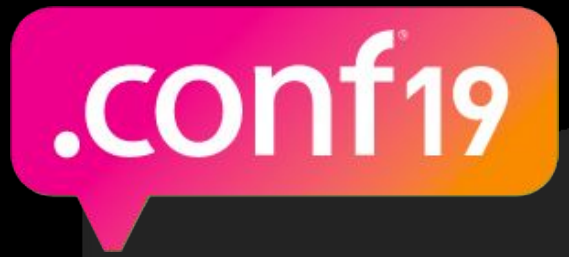
PROFICIO

The SOC of the Future

SECS2839

Brad Taylor, CEO
Proficio



AGENDA

01 About Proficio

02 What We See

03 Challenges

04 Recommendations

05 Proficio's Approach

06 Q&A

PROFICIO

ABOUT PROFICIO

- Founded in 2010
- Managed Detection & Response
- Splunk MSSP
  - Hosted or Client Owned
  - 100+ Customers Using Splunk
- Addressing enterprise requirements
- Global reach
- Billions of security events monitored daily

PROFICIO

SAN DIEGO, CA USA

BARCELONA, SPAIN

SINGAPORE

SOC 2 TYPE 2

INDUSTRY STANDARD FRAMEWORK MODEL

150+ CERTIFICATIONS & ACCREDITATIONS

PROFICIO

MANAGED DETECTION AND RESPONSE

SOC-AS-A-SERVICE (MSSP & MDR)

- 24x7 Monitoring, Investigations, and Alerting
- Actionable Alert Notifications
- Cloud or Hybrid On-Premise SIEM
- Threat Intelligence Platform

SECURITY BUSINESS INTELIGENCE DASHBOARD

- Visibility to Security Posture
- Risk Scorecard & Peer Comparison
- Threat Response Ticketing & Peer Comparison

MANAGED SECURITY SERVICES

- Firewall, IPS, WAF, SIEM, Scan, VLMaaS, and EDR

INCIDENT RESPONSE

- SOAR - Automated Attack or Compromise Response
- Managed Endpoint Protection Response Services

THE SOC OF THE FUTURE

The SOC of the future will have only two employees, a **security engineer** and a **dog**.

The engineer will be there to feed the dog.

The dog will be there to bite the engineer if he/she touches the system.

Adapted from Warren Bennis

WHAT DO WE SEE IN SOCs TODAY

- MANAGE
  - High number of Notables per day
  - Understaffed for SOC Threat Detection
  - Failure to perform Asset, Policy, and Data Modeling
  - High risk due to missing log sources or improper logging
  - Lack of visibility into Security Gaps
- DETECT
  - Majority average only a dozen well-tuned Use Cases
  - Lack of Investigation Playbooks
  - Limited Integrated Threat Intelligence
  - Limited use SOAR
- RESPOND
  - Over 50% do not engage every threat identified by SOC
  - No Automated Response
  - Lack of tracking metrics of full lifecycle of security event through remediation

WHAT ARE YOUR OBJECTIVES AND KEY RESULTS?

- VISIBILITY
  - Detect indicators early
  - Accuracy of detection
  - Business Context
- RESPONSE ORCHESTRATION
  - Categorized
  - Orchestrated
  - Triaged and ticketed
  - Automated when possible
  - Manual where needed
- BUSINESS INELLIGENCE FOR SECURITY PROGRAM
  - Risk assessment
  - Trends, root cause, and progress
  - Response metrics

CHALLENGES

TECHNOLOGY

SKILLS GAP

THREAT LANDSCAPE

PROFICIO

CHALLENGES - THREAT LANDSCAPE

Bigger More Diverse Attack Surface

- IoT
- Cloud
- Mobile

Increased Attacker Sophistication

- AI-enabled
- Adversarial Machine learning
- Unknown Threats

Visibility and Response

- Faster detection
- Instant Response
- Quantification of risk
- Actionability

PROFICIO

CHALLENGES - SKILLS GAP

- Less time for
  - Investigations
  - Threat Hunting
  - Incident Response
- Budget pressure
- Staff turnover and burnout
- Reduced productivity
- Human error
- Under utilization of technology
- Less time spent on business alignment

CHALLENGES - TECHNOLOGY

- Technology Selection
  - Threat detection
  - Automation
  - SOAR
  - AI/ML
- Technology Implementation
  - Integration with existing point tools
- Technology Management
  - Maximizing value
  - Mapping human skills to technology
- Business Intelligence for Security
  - Visibility, Risk and Security Posture
  - Operational KPI's
  - Peer Comparison

PROFICIO

RECOMMENDATIONS – THREAT LANDSCAPE

Threat Information

- How does this threat work?
  - Tactics, Techniques, and Procedures
- What is the risk?
- Who is the threat actor?

