Benefits:

- **Fastest end-to-end response time**
  Provides real-time threat response & remediation – reducing average IR time to less than 15 minutes
- **Complete endpoint visibility**
  Records 100% of activity to speed IR & enable proactive threat hunting
- **Accelerate investigations**
  Information you need is always available, never hit a blind spot
- **Detailed attacker forensics**
  See where the attacker went and what they did
- **Find threats missed by defenses**
  Reduce dwell time and damage done
- **Disrupt future attacks**
  Know root cause, then address gaps and blind spots
- **Reduce IT involvement**
  Eliminate unnecessary reimaging and tickets
- **Optimized for on premise deployments**
  Minimal infrastructure requirements – your data is your data

Use Cases:

- Breach preparation
- Attack detection
- Alert validation and triage
- Incident response
- Attack isolation
- Threat hunting
- Remediation
- Threat banning
- Prioritized patch management

PROFICIO

Managed Endpoint Detection and Response Services

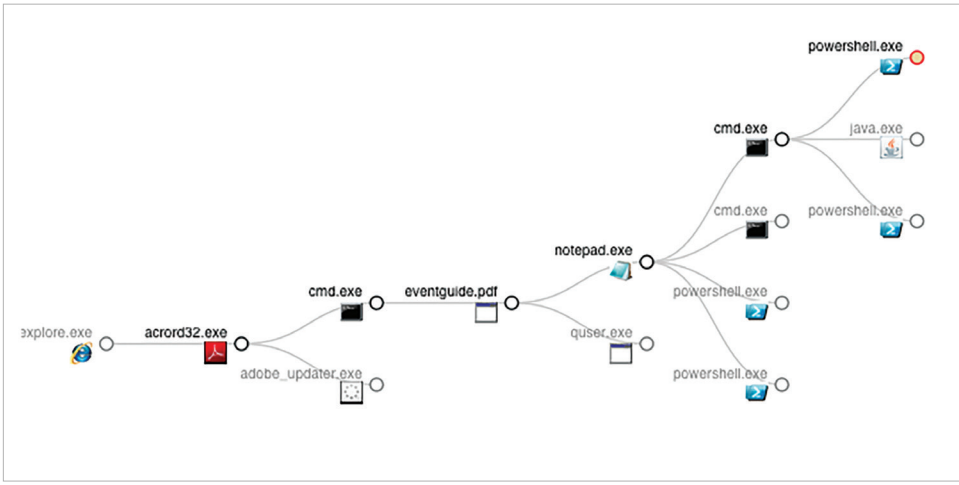
CYBER SECURITY CRIMINALS ARE INNOVATING AT A TERRIFYING PACE.

Most breaches take 15 minutes or less to compromise a system. Accurate detection and the ability to respond quickly is paramount. Most Security Operations Centers (SOCs) do not have the comprehensive visibility necessary to quickly make informed decisions to quickly respond to threats.

Proficio's Managed Detection and Response service combines best of breed Endpoint Detection and Response solutions with Proficio's ProSOC service to provide unparalleled Incident Response services to detect and respond to threats on the endpoint.

Features

- Market leading technology to actively monitor Endpoint alerts 24x7
- Correlate alerts with additional log data in ProSOC
- Perform a structured confirmation process of Endpoint suspicious alerts
- Take initial remediation action from the Endpoint console
- Collect & Centrally Store Security Events from all endpoints including (Servers, Desktops, Laptops, POS)
- Monitor running processes
- Monitor inbound/outbound network connections



Visualize the complete attack kill chain to determine root cause, visualize lateral movement and accelerate investigations.

Event Correlation

- Run events collected through advanced event detection and correlation engine
- Apply threat intelligence correlation
- Apply behavior rules correlation
- Apply holistic security event correlation (firewalls, IPS, DLP, AV, PROXY etc.)
- Identify malicious and suspicious executable
- Track connectivity, including connectivity to blacklisted IP Addresses
- Find evidence of malware attacker activities persistence
- Correlate path connectivity
- Trigger additional collection based on conditions (such as malware-like behavior)
- Trigger file interrogation (Sandbox)
- Based on automated correlation create incident ticket for further manual investigation

Investigation

- Perform Manual investigation and review by SOC analyst
- Review all event information
- Review all automated correlation event triggers
- Review all collected files, user activities, network connections, logon activities, running processes, system changes, IO Events
- Package and present incident findings on an on-going basis

Response Capabilities

- Escalate incident with customer
- Contain endpoint
- Remediate endpoint (remove malware, or other IOC's)
- Issue ticket for re-image
- Block/Unblock Hash

About Proficio:

Proficio is a leading provider of cloud-based security solutions that are changing the way organizations defend against advanced threats and prevent security breaches. We do this by providing the most advanced cloud-based services that eliminate the need for added headcount or costly software and hardware systems.

Learn more at Proficio.com

In the Cloud, On-Premises or a Hybrid

Every organization is unique; that's why ProSOC offers the most flexible service in the industry and can address just about any deployment model out there. You may choose to outsource all aspects of SIEM administration, event logging, and 24x7 expert monitoring, or perhaps you prefer a hybrid model, where we provide a managed, cloud-based SIEM service and you monitor and remediate your own security events. Even if you choose to maintain your own on-premises SIEM system, we can help you remotely administer your SIEM or monitor alerts outside normal business hours.

Future Ready

ProSOC is designed to address the ever-changing threat landscape. It monitors and protects data and applications stored in cloud infrastructures, like AWS, using virtual relays and cloud-based IDS software. It also helps address issues arising from BYOD and the deployment of wireless applications by monitoring mobile device users and applications for unauthorized or suspicious behavior.

Proficio Headquarters:
3264 Grey Hawk Court
Carlsbad, CA 92010
+1-800-779-5042
www.proficio.com

Proficio Asia:
51 Changi Business Park
Central 2
#03-11 The Signature
Singapore 486066
+65-6996-9185

Proficio Australia and NZ:
264 George Street
Sydney, NSW 2000
Australia
+61-2-8607-8556

PROFICIO