PLUTORA

Value Stream Management

An ideal framework for DevSecOps and Continuous Security

This eBook explains what Continuous Security is, why Continuous Security is critical to securing your enterprise, how Continuous Security solutions, based on Value Stream Management Platforms, such as Plutora's, can help your organization achieve high levels of security and what is needed to accomplish a Continuous Security solution for your organization.

Table of Contents

Continuous Security Landscape 4

Continuous Security Defined 6

Value Stream Management for Continuous Security 7

VSM Platforms for Continuous Security 10

Plutora's VSM Platform Meets Continuous Security Requirements 12

Continuous Security Pain-Points 14

- Security visibility over the end-to-end value stream 16
- Business and Operation Impacts 17
- Different Stakeholders Need Different Information 19
- Disconnected People and Teams 20
- Disconnected Processes and Tools 22
- Separate Pre-Prod and Prod Environments 23
- Disparate Security Metrics 24
- Scope of Data Collection 25
- Security API 26
- Real-Time Threat Detection 27
- Synthetic Security Monitoring 28
- Automated Security Response 29

Benefits of VSM-Based Continuous Security Solutions 30

Call to Action 32

Key Takeaways 35

Continuous Security Landscape

There is no such thing as 100% security. The threat landscape evolves continuously. Enterprises wishing to secure valuable assets, operations, finances, and reputations must continuously do everything they can to understand and mitigate security risks for themselves and their stakeholders.

As indicated in the book "Engineering DevOps", by Marc Hornbeek, Continuous Security encompasses security practices in both development and deployment processes. DevSecOps continuous delivery practices provide opportunities to improve security posture by using practices before deployment, while SRE-Ops continuous operations practices provide opportunities to secure production environments after deployment. Both DevSecOps and SRE-Ops have the tenet that security is everyone's responsibility.

Despite these good practices and tenets, the current state of many organizations is that pre-production DevSecOps teams and in-production SRE-Ops teams operate in silos with the deployment-to-production process being the primary boundary between them. True Continuous Security requires that pre-production DevSecOps teams and in-production SRE-Ops teams operate security practices collaboratively, end-to-end, across the entire value stream from planning through and into operations.

There are numerous examples of “supply-chain attacks” where attackers have taken advantage of silos by injecting malicious code into pre-production processes or code sources, and then exploiting the code when deployed to production. For example, the SolarWinds Orion network monitoring tool supply chain attack occurred because credentials within the source code management system of the tools vendor was compromised, which enabled attackers to inject backdoor malware code into the tool. Once that code was released and deployed to thousands of organizations, the attackers were able to gain access to client information, which remained undetected for a long time.

According to a December 2021 Global Security Attitude Survey by CloudStrike, supply chain attacks are on the rise by 430%, and 59% of organizations that suffered their first software supply chain attack did not have a response strategy.

What is needed is an end-to-end security management practice that provides visibility and rapid response actions across the many end-to-end value streams of enterprises, from planning, development, integration (including code and tools from suppliers), through deployment and in-production operations. A comprehensive solution that encompasses both pre-production and in-production processes requires an architecture and capabilities that are suitable for automation of end-to-end security practices. This eBook will explain how Value Stream Management platforms such as Plutora’s have the capabilities needed for Continuous Security solutions.

Continuous Security Defined

There is no standard industry definition for Continuous Security. Some definitions that exist equate Continuous Security to DevSecOps. However end-to-end security assurance is often limited due to silos. DevSecOps practices are not sufficient to secure enterprise operations.

Despite "Ops" being part of the name, software development teams using DevSecOps practices are concerned with securing the delivery pipeline and deliverables to production, while SRE-Ops teams are more concerned about securing production environments after deployment to production. Meanwhile, the software security teams tend to be a separate silo, focusing security expertise and efforts primarily on defensive production side security practices. Security teams' engagement with preventative software deliveries through recent DevSecOps practices is growing as more and more organizations transform their applications to take advantage of DevOps and SRE practices.

The bad actors see the boundaries of these silos as big cracks in the metaphorical organization's castle walls, which are ripe for exploitive breaches. As indicated in *Figure 1*, Continuous Security is the combined set of DevSecOps security practices that continuously work to reduce the chance of delivering vulnerabilities, and defensive SRE-Ops security practices that protect software deployed to production, both supported intimately by security experts as coaches.

In other words, continuous security is concerned with the entire value stream which includes the end-to-end spectrum of practices from planning through design, coding, integration, delivery, and in-production.

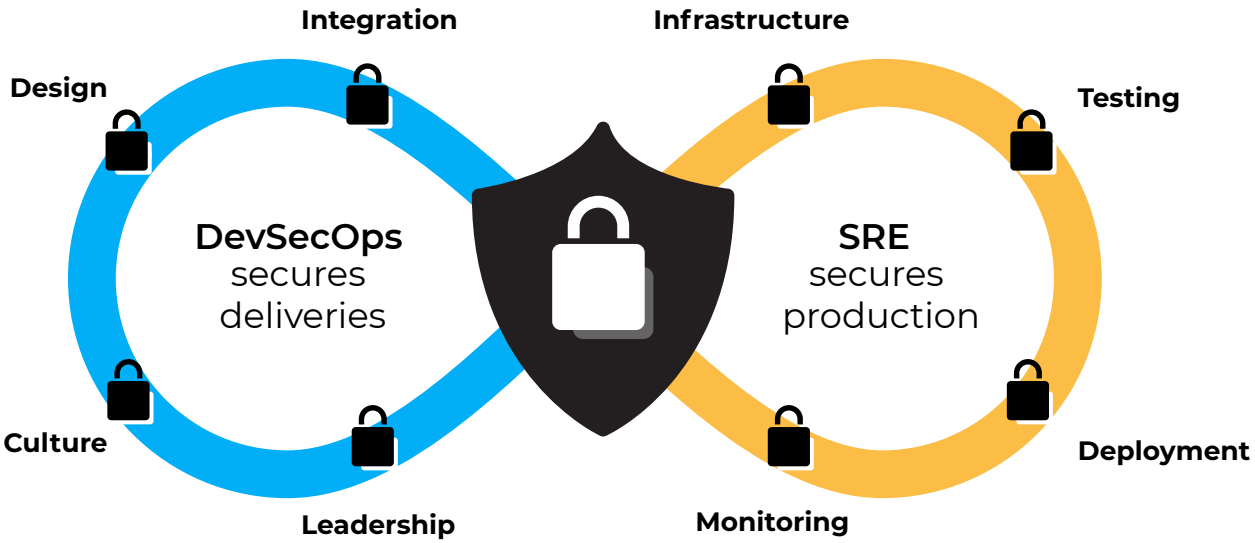


Figure 1. Continuous Security

Value Stream Management for Continuous Security

Value streams are everything in the software delivery lifecycle (SDLC) from idea to production needed to deliver software products or services to customers.

Enterprises typically have many operational value streams to deliver a portfolio of services and improvements to those services to customers. To manage value streams, organizations need to first gain end-to-end visibility and control of the multiple, interconnected value streams throughout their portfolio.

Value Stream Management (VSM) enables organizations to deliver high quality software faster to their customers while reducing risk, including security risks. Continuous security depends on strategic collaboration and integration of people, processes, and technology practices.

As illustrated in *Figure 2*, Value Stream Management encompasses all the people, process and technologies components that contribute to each stage in the value streams, including security risk management.

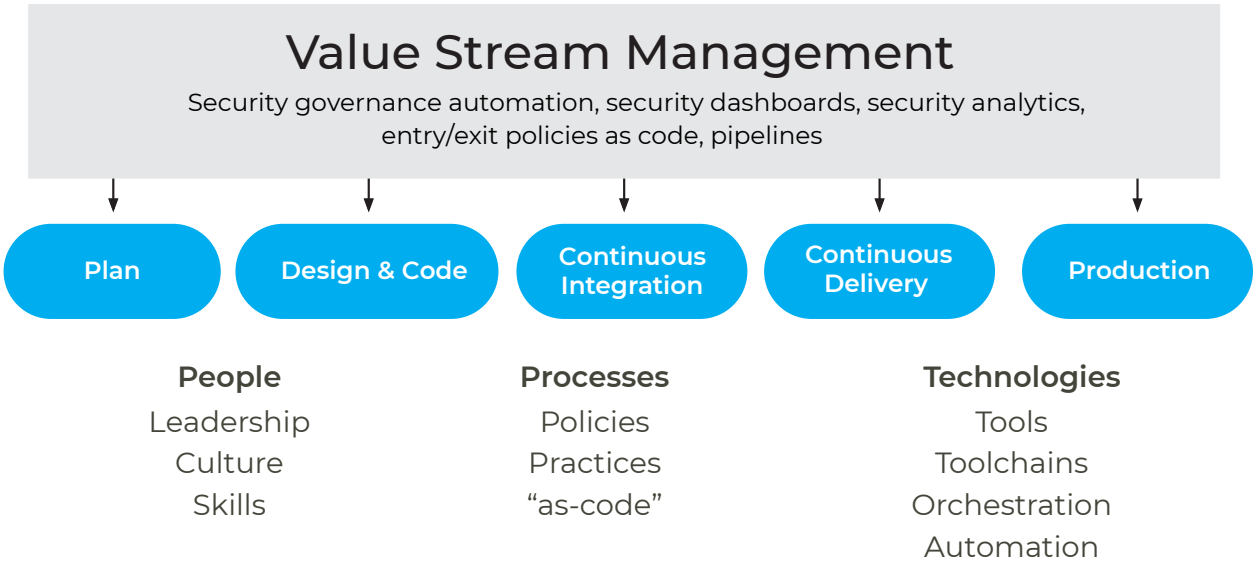


Figure 2. VSM with Security - People, Process and Technologies

As illustrated in *Figure 3*, in high performance organizations, people from across the spectrum of roles and value stream steps in an organization have specific accountabilities for security, but also collaborate and share responsibilities to ensure security practices are addressed. Value Stream Management aims to reduce communication gaps between departments and roles. VSM platforms provide capabilities to support communication of security information between teams.