Threat Impact

- Incident history
- Asset Categorization
- Criticality of event
- Priority of response

Recommendations

- Business Context Models
- Response Plan Checklist
- Remediation strategies
- Threat detection improvements

PROFICIO

RECOMMENDATIONS
STRATEGIES FOR ADDRESSING SKILL SHORTAGES

Accelerate Hiring

- Compensation
- Hire more women
- Partner with universities
- Hire Vetrans

Reduce Need for Hiring

- Automate
- Increase productivity
- Collaboration
- Training
- Retention programs

Change Hiring Dynamic

- Outsource
- Co-management
- Move SOC
- Distributed SOC

PROFICIO

RECOMMENDATIONS - TECHNOLOGY

Commercial vs. Opensource

- Time to operationalize
- Internal & External resources
- Security
- Operational Tools

People Process and Technology

- Planning
- Implementation
- Management

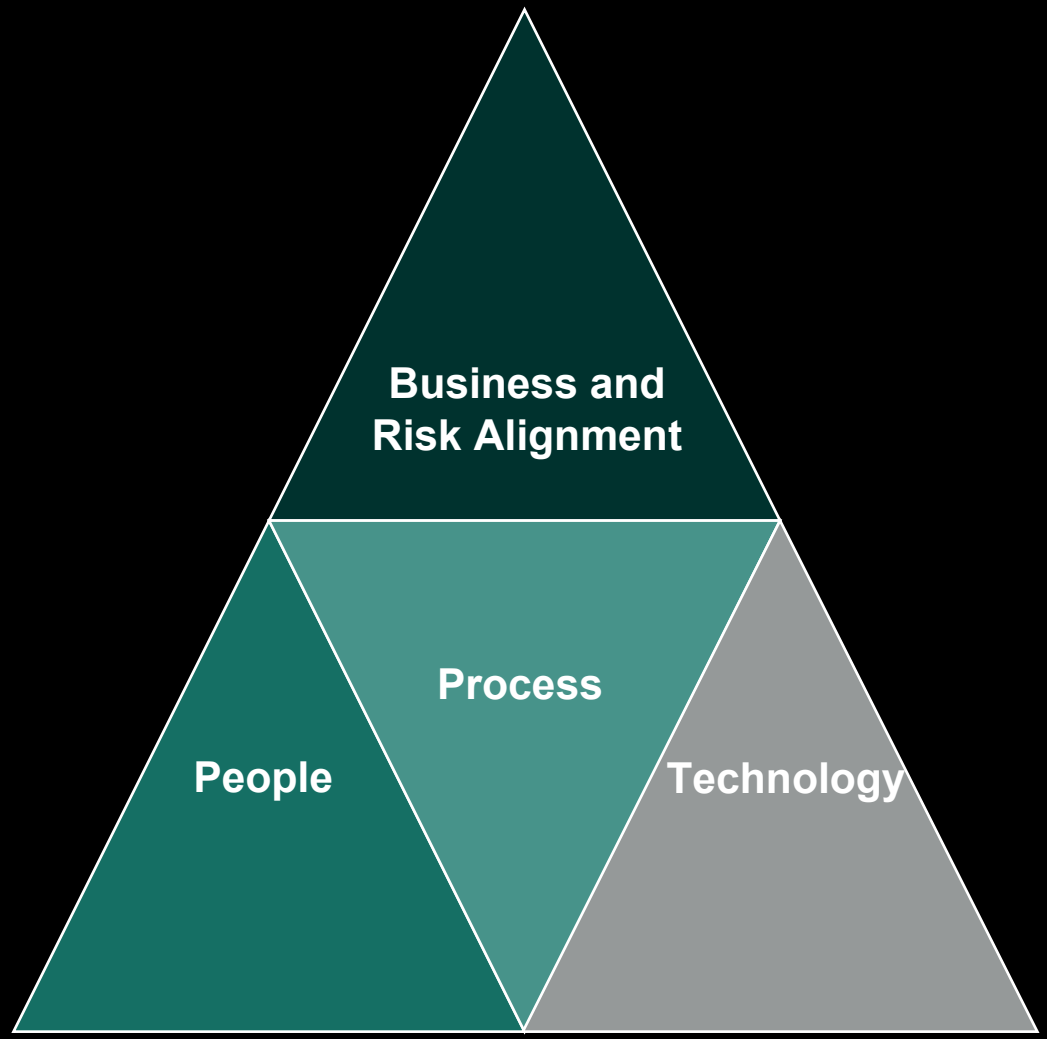
Why Select Splunk for SOC of the Future

- Technology
- Vision
- Ecosystem

PROFICIO

PROFICIO'S APPROACH

- Leverage what has worked
  - Global SOCs
  - Career paths for Analysts
  - Log Enrichment
  - Use Case development process
  - SOAR
  - Business Context Modeling
- Future forward
  - AI / ML
  - Search
  - Cloud
  - Process Automation
- Continuous improvement
  - Data => Insight => Change



PROFICIO

PROFICIO'S APPROACH – THREAT INVESTIGATION

1. THREAT INFORMATION

- TACTICS: Execution, Persistence, Privilege Escalation, Credential Access. The threat is categorized as CryptDOS in relationship to APIHook Browser Hijacker which is malware that is known to slow down systems and impact performance.
