damaged the firmware of 600,000 servers, which had to be replaced because of the attack.

Laws and Regulations impacting the organization.

- Presently, implementing Applications and Services can include vulnerabilities and malware, which can cost your company lost revenue, brand reputation, fines and penalties, burdening your staff and resulting in elevated levels of turnover.

- A method must be implemented to catch vulnerabilities and malware prior to production acceptance.

- New Laws have been mandated in the United States and Europe to address the problems, including:
-
    - **Executive Order 14028** – Improving Nation's Software Security Supply Chain and mandating SBOMs.

- **OMB M-22-18** and M-23-16 – Improving the Defense and Resilience of Government Networks
- **SEC Rule 2023-139** – Disclosure of Material Cybersecurity breaches to protect shareholders.
- **FDA** – Control over medical device supply chain and cybersecurity problems
- **CRA** – European Cyber Resilience Act – Hardware and Software Components cyber requirements
- **DORA** – Digital Operational Resilience Act – Strengthen the financial sectors resilience.
- **GDPR** – EU Digital Rights of their Citizens
- **NIS2 Directive** - A high common level of cybersecurity
- **Deploying AI Security Systems -** joint paper from CISA, NSA, and DOJ on employing AI Security

- Once the development process is upgraded and new Standards and Procedures created, an Awareness Program must be developed and the Staff Trained.

- New Procedures must be integrated into the staff's daily process for new and changed applications and services, with automated support through RPAs whenever feasible.

International Laws

Companies that collect data on citizens in the European Union (EU) need to comply with strict new rules around protecting customer data. The General Data Protection Regulation (GDPR) sets a new standard for consumer rights regarding their data, but companies will be challenged as they put systems and processes in place to maintain compliance.

Compliance will cause concerns and new expectations on security teams. For example, the GDPR takes a wide view of what constitutes personal identification information.

Companies will need the same level of protection for things like an individual's IP address or cookie data as they do for name, address and Social Security number.

The GDPR defines roles that are responsible for ensuring compliance:

- data controller, and
- data processor and the data protection officer (DPO).

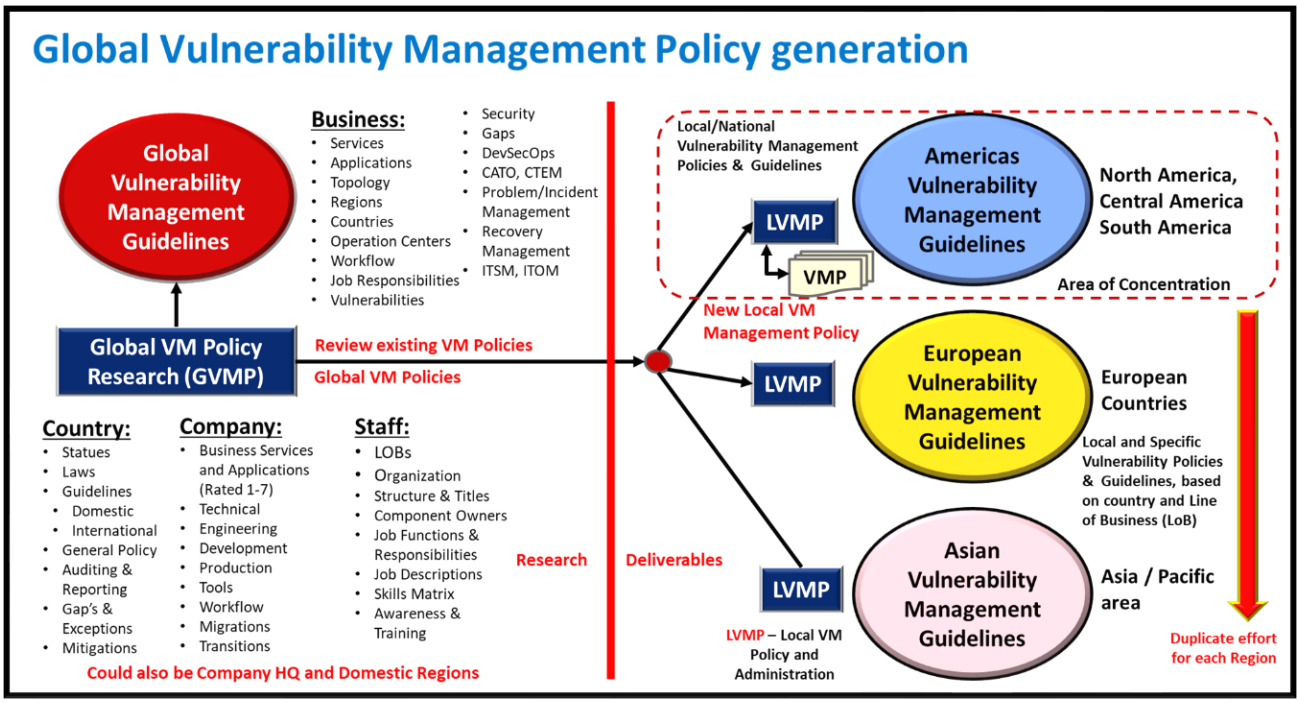
The data controller defines how personal data is processed and the purposes for which it is processed. The controller is also responsible for making sure that outside contractors comply.