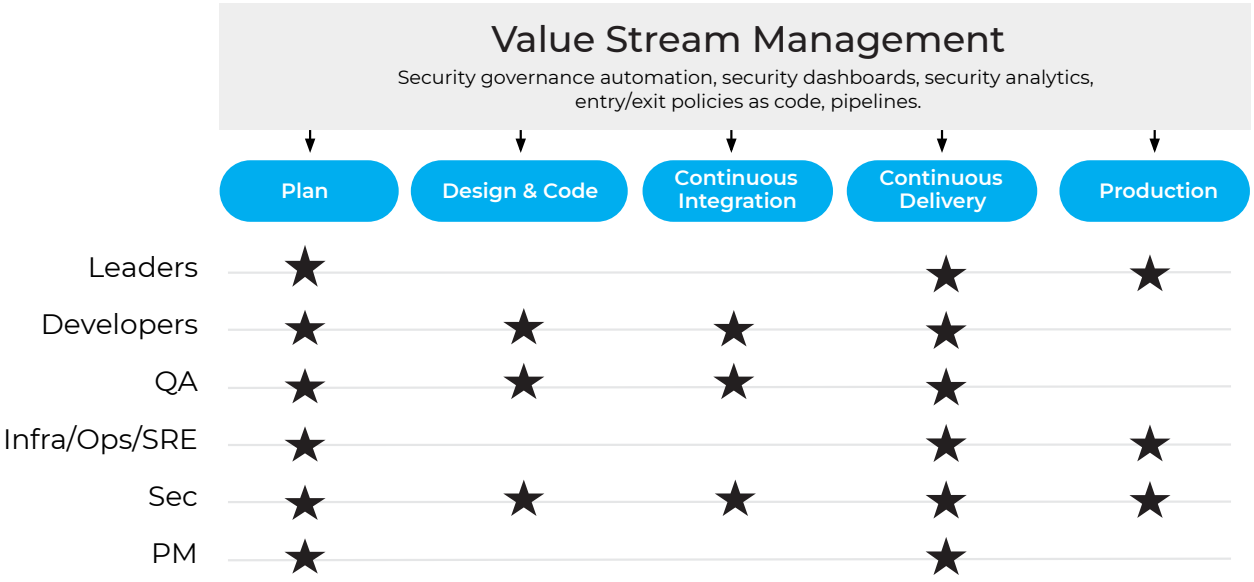


Figure 3. VSM Continuous Security Platform – People

Figure 4 illustrates that continuous security assurance requires automation of multiple security assurance processes at each step in the value stream. VSM platforms provide consistent capabilities to enable orchestration and automation of security practices.

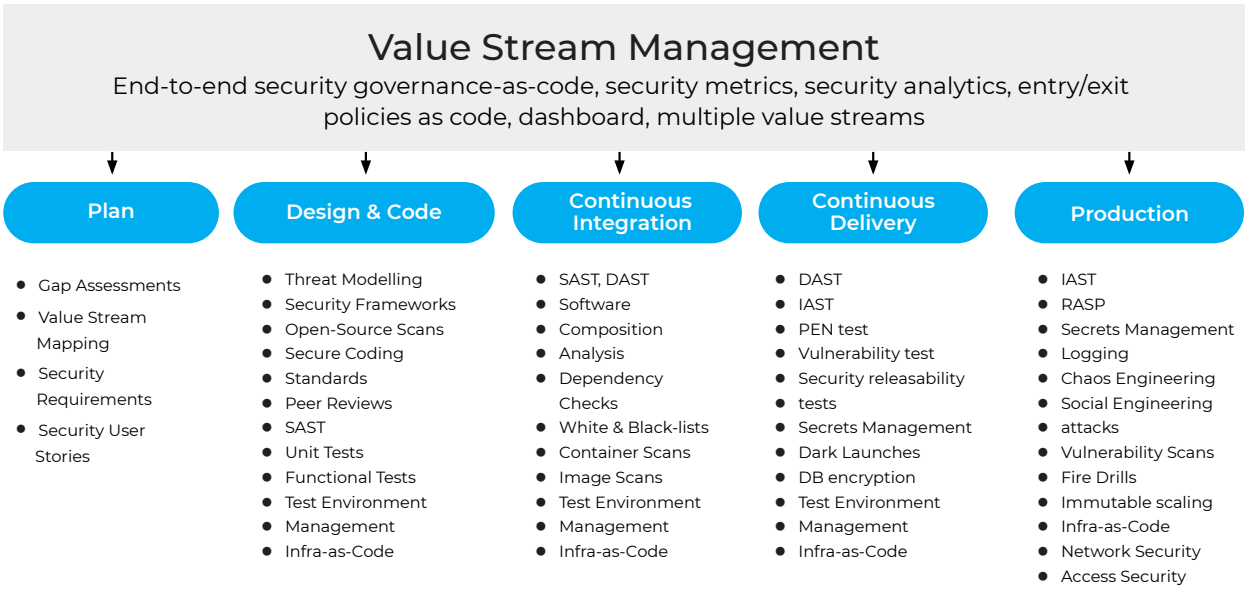


Figure 4. VSM Continuous Security Platform –Processes

Automation depends on tools that are designed for specific security controls. *Figure 5* shows examples of specialized security tools that are essential to operate security processes at different states of the value stream. These tools operate together as an interconnected continuous tool chain. A value stream management platform provides the ability to connect the tools together and use common automation capabilities to automate security practices across the value stream.

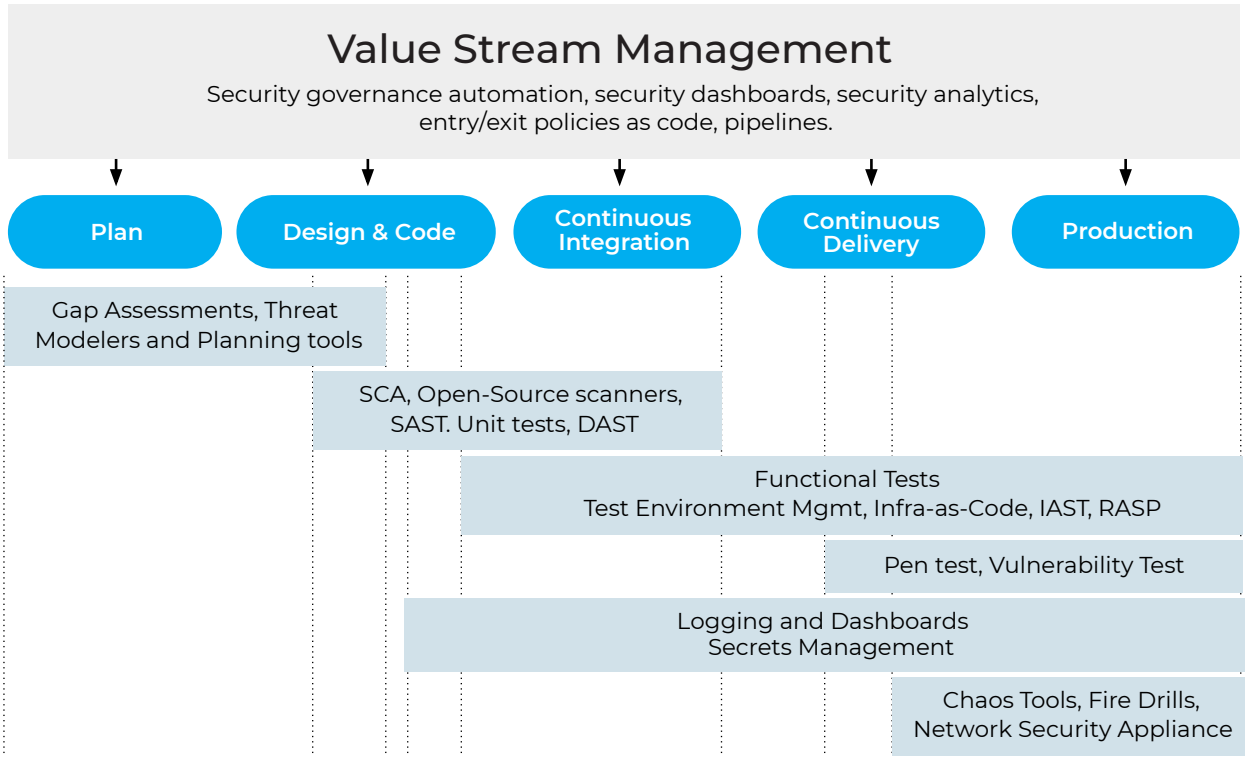


Figure 5. VSM Continuous Security Platform –Technologies

VSM Platforms for Continuous Security

The implementation of an enterprise Continuous Security solution architecture can be accelerated by leveraging existing Value Stream Management (VSM) Platforms.

The continuous security architecture, shown in *Figure 6*, illustrates why a true Continuous Security architecture, with visibility and controls over DevSecOps-level development environments and SRE-lead production environments, requires more than traditional Security Information and Event Management (SIEM) dashboards which are typically derived from individual or a limited number of security tools.