- TECHNIQUES: Service Execution, Hooking.

MITRE | ATT&CK™

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Service Execution 1	Hooking 1	Hooking 1		Hooking 1					

- PROCEDURES: The attacker's domain has been observed communicating with other malicious files that pose threats more serious than denial of service, like backdoor-related malware that downloads more malware.

- SEVERITY: 3-Medium
- RISK: 3-Medium
- THREAT ACTOR: Cybercriminals – Unknown

PROFICIO

PROFICIO'S APPROACH – THREAT INVESTIGATION

2. CLIENT INFORMATION

- THREAT IMPACT: 4-High. This threat could impact heavily in your organization, based on the lack of controls and security policies

- INCIDENT HISTORY : INCXXXXXXX, INCXXXXXXX, INCXXXXXXX. We can confirm these IOCs have been first observed in your network 3 months ago.

- DEVICE CORRELATION: Endpoint AV, NGFW, IDS. We have found log events related to this threat on different devices, helping us to confirm the incident and threat behavior associated.

3. RECOMMENDATIONS

- We recommend you remove any CryptDOS-associated software from the identified hosts, including performance-degrading toolbars. Please Isolate the systems affected and run containment actions through you EDR Solution in order to remove any traces of potential malware. Only install toolbars and extensions from trusted sources that can be verified; installation permissions can be managed using group policies.

