POSEIDON
TRIDENT OF INNOVATION

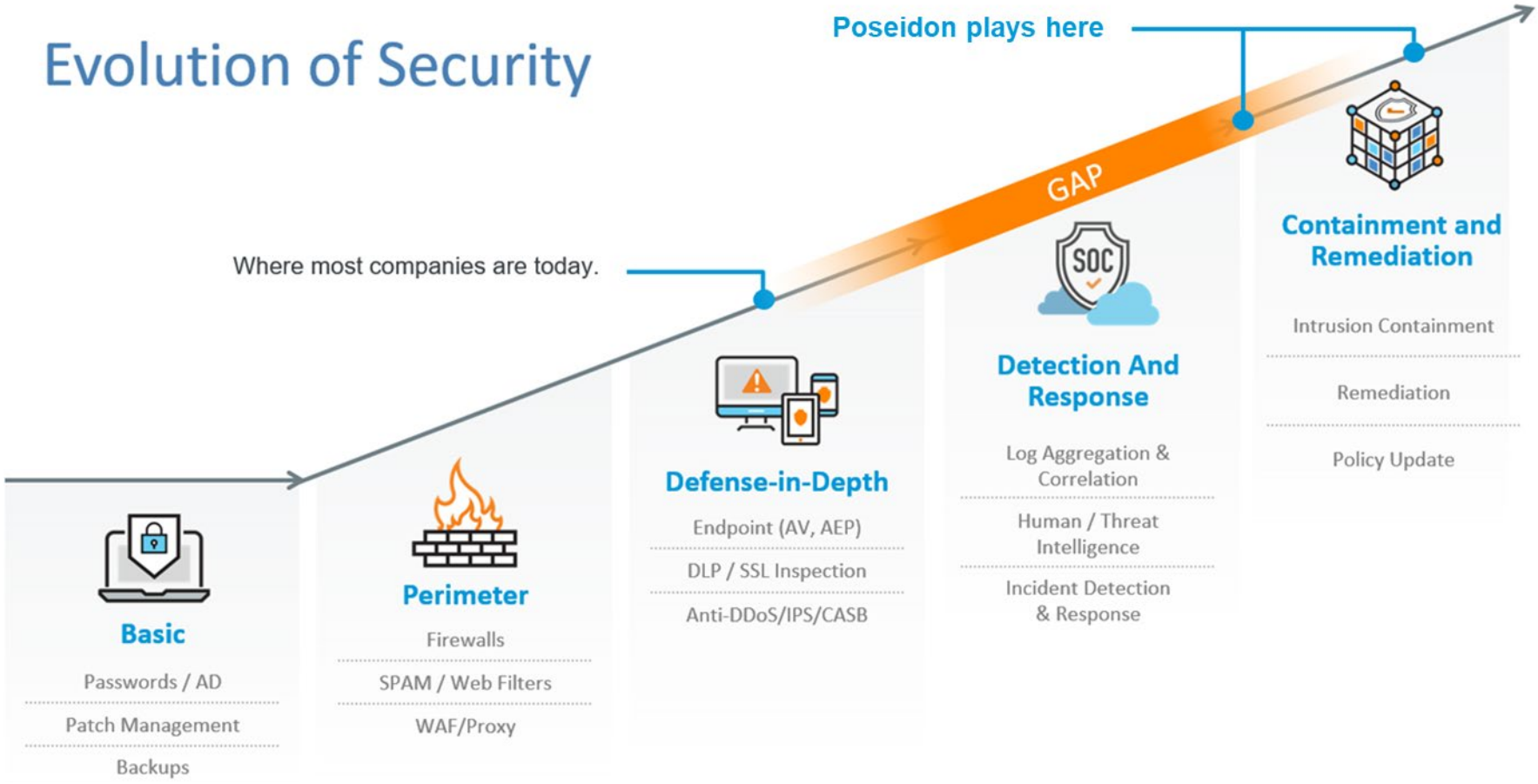
Network Security Operations Center Overview

January 1, 2021

Agenda

1. Customer Challenges – The Why
2. TRITON – The What
3. TRITON – The Technology
4. Demo / Reports / Onboarding

Customer Challenges – The Why



Customer Challenges

Too Many Point Products

Too Many Alerts

Lack of Centralized Security Visibility

No/Limited Security Expertise

No Incident Response Capabilities

Do Not Have 24/7 Coverage

Where Do We Play?

