CYLANCE™ ThreatZERO™

CONSULTING

THREATZERO™ + SIEM SERVICES

SIEM Add-On Services

With the increasing use of Security Information and Event Management (SIEM) platforms, enterprises are achieving greater situational awareness. This use requires the integration of multiple security and administrative solutions in order to provide the most accurate and actionable information for analysts within the enterprise.

For clients who utilize SIEM within their environment, ThreatZERO Services provides three levels of SIEM integration. ThreatZERO Services are available to assist with initial setup, in-depth integration, or a full process review and custom development of correlation and process. As with all of our services, our team is capable of scoping and providing a solution for your unique environment.

SIEM Review

With the SIEM Review add-on, enterprises receive the following for the supported SIEM platforms (QRadar, McAfee SIME (Nitro), Splunk, Archsight, SumoLogic, and LogRythym):

Initial Data Source Setup – Provide initial setup of data source utilizing third-party parsers or the Cylance-designed parser for supported SIEM platforms

Communication Verification – Setup and verify the forwarding and communication from Cylance Console

SIEM Plus

With the SIEM Plus add-on, enterprises get the SIEM Review add-on with the following additional services:

Alert Creation – Assist in creating alerts specific to the Cylance Data Source setup as part of the SIEM Review

Rule Creation – Assist in the creation of rules specific to the Cylance Data Source setup as part of the SIEM Review

Knowledge Transfer – Provide informal knowledge transfer on the manipulation of the alerts and rules created for the Cylance Data Source, including SIEM Review steps

SIEM Advanced

With the SIEM Advanced add-on, enterprises will get the SIEM Plus add-on with the following additional services:

Client Process Review – Review current SIEM processes to identify gaps and incorporate Cylance data into processes

Client Additional Data Source Review – Review of additional data sources currently in use, and potential data sources available in environment but not in use

Correlation Development – Develop correlation rules and mechanisms for utilizing available data sources efficiently while incorporating into recommended processes and procedures

What You Get With SIEM Add-On

	Initial Data Source Setup	Communication Verification	Alert Creation	Rule Creation	Knowledge Transfer	Client Process Review	Client Additional Data Source Review	Correlation Development
SIEM Review	✓	✓	✖	✖	✖	✖	✖	✖
SIEM Plus	✓	✓	✓	✓	✓	✖	✖	✖
SIEM Advanced	✓	✓	✓	✓	✓	✓	✓	✓

Additional Add-On Services for ThreatZERO

Health Check – Regularly scheduled review and analysis of CylancePROTECT's operational health and general threat posture to maintain optimization and operationalization. Includes in-depth reports detailing configuration health, threat data review, and complete remediation recommendations. Reduce risk and maintain ThreatZERO status with regularly scheduled health checks.

Training – Standard and custom training solutions on CylancePROTECT, general implementation, best practices, and completely customized topics are available. This includes small audience to full classroom programs. Optimize your security knowledge and investment in Cylance.

Related Services and Products

Industrial Control Systems

- ICS Infrastructure Assessment
- ICS Compromise Assessment
- Building Automation Systems
- Incident Response Services for Control Systems

Internet of Things / Embedded

- Incident Response for IoT and Embedded Systems
- Penetration Testing for Embedded Systems

Training

- Custom Incident Response and Forensics Training
- ICS for Beginners (SANS)

Enterprise Security Services

- Internal / External Penetration Testing
- Social Engineering
- Web Application Assessment

Incident Response and Compromise Assessment

- Malware and Incident Response Retainer Services
- Incident Readiness Assessment
- Emergency Incident Response

About Cylance

Cylance is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end-users proactively solve the world's most difficult security problems.

Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated machine learning and artificial intelligence with a unique understanding of a hacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats. For more information, visit cylance.com.

Contact Cylance Professional Services to begin your journey to ThreatZERO today!

+1 (877) 97DEFEND
proservices@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700 Irvine, CA 92612

CYLANCE™ ThreatZERO

R1_20160428