USE CASE DEVELOPMENT

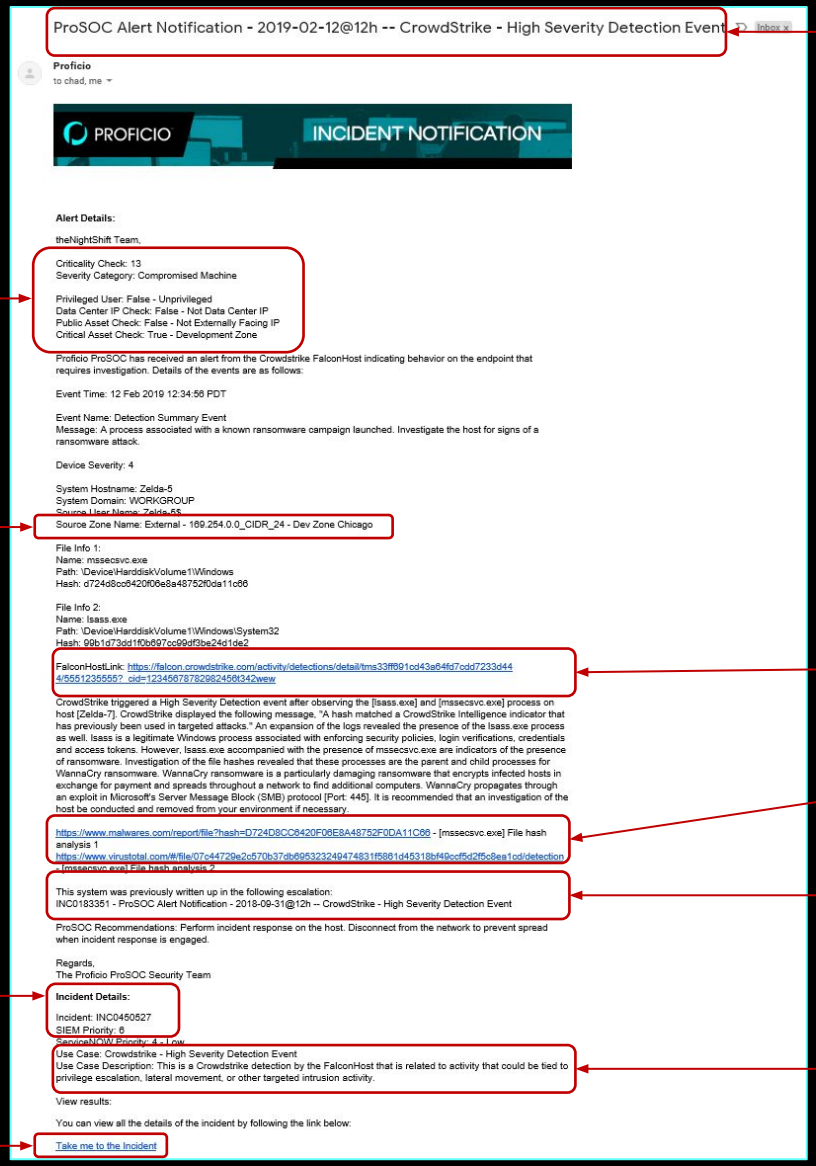
Business Drivers
Direct Financial Loss
Reputational Damage
Legal and Regulatory Obligations
Enable Business
Business Continuity
Strategic and Commercial Interests

Threat Actors
Professional Criminals
State Actors
Terrorists
Hacktivists, Cyber vandals and Script Kiddies
Internal Actors
Private Organizations
Multiple Actors

Detection Technologies
SIEM
Big data Analytics
NIDS/NIPS
HIPS
Anti-malware
Network Anomaly Detection
Email Protection

Log Sources
Firewall
Network Traffic
OS Logging
Application Logs
Web Application Logging
Database Logs
Proxy Logs

SAMPLE TRIAGED ALERT



ProSOC Alert Notification - 2019-02-12@12h -- CrowdStrike - High Severity Detection Event

Proficio
to chad, me

PROFICIO INCIDENT NOTIFICATION

Alert Details:

theNightShift Team,

Criticality Check: 13
Severity Category: Compromised Machine

Privileged User: False - Unprivileged
Data Center IP Check: False - Not Data Center IP
Public Asset Check: False - Not Externally Facing IP
Critical Asset Check: True - Development Zone

Proficio ProSOC has received an alert from the Crowdstrike FalconHost indicating behavior on the endpoint that requires investigation. Details of the events are as follows:

Event Time: 12 Feb 2019 12:34:56 PDT

Event Name: Detection Summary Event
Message: A process associated with a known ransomware campaign launched. Investigate the host for signs of a ransomware attack.

Device Severity: 4

System Hostname: Zelda-5
System Domain: WORKGROUP
Source User Name: Zelda-5$

Source Zone Name: External - 169.254.0.0_CIDR_24 - Dev Zone Chicago

File Info 1:
Name: mssecsvc.exe
Path: \Device\HarddiskVolume1\Windows
Hash: d724d8cc6420f06e8a48752f0da11c66

File Info 2:
Name: lsass.exe
Path: \Device\HarddiskVolume1\Windows\System32
Hash: 99b1d73dd1f0b697cc99df3be24d1de2

FalconHostLink: https://falcon.crowdstrike.com/activity/detections/detail/tms33ff891cd43a84fd7cdd7233d444/5551235555?_cid=1234567878298245fd342wew

CrowdStrike triggered a High Severity Detection event after observing the [lsass.exe] and [mssecsvc.exe] process on host [Zelda-7]. CrowdStrike displayed the following message, "A hash matched a CrowdStrike Intelligence indicator that has previously been used in targeted attacks." An expansion of the logs revealed the presence of the lsass.exe process as well. lsass is a legitimate Windows process associated with enforcing security policies, login verifications, credentials and access tokens. However, lsass.exe accompanied with the presence of mssecsvc.exe are indicators of the presence of ransomware. Investigation of the file hashes revealed that these processes are the parent and child processes for WannaCry ransomware. WannaCry ransomware is a particularly damaging ransomware that encrypts infected hosts in exchange for payment and spreads throughout a network to find additional computers. WannaCry propagates through an exploit in Microsoft's Server Message Block (SMB) protocol [Port: 445]. It is recommended that an investigation of the host be conducted and removed from your environment if necessary.