At the highest level, an Enterprise Continuous Security architecture requires a Smart UI layer to consume security data from many DevSecOps and SRE sources and to organize data sets into different display formats that suit the needs of different types of stakeholders. For example, executives want strategic level summaries that help them direct security actions across their entire organization while DevOps or SRE engineers want more detailed information to assist in their roles. This layer also provides the flexibility to provide compliance data to auditors.

The underlying layers consist of data collectors that collect information from DevSecOps and SRE tools across the enterprise value streams into a Data Lake. In this way an API can be used to access any data in the Data Lake, as needed, to meet the various needs of different dashboard stakeholders. While not shown on this diagram, this architecture provides the flexibility for other automated programs to access data from the Data Lake to effect automated actions and response to security events and to implement sophisticated analysis and observability programs.

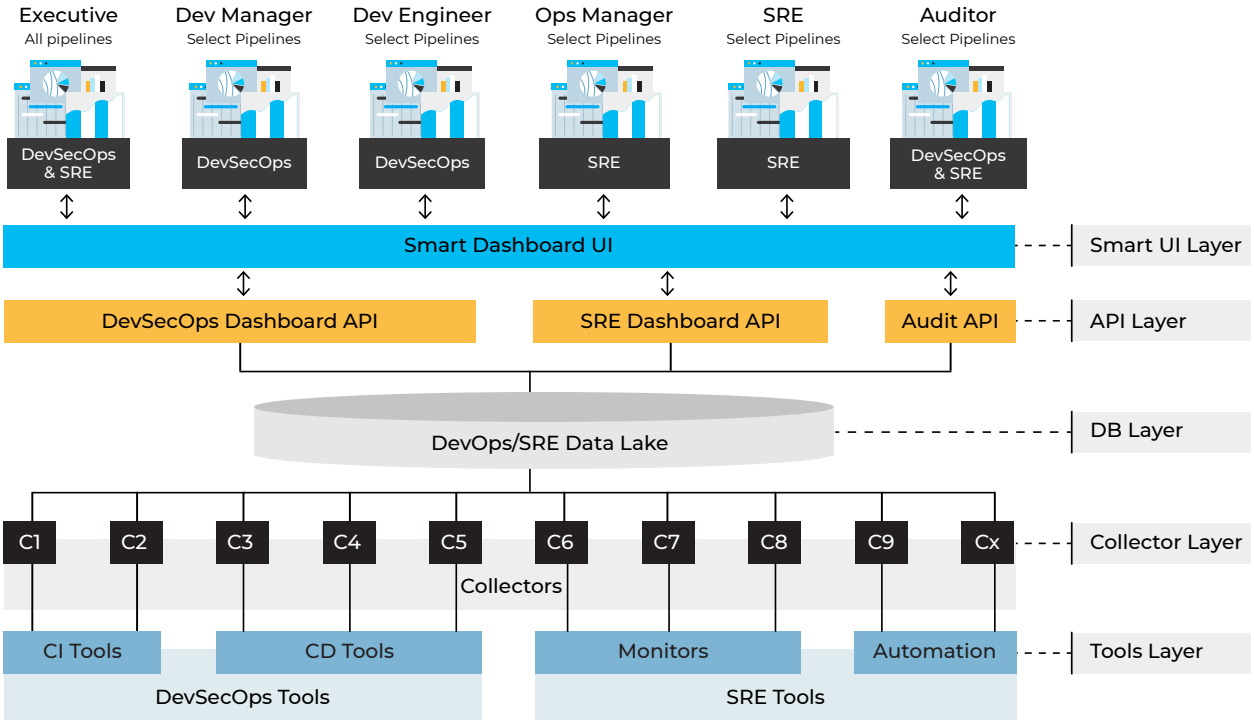


Figure 6. Continuous Security Framework Architecture

Plutora's VSM Platform Meets Continuous Security Requirements

The Plutora VSM platform is designed to support visibility, analysis, orchestration, and automation of enterprise value streams. Available tool plugins enable the VSM platform to control and observe a large variety of existing security tools into a toolchain and can be extended to others.

A common data model at the heart of the system enables a common approach for security data storage and analysis.

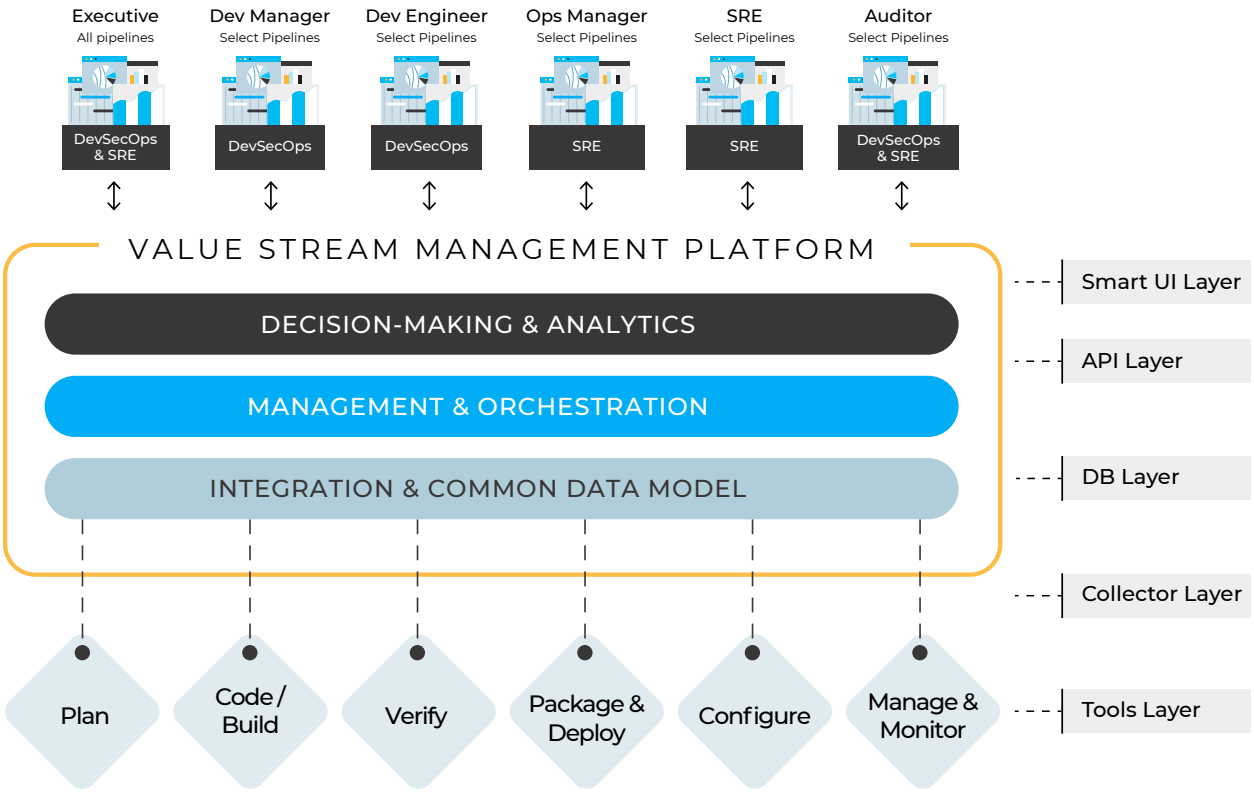


Figure 7. Plutora's VSM Platform as a Continuous Security Framework

Figure 8 shows a comparison of the Plutora VSM platform capabilities, shown in *Figure 7*, to the Continuous Security Dashboard architecture presented in *Figure 6*. The comparison indicates a one-to-one correspondence. The VSM tool has the requisite flexible data models, large number of tool plugins, flexible dashboarding and automation capabilities that map directly onto the architecture layers and requirements presented in the prior visuals.

There is no need to develop a customized framework for your Continuous Security solution, because VSM platforms like Plutora's address continuous security pain-points as explained in the following sections.

Value Stream Management Platform Capability	Current Capability? I (1-5)
Smart UI layer suitable to create different dashboards for different stakeholders.	5
Integrate data so that people across DevSecOps Deployment and SRE Production teams can see the same information.	5
Compatible with DevSecOps and SRE processes and tools.	5
Compatible with pre-production and production deployment environments.	5
Create metrics for DevSecOps and SRE Security in production.	5
Collectors and Security Data Lake for DevSecOps and SRE data.	5
Flexible API for security data transfers from DevSecOps and SRE sources.	5
Realtime security data transfer performance from DevSecOps and SRE sources.	5
Orchestration and automation capabilities suitable for synthetic security monitoring.	5
Orchestration and automation capabilities suitable for triggering automated security responses.	5
CSDR Scores	5

Figure 8. VSM Platform Matches Continuous Security Requirements

Continuous Security Pain-Points

As organizations advance to more mature, higher performance evolutions of their digital transformations, they need more advanced security assurance technologies and practices to achieve Continuous Security by addressing key pain-points and requirements including those listed below.

- Security visibility over the end-to-end value stream.
- Overcoming business and operational requirements for security.
- Smart UI layer suitable to create different dashboards for different stakeholders.
- Integrating data so that people across DevSecOps Deployment and SRE Production teams can see the same information.
- Compatibility with DevSecOps and SRE processes and tools.
- Compatibility with pre-production and production deployment environments.
- Creating metrics for DevSecOps and SRE Security in production.
- Collectors and Security Data Lake for DevSecOps and SRE data.
- Flexible API for security data transfers from DevSecOps and SRE sources.
- Realtime security data transfer performance from DevSecOps and SRE sources.
- Orchestration and automation capabilities suitable for synthetic security monitoring.
- Orchestration and automation capabilities suitable for triggering automated security responses.

