CUSTOMER:
MedTech market leader

CHALLENGE:
Building the context necessary to automate and accelerate key processes around insider threat analysis and remediation

SOLUTION:
Bay Dynamics Risk Fabric

BENEFITS:

- Automated analysis and reporting of the most problematic security events
- Created repeatable automated processes to consistently improve threat hunting
- Gained the ability to identify and prevent evolving threats as they occur
- Massively improved the productivity of human analysts of all skill levels

91% increase in mean time to response

Bay Dynamics®

Bay Dynamics Risk Fabric

MedTech Leader Automates Threat Hunting Using Dedicated Machine Learning and Analytics

Based in the United States, this medical technology manufacturer designs, builds and sells thousands of highly innovative products to customers around the world. Driven by a wide range of globally distributed research and development capabilities, along with related business and manufacturing operations, the company maintains highly rigorous cyber security parameters to safeguard its lifeblood intellectual property.

The Challenge: Accelerating Insider Threat Analysis

Based on the requirement to enable its security analysts and SOC teams to more efficiently handle problematic events as they occur and trigger related remediation, the manufacturing giant sought to create an automated approach to insider threat hunting. To build on its existing investments in robust security infrastructure – including endpoint security, data loss prevention (DLP), cloud access security broker (CASB) and authentication tools, among others – the company sought a solution that could process large volumes of data to automatically identify malicious or problematic activities.

By adding a source of integrated analysis to centralize investigation of event data generated across its existing tools, backed by dedicated Machine Learning, the company aimed to accelerate response, automatically identifying high risk issues. Further, using cross-platform analytics to gain the context necessary to understand the combined intent and impact of various types of behaviors was identified as a key capability to prioritize and remediate critical threats.

The Solution: Deploying Bay Dynamics Risk Fabric

Having implemented Bay Dynamics Risk Fabric alongside its existing security stack, the company’s incident response teams and security operations center (SOC) analysts set out to create proactive, repeatable processes around automated hunting for insider threats.

Utilizing Risk Fabric’s out of the box Risk Models and dashboards, and adapting those capabilities to meet unique requirements, the experts gained the ability to rapidly identify alerts that represented truly unusual behaviors, such as indicators of account compromise or attempted data exfiltration. Driven by the product’s underlying Machine Learning, the organization was also able to rapidly classify and de-escalate numerous high-volume, low risk alerts, allowing analysts to focus on critical issues.

Using this approach, Risk Fabric was further utilized to create daily monitoring practices focused on targeted response to highly problematic events, such as cloud-based alerts where failed authentication converged with unusual behavior tied to specific policies. Further, the solution’s Machine Learning capabilities also enabled continuous refinement of these techniques informed by direct input from human experts.

> “
>
> We went from chasing individual alerts and performing time consuming manual investigation to an automated approach that allowed us work smarter and faster.
>
> – SOC Director
>
> MedTech manufacturing giant

Choosing Bay Dynamics Risk Fabric

Ultimately, for this company, Bay Dynamics Risk Fabric represented the most strategic approach to automated threat hunting for numerous factors, including:

1. Rapid integration of relevant security system and IT data sources to automatically create the context necessary to inform cross-platform analysis.
2. Automated identification of truly problematic events based on analytics-driven understanding of high-risk behaviors and alerts.
3. The ability to continuously improve Risk Models to focus analysis on specific activities such as attempted data theft.
4. Machine Learning capabilities that established baselines for comparative analysis and increased precision based on use by analysts.

Results: Automated Threat Monitoring

Once the company deployed Bay Dynamics Risk Fabric, applying its Risk Models to highlight those people and events that truly required detailed investigation, it saw immediate results.

By enlisting the solution to focus daily analysis on highly problematic events such as failed authentication, unusual applications interactions [ex. Salesforce.com], and improper data handling and communication with known bad IPs, analysts gained the context needed to better target response. Further, by isolating and revising policies generating high volumes of alerts tied to accepted business processes, ongoing analysis could be significantly improved.

With Risk Fabric integrated into its security architecture, the medical manufacturing giant achieved a wide range of measurable benefits, including:

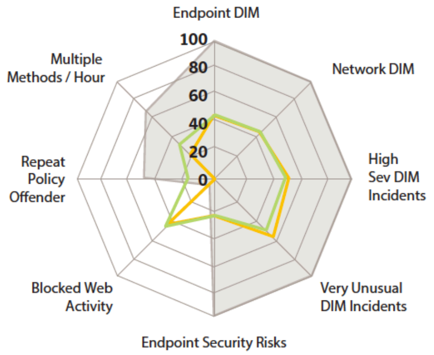
- Creation of more efficient threat hunting processes focused on daily and continuous analysis of specific behaviors and Risk Models.
- The ability to identify emerging threat indicators to proactively mitigate potential impacts such as data loss, before they occur.
- Ongoing improvement of business processes and policies to reinforce strict security guidelines and work directly with involved stakeholders.
- Measurable acceleration and advancement of remediation processes related to both high risk and low risk events.

How it Works: Risk Fabric

Bay Dynamics Risk Fabric provides the advanced analytics necessary to directly address today's leading data security challenges. Backed by patented Machine Learning and integration with every form of security infrastructure, Risk Fabric creates the visibility and context necessary to pinpoint emerging threats, optimizing both human and technical resources.

Delivered via targeted use cases that enable rapid prioritization, investigation and remediation of threats, along with continuous improvement of related polices and business processes, Risk Fabric allows organizations to translate huge volumes of available data into actions that minimize risk.

Risk Rating Vectors



Looking Ahead: Increasing Automated Techniques

Going forward, the MedTech company is working to continuously improve its threat hunting techniques through further refinement of Risk Fabric's Risk Models, and related workflows, including risk remediation and policy reviews.

By increasingly refining those factors being analyzed and prioritized by Risk Fabric and building that information into automated reporting and remediation workflows, the company is hoping to cover even more ground with existing analyst resources, while broadening the program to connect with a wider range of security and business officials.

Importantly, by continuously improving its insider threat hunting processes using Risk Fabric, the company is confident that it can accurately pinpoint potential problems before they result in cyber breaches and potential data loss.

About Bay Dynamics

Bay Dynamics enables enterprise organizations to identify, prioritize and mitigate their most critical cyber risks based on a strategic array of real-world conditions. Our flagship User and Entity Behavior Analytics (UEBA) and risk analytics software solution, Risk Fabric, integrates and analyzes security data across the full breadth of existing security infrastructure to pinpoint emerging threats and enable rapid remediation. For more information visit **www.baydynamics.com** or connect with us on **Twitter** and **LinkedIn**.