Secureworks®

Advanced Remediation Management

Deeper event analysis and investigation enabling timely, personalized and informed security decisions.

Adding Context to Event Management

Most enterprise organizations have a security model that includes a first layer of security event management, responsible for notification, correlation and filtering. However, the number of events escalated through to the next level still requires overwhelming support resources, which can distract an organization's focus from real threats. Providing advanced telemetry and personalized correlation, with the addition of business context, to a security event is a challenge for any organization. Without the skills or coverage to provide deeper analysis, support teams don't have the information to know what needs attention and what action to take first. In addition, organizations are struggling to realize efficiencies and demonstrating returns on technology investments is difficult.

Organizations require a comprehensive solution that is scalable, fully integrated, and in step with your personnel and infrastructure.
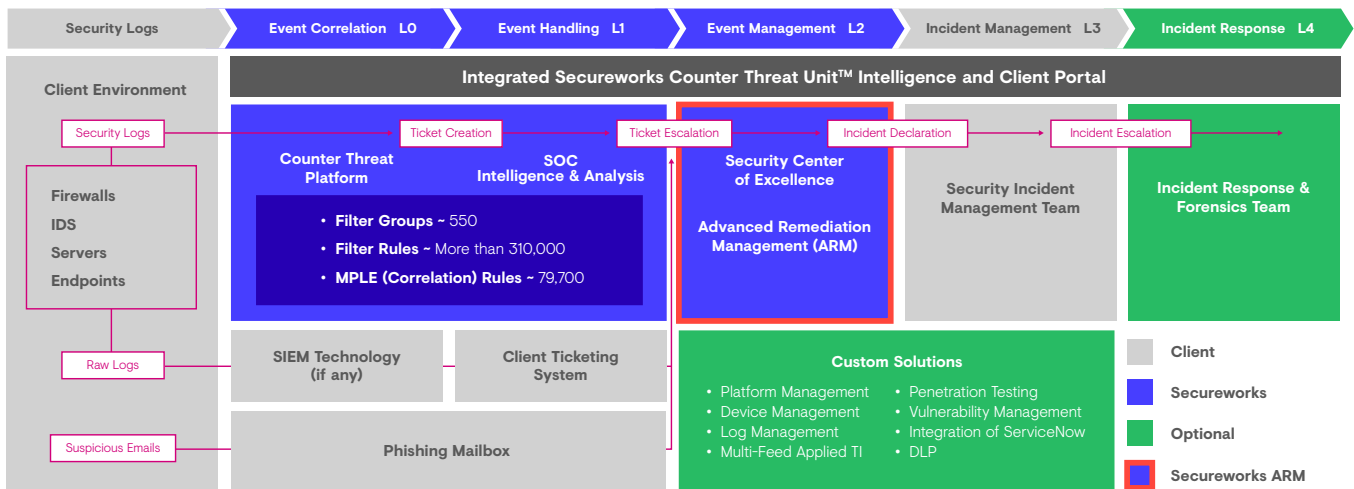
How Secureworks Helps

Secureworks Advanced Remediation Management (ARM) is designed to be a seamlessly integrated managed service that provides you with a highly skilled cross-functional team to deliver deeper event analysis (L2) utilizing the Secureworks Counter Threat Platform™ (CTP) and integrated Secureworks Threat Intelligence. Personalized correlation and analysis of various client-deployed security platforms results in further escalation or remediation as needed.

Our ARM service swivels between systems to provide a deep level of analysis, yielding clear business context that consolidates everything into one big picture, enabling you to take intelligent action with respect to your security.

Our team also coordinates remediation and provides continuous service improvement and feedback to our other managed security services for sustained improvements.

Client Benefits

- Seamlessly integrates into the client's security environment

- An elite, highly skilled team delivers deeper event analysis, utilizing The Secureworks Counter Threat Platform™ (CTP), client tools and many cross-functional teams

- Personalized correlation and analysis utilizing client-deployed security platforms

- Escalation or remediation of security incidents for corrective action with defined business and threat context

- Enables you to make timely and most informed security decisions possible

Security Logs	Event Correlation L0	Event Handling L1	Event Management L2	Incident Management L3	Incident Response L4

Integrated Secureworks Counter Threat Unit™ Intelligence and Client Portal

Client Environment

- Security Logs → Ticket Creation → Ticket Escalation → Incident Declaration → Incident Escalation

Firewalls
IDS
Servers
Endpoints

Counter Threat Platform — **SOC Intelligence & Analysis**

- **Filter Groups** ~ 550
- **Filter Rules** ~ More than 310,000
- **MPLE (Correlation) Rules** ~ 79,700

Security Center of Excellence

Advanced Remediation Management (ARM)

Security Incident Management Team

Incident Response & Forensics Team

Raw Logs

SIEM Technology (if any) — **Client Ticketing System**

Suspicious Emails

Phishing Mailbox

Custom Solutions
- Platform Management
- Device Management
- Log Management
- Multi-Feed Applied TI
- Penetration Testing
- Vulnerability Management
- Integration of ServiceNow
- DLP

Legend:
- Client
- Secureworks
- Optional
- Secureworks ARM

Why Secureworks ARM?

Advanced Remediation Management

Additional Layers of Processing and Review

Most industry event management (Level 2) offerings only include an analysis layer that includes monitoring, triage, dispatching and context.

Our ARM has an additional advisory and governance layer that provides:

- Advisement on tuning and compliance, remediation guidance, and in-depth root cause analysis
- A program manager that runs operational, tactical and strategic governance processes on your behalf

More Coverage Than a Dedicated Resident

- 12x5 and 24x7 options deliver more working hours than traditional 8 hour work days
- No sick days, or vacations
- No service disruption to your vorganization if key staff leave

Scalability

A managed service that can adapt as your needs do with tiered options to increase or decrease based on your consumption patterns.

Our Security Experts

Secureworks hires only the best and brightest. From our in depth technical hiring process to our continued investment in our consultants through generous training programs, we find and cultivate excellence. We don't follow standardized scripts; we anticipate emerging threats and help you identify, respond faster and recover from a security incident.

Integrated Threat Intelligence

Our CTP is at the core of our intelligence-driven information security solutions. Across our global client ecosystem, our elite team analyzes billions of network events to discover potential threats, deliver countermeasures and generate intelligence and valuable context regarding the intentions and actions of adversaries.

Solution Features

- Coverage: 12x5 (M-F) and 24x7 options available

- Security event supported sources include Secureworks CTP, Client Ticketing system and escalated suspicious emails

- Level 2 Events processing includes Analysis, Advisory and Governance layers of review

- Services include: Personalized Correlation, Addition of Business Context, Coordination of Remediation, Accountability

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Secureworks®