https://www.malwares.com/report/file?hash=D724D8CC6420F06E8A48752F0DA11C66 - [mssecsvc.exe] File hash analysis 1
https://www.virustotal.com/#/file/07c44729e2c570b37db69532324947483 1f5881d45318bf49ccf5d2f5c8ea1cd/detection - [mssecsvc.exe] File hash analysis 2

This system was previously written up in the following escalation:
INC0183351 - ProSOC Alert Notification - 2018-09-31@12h -- CrowdStrike - High Severity Detection Event

ProSOC Recommendations: Perform incident response on the host. Disconnect from the network to prevent spread when incident response is engaged.

Regards,
The Proficio ProSOC Security Team

Incident Details:

Incident: INC0450527
SIEM Priority: 6
ServiceNOW Priority: 4 - Low

Use Case: Crowdstrike - High Severity Detection Event
Use Case Description: This is a Crowdstrike detection by the FalconHost that is related to activity that could be tied to privilege escalation, lateral movement, or other targeted intrusion activity.

View results:

You can view all the details of the incident by following the link below:

Take me to the Incident

SIEM Case ID

Custom Asset Lookup

Zone Modeling

Native Log Source Enrichment

External Data Enrichment

Internal Data Enrichment

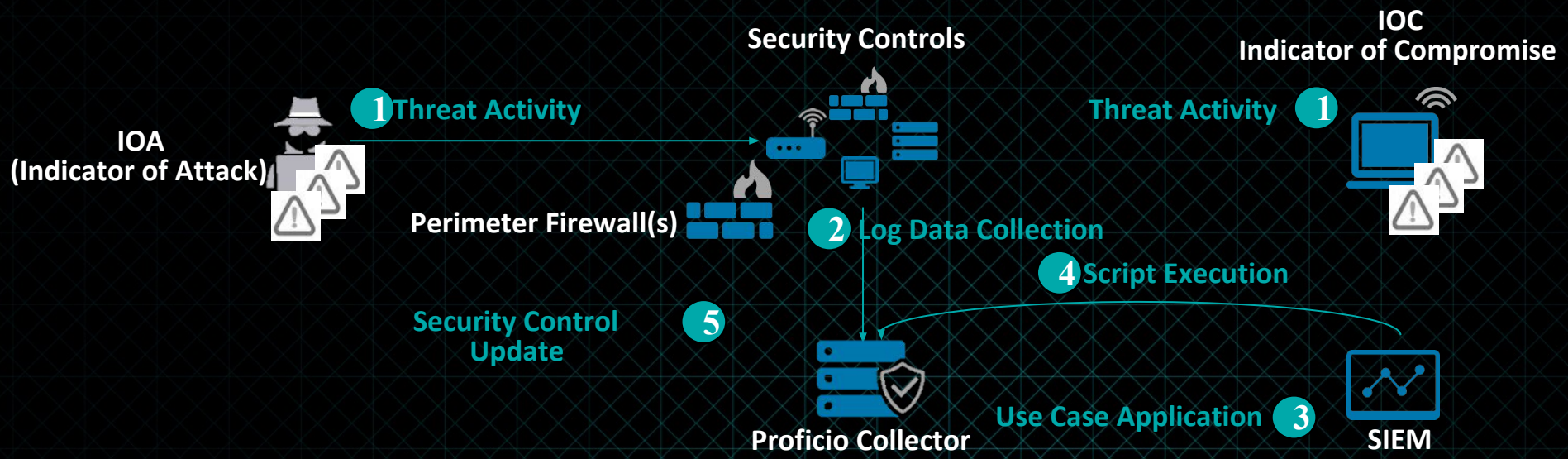
ITSM Details

Use Case Metadata

Incident Link

PROFICIO

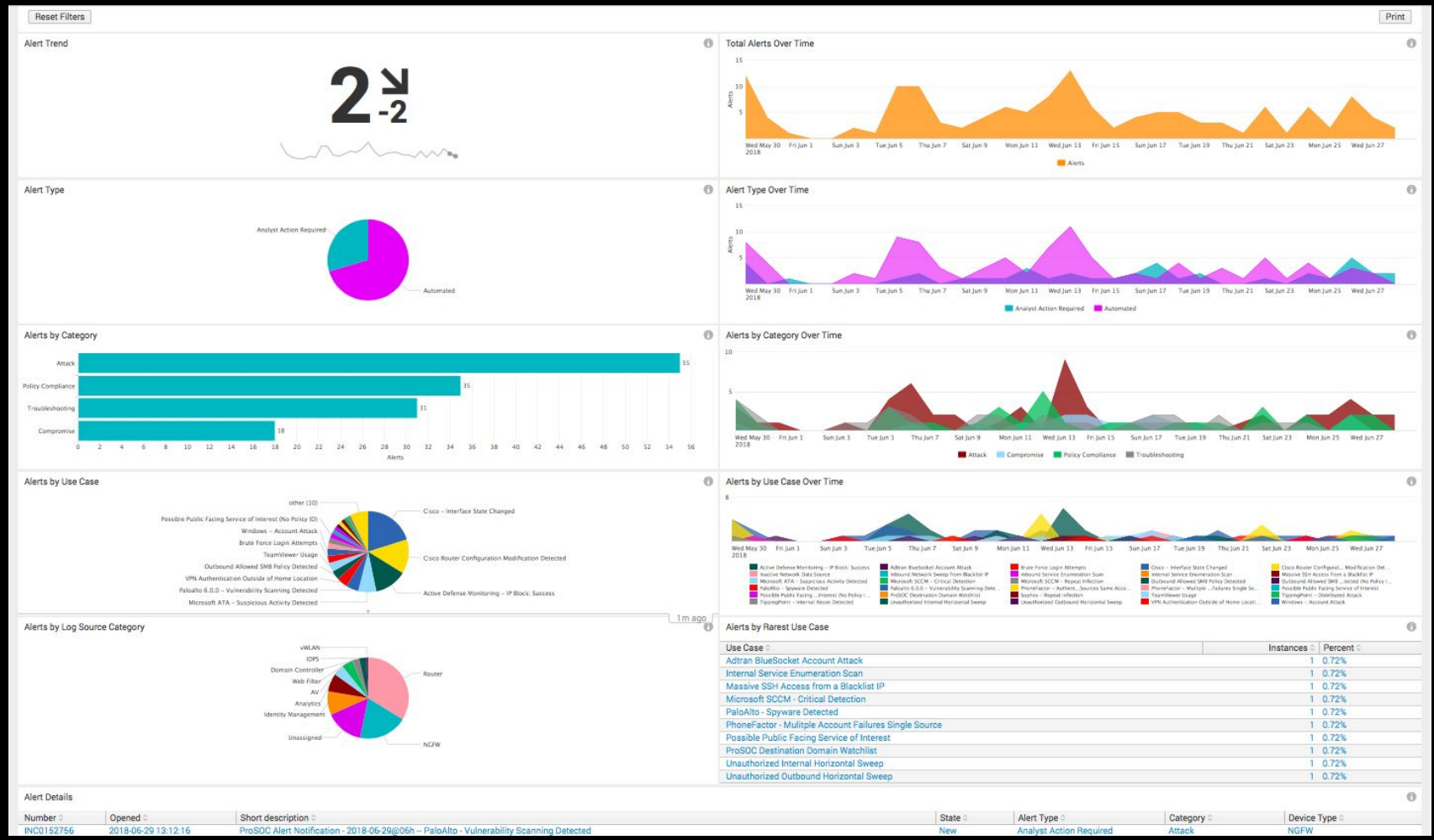
ACTIVE DEFENSE AUTOMATED RESPONSE



Step	Action	Description
1	Threat Activity	Activity related to threats is detected either as indicators of attack (IOA) or indicator of compromise (IOC). The activity is captured in various security control logs.
2	Log Data Collection	Logs are collected from various security controls in the client environment and submitted to the Proficio Collector for secure transmission to a Proficio Managed SIEM.
3	Use Case Application	Correlation use cases are applied to the logs collected. Proficio and the client choose a set of correlation use cases related to specific IOC and IOA activity that initiates an automated response. Use case triggers are also processed through client business context and client specific whitelisting.
4	Script Execution	Proficio's SIEM executes a script and sends the applicable parameters on ProSOC Collector(s) to update applicable security controls in the Active Defense Chain.
5	Security Control Update	Proficio's SIEM Collector(s) sends appropriate calls to the security control(s) to update the security control to block the indicator.

