आधुनिक साइबर सुरक्षा संचालन में सीम की भूमिका

सरकारी डिजिटल पारिस्थितिकी तंत्र में खतरे की पहचान, परिचालन दृश्यता और लचीलापन सुदृढ़ करना

संपादित : **मोहन दास विश्वम्**

आज के तेजी से विकसित होते साइबर-खतरे के परिदृश्य में, सरकारी विभाग सार्वजनिक सेवाओं, नागरिक-केंद्रित अनुप्रयोगों और महत्वपूर्ण अवसंरचना संचालन को सुचारु रूप से संचालित करने के लिए सुरक्षित और निर्बाध डिजिटल प्रणालियों पर अत्यधिक निर्भर हैं। साइबर खतरों की बढ़ती जटिलता और व्यापकता के कारण सुरक्षा निगरानी और घटना-प्रतिक्रिया के लिए एक केंद्रीकृत एवं सक्रिय दृष्टिकोण की आवश्यकता अनिवार्य हो गई है।

सिक्योरिटी इन्फॉर्मेशन एंड इवेंट मैनेजमेंट (सीम) इस आवश्यकता को पूरा करने में महत्वपूर्ण भूमिका निभाता है। यह संगठनों को सर्वर, एंडपॉइंट, अनुप्रयोगों और नेटवर्क उपकरणों से अभिलेखीय डेटा एकत्रित करने, सहसंबंध स्थापित करने और उसका विश्लेषण करने में सक्षम बनाता है। कच्चे घटना डेटा को उपयोगी सुरक्षा अंतर्दृष्टि में परिवर्तित करते हुए, सीम प्रणालीगत गतिविधियों का एक समग्र दृष्टिकोण प्रदान करता है और वास्तविक समय में असामान्य व्यवहार की पहचान करने में सहायता करता है।

घटनाओं के पारस्परिक संबंध और अभिलेखों के एकरूपीकरण के माध्यम से सीम संभावित खतरों की पहचान करता है, प्राथमिकता आधारित चेतावनियाँ देता है और समयबद्ध प्रतिक्रिया सुनिश्चित करता है। साथ ही, यह डिजिटल साक्ष्य जांच, प्रवृत्ति विश्लेषण तथा सर्ट-इन और एनआईसी जैसे राष्ट्रीय ढाँचों के अनुरूप अनुपालन में सहायक होता है।

संवेदनशील डेटा और महत्वपूर्ण सार्वजनिक सेवाओं के प्रबंधन की जिम्मेदारी निभाने वाले सरकारी संगठनों के लिए, सीम एक आधारभूत क्षमता के रूप में कार्य करता है। यह न केवल सुरक्षा स्थिति को सुदृढ़ करता है, बल्कि परिचालन दृश्यता को बेहतर बनाता है और उभरते साइबर जोखिमों के विरुद्ध संस्थागत लचीलापन सुनिश्चित करता है।

एस. वी. च. सुब्बा राव
उप महानिदेशक व एसआईओ
sagar.ambati@nic.in

एरिना किरन कुमार
तकनीकी निदेशक
erina.kiran@nic.in

सीम अब केवल अभिलेख प्रबंधन उपकरण नहीं रहा, बल्कि आधुनिक डिजिटल प्रणालियों के लिए एक बुद्धिमान सुरक्षा आधार के रूप में विकसित हो रहा है। केंद्रीकृत दृश्यता, उन्नत विश्लेषण और कृत्रिम बुद्धिमत्ता आधारित क्षमताओं के संयोजन के माध्यम से यह संस्थानों को प्रतिक्रियात्मक सुरक्षा से सक्रिय सुरक्षा की ओर ले जाता है। विशेषकर जटिल सरकारी वातावरण में यह सुदृढ़, अनुपालक और भविष्य-तैयार साइबर सुरक्षा संचालन के लिए अनिवार्य बन गया है।

सीम प्रौद्योगिकी कैसे कार्य करती है

सीम समाधान एक संरचित और सतत प्रक्रिया के माध्यम से कार्य करते हैं, जिसमें किसी संगठन के सूचना प्रौद्योगिकी परिवेश से सुरक्षा-संबंधी डेटा का संग्रहण, प्रसंस्करण और विश्लेषण किया जाता है। इसमें प्रणाली अभिलेख, उपयोगकर्ता गतिविधियाँ, नेटवर्क यातायात, अंतिम उपकरण, अनुप्रयोग और सर्वर शामिल होते हैं, जिससे सुरक्षा घटनाओं की व्यापक दृश्यता प्राप्त होती है।

सीम प्रणाली के कार्य को निम्नलिखित प्रमुख चरणों के माध्यम से समझा जा सकता है:

- **डेटा संग्रहण:** सीम प्लेटफ़ॉर्म विभिन्न स्रोतों से अभिलेख और घटना डेटा एकत्रित करते हैं, जैसे अग्नि-प्राचीर (फायरवॉल), अनधिकृत प्रवेश पहचान प्रणालियाँ, सर्वर, डेटाबेस और मेघ परिवेश, जिससे संपूर्ण अवसंरचना पर व्यापक कवरेज सुनिश्चित होता है।
- **डेटा मानकीकरण और समेकन:** एकत्रित डेटा को एक समान प्रारूप में ढाला जाता है, जिससे विभिन्न प्रणालियों से प्राप्त घटनाओं की सामूहिक तुलना और विश्लेषण संभव हो सके।
- **घटना सहसंबंध:** सीम पूर्व-निर्धारित नियमों, सांख्यिकीय प्रतिमानों और खतरा-सूचना के आधार पर संबंधित घटनाओं को जोड़ता है, जिससे ऐसे पैटर्न की पहचान होती है जो दुर्भावनापूर्ण गतिविधि का संकेत दे सकते हैं।
- **खतरा पहचान और चेतावनी:** सहसंबंध और विश्लेषण के आधार पर प्रणाली असामान्यताओं की पहचान करती है और प्राथमिकता-आधारित चेतावनियाँ उत्पन्न करती है, जिससे सुरक्षा दल उच्च-जोखिम वाली घटनाओं पर ध्यान केंद्रित कर सकें।
- **प्रतिक्रिया और जाँच:** सीम घटना-प्रतिक्रिया में संदर्भित जानकारी प्रदान कर सहायता करता है, जिससे जाँच, नियंत्रण और सुधार की प्रक्रिया तेज़ और प्रभावी होती है। उन्नत प्रणालियाँ स्वचालित प्रतिक्रिया भी आरंभ कर सकती हैं।

यह संरचित कार्यप्रवाह सीम को विशाल मात्रा में कच्चे डेटा को उपयोगी सुरक्षा बुद्धिमत्ता में परिवर्तित करने में सक्षम बनाता है, जिससे संगठन समय रहते खतरों की पहचान कर सकें, प्रभावी प्रतिक्रिया दे सकें और निरंतर सुरक्षा निगरानी बनाए रख सकें।

सीम के मुख्य घटक

एक सीम प्रणाली कई एकीकृत घटकों पर आधारित होती है, जो मिलकर सूचना प्रौद्योगिकी परिवेश में पूर्ण दृश्यता, पहचान और प्रतिक्रिया की क्षमता प्रदान करते हैं। ये घटक बड़े पैमाने पर डेटा संसाधित करने, खतरों की पहचान करने और सुरक्षा संचालन को प्रभावी बनाने में सहायक होते हैं:

- **अभिलेख डेटा प्रबंधन:** यह सीम की आधारशिला है, जो विभिन्न स्रोतों से अभिलेख डेटा का संग्रहण, भंडारण और प्रबंधन करता है। यह डेटा की अखंडता, मानकीकरण और विश्लेषण, लेखा-परीक्षण तथा अनुपालन के लिए उपलब्धता सुनिश्चित करता है।
- **सुरक्षा घटना प्रबंधन (एसईएम):** यह वास्तविक समय में सुरक्षा घटनाओं की निगरानी और विश्लेषण पर केंद्रित होता है। विभिन्न स्रोतों से प्राप्त जीवंत डेटा के सहसंबंध के माध्यम से यह संदिग्ध गतिविधियों की त्वरित पहचान और तत्काल चेतावनी उत्पन्न करता है।
- **सुरक्षा सूचना प्रबंधन (एसआईएम):** यह ऐतिहासिक डेटा के भंडारण और विश्लेषण का कार्य करता है, जिससे घटना जाँच, प्रवृत्ति विश्लेषण और अनुपालन प्रतिवेदन को समर्थन मिलता है।
- **घटना सहसंबंध और विश्लेषण:** यह विभिन्न प्रणालियों से प्राप्त डेटा को नियमों, सांख्यिकीय प्रतिमानों और खतरा-सूचना के आधार पर संयोजित करता है, जिससे जटिल या छिपे हुए खतरों की पहचान की जा सके।