See What are the GDPR Requirements for details.

- How GDPR has inspired a global arms race on privacy regulations
- The EU's GDPR
- Laws across Asia-Pacific

- Laws in US states
- California's CPRA
- Laws in Canada
- Australia's CDR and
- Australia's proposed GDPR-inspired privacy law
- New Zealand's Privacy Act
- The UAE's data law
- China's PIPL

What is a Resilience Operations Center



The **Resilience Operations Center (ROC)** is a strategic framework that organizations adopt to enhance their operational resilience and effectively manage supply chain risks. The key aspects of a ROC are:

1. **Purpose and Principles**:
   a. The ROC aims to achieve and maintain operational resilience by aligning risk management with organizational goals.
   b. It breaks down silos within an organization and modernizes threat detection and mitigation using technologies like automation, artificial intelligence, and natural language processing.
   c. By adhering to these principles, organizations gain insight and agility to capitalize on unforeseen opportunities.

2. **Challenges to Operational Resilience**:
   a. Operational resilience breakdowns can occur due to factors like:
      1. Weak governance processes at distinct levels (board, senior management, etc.).
      2. Incomplete business continuity management for critical operations functions.
      3. Lack of scenario planning and analysis to anticipate disruptions.
      4. Insecure information systems and ineffective monitoring.
3. Addressing these inefficiencies is crucial to prevent financial losses and mitigate operational risks.
4. **ROC Success Factors**:
   a. Understand industry-specific operational risks.
   b. Prioritize IT hygiene, including active threat monitoring and security patching.
   c. Combine scenario planning with forecasting to refine plans.
   d. Maintain secure information systems and effective monitoring practices.

In summary, the ROC framework provides organizations with the tools to proactively manage risks, enhance resilience, and respond effectively to supply chain challenges. Whether it is financial services, manufacturing, or any other industry, the ROC helps organizations stay prepared and agile in the face of modern risks.

Benefits associated with a Resilience Operations Center (ROC)

The **Resilience Operations Center (ROC)** represents an innovative approach to modern supply chain security and continuity, delivered through an enterprise-wide framework that ensures risk management objectives are tied to organizational goals. It brings previously siloed groups together to form agile and informed teams that are empowered to use data intelligently and react quickly to changing circumstances. The ROC framework is deployed in a variety of industries, and they are using ROCs to dramatically change outcomes for the better.
A ROC is effective at fostering Operational Resilience because it helps organizations overcome difficult internal challenges, including:

- **Shifting behavior from response to prevention.** Deep, comprehensive planning helps teams anticipate events, evaluate alternatives, prevent disruptions, and model all scenarios and options. Reacting to events as they happen is not sufficient in today's competitive market.
- **Making risk management an organization-wide job**, not the domain of one person or team. Most approaches to managing risk are siloed within business units, such as procurement, supply chain operations, and IT, or in single focus organizations, such as information security and compliance. When everyone is a stakeholder, organizations improve how they coordinate, collaborate, prepare, and respond.
- **Managing risk beyond the walls of your company**. Organizations rely on an extensive network of suppliers and partners for developing and producing their products and services. Identifying relationships in the extended supply chain to the

Nth tier helps organizations decide if those connections are good or bad business choices, thereby identifying and preventing potential risk. And, most importantly, remember that you are a third party to myriad other organizations, which are now looking at you through their own risk management lens.

