DYOGUARD FAQs

CREATED BY DYOPATH

Is this cyber security service giving me the proverbial “Iron Dome” of complete protection, or is it a shared responsibility? If it is a shared responsibility, what am I still responsible for?

DYOGUARD is a complete, “start to finish” security solution for incident monitoring and management at an organizational level, as well as offering additional features designed to increase visibility at a user level.

Consider DYOGUARD like the White House’s Secret Service: We are here to monitor, anticipate, and respond to all threats that make it past other defensive tools and measures already in place. In this way you are still responsible for implementing tools like firewalls, user behavior analytics, and phishing training, but we are there to equip you every step of the way.

What layers of cyber security are included? Are user behavior analytics,predictive analysis, and AI included? Are you using SOAR?

DYOGUARD is centered around the endpoint security and SIEM layers. At these layers, we do leverage predictive analysis, SOAR, and AI at the bleeding edge. We do have a solution for user behavior analytics (UBA) as a strategic add-on.

Will this include monthly reporting? What can I expect on a high level for the reporting to provide visibility into?

Yes, monthly reporting is available from within the portal at no additional cost.

What systems or network will this integrate to, such as my O365 environment? Will it integrate with my other security tools such as firewalls, spam filter, and MFA to act as a control against them?

Yes, DYOGUARD integrates into all of these systems. We offer unlimited integrations to ensure all of your systems are covered.

Which compliance frameworks will DYOGUARD address? Does it align to NIST?

Using DYOGUARD Protect, ProtectPro, and our supplemental strategic vCISO services will address any compliance framework or standard you require. We commonly work with NIST CSF, 800 Series frameworks, CMMC, ISO, CIS, and PCI-DSS, as well as international standards like GDPR.

Will we be able to access forensics in the event of an incident?

Yes, absolutely! Not only will you have forensics in the event of an incident, but we will be able to conduct the Incident Response much quicker as a result of having this in place.

Does it integrate to my IOT devices?

If IoT devices are able to log, they can be ingested to a SIEM via SysLog servers or (potentially) via SNMP. If the tools in question are interconnected to management platforms, it’s possible to allow for API feeds to the SIEM.

I have my own tools, but I need help staffing my SOC. Can you provide me with SOC labor only?

Depending on the tools you’re currently using, we can provide a tailored staff augmentation solution with SOC analysts. However, be advised that this is not DYOGUARD; staff augmentation is quite different.

DYOGUARD is a cybersecurity program that takes a subset of layers in concert and provides a comprehensive solution that acts as a method of defense, response, and a control against other tools. We need to understand what outcome you're trying to achieve with this direction so we can determine which one of our solutions fits best, be it DYOGUARD or MSP staff augmentation services.