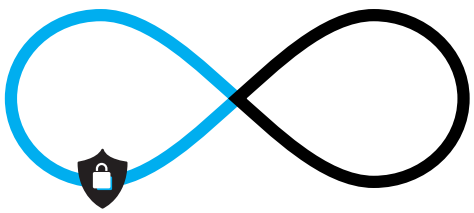
The following pages explain each of the pain-points and how the Plutora VSM platform addresses each pain-point.

Security visibility over the end-to-end value stream

There is no shortage of security dashboards. When asked about security dashboards, most security teams proudly demonstrate their favorite **Security Information and Event Management (SIEM) Dashboards.** Many security product vendors offer a dashboard solution for SIEM applications that spotlight the features of the tools that they sell. The more complete SIEM dashboards **provide a more consolidated view of data to show a "big picture" understanding of your cybersecurity threat landscape** by collecting, aggregating, and analyzing security threats and operational data generated from tools deployed to production infrastructures.

A Continuous Security Dashboard, on the other hand, as shown in *Figure 9*, provides visibility of end-to-end security controls across the value stream including not only in-production security controls, but also DevSecOps security data development security controls.

By combining development and production security collectors and controls within a single VSM platform a Continuous Security Dashboard can provide more comprehensive end-to-end visibility of security controls and activities.



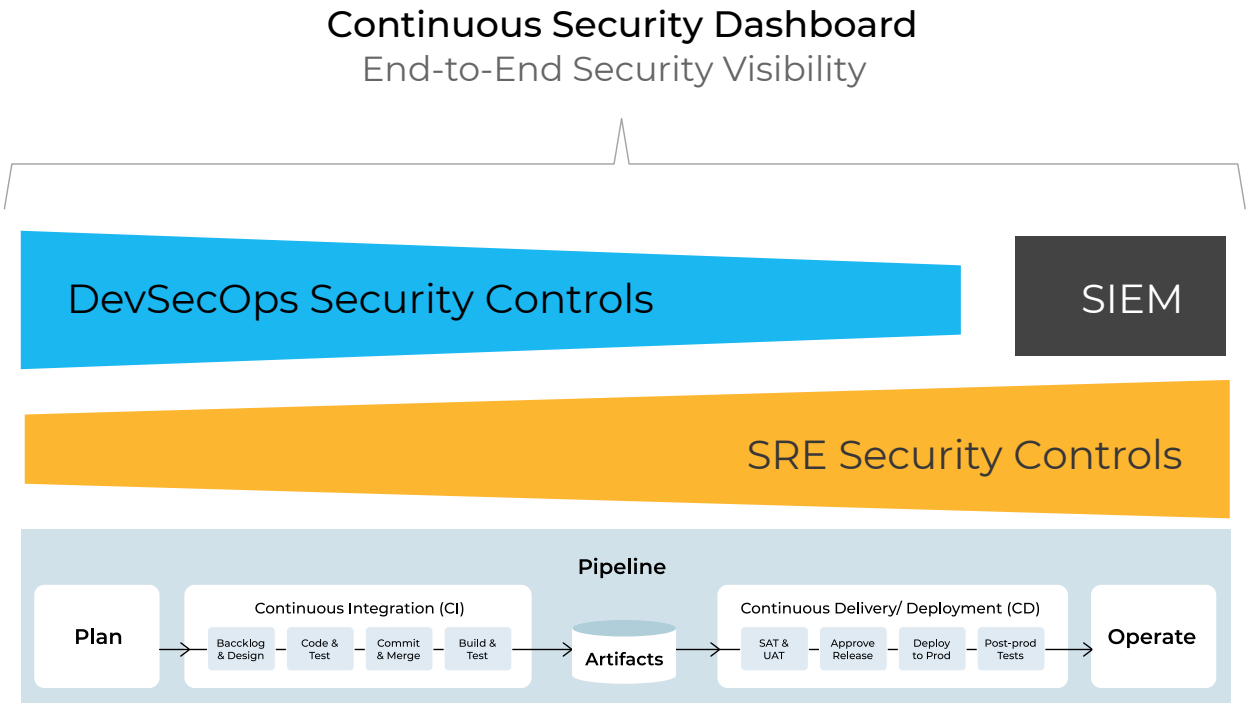


Figure 9. Enterprise Continuous Security Dashboard

Business and Operation Impacts

The lack of an end-to-end Continuous Security solution can impact the operation and business severely, as shown in *Figure 10*.

When DevSecOps teams and SRE-Ops teams do not have a consistent view of security data then collaboration around security monitoring and security issue resolution is impacted. Each team has a view limited by the dashboard for their own silo. This inhibits their ability to share their expertise, tools, processes, and data. Each silo too often gets locked into their local solutions that differ from those they need to collaborate with.

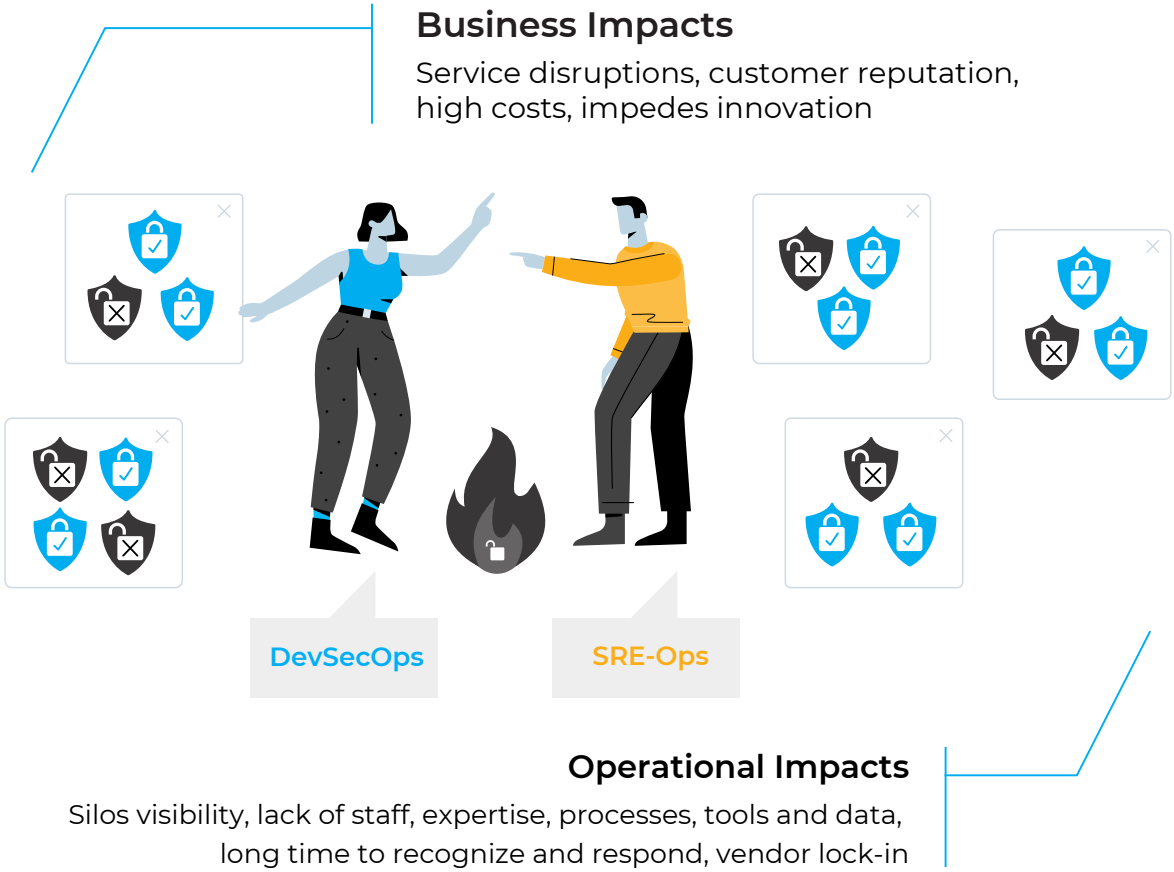


Figure 10. Pain-Point – Business and Operational Impacts

At the business level this can result in unnecessary long service disruptions, impacting customer reputation, increasing costs, and reducing innovation.

Plutora's VSM Plutora platform has the capabilities needed to provide end-to-end visibility, orchestration and controls necessary to implement the breadth of people, processes and technology practices under a single end-to-end framework.

Different Stakeholders Need Different Information

Different stakeholders have specific needs for security information, as shown in *Figure 11*. A well-engineered Continuous Security Dashboard and associated enterprise architecture has access to the breadth of data and flexible dashboard analysis and presentation tools to meet the entire range of special requirements.

