

The Growing Case for Managed SOC

Matt Farry - Chief Product Officer



Into The 2000s

Passwords

Identity Makes a Comeback

Into The 2000s

Passwords

2010s

Active
Directory

Today

Cloud Identity
+ MFA

Next?

Identity as the
Control Plane

99.9%

Compromised accounts W/O MFA

(Microsoft)

88%

web-application attacks using stolen credentials

(Verizon DBIR)

**Required;
Not Requested**

	Question	Response
SMIR # 1	<i>Select one response:</i> Which description best reflects the Applicant's security operations program?	
	Applicant does not have anyone (internal or external) dedicated to monitoring security operations (a "Security Operations Center" or SOC).	
	Applicant has a SOC, but it's not 24/7 (can be internal or external).	
	Applicant has 24/7 monitoring of security operations by a 3rd party (such as a Managed Security Services Provider).	
	Applicant has 24/7 monitoring of security operations internally (regardless of whether or not a 3rd party is also used).	
SMIR # 2	<i>Select all responses that are true:</i> With respect to the Applicant's security and network monitoring capabilities:	
	Applicant uses a "Security Information and Event Monitoring" or SIEM tool to correlate the output of multiple security tools.	
	Applicant monitors network traffic for anomalous and potentially suspicious data transfers.	
	Applicant monitors for performance and storage capacity issues on all servers (such as high memory or processor usage, or no free disk space).	
	Applicant has tools to monitor for data loss (DLP) <u>and they are in blocking mode</u> .	
	Applicant has tools to monitor for data loss (DLP), but they are <u>not</u> in blocking mode.	
	None of the above/Don't know.	
SMIR # 3	What is the Applicant's average time to triage and contain security incidents of workstations for the most recent completed quarter?	
	<30 minutes	
	30 minutes-2 hours	
	2-8 hours	
	8 hours-3 days	
	>3 days	
	Applicant does not track this metric/Don't know.	
SMIR # 4	What percentage of the Applicant's "Vital Assets" are being logged and forwarded to a SIEM solution?	
	0-30%	
	31-50%	
	51-70%	
	>= 71%	
	Don't know	
	Not applicable (no SIEM)	
SMIR # 5	How long does the Applicant's SIEM solution retain logs?	
	Less than 30 days	

does not have anyone (internal or external) dedicated to monitoring security operations (a "Security Operations Center" or SOC).
has a SOC, but it's not 24/7 (can be internal or external).
has 24/7 monitoring of security operations by a 3rd party (such as a Managed Security Services Provider).
has 24/7 monitoring of security operations internally (regardless of whether or not a 3rd party is also used).

Who's Watching?

How Quick Are They?

average time to triage and contain security incidents of workstations for the most recent completed quarter?
<30 minutes
30 minutes-2 hours
2-8 hours
8 hours-3 days
>3 days
Applicant does not track this metric/Don't know.

SOC

Build or Borrow

Cost To Build

In-House SOC



Managed SOC



Time to Operational

12 to 18 months

Days - Weeks

Staffing Model

Full-time hires, high turnover risk

Shared expert team, provider manages retention

Technology Stack

Multiple vendor contracts, self-integrated

Pre-integrated, continuously updated

Cost Predictability

Variable, capital-intensive

Predictable subscription model

Scalability

Requires additional headcount

Scales with your environment

Threat Intel

Limited to internal telemetry

Enriched by cross-client intelligence

Alert Fatigue Risk

High without mature tuning

Managed with automated response and pre-tuned detection playbooks.

The CYBERSECURITY SQUEEZE





(Again)