- **उपयोगकर्ता और इकाई व्यवहार विश्लेषण:** यह मशीन अधिगम के माध्यम से उपयोगकर्ताओं और प्रणालियों के सामान्य व्यवहार का आधार निर्धारित करता है और असामान्यताओं, जैसे आंतरिक खतरों या समझौता किए गए खातों, की पहचान में सहायता करता है।
- **खतरा-सूचना एकीकरण:** यह बाहरी खतरा स्रोतों को शामिल कर पहचान क्षमता को सुदृढ़ करता है, जिससे ज्ञात हमलों के पैटर्न और उभरते जोखिमों की बेहतर पहचान हो सके।
- **चेतावनी और घटना-प्रतिक्रिया:** यह पहचाने गए खतरों के आधार पर प्राथमिकता-आधारित चेतावनियाँ उत्पन्न करता है और संरचित प्रतिक्रिया प्रक्रियाओं—जाँच, नियंत्रण और सुधार—को समर्थन प्रदान करता है। उन्नत प्रणालियाँ स्वचालित प्रतिक्रिया भी सक्षम कर सकती हैं।
- **प्रतिवेदन, लेखा-परीक्षण और अनुपालन:** यह डैशबोर्ड, प्रतिवेदन और लेखा-परीक्षण अभिलेख प्रदान करता है, जो नियामकीय अनुपालन के लिए आवश्यक होते हैं, साथ ही सुरक्षा स्थिति और परिचालन प्रवृत्तियों की समझ भी देते हैं।

सीम का एआई आधारित विकास

जैसे-जैसे साइबर खतरे आकार और जटिलता में बढ़ रहे हैं, पारंपरिक सीम प्रणालियाँ अब कृत्रिम बुद्धिमत्ता और मशीन अधिगम से संचालित बुद्धिमान एवं अनुकूलनशील मंचों में विकसित हो रही हैं। यह परिवर्तन संगठनों को केवल प्रतिक्रियात्मक निगरानी से आगे बढ़कर पूर्वानुमान आधारित और स्वचालित सुरक्षा संचालन की दिशा में सक्षम बना रहा है।

कृत्रिम बुद्धिमत्ता आधारित सीम समाधान वास्तविक समय और ऐतिहासिक डेटा की विशाल मात्रा का विश्लेषण कर पैटर्न, असामान्यताओं और उभरते आक्रमण तरीकों की अधिक सटीक पहचान करते हैं। निरंतर सीखने की क्षमता के कारण ये प्रणालियाँ सूक्ष्म विचलनों को भी पहचान सकती हैं, जो आंतरिक खतरों, समझौता किए गए खातों या अज्ञात हमलों का संकेत हो सकते हैं।

स्वचालन आधुनिक सीम क्षमताओं का एक महत्वपूर्ण पहलू है। समन्वय ढाँचों के साथ एकीकृत होकर, सीम प्रणालियाँ पूर्व-निर्धारित प्रतिक्रियाएँ आरंभ कर सकती हैं, जिससे मानवीय हस्तक्षेप कम होता है और सुरक्षा घटनाओं को शीघ्र नियंत्रित किया जा सकता है। इससे प्रतिक्रिया समय में सुधार होता है और सुरक्षा दलों पर कार्यभार भी कम होता है।

इसके अतिरिक्त, कृत्रिम बुद्धिमत्ता चेतावनियों की प्राथमिकता निर्धारण और अनावश्यक संकेतों को कम करने में भी सहायक होती है। संदर्भ-आधारित विश्लेषण के माध्यम से यह गलत चेतावनियों को फ़िल्टर करती है, जिससे सुरक्षा विश्लेषक उच्च-प्रभाव वाले खतरों पर ध्यान केंद्रित कर पाते हैं और निर्णय लेने की क्षमता बेहतर होती है।

सीम का विकास उभरते साइबर सुरक्षा ढाँचों और संरचनाओं के साथ भी जुड़ा हुआ है। मेघ परिवेश, शून्य-विश्वास मॉडल और विस्तारित पहचान एवं प्रतिक्रिया मंचों के साथ एकीकरण से वितरित और मिश्रित अवसंरचनाओं में दृश्यता का दायरा बढ़ रहा है। साथ ही, डेटा गोपनीयता और नियामकीय अनुपालन पर बढ़ते जोर ने शासन और लेखा-परीक्षण की तैयारी में सीम की भूमिका को और सुदृढ़ किया है।

भविष्य में सीम और अधिक विस्तार योग्य, स्वचालित और संदर्भ-सजग प्रणाली के रूप में विकसित होगा—जो केवल निगरानी उपकरण नहीं, बल्कि साइबर सुरक्षा पारिस्थितिकी तंत्र का केंद्रीय बुद्धिमत्ता स्तर बनेगा। यह विकास विशेष रूप से सार्वजनिक क्षेत्र में संगठनों को लचीलापन बढ़ाने, सेवाओं की निरंतरता सुनिश्चित करने और उन्नत साइबर खतरों से आगे रहने में महत्वपूर्ण भूमिका निभाएगा।

सीम कार्यान्वयन के लिए श्रेष्ठ अभ्यास

प्रभावी सीम कार्यान्वयन के लिए एक रणनीतिक दृष्टिकोण आवश्यक है, जिसमें प्रौद्योगिकी, प्रक्रियाएँ और मानव संसाधन संगठन के सुरक्षा उद्देश्यों के अनुरूप हों। एक सुव्यवस्थित सीम प्रणाली न केवल खतरे की पहचान को बेहतर बनाती है, बल्कि दीर्घकालिक दक्षता और विस्तार क्षमता भी सुनिश्चित करती है।

- **स्पष्ट उद्देश्य निर्धारित करें:** सीम के उपयोग हेतु स्पष्ट लक्ष्य तय करें, जैसे खतरा पहचान, अनुपालन या घटना-प्रतिक्रिया। इससे प्राथमिकताएँ तय करने और प्रणाली को सही ढंग से विन्यस्त करने में सहायता मिलती है।
- **समग्र डेटा एकीकरण सुनिश्चित करें:** अग्नि-प्राचीर, अंतिम उपकरण, पहचान प्रणालियाँ, अनुप्रयोग और मेघ परिवेश से अभिलेखों को एकीकृत करें, ताकि व्यापक दृश्यता और सटीक पहचान संभव हो।
- **महत्वपूर्ण स्रोतों को प्राथमिकता दें:** प्रारंभ में उच्च-मूल्य प्रणालियों जैसे सक्रिय निर्देशिका, नेटवर्क उपकरण और मेघ मंचों पर ध्यान केंद्रित करें।
- **निरंतर निगरानी और सुधार सक्षम करें:** सहसंबंध नियमों, डैशबोर्ड और चेतावनियों की नियमित समीक्षा और अद्यतन करें, ताकि बदलते खतरे के अनुरूप प्रणाली प्रभावी बनी रहे।
- **स्वचालन और खतरा-सूचना का उपयोग करें:** स्वचालन और समन्वय क्षमताओं को शामिल कर प्रतिक्रिया प्रक्रिया को सरल बनाएं तथा खतरा-सूचना स्रोतों को अद्यतन रखें।
- **दल की क्षमता और प्रशिक्षण सुदृढ़ करें:** सुरक्षा संचालन दल को आवश्यक कौशल प्रदान करें, जिससे वे चेतावनियों को समझ सकें, घटनाओं की जांच कर सकें और प्रणाली का अनुकूलन कर सकें।
- **विभागीय सहयोग को बढ़ावा दें:** सूचना प्रौद्योगिकी, सुरक्षा और अनुपालन दलों के बीच समन्वय स्थापित करें, ताकि संचार और प्राथमिकताओं में सामंजस्य बना रहे।
- **अनुपालन और लेखा-परीक्षण की तैयारी सुनिश्चित करें:** अभिलेख संरक्षण, प्रतिवेदन और लेखा-परीक्षण मार्ग सुनिश्चित कर नियामकीय आवश्यकताओं के अनुरूप प्रणाली को तैयार रखें।

निष्कर्ष

आज के गतिशील खतरे के परिदृश्य में सीम साइबर सुरक्षा का एक प्रमुख घटक बन चुका है, जो एकीकृत दृश्यता, वास्तविक समय पहचान और उपयोगी अंतर्दृष्टि प्रदान करता है। कृत्रिम बुद्धिमत्ता का समावेशन इसे और अधिक बुद्धिमान और अनुकूलनशील बना रहा है, जिससे तेज़ खतरा पहचान, बेहतर चेतावनी प्राथमिकता और प्रभावी घटना-प्रतिक्रिया संभव हो रही है।

जैसे-जैसे साइबर खतरे विकसित होते रहेंगे, सीम संगठनात्मक लचीलापन बढ़ाने, अनुपालन सुनिश्चित करने और सेवाओं की निरंतरता बनाए रखने में महत्वपूर्ण भूमिका निभाएगा। स्वचालन और पूर्वानुमान आधारित क्षमताओं की दिशा में इसका निरंतर विकास सुरक्षा संचालन को अधिक प्रभावी और संगठन के व्यापक उद्देश्यों के अनुरूप बनाएगा।

अधिक जानकारी के लिए संपर्क करें

एस. वी. च. सुब्बा राव
उप महानिदेशक एवं एसआईओ
एनआईसी आंध्र प्रदेश राज्य केंद्र
तृतीय तल, आर एंड बी बिल्डिंग, एमजी रोड
विजयवाड़ा, आंध्र प्रदेश – 520010
ईमेल: sio-ap@nic.in, फ़ोन: 0866-2468341