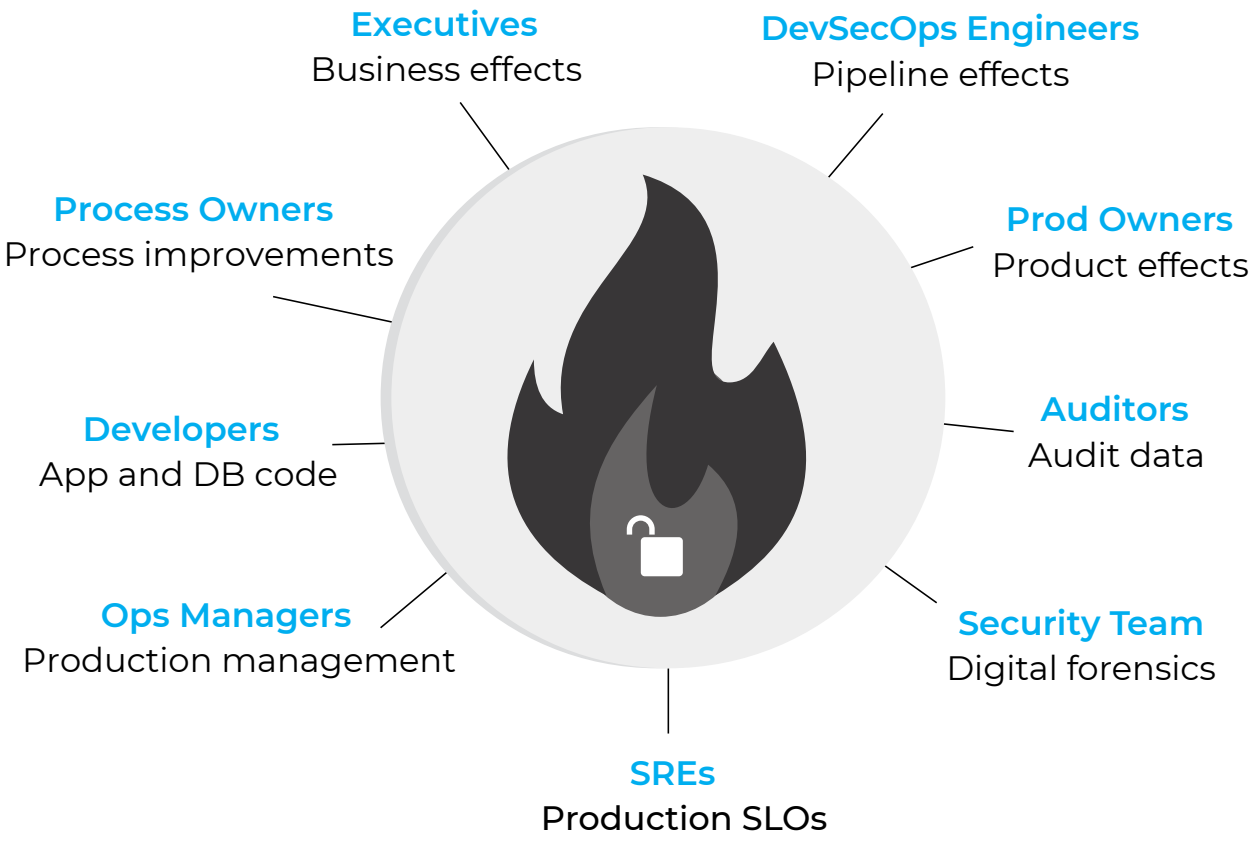


Figure 11. Pain-Point: Different Stakeholders Need Different Information

For example:

- Executives need to see Business affecting security information to know where to direct action at the business level.
- DevSecOps engineers need CI/CD pipeline security data to monitor security tools and integrate new automated security tools into continuous delivery toolchains.
- SREs need to monitor Service Level Objectives and in-production security tools to respond quickly to security incidents and automate toilsome tasks for in-production security processes.
- Security engineers need real-time access to security data to rapidly diagnose security events and engage with other team members across the enterprise.

Plutora's VSM solution supports customizable dashboards that can be tailored to each stakeholders' specific needs.

Disconnected People and Teams

According to a recent report by Everbridge, 50% of technical leaders say silos of tools and data prevent collaboration when it matters most.

The scenario illustrated in *Figure 12* is, unfortunately, typical of too many enterprises that must react to security events without a Continuous Security Dashboard.

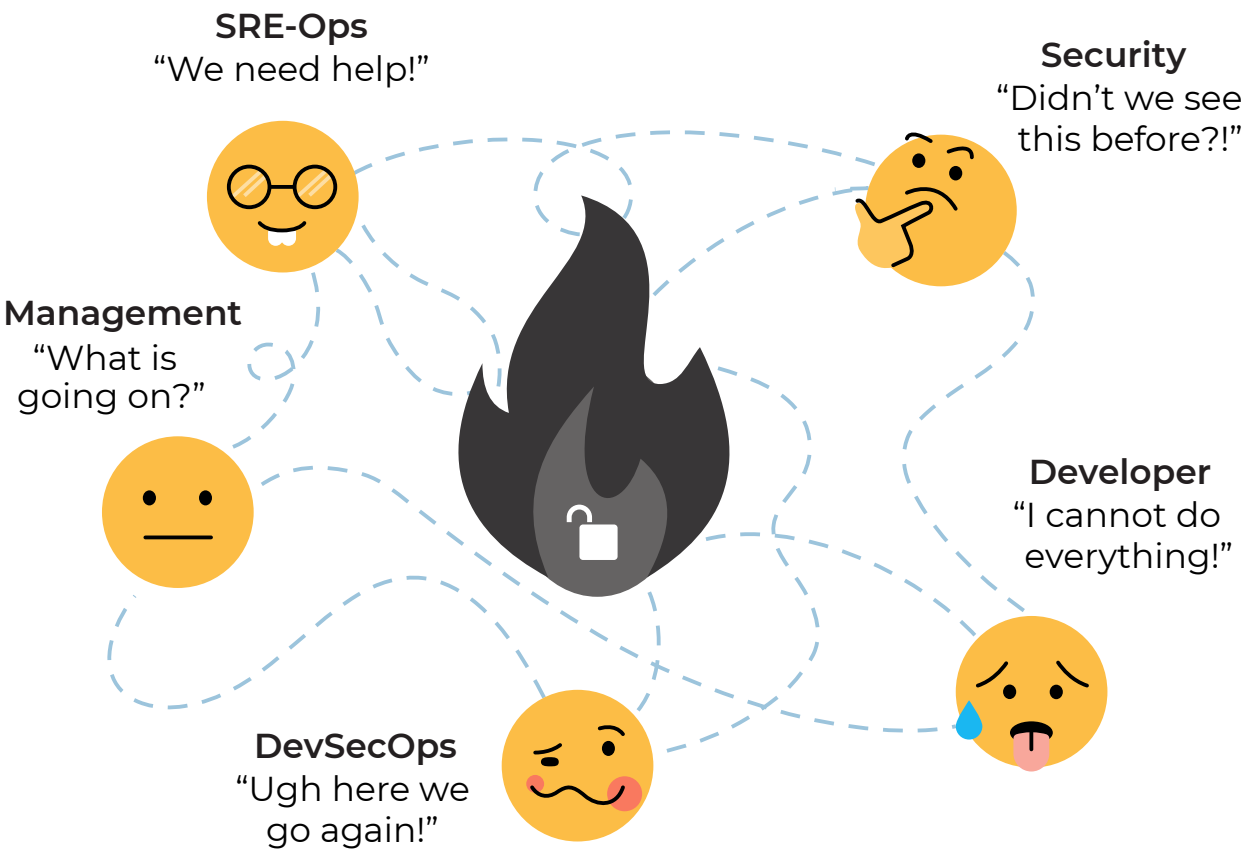


Figure 12. Pain-Point – Disconnected People and Teams

Managers really do need to know “what is going on.” The SRE-Ops team may indeed cry for help from Development and DevSecOps teams who, in turn, are frustrated each time because they do not have the required security expertise or diagnostic information, and meanwhile the Security team with their private SIEMS wonder what all the fuss is about because they see security events all the time.

Continuous Security Dashboards are needed to ensure people with different roles and responsibilities across the enterprise are equally informed and not disconnected.

The Plutora VSM platform provides a common framework for implementation of common processes that ensure seamless communication between teams.

Disconnected Processes and Tools

The scenario shown in *Figure 13*, where the developers have a different issue tracking system than the SRE-Ops or security team is a typical example of disconnected processes and tools that can cause bottlenecks in security information flow.

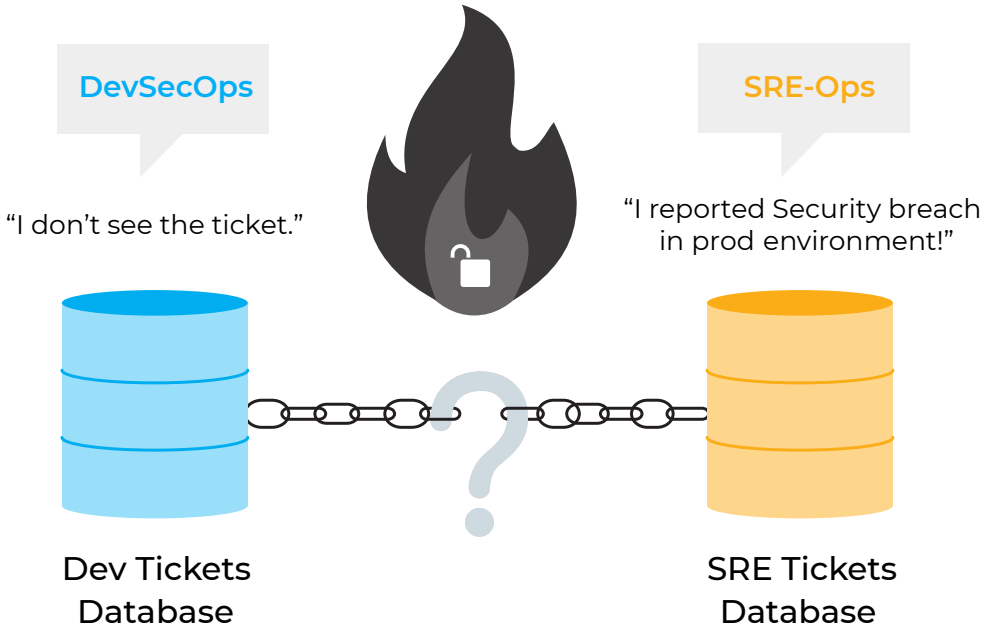


Figure 13. Pain-Point – Disconnected Processes and Tools

Similar examples occur when the different teams use different security scanning tools or different security testing tools. They are unable to efficiently share information and processes.