ProCap 360 displays Vulnerabilities and their Score.

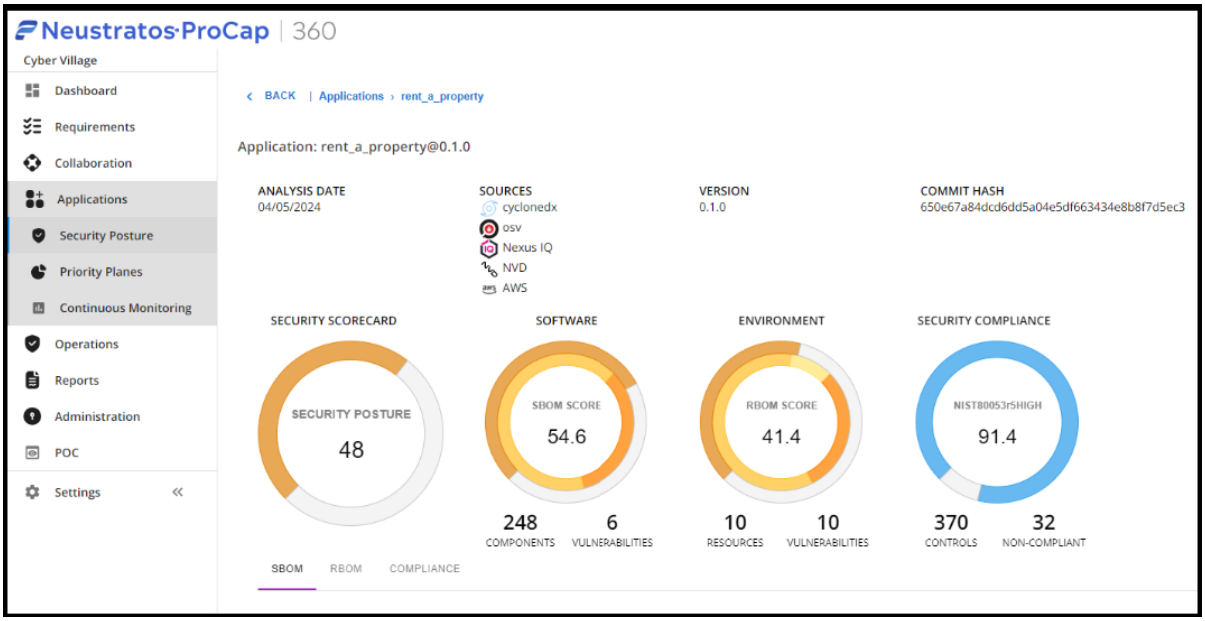


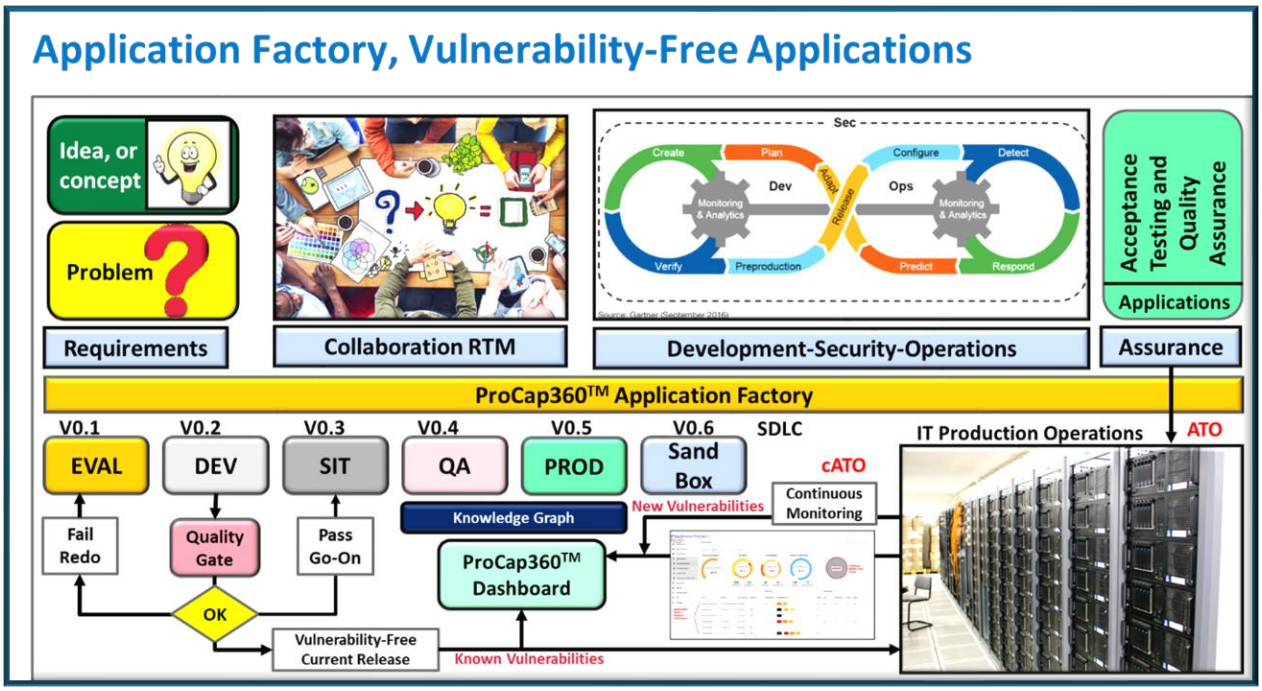
Figure 1: Acceptable vulnerability security scorecard for a Gateway to Production.

Vulnerability management tools like **ProCap 360** use SBOM components to calculate and communicate an application security score. In the example above, the Application Security Posture is forty-eight, the sum of SBOM Score and RBOM scores are divided by two. The SBOM score is 54.6 across 248 components with six vulnerabilities. The environment score is 41.4, as shown by the RBOM Score, and the NIST800r5r5HIGH, which checks 370 controls and found 32 Non-Compliant. Applications can be examined in any environment (Development, Test, Production, etc.).

A drill-down screen provides programs that are included in the application. The application name is shown under the APP column. Its version is shown under the Version column, and the Last Analysis date is provided. The Sources column lists the public vulnerability databases that were searched to define this vulnerability. The are thirty-three components listed with their associated Vulnerabilities. Drill-down functions are provided to look up the vulnerability, its identifier, description, and recommended mitigation.

Gates can be established to stop an application from leaving one development stage until it has achieved a specified Security Posture. Through this technique, you can control the development and maintenance of applications to adhere to vulnerability-free requirements.

Application Factory and producing vulnerability free applications.



An Application Factory is employed to build business applications, products, and services. Starting with an Idea for a new business service, the idea goes through Brainstorming, collaboration, innovations, and a final concept with requirements gathered through stakeholders into a Requirements Transparency Matrix (RTM). The Engineering department creates solutions that meet RTM requirements, and an Agile Epic is created, then Agile Features and Functions defined, and finally Agile Stories are used to develop the services.

By following the steps diagramed above, you will ensure all application components are at current release levels and free of known vulnerabilities. Utilizing Continuous Monitoring will detect new vulnerabilities that impact production applications, so that quick mitigations can be applied to reduce exposures to hackers.

Contact us for more information.

Thomas Bronack, CBCP
President, Data Center Assistance Group, LLC
Email: bronackt@gmail.com or
bronackt@dcag.com
Website: http://www.dcag.com
Phone: (917) 673-6992