NIST

53% cost per incident is spent in detection and response

240 days to detect a security incident

46 days to respond to security incident

1 Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

2 Protect

- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

3 Detect

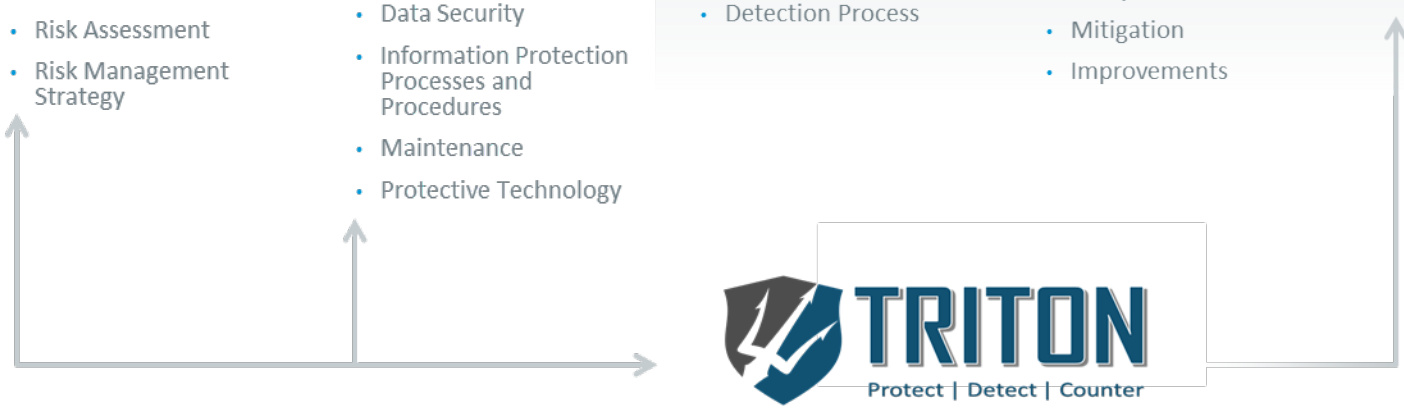
- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

4 Counter

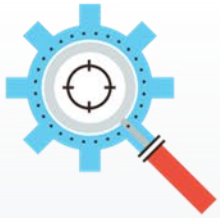
- Counter Planning
- Communications
- Analysis
- Mitigation
- Improvements