The inefficient ping-ponging of security information between production side data with resolvers in development and security teams can be avoided when all parties are using the same tools and processes for monitoring and resolving security concerns.

Separate Pre-Prod and Prod Environments

While DevSecOps has “Ops” in the name, there is typically a big boundary between pre-production environments and production environments, as illustrated in *Figure 14*. The DevSecOps side does not permit SRE-Ops to access the pre-prod environment and the SRE-Ops side does not permit Developers to access production. While there are many valid reasons for segregated access control policies this can impede the efficient flow of security information during security events, just when it is needed the most.

Figure 14. Pain-Point – Pre-Prod and Prod Environments

The Plutora VSM platform can be configured to stand-up both pre-production and production environments.

The Plutora VSM platform solves this concern by allowing all types of tools to connect through the common framework.

Disparate Security Metrics

DevSecOps and SRE-Ops have distinct metrics of interest to their job role. To get the most out of each team's specialist expertise, while ensuring all teams are working from a common data set, Continuous Security Dashboards, and underlying interconnected architecture, need capabilities to customize metrics for use in the dashboards.

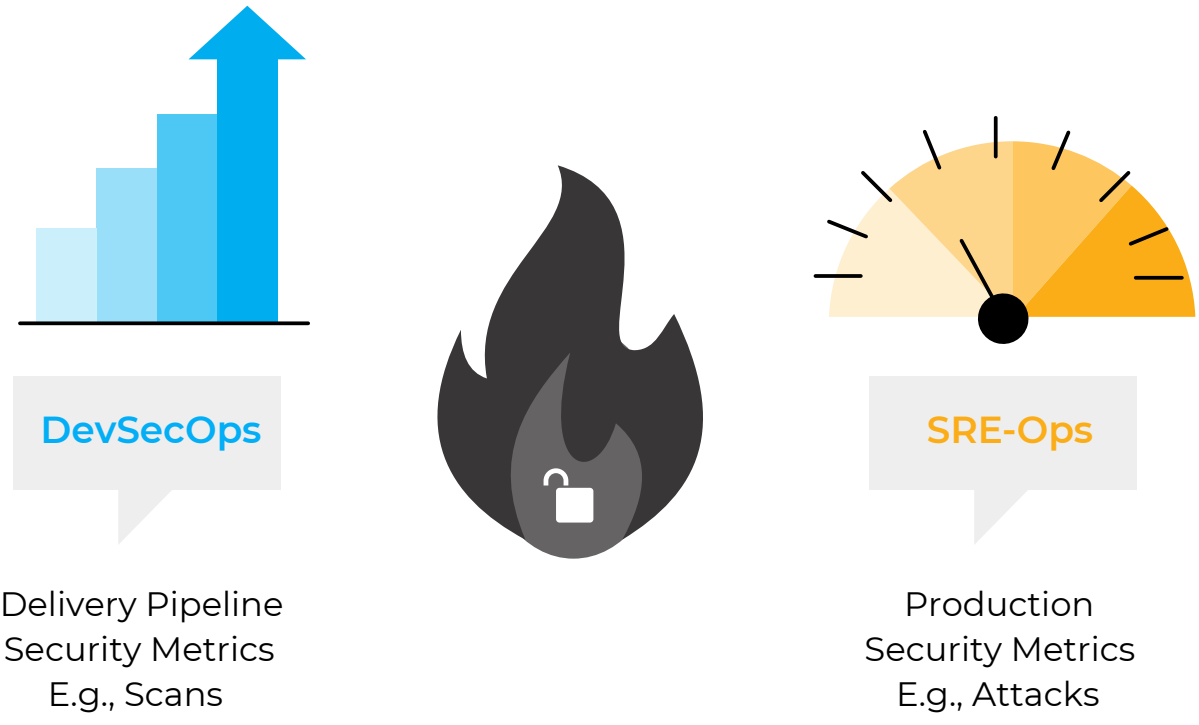


Figure 15. Pain-Point – Disparate Security Metrics

As shown in *Figure 15*, each specialist role, such as DevSecOps people and SRE-Ops people, need ready access to the data that is most relevant to their specific job roles, and at the same time they need to be confident that they are doing their analysis on a common source of security data that is equally relevant to other team players in their respective job roles.

Plutora's VSM platform can implement typical and customized metrics.

Scope of Data Collection

Continuous Security Dashboard architectures must ensure that the security information collection methodologies and security information data formats are consistent across the wide variety of DevSecOps and SRE-Ops tools in use across enterprise value streams, as shown in *Figure 16*.

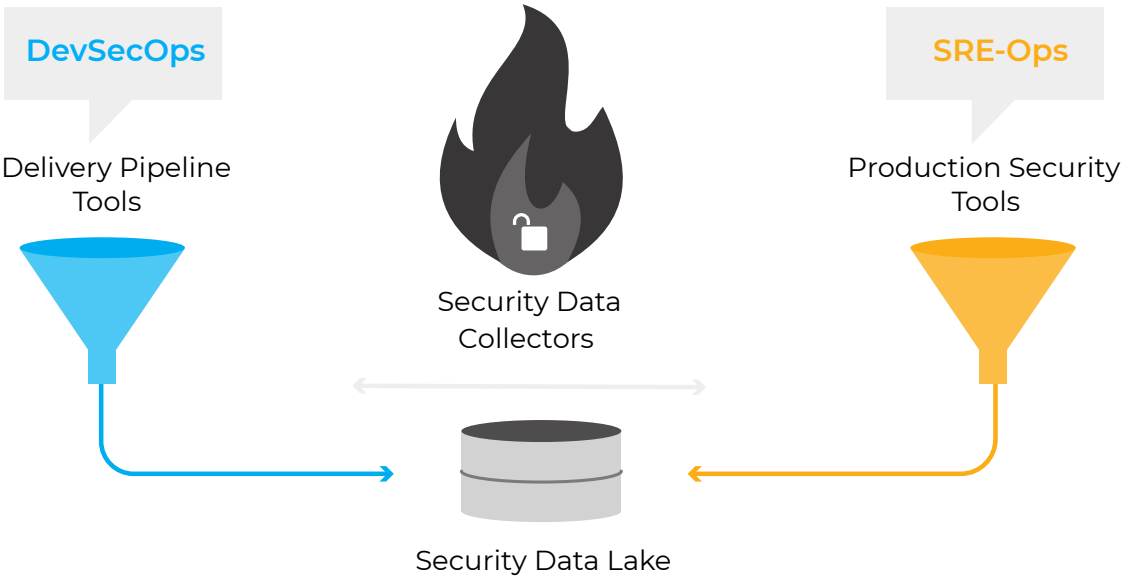


Figure 16. Pain-Point – Scope of Data Collection

In this way the entire system is not only more efficient to build and maintain but is easier to evolve and improve as new tools and security controls are added in the future. In addition, the reliability of the entire Continuous Security Dashboard system is improved because the common framework will benefit all applications over time as the system is scaled and adopted by more and more applications.

Plutora's VSM platform can support any number of collectors and be the basis for further evolution as new security tools and processes are added, and as the continuous security system evolves with ongoing requirements and improvements.

Security API

A security API layer in the Continuous Security Dashboard architecture is required to control and access tools from both DevSecOps pre-production and SRE-Ops production environments, as shown in *Figure 17*.

This enables the data from the Data Lake and security collectors to be consumed on-demand by the upper Smart UI layer as a service. With a well-defined API service layer boundary in place, it can then be used for efficient automated testing of the system itself, thus improving time-to-quality and quality coverage improvement. It can also be leveraged by advanced security DevSecOps and SRE-Ops and Security-audit automation applications that can be positioned above this layer.

