BDO DIGITAL

Maximize Your Investments, Improve Your Security with Sentinel

March 20, 2024

With You Today

ROB PHILPOTTS
Cyber Threat Management and Response Director
BDO Digital

rphilpotts@bdo.ca

FRANCISCO CANO
Cybersecurity Manager
BDO Digital

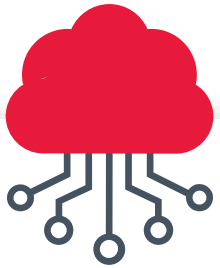
fcano@bdo.com

Agenda

- The Sentinel Opportunity
- Common Challenges vs Desired Outcomes
- Enabling Sentinel for People, Process and Technology
- Adoption Approach for Your Organization
- How BDO Can Help

The Sentinel Opportunity

In considering **Microsoft Sentinel**, one doesn't have to consider the replacement of their entire security stack, or the re-training of all their staff. Sentinel takes a wide embrace of contemporary technologies through native integrations and the ability to accommodate unique data sources through the development of powerful use cases. Rest assured, in considering your move to Sentinel, your existing technologies and skills can continue to thrive.



Common Situations in Considering Sentinel

- Security staff are overwhelmed chasing security ghosts
- An organization's current risk posture is hard to ascertain, am I protected?
- Security skills in the current solutions are well understood and risky to change
- Looking to take advantage of automation to maximize current staffing efficiency
- Looking to correlate security incidents across multiple log sources

Sentinel Implementation

Your Organization

Improve Your Security

Desired Outcomes

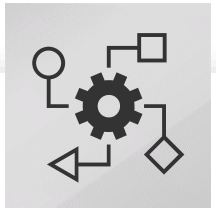
- Core familiar security technologies integrated to Sentinel
- Organization benefits immediately by combining current security solutions with Sentinel AI
- Advanced, high confidence contextualized alerts reduces burden on team pursuing low payoff tasks
- Team will gravitate towards using Sentinel as it improves collation and critical thinking
- Live KPIs on coverage and effectiveness thanks to Sentinel's ability to provide live readouts

ENABLING SENTINEL

Improving People, Process and Technology

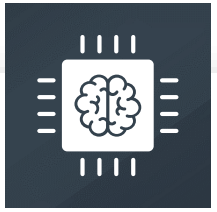
People

Security theatre is replaced by people being able to carry out high payoff actions vs. digging through the minutiae of legacy SIEM systems. Staff skills on current technology still apply as Sentinel integrate with present day solutions seamlessly.



Process

Relevant SOC workflows can be built once and documented and applied concurrently. No longer is the process separate from the technology, it's part of the technology meaning that the full incident response lifecycle is realized.



Technology

Sentinel is an unprecedented SIEM technology that is bringing value far above and beyond legacy SIEMs. It allows for integration of current investments which means you can embrace this new technology without replacing all of your solutions.

PEOPLE

People Improvements Include:

- People become more productive and focused on higher payoff security tasks vs. legacy systems
- Richly contextualized detection means that the investigator spends less time piecing things together
- The use of a standard query language means that critical thinkers can quickly add their own context
- Enhanced by co-pilot, Sentinel users become super-powered to see through an incident end to end
- Investigators can provide feedback back to the system to ensure that false-alarms get reduced
- Availability of automation means mundane tasks can be carried out quickly leaving the analyst to investigate

PROCESS

Process Improvements Include:

- Much of one's documented playbooks can be moved to be not just stored in Sentinel, but actually applied
- Workbooks present complex workflows in simple steps allowing for faster design and calibration
- Response can be added to one's Sentinel workflows by automation ensuring realization of incident lifecycle
- Logistics of change and improvement are greatly reduced. All are able to add to process improvement
- Apply continuous improvement to refine your operational procedures

TECHNOLOGY

Technology Improvements Include:

- Analytics driven approach means a multi-factor predictive approach to detection
- Ease of automation across mundane tasks such as enrichment of alert observations and response
- Ability to integrate a wide variety of technologies without re-investing in new ones
- Thorough correlation and collation of findings, self-learning

ENABLING SENTINEL

An Approach for Your Organization

Activities

Phase 1	Phase 2	Phase 3	Phase 4		
Assess	**Plan & Design**	**Implement**	**Operate & Optimize**	2 Weeks	4 Weeks
Gain a thorough understanding of your attack surface, operational processes, IT environment, staffing and key performance indicators. ▶ Critical assets and infrastructure ▶ SIEM Design, Log Aggregation ▶ Security processes including investigation, automation and remediation ▶ Existing security portfolio/attack surface including all data sources ▶ Availability and capability of the existing security staff ▶ Compliance requirements ▶ Identify integration with ITSM ▶ Metrics and Dashboards	Designing a feasible roadmap to encompass logging, detection, response and awareness. ▶ Logging – design a robust logging and integration strategy across Sentinel and relevant in-scope technologies ▶ Detection – Analytic rule selection and integration of smart alerting sources then follow up with compliance and last mile visibility use cases ▶ Response – Design essential manual and integrated response procedures, uplift and include existing processes as relevant. ▶ Dashboard and Reporting – Design essential metrics and KPIs	Integrate and calibrate data sources to Sentinel, while enabling related analytic rules and removing false positives. ▶ Support deployment of collection points (e.g., syslog) and related infrastructure (e.g., load balancers) as necessary ▶ Calibrate and Enable Microsoft native integrations across your security suites ▶ Connect log sources such as event, network and cloud logs as applicable ▶ Enable analytic rules and calibrate initial parameters, eliminate false positives ▶ Enable last mile visibility and compliance required use cases ▶ Establish health check measures such to ensure uptime and log availability ▶ Integrate incidents to enterprise ITSM	Optimizing Sentinel and Operationalizing your SOC to feasibly address your detection and response. ▶ Review analytic rules and resulting alerts on a periodic basis ▶ Ensure system self-learning by applying incident feedback continuously ▶ Assess ingested logs for relevance, effect and cost efficiency ▶ Continue to refine metrics and KPIs ▶ Deploy automated response where possible. ▶ Refine and build new use cases ▶ Finalize essential playbooks for investigation and response.	Transition	Extended Support

BDO Sentinel Consultation

Get an overview of Microsoft Sentinel and discover the potential it has to identify potential threats and vulnerabilities across your entire digital environment.

Know where you stand:

- Understand the reach of your security solutions
- Discover your maximum threat detection potential

Consultation Objectives:

- Discover current security solutions
- Discuss current SIEM setup, alerting experiences
- Ascertain high level alert flows, quality and outcomes
- Discuss value of Sentinel implementation given security context
- Seek to identify full scope
- Work with Microsoft to identify possible incentives
- Develop over proposal for Sentinel enablement project

Q & A

BDO DIGITAL

BDO Digital, LLC is a Delaware limited liability company, and a wholly-owned subsidiary of BDO USA, P.C.

BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information on BDO Digital, LLC please visit:

www.bdodigital.com

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.