END CYBER THREATS: Active Response

Generalized Response Framework

- Active Response capabilities allow for action to be taken against threats as they are detected, minimizing the potential damage they can cause and reducing incident response time.
- These capabilities allow Arctic Wolf Security Teams to proactively stop a threat in your identity, network, email and EDR environments.
- Change your technologies without impacting the ability to respond to threats with the generalized response framework.

ACTIVE RESPONSE: Endpoint

Isolate compromised hosts to quickly stop an attack before it can spread

Generalized Response Framework

- Host containment enables immediate action against threats on your endpoints, ensuring rapid containment and mitigation of risks.
- By containing threats at the host level, organizations can maintain operational continuity for unaffected systems, mitigating disruptions to business operations.

Supported Integrations

CROWDSTRIKE

SentinelOne

ARCTIC WOLF AGENT

Microsoft Defender

TANIUM

vmware Carbon Black

Host Contain and Un-Contain Use Cases & Outcomes

- **Rapid Response to Threats**: This prevents the spread of malware or unauthorized access to other parts of the network, reducing the potential impact of security incidents.
- **Minimization of Damage**: Limit the attacker's ability to exfiltrate data, disrupt operations, or escalate privileges within the network.
- **Prevention of Lateral Movement**: Containment prevents attackers from moving laterally within the network to compromise additional systems or escalate their privileges.
- **Protection of Critical Assets**: It ensures that essential systems and data remain secure, safeguarding the integrity, confidentiality, and availability of organizational resources.
- **Adaptive Security**: Once the threat has been neutralized and the compromised system is restored to a secure state, it can be reintegrated into the network, maintaining operational continuity while ensuring security.

ENDPOINT: Host Containment

Threat Confirmation

- The Arctic Wolf Triage Team determined that the threat is a true positive and action needs to be taken rapidly to stop the threat from advancing

Remediation

- Arctic Wolf works with the customer to fully remediate the threat
- Arctic Wolf confirms remediation is successful and reintegrates the endpoint back to the network

Investigation Triggered

- Arctic Wolf Security Teams receive a detection that triggers an investigation – this detection and suspicious activity can originate from supported integrations, novel Arctic Wolf Detections or the Arctic Wolf Agent

Host Containment

- Arctic Wolf initiates immediate host containment to stop the threat and the asset is disconnected from the network

Security Journey

Arctic Wolf works with the customer to identify areas of improvement related to this incident such as:

- Enforce stricter controls over password or MFA
- Enforce more restrictive privilege to sensitive documents
- Recommend any patches or software updates
- Recommend user awareness training to highlight the danger of visiting unknown websites and how to recognize a phishing campaign

Arctic Wolf Platform | Arctic Wolf Triage Team | Customer | Concierge Security Team

ACTIVE RESPONSE: Identity

Quickly stop cyber threats before they spread with response actions for your identity infrastructure

Generalized Response Framework

- Response actions enable immediate action against threats in your identity infrastructure, ensuring rapid containment and mitigation of risks.
- With the ability to neutralize unauthorized access attempts or anomalous activities, organizations fortify their environment against evolving threats, defend crucial assets, and protect users while causing minimal disruption to business.

Supported Integrations

Microsoft Entra ID

DUO

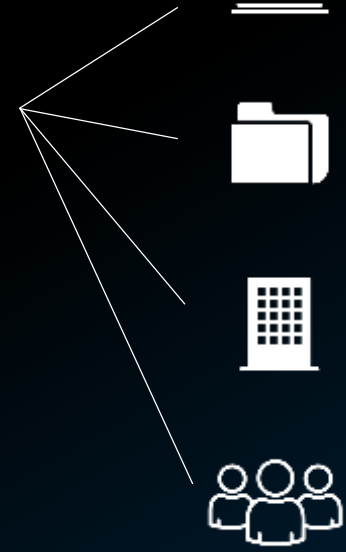
okta

Response Actions:

- **Disable and Enable a User**: Being able to disable affected user accounts prevents unauthorized users from exploiting compromised accounts to gain access to additional resources or escalate privileges within the systems. (Cisco Duo, Okta and Entra ID)
- **Close User Connections**: Terminating a connection can help prevent the unauthorized extraction or transmission of data and can be an effective defense mechanism against DoS attacks. (Okta and Entra ID)
- **Add or Remove a User from a Security Group**: This response action ensures that in the event a bad actor has gained access to a particular security group, their access is quickly revoked. (Cisco Duo, Okta and Entra ID)
- **Force Password Reset**: Forcing password resets for users helps Arctic Wolf contain an incident by invalidating potentially compromised credentials and prevents further unauthorized access or data exfiltration while investigations are underway. (Okta and Entra ID)

IDENTITY: Disable a User

1 A threat actor has compromised a user and can now leverage this user to advance their attack



2 Suspicious activity is detected by the Arctic Wolf Platform and the Arctic Wolf Security Teams are alerted

3 Arctic Wolf investigates, determines that this is a true threat, and disables the user – the threat actor can no longer use the compromised user to move in the customer environment, escalate privilege, or exfiltrate data

ARCTIC WOLF SECURITY TEAMS

4 Arctic Wolf Security Teams work with the customer on any additional remediation, as well as posture hardening to prevent similar threats in the future

ACTIVE RESPONSE : Network

Taking action to mitigate the risk of evolving web-based cyber threats

Generalized Response Framework

- Intercepting threats at the network level prevents malicious entities from infiltrating systems and accessing sensitive data before they reach their intended targets.

Supported Integrations

zscaler™ FORTINET® paloalto® NETWORKS

Response Action for Secure Web Gateway

- **Block URL**: Blocking malicious URLs at the secure web gateway prevents threats from reaching endpoints, reducing the likelihood of malware infections, data breaches, and other security incidents.
- **Add IP Address to Deny List:** Adding an IP address to a deny list at the firewall provides an effective way to block known malicious traffic from accessing the network. This reduces the risk of intrusions and data breaches, and prevents bad actors from communicating with internal systems.

ACTIVE RESPONSE : Email

Protect unsuspecting users by actively removing malicious emails from their environment

Generalized Response Framework

- Active response capabilities in email environments provide real-time protection against phishing, malware, and other email-based attacks by quickly detecting and responding to suspicious activities.
- By acting swiftly, Arctic Wolf minimizes the risk of users falling victim to social engineering attacks and prevent malware from spreading across your organization.

Response Action for Cloud Email Solutions

- Delete an Email: Malicious emails may contain attachments or embedded links that deliver malware payloads to recipients' devices. By promptly moving or deleting these emails, Arctic Wolf can prevent malware from being downloaded or executed, minimizing the risk of malware infections and subsequent damage to systems and data.

Supported Integrations

Microsoft 365 mimecast