5 Recover

- Recovery Planning
- Improvements
- Communications



Solution: TRITON



Comprehensive

Unified Security with centralized view

24x7 Monitoring

Focused on Managed Detection and Response

Predictable Pricing

Fixed annual price faster, better, cheaper

Behind the Scenes of SOC

Equipping a SOC: Technology

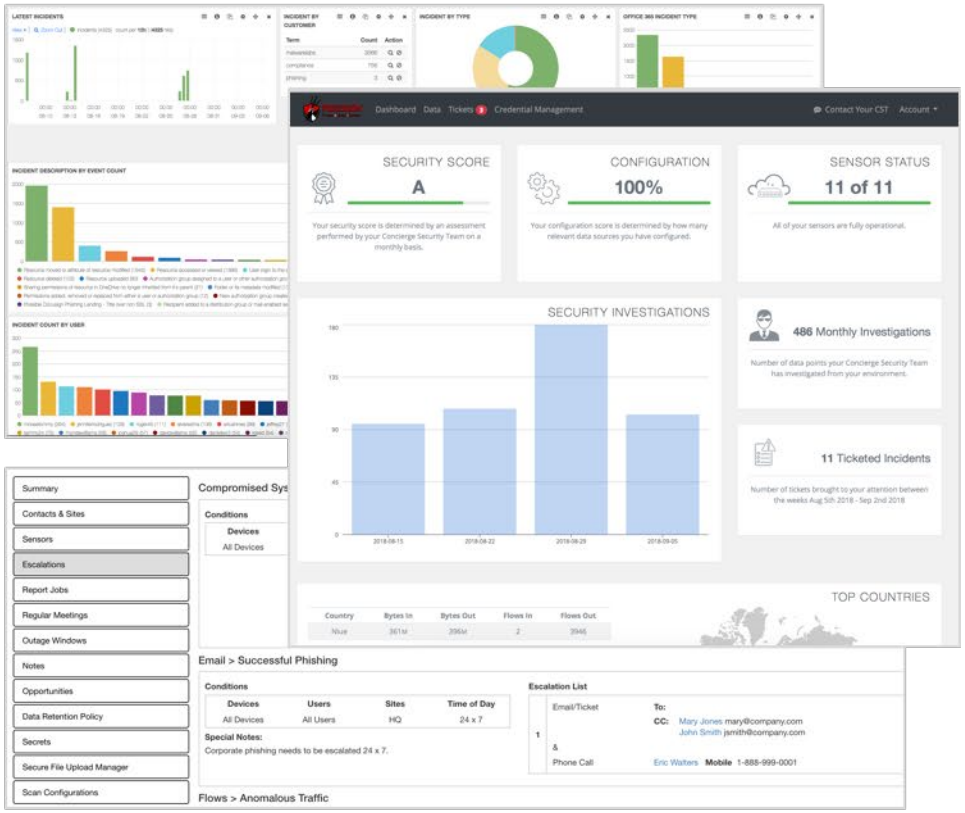
- Telemetry (IDS, Security Tools, Logs, etc.)
- SIEM/Platform
- Threat Intelligence
- Workflow tools
- Sandboxes, OSINT, Scripts, etc.

Staffing a SOC: People

- Operators
- Analysts (usually tiered)
- Managers
- R&D (platform support/customization, research, etc.)

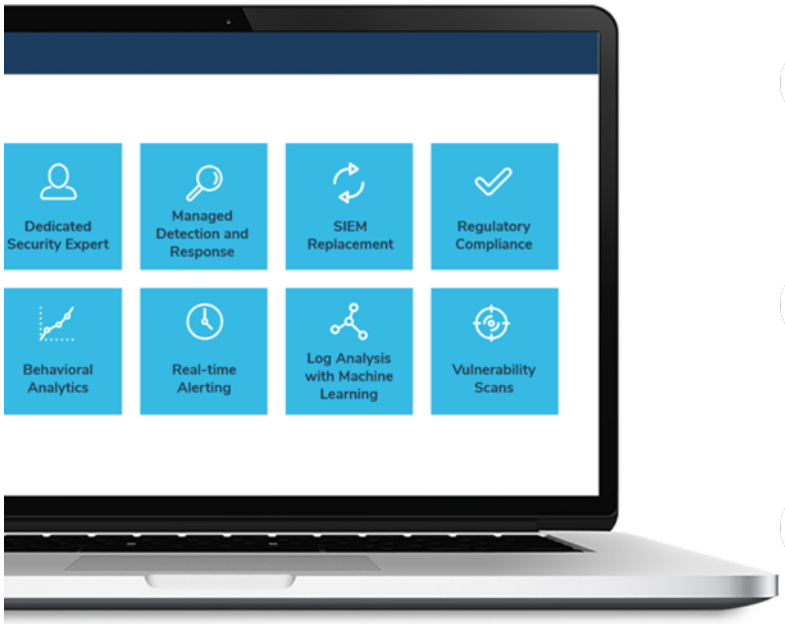
Operationalizing a SOC: Processes

- Training
- Triage/Forensics
- Threat hunting / deep dives
- Incident response



TRITON
Protect | Detect | Counter

Capabilities



Threat Management

- Full visibility of threats within your environment
- Actionable security intelligence to improve your security posture

Reduced Cyber Risk

- Greater cyber defense; reduced cyber risk
- Best practices in security operations through your CSE

