DNV
CYBER

XDR for Microsoft

When it comes to the increasing interconnectedness of the various security tools your company uses, the status quo is that there really isn't one. As the complexity of your environment grows, you will continuously run across new challenges that do not respect the boundaries of the different cyber domains you aim to protect. You always have the option of building custom-made technical integrations to enable cross-domain detection & response, but our claim is that this path has hit a brick wall.

With the amount of complexity involved there isn't really a feasible way to scrounge up the time or the resources to build and maintain these technical integrations yourself. This is why we believe that you should adopt an ecosystem-based approach that consists of choosing a pre-integrated XDR ecosystem, letting you outsource the technical integration headache to a credible and future-proof vendor.

The Value you should expect:

Microsoft delivers a comprehensive and consolidated security ecosystem, that enables us to detect anomalies in the critical domains (end user devices, identities, servers, clouds, collaborative tools) of our customer's environment. Microsoft is in a unique position with its products & services in its position as an overall IT Infrastructure provider. In the security domain Microsoft is recognized as a leader in the market and invests heavily in the development of their capabilities, with a particular focus on securing their own and connected infrastructure environments. Microsoft also continuously acquires new capabilities from the market to be integrated into their existing ecosystem for their customers benefit.

DNV
CYBER

Technology Management

Microsoft continuously develops their capabilities to meet the evolving threat landscape. To meet this continuous change, we provide visibility on recent developments in the Microsoft ecosystem including new features and changes and report these to you.

We don't stop at reporting but also help you ensure that your Microsoft ecosystem reflects the realities in the threat landscape as well as any new features delivered by Microsoft in their security platform. We do this by maintaining all relevant capabilities, e.g. System Basic Settings, Detection Rules, Prevention Policies, Exclusions, for you. What this means is that you don't need to hire any people to maintain the platform for you, we've got you covered with a turn-key service.

Periodic Investigation:

We believe that an enterprise-grade security operations capability should not limit analysis only to more critical events, since there is clear value to be found in analysing relevant lower-level events every now and then. This is why we conduct so called "Periodic Investigations" where we analyse these relevant lower-level events for any emerging trends that aren't caught in the day-to-day incident handling process. We use these trends to proactively harden your environment.

Continuous Cybersecurity Posture Management:

We believe proactivity should be built into any service an outsourced cybersecurity partner delivers to you. That is why we leverage the Microsoft ecosystem recommendations along with the analytics, reporting and threat intelligence the platform provides to continuously manage and reduce your attack surface. Practical examples of the work we do in posture management are combatting bad administrative practices, countering unsafe user behaviour and remedying system misconfigurations that all could expose your organization to attack.

Additional Consultancy:

We know that all your needs won't necessarily be covered by these service packages, and we are always happy to serve you in your wider cybersecurity consultancy needs. We have a wide range of expertise's covering cyber strategy, digital identity, GRC, certification in both IT and OT environments across our more than 500 cybersecurity experts.