HELP IT LEADERS UNDERSTAND RISK

- Trend Analysis
- Dive into Root Cause
- Where do we need new controls
- Risk Score based on Threat Prevention and Visibility
- Is your SOC performing human investigations



PROFICIO

MEASURE METRICS AND CONINUOUSLY IMPROVE

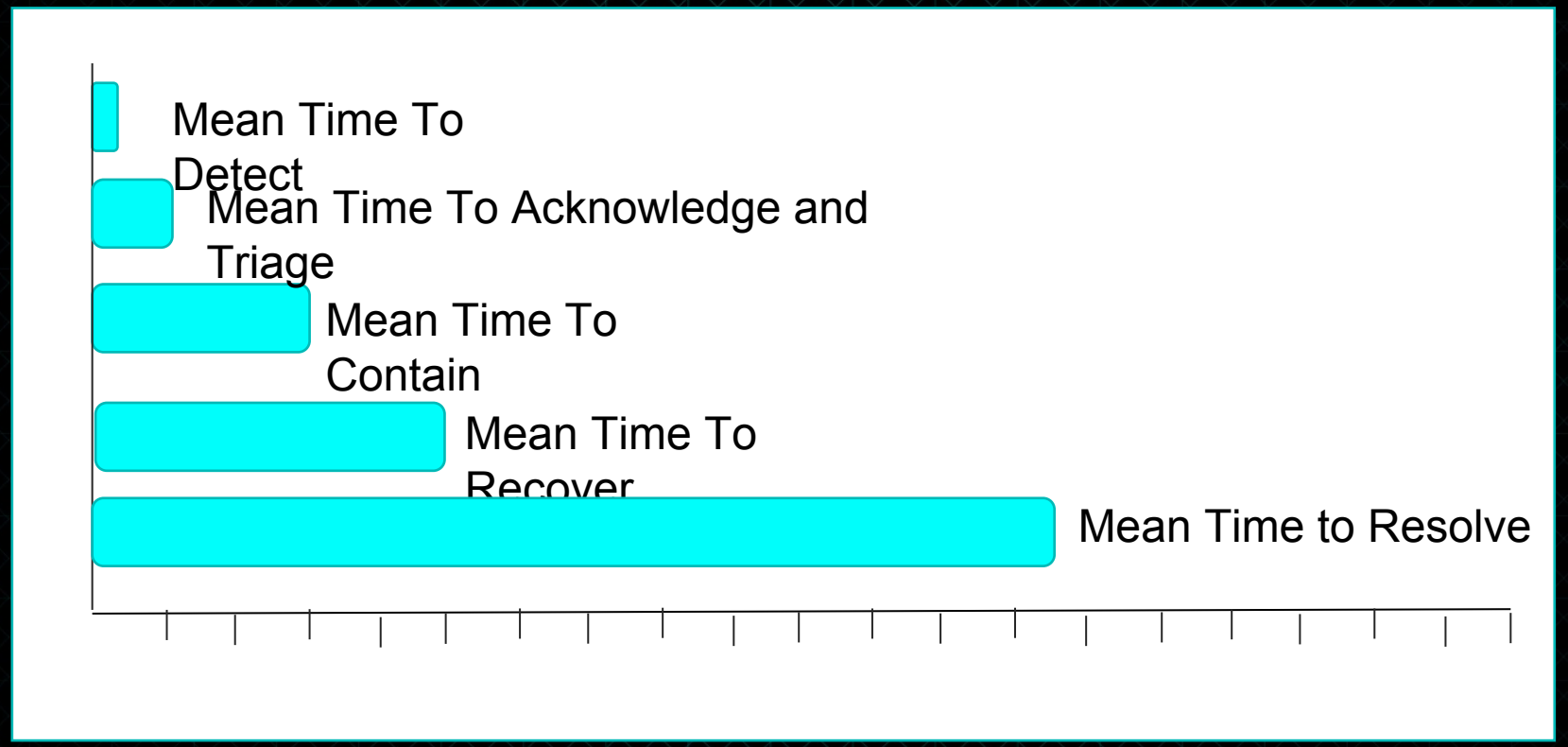
30 MINUTES?

+ 30 MINUTES?