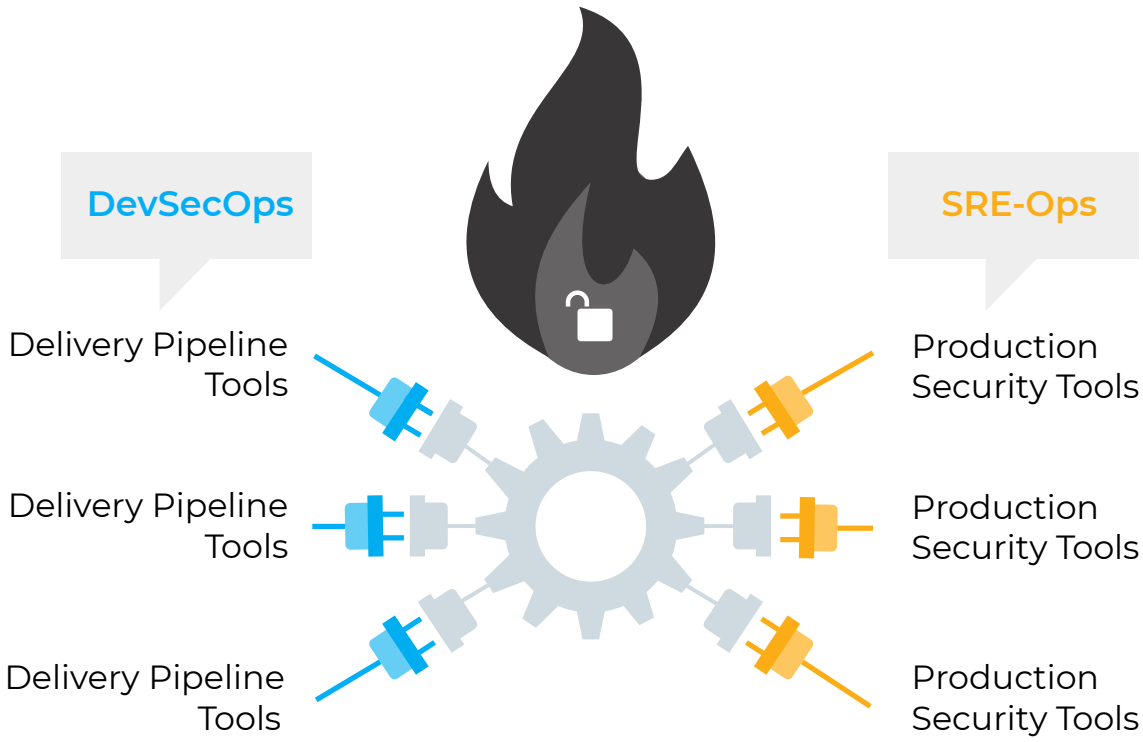


Figure 17. Pain-Point – Security API

Real-Time Threat Detection

Attacks are often difficult to detect because they happen quickly and the indicators can be dispersed across different data sources, such as network servers, end-points, and applications. *Figure 18* shows some use cases where security information is needed in real-time.

The Continuous Security architecture, with real-time access to security data across multiple value streams can quickly collect and analyze data from many security control collection points.

Real-time security data correlation and analysis applications can use the framework to sift through an array of security controls in real time that otherwise would be nearly impossible to do manually.

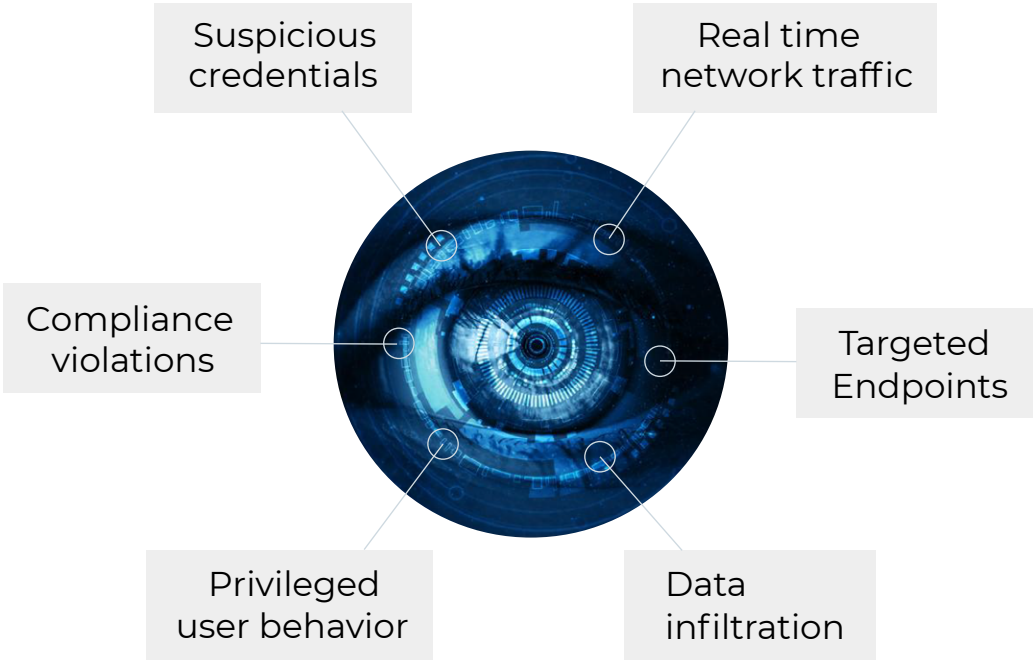


Figure 18. Pain-Point – Real-Time Threat Detection

Synthetic Security Monitoring

To meet increasing demands for security responsiveness the Continuous Security Architecture can be used to implement synthetic security monitoring and even continuous Security Chaos Engineering programs.

As illustrated in *Figure 19*, Programs written at the SmartUI layer can drive automated testing actions and security testing use cases, while the Dashboards can be used to monitor the results of the actions.

This is an ideal closed-loop security testing system that would be extremely difficult to accomplish if there were separate SIEM systems to program and coordinate inputs and outputs.

Simulate user security actions

Monitor your system reactions

Figure 19. Pain-Point – Synthetic Security Monitoring

Automated Security Response

Figure 20 shows how the Continuous Security Dashboard architecture enables an enterprise to further step up their security automation.

The Smart UI layer can be used to build tools that will automate notifications and responses to security events.

For example, a tool running at this layer could detect a container under attack and through connection with Infrastructure-as-Code tools automatically replace a container with another to kill the attack without disrupting service.

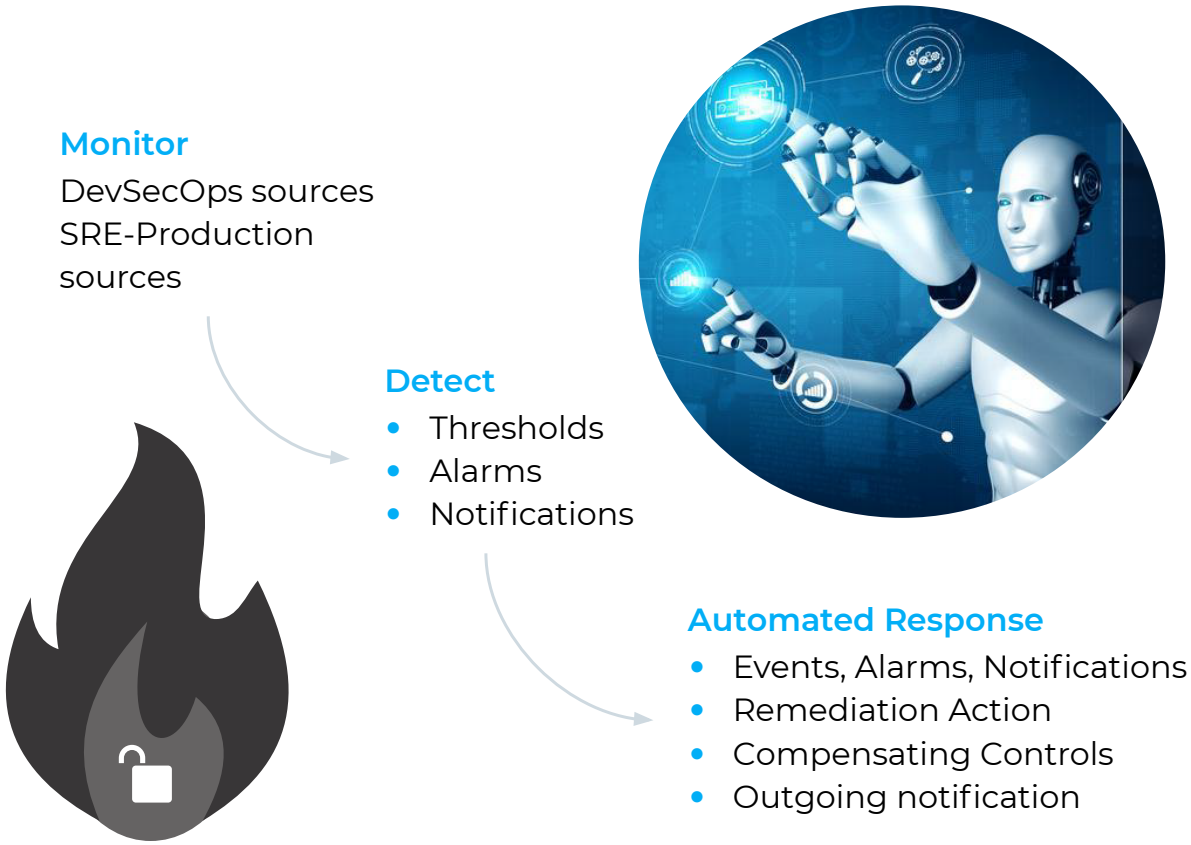


Figure 20. Pain-Point – Automated Security Response

Benefits of VSM-Based Continuous Security Solutions

Continuous Security platforms that aggregate and consolidate security information across end-to-end value streams offer a lot of advantages over more limited scope SIEM systems and dashboards, as shown in *Figure 21*.

At the operational level, the Continuous Security platform provides a common source of truth for all development, production, and security stakeholders across the enterprise value stream. This enables more

informed and intelligent risk mitigation strategies, which in turn enables a more seamless response from resolvers from across the value stream. The platform makes it quicker to identify the source of security problems, understand the effects, provide context, and improve collaboration between development, operations, and security teams. The consolidated security data can be used to automate resolution actions, validate solutions governance practices and be a basis for continuous improvement.

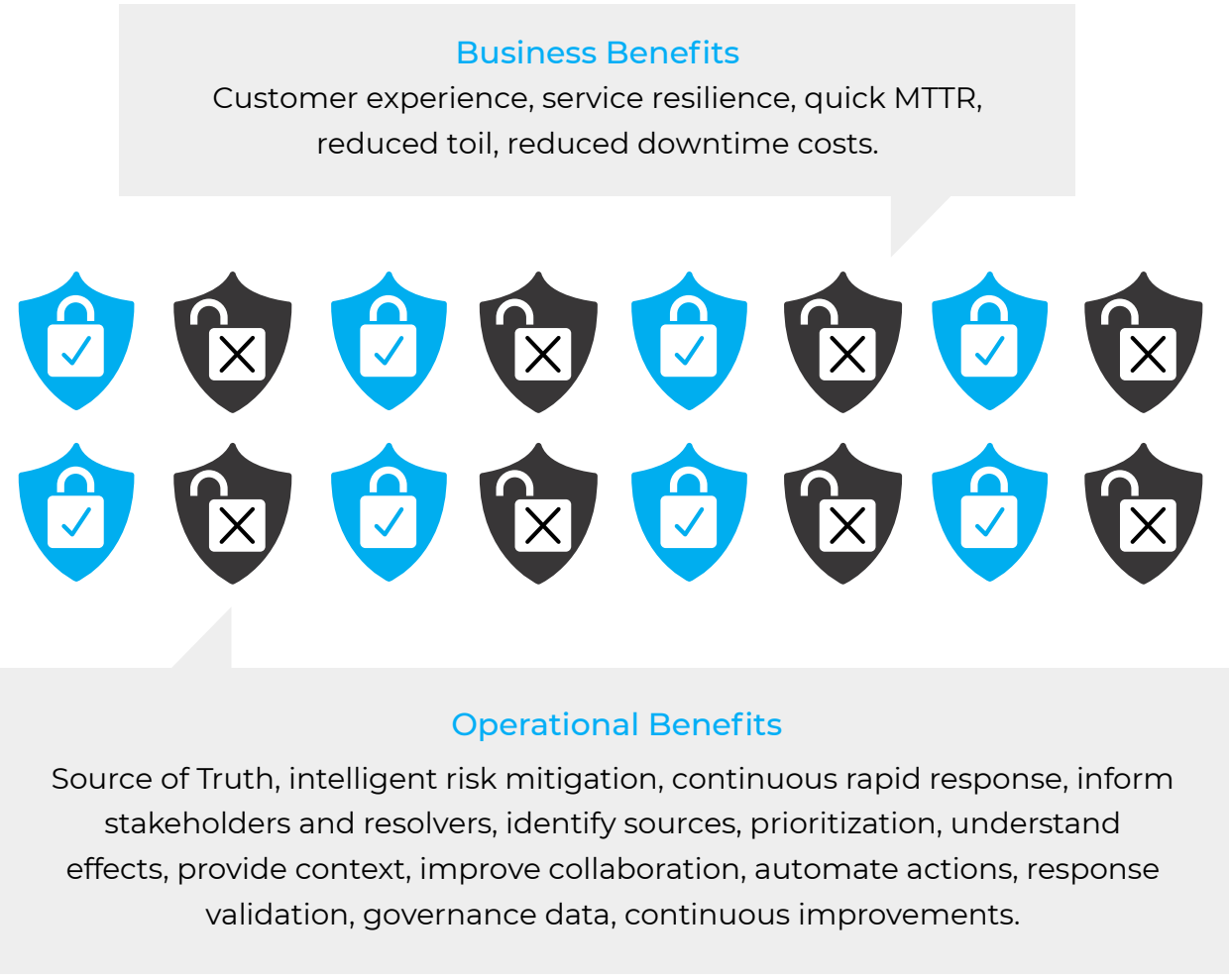


Figure 21. VSM Continuous Security Solution Benefits

At the business level, these operations benefits enable the organization to be more responsive to security concerns, thus enhancing customer experiences, service resilience, reduced operations toil and reduced costs caused security events.

Call to Action

This eBook explained pain-points and requirements that are addressed by a VSM-based Continuous Security architecture. So how do you know if your organization needs a solution?

Continuous Security Requirement (CSR)	Importance?	Current Capability?	GAP
	I (1-5)	C (1-5)	Score (I/C)
Security visibility over the end-to-end value stream	4	1	4.0
Overcome business and operational requirement for security	4	1	4.0
Smart UI layer suitable to create different dashboards for different stakeholders.	3	1	3.0
Integrate data so that people across DevSecOps Deployment and SRE Production teams can see the same information.	4	2	2.0
Compatible with DevSecOps and SRE processes and tools.	4	1	4.0
Compatible with pre-production and production deployment environments.	5	2	2.5
Create metrics for DevSecOps and SRE Security in production.	4	1	4.0
Collectors and Security Data Lake for DevSecOps and SRE data.	5	2	2.5
Flexible API for security data transfers from DevSecOps and SRE sources.	5	2	2.5
Realtime security data transfer performance from DevSecOps and SRE sources.	4	2	2.0
Orchestration and automation capabilities suitable for synthetic security monitoring.	4	2	2.0
Orchestration and automation capabilities suitable for triggering automated security responses.	4	1	4.0
CSDR Scores	**4.3**	**1.5**	**3.0**

Figure 22. Continuous Security Requirement Assessment Tool

Figure 22 shows a simple Continuous Security Requirements assessment tool that you can use to assess your organizations' Continuous Security Requirements. For each requirement statement in the chart you simply enter an importance score and a current capability score. The tool uses these scores to compute a Gap score for each requirement and an overall Gap score.

A gap score of 2.5 or more is a strong indicator that you could benefit from a Continuous Security solution. This tool and other practical calculators and assessment tools are available to download for free from my website.

Once you determine that a Continuous Security Dashboard solution is important to improving your organization's security posture, VSM solutions like Plutora can help accelerate and improve your path to continuous security.

The following are steps to accomplishing that.

- Leadership vision, sponsorship, and alignment around the need to accelerate Continuous Testing.
- Discover current state using the Continuous Security Requirements (CSR) tool.
- Choose a solution using the same CSR tool as a guide for selection criterion.
- Pick an application to use as a model (one with a high CSR Gap score).

» Implement the CSD for the model application.

» Operationalize the solution (determine success metrics). (such as CSR Gap score improvement)

» Expand adoption to other applications.

The implementation of a comprehensive continuous security solution will require multiple phases of work. *Figure 23* is a sample roadmap for implementing different stages of a solution.

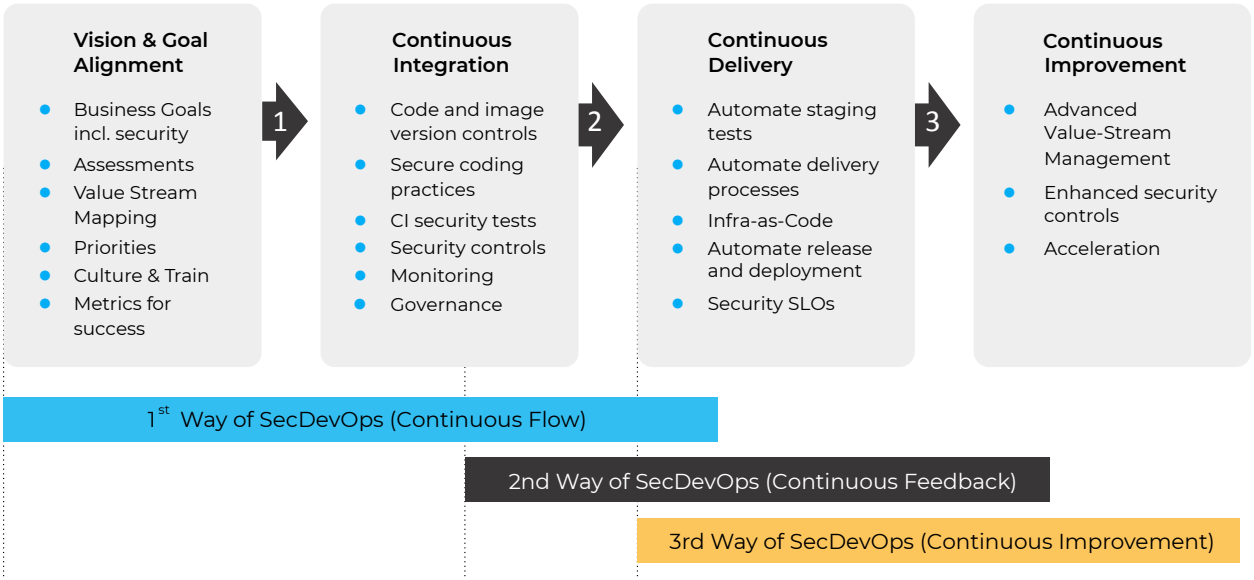


Figure 23. VSM Continuous Security Platform RoadMap

Key Takeaways

- The need for security visibility solutions over DevSecOps Pre-Prod and SRE-Ops production environments has never been greater.
- A Continuous Security solution provides real-time security assurance for end-to-end DevSecOps and SRE-Ops environments.
- Value Stream Management solutions, including Plutora's have the right architecture to match requirements for Continuous Security solutions.
- The roadmap and CSR tool provided in this eBook can help accelerate your progress towards a comprehensive Continuous Security solution.

Author

Marc Hornbeek | *CEO, Engineering DevOps Consulting*

Marc was awarded Outstanding Engineer of 2016 by IEEE Western USA Region 6 for outstanding contributions to the field of automation applied to development and testing of networks, systems, protocols, labs, and DevOps. Marc has more than 39 years of experience architecting, designing, developing, and managing high-performance solutions for IT infrastructures that are deployed in commercial and government applications globally. He has served as executive, senior management, and solution architect for companies including Trace3, Bell-Northern Research, Tekelec, ECI Telecom, EdenTree Technologies, and Spirent Communications. Marc is a regular speaker at DevOps and IEEE events, a blogger on DevOps.com, and of course author for the DevOps Institute.