momentive™

CUSTOMER PROFILE

Customer
Momentive

Industry
Technology

Founded
1999

Location
Global (San Mateo, CA)

Tools
SIEM, EDR, SOAR, Cloud Data Lake

Improved maturity score from **19%** to

90%

within a year

Saved over

$600K

in detection efficiency by leveraging a no-code threat detection builder and content library

Goals

- Gain ongoing visibility into detection coverage
- Boost the SOC's threat detection capability
- Continuously build, test, and deploy detections to defend against current and emerging threats

Challenges

- Tedious and manual effort to gain structured visibility into detection coverage
- Inability to operationalize MITRE ATT&CK framework across the SOC
- Inability to build, test, and deploy detections at the speed of changing landscape

Highlights

- Determined detection coverage in 5 hours instead of 1,000+ hours manually
- Improved maturity score from 19% to 90% within a year
- Saved over $600K in detection efficiency by leveraging a no-code threat detection builder and content library

Background

Momentive, the maker of SurveyMonkey, equips decision-makers with insights they need to make decisions with confidence. More than 345,000 organizations worldwide rely on them to deliver better customer and product experiences, increase employee engagement and retention, and unlock growth and innovation.

Momentive prides itself on building a world-class security operations center (SOC) that remains nimble in detecting and responding to threats and continuing to reduce risk to the organization. As with most global organizations, Momentive leverages a number of tools in their technology stack that their SOC team uses to be efficient and effective against threats. The team employs a defense-in-depth approach and industry-leading tools to prevent, detect and respond to threats pertinent to the organization.

Challenges

As Aristotle once said, "Knowing yourself is the beginning of all wisdom," and that is precisely what Momentive's SOC team sought to do as they started their transformation journey. They first began with identifying blindspots, which proved challenging given the various tools and capabilities deployed in their environment. In order to gain a holistic view of their coverage and gaps, Senior Manager of Information Security Ajish John explored building a homegrown solution. They needed a solution that would export their current detections, map them to the MITRE ATT&CK framework, classify log sources, do adversary to tactics, techniques, and procedure (TTP) mapping, and then adapt and update as the threat landscape evolved. This manual exploration took about two months, and given the requirements, the team abandoned efforts to build a minimum viable product. During this analysis, Ajish identified feature gaps within their SIEM that limited the agility and scalability of detection development. He estimated that about 40% of the team's efforts were spent developing detections. As a result, Ajish and the Momentive SOC team sought to adopt a solution that could act as a force multiplier for the team and bridge functionality gaps in their existing tools.

Enter Anvilogic

Gaining visibility into detection coverage while operationalizing the MITRE framework is why the Anvilogic Modern SOC platform appealed to Ajish. In what took his team two months to do manually, Anvilogic was able to identify their detection coverage automatically in about five hours. Since deploying Anvilogic, the Momentive SOC team (consisting of Janice Chen, Nathan Weatherford, and Saurabh Jangid) has helped fill in the gaps of their SIEM — raising their maturity score from 19% to 90% within a year. The additional coverage and increased maturity have reinforced the confidence of new and existing enterprise customers, who trust Momentive's ability to deliver bleeding-edge solutions while keeping security and privacy at its center.

In addition to gaining visibility into their coverage, Momentive leveraged Anvilogic's ready-made detection content for their existing cloud and endpoint tools, thus gaining back time from researching, building, testing, and deploying detections they would've had to do manually with their current SIEM. As a result, within a year, the Momentive team deployed over 500 detections, saving them over $600K in detection efficiency — effectively force-multiplying the team's efforts.

Looking ahead, Ajish says now that they have continuous visibility into their detection coverage, he and his team can leverage the platform to gain better recommendations on what's next to prioritize, what to allowlist, and start doing triage and analysis: "Anvilogic has been essential to getting us where we are and is the best partner we have in the security space."

> *Before Anvilogic, it was a manual process going across different consoles. With the detection engineering part of Anvilogic, it has significantly saved us time. We weren't able to achieve this type of coverage if we were to do this manually.*
>
> – **Ajish John**
> *Senior Manager of Information Security, Momentive*