+ 2 HOURS?

+ 8 HOURS?

+ 14 DAYS?



SOC

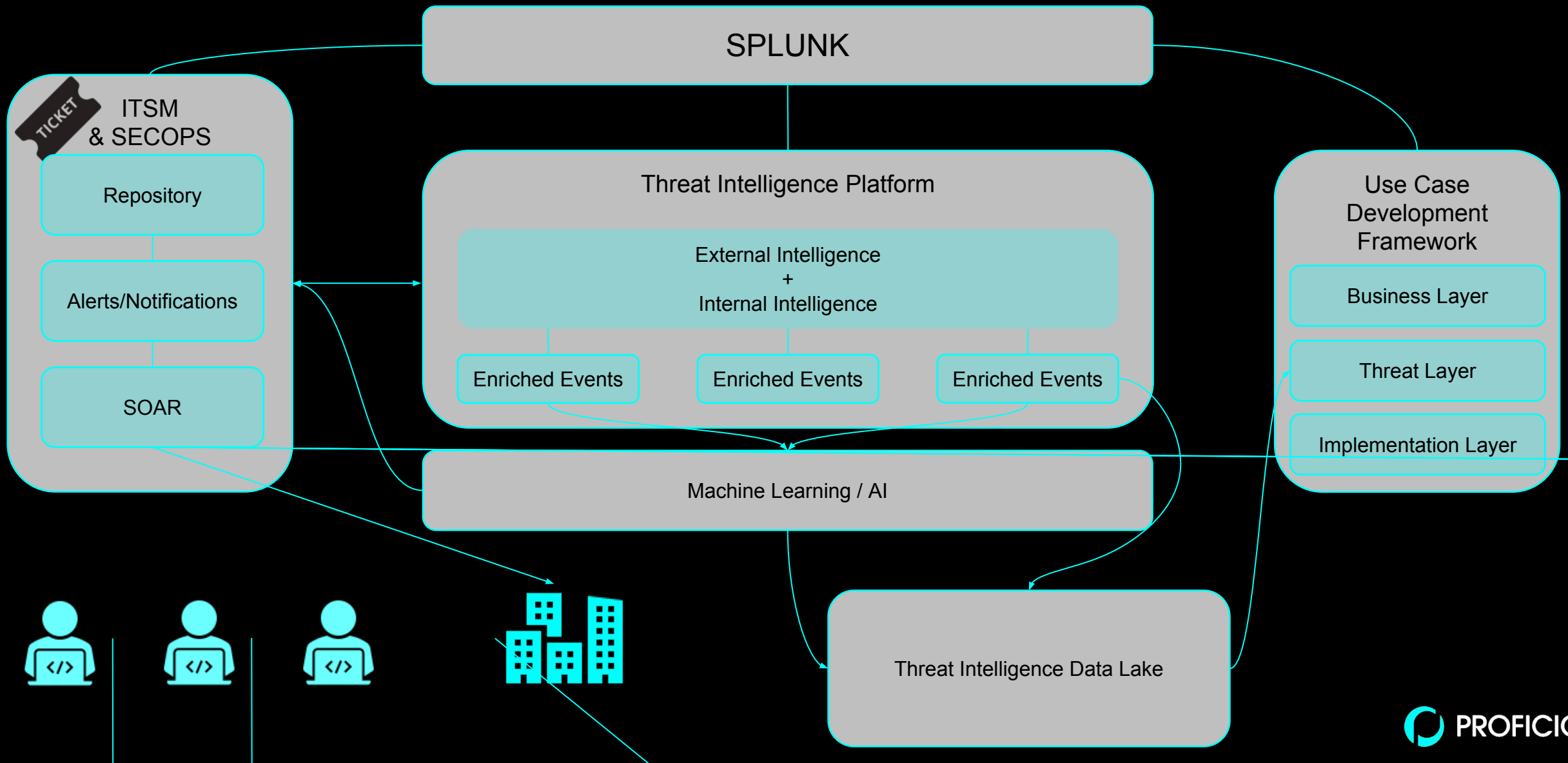
SECURITY

OPERATIONS / SECURITY / EXECUTIVE

NIST INCIDENT RESPONSE STAGES

PROFICIO

SOC OF THE FUTURE ARCHITECTURE



QUESTIONS?

BOOTH 123

WWW.PROFICIO.COM | INFO@PROFICIO.COM