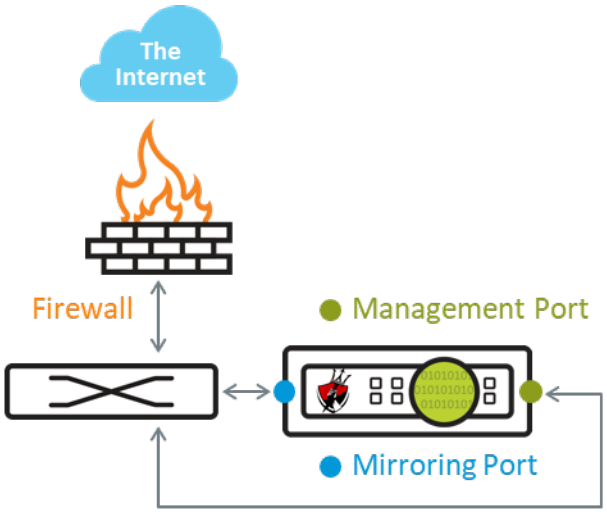
Unified Security

- NSOC-as-a-Service is backed by hardware, software, maintenance
- People and processes to address your business risks

Security Operations Effectiveness

- Visibility of your current security posture
- Effective and prioritized incident response

Sensor Details



- SPAN/Mirror Ingress/Egress
- Managed Intrusion Detection System (IDS)
- Flow Aggregator/Creator (IPFIX)
- Network Security Monitoring (NSM)
- Log Aggregator (syslog)
- Asset Profiling

Poseidon Custom:

Not Exhaustive Ruleset Categories

Activex	Dshield	Mobile_malware	Shellcode
Attack_response	Exploit	Netbios	SMTP
Botcc	FTP	P2P	SNMP
Chat	Games	Policy	SQL
Ciarmy	ICMP_info	Pop3	Telnet
Compromised	ICMP	Rbn-malvertisers	TFTP
Current_events	Imap	Rbn	TOR
Deleted	Inappropriate	RPC	Trojan
DNS	Info	SCADA	User_agents
DoS	Malware	SCADA_special	VoIP
Drop	Misc	Scan	Web_client
Web_server	Web_specific_apps	Worm	

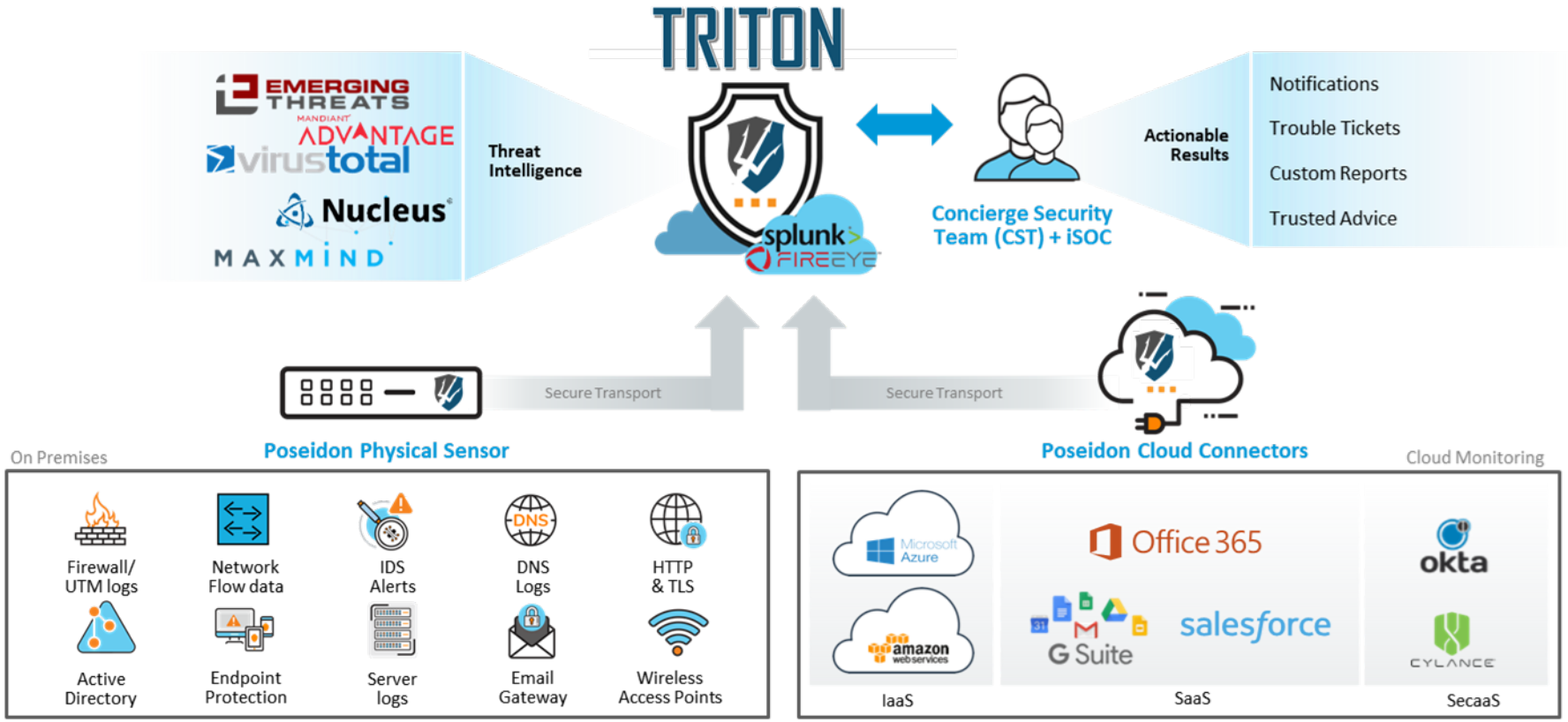
ET PRO:

37,000 Rules
50+ New Daily Rules
50 Categories
(e.g., protocol specific attacks, network behaviors, botnets, vulnerabilities, exploits, malware C2, SCADA network protocols, exploit kit activity, etc.)

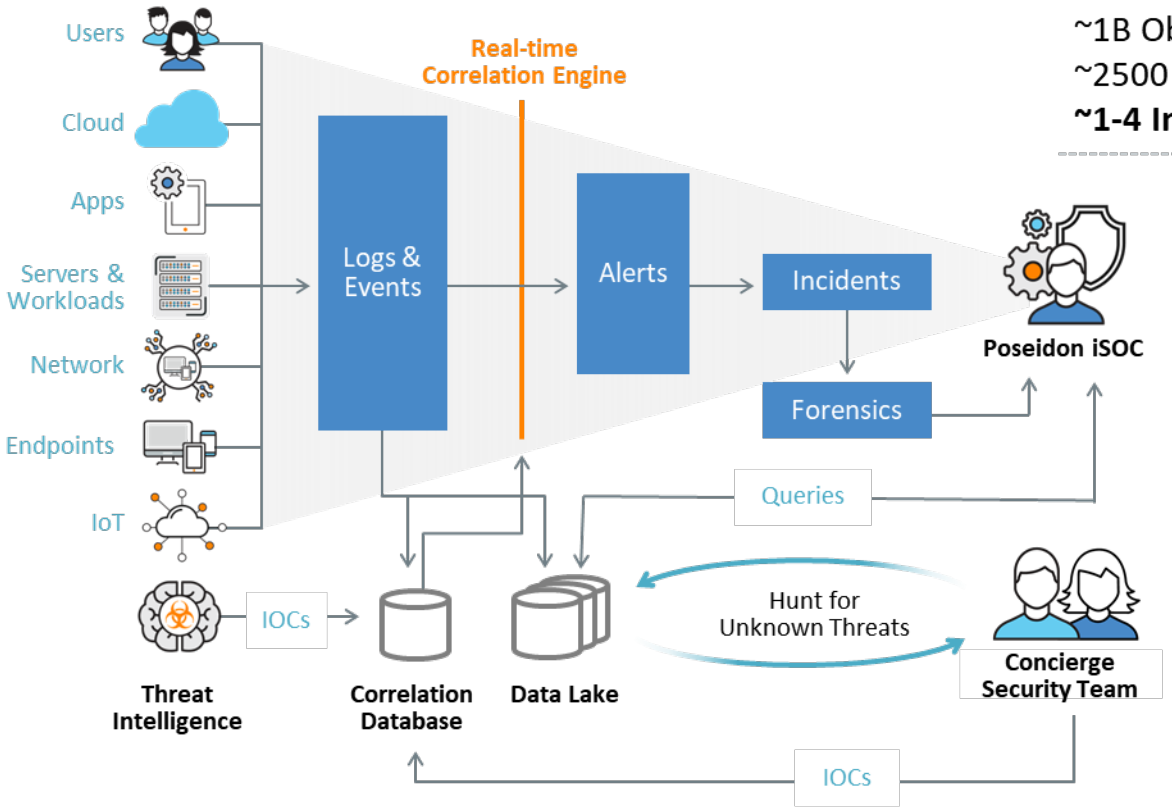
Asset Profiling:

Active Directory (users/groups) via WinRM/WMI
Device Profiling (NMAP/SNMP)
Windows Details (last logged on user, SP's installed, etc.)

Technology—Architecture Overview



Backend Concierge Security Team Process



~1B Observations/Week
~2500 Investigations/Week
~1-4 Incidents/Week

2500 Users
250 Servers
10 Sensors

Real-time Correlation

- Analyze billions of events
- Real-time correlation against IOCs
- Reduced false positives

Forensics

- Search and research quickly
- Construct blast zone analysis and remediate

Hunt

- Hunt for unknown threats with deep analytics and machine learning
- Identify new IOCs to improve monitoring

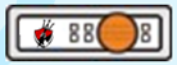
Poseidon NSOC™ Concierge Onboarding

Accelerate Time to Value with Streamlined Service Installation!

Technical Kickoff

Technical Readiness

- Review contracts, establish timeline
- Define project plan and review SLAs
- Gather technical details



NSOC Essentials

Sensor Deployment and Log Setup

- Install sensors in primary location(s)
- Identify essential log sources
- Setup portal users and basic escalation

Poseidon NSOC Readiness

Finalize Onboarding

- Add remaining sensors and log sources
- Complete sensor installation for remote locations
- Configure external vulnerability scans to identify exposed services
- Validate that log sources are generating usable data

Poseidon NSOC Service Acceptance & Customization

- Introduce Concierge Security Team
- Review external vulnerability scan settings and fine-tune service
- Discuss any log source ingestion that would require security customization
- Identify your reporting and compliance needs
- Train customer portal users

Quarterly Meeting (Default Agenda)

Agenda

Introductions

Summary of Past 3 Months

Roadmap

Customer Update/Initiatives

3 Month Summary

1.5 Billion unique observations collected over the last 3 months

Poseidon has reviewed 1607 incidents over the past 3 months, of which 7 have been escalated to you.

3 adware | 1 malware/botnet

1 phishing | 1 anomalous traffic

Service Investment Areas

Cloud Sensing

Poseidon Sensing—CloudWatch, CloudTrail, VPC Flows, Application Logs

Office365 Monitoring Admin API

Salesforce, Okta, Google Apps, Cylance

Log Search

Endpoint Visibility / Containment

Customer Update

Compliance Initiatives/Audit Cadence

NIST Framework

PCI/HIPAA/SOX Audit Timeframe

Security Tool Investigations?

What else can we do to help?

Risk/Recommendation

Areas of Concern

Critical Vulnerability on firewall—Cisco ASA / IOS IKE Fragmentation

Out dated Java/Flash

Call to Action

Patch firewall ASAP

Upgrade Java/Flash where possible

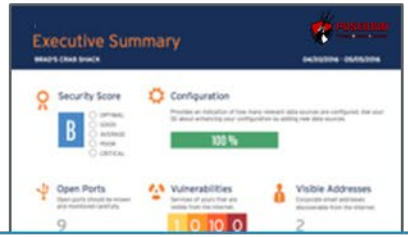
Ingest new EPP logs (Cylance)

Normal Reports Delivered (default/optional)

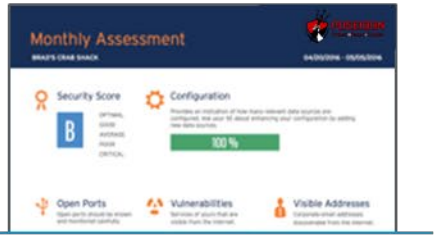
Security Review
Weekly/Monthly

Open/Closed Incidents
Weekly

External Vulnerability
Monthly / On-Demand



Executive Summary
End of First Month



Monthly Assessment
Monthly

Quarterly Assessment
Quarterly (along with CSE/CSM meeting)

Questions

For Questions, please email us at:
info@poseidon-us.com
or call (727) 493-2351

Thank you and looking forward to solving